

REGISTER OF DELETIONS

66. The following services are part of baseline 2.0 of the C3 Taxonomy and do not return in baseline 3.1 because they were deleted or subsumed into other taxonomy elements:

- a. Capability Codes;
- b. Capability Hierarchy Framework;
- c. Capability Statements;
- d. CIS Security Information;
- e. CIS Security;
- f. COI-Enabling CIS Security Services;
- g. COI-Enabling SMC Services;
- h. COI-Specific CIS Security Services;
- i. COI-Specific SMC Services;
- j. Groupings;
- k. Mission Type - Antiterrorism (AT);
- l. SMC Information; and
- m. SMC.

RELEASE NOTES FOR THE C3 TECHNICAL SERVICES TAXONOMY, BASELINE 3.1

INTRODUCTION

1. The C3 Technical Services Taxonomy was first introduced in 2015 as a companion to Baseline 2.0 of the C3 Taxonomy. Its purpose is to provide a consistent common language and understanding of the CIS technical services landscape. As such, it simplifies the identification and standardization of interoperability points, and promotes the fast development and reuse of relevant technology solutions. The development was a consensus building effort with experts from national experts, academia and industry contributed their perspectives and knowledge.
2. The new baseline is a result of the MC tasking to address the needs of the FMN community, and to harmonize with the NATO Interoperability Standards and Profiles (NISP) and FMN Spiral Specifications.
3. This document provides the release notes for the C3 Technical Services Taxonomy Baseline 3.1, including a register of changes and deletions.

MAIN ISSUES

4. Once a baseline of a taxonomy is produced, it is followed by a persistent effort to further improve the arrangement and definition of taxonomy elements and to accommodate changes that are being inspired by contemporary developments in technology, policies and implementations.
5. There are a couple of main issues that had a significant influence on the development of the new baseline, such as: the harmonization of Service Management and Control (SMC) and CIS Security; the separation of logistics and medical services; and the introduction of services for the cyberspace domain, for CIS functions and data science.
6. In the processing of Baseline 3.0 by the NATO C3 Board, concerns were raised about the clarity and consistency in addressing the distinction between classified and non-classified information. The terminology in the taxonomy was deemed ambiguous or inappropriate, especially for the reference to security policies and security domains.
7. In response, it is acknowledged that NATO has distinct policies and directives for classified vs. non-classified information. However, it needs to be emphasized that the taxonomy is solution- and organization-agnostic. In other words: it is not an exclusive NATO taxonomy per se. As such, for instance, the reference to "security policies" in the text does not refer explicitly to the NATO Security Policy. The intent has always been to offer a taxonomy for a wider adoption

NATO UNCLASSIFIED
Releasable to NORTH MACEDONIA

past NATO, including nations and organizations. Nevertheless, in whatever form and function, the taxonomy should not disrupt its applicability for NATO in any context.

8. The following changes have been implemented in Baseline 3.1 in order to establish compliancy with these concerns.

- a. "security policies" are changed to "information security and management policies".
- b. "CIS Security policies" are changed to "CIS Security measures".
- c. "security domains" are changed to "information domains".

9. The result is a C3 Technical Services Taxonomy that more accurately reflects the technical services landscape and provides a robust framework for architectural work in support of NATO Enterprise, Alliance, and Federation partners.

REGISTER OF CHANGES

10. The following paragraphs list and clarify the changes that are made from baseline version 2.0 to 3.1. These changes are combined per layer and numbered in accordance with the corresponding chapters in the C3 Technical Services Taxonomy Report.

11. The register does not include minor changes that do not alter the context and meaning of service definitions, such as grammatical and typographical errors.

COI-Specific Services

12. Paragraph 3.1.1 - Renamed "Joint Services" to "Joint Domain Services". Changed the description for clarification of joint and combined forces.

13. Paragraph 3.1.1.2 - Added "Force Generation and Activation Services".

14. Paragraph 3.1.1.3 - Added "CONOPS Development Services".

15. Paragraph 3.1.1.4 - Renamed "NATO Crisis Response Measures Services" to "Crisis Response Measures Services". Changed the description for clarification.

16. Paragraph 3.1.2 - Renamed "Air Services" to "Air Domain Services".

17. Paragraph 3.1.3 - Renamed "Maritime Services" to "Maritime Domain Services".

18. Paragraph 3.1.3.1 - Changed the description of "Recognized Maritime Picture Services" for clarification of the Maritime Operational Picture.

19. Paragraph 3.1.3.2 - Added "Maritime Reference Object Management Services".

20. Paragraph 3.1.3.5 - Added "Subsurface Warfare Services".

NATO UNCLASSIFIED
Releasable to NORTH MACEDONIA

21. Paragraph 3.1.3.6 - Renamed "Mine Warfare Services" to "Naval Mine Warfare Services". Changed the description to more accurately describe the type of operations and the services characteristics.
22. Paragraph 3.1.3.7 - Added "Maritime Vessel Management Services".
23. Paragraph 3.1.4 - Renamed "Land Services" to "Land Domain Services".
24. Paragraph 3.1.5 - Added "Cyberspace Domain Services".
25. Paragraph 3.1.5.1 - Moved "Recognized Cyber Picture Services" from "COI-Specific CIS Security Services".
26. Paragraph 3.1.5.2 - Added "Cyberspace Operations Planning Services".
27. Paragraph 3.1.5.3 - Added "Cyberspace Effects Coordination Services".
28. Paragraph 3.1.5.4 - Added "Cyberspace Treat Analysis Services".
29. Paragraph 3.1.6 - Renamed "JISR Services" to "Intelligence and ISR Functional Services".
30. Paragraph 3.1.6.1 - Added "Recognized Intelligence Picture Services".
31. Paragraph 3.1.6.2 - Added "Intelligence Analysis Services".
32. Paragraph 3.1.6.3 - Added "ISR Collection Services".
33. Paragraph 3.1.6.4 - Renamed "Intelligence Requirements Management Services" to "Information Requirements Management Services".
34. Paragraph 3.1.6.5 - Renamed "JISR Analysis and Production Services" to "Intelligence Production Services".
35. Paragraph 3.1.6.7 - Added "Collection Management Services".
36. Paragraph 3.1.7 - Renamed "Electronic Warfare Services" to "Electronic Warfare Functional Services".
37. Paragraph 3.1.7.1 - Added "Recognized Electromagnetic Picture Services".
38. Paragraph 3.1.7.11 - Added "Electronic Order of Battle Services".
39. Paragraph 3.1.7.2 - Added "Electromagnetic Operations Planning Services".
40. Paragraph 3.1.7.3 - Added "Emitter TECHINT Services".

NATO UNCLASSIFIED
Releasable to NORTH MACEDONIA

41. Paragraph 3.1.7.6 - Added "Electronic Surveillance Services".
42. Paragraph 3.1.7.7 - Added "JIPOE / COA EW Services".
43. Paragraph 3.1.7.8 - Added "Electronic Attack Services".
44. Paragraph 3.1.7.9 - Added "Electronic Defence Services".
45. Paragraph 3.1.7.11 - Added "Electronic Order of Battle Services".
46. Paragraph 3.1.8 - Renamed "Environmental Services" to "Environmental Functional Services".
47. Paragraph 3.1.9 - Renamed "Logistics Services" to "Logistics Functional Services".
48. Paragraph 3.1.9.1 - Changed the description of "Recognized Logistics Picture Services" to provide more operational context.
49. Paragraph 3.1.9.2 - Added "Logistics Planning Services".
50. Paragraph 3.1.9.3 - Added "Movement Services".
51. Paragraph 3.1.9.4 - Added "Asset Tracking Services".
52. Paragraph 3.1.10 - Added "Medical Functional Services".
53. Paragraph 3.1.10.1 - Moved "Recognized Medical Picture Services" from "Logistics Services". Changed the description to add relation to decision-making.
54. Paragraph 3.1.10.2 - Added "Medical Regulating Services".
55. Paragraph 3.1.10.3 - Added "Teleconsultation Services".
56. Paragraph 3.1.10.4 - Moved "Casualty Rate Estimation Services" from "Logistics Services".
57. Paragraph 3.1.10.5 - Added "Epidemiology Services".
58. Paragraph 3.1.10.6 - Added "Medical Documentation Services".
59. Paragraph 3.1.10.7 - Added "Trauma Registry Services".
60. Paragraph 3.1.11 - Renamed "CIMIC Services" to "CIMIC Functional Services".
61. Paragraph 3.1.12 - Renamed "ETEE Services" to "ETEE Functional Services".
62. Paragraph 3.1.13 - Added "CIS Functional Services".

NATO UNCLASSIFIED
Releasable to NORTH MACEDONIA

- 63. Paragraph 3.1.13.1 - Added "Recognized CIS Picture Services".
- 64. Paragraph 3.1.13.2 - Moved "Cyber Defence Services" from "COI-Specific CIS Security Services".
- 65. Paragraph 3.1.13.3 - Added "ITSM Services.
- 66. Paragraph 3.1.13.5 - Moved "Spectrum Management Services" from "COI-Specific SMC Services".
- 67. Paragraph 3.1.13.6 - Moved "Advanced Threat Management Services" from "COI-Specific CIS Security Services".
- 68. Paragraph 3.1.13.7 - Moved "Electronic Key Management Services" from "COI-Specific CIS Security Services".
- 69. Paragraph 3.1.13.8 - Added "Security Information and Event Management Services".

COI-Enabling Services

- 70. Paragraph 3.2.1.2 - Added "Overlay Services".
- 71. Paragraph 3.2.1.3 - Changed the description of "Symbology Services" for clarification.
- 72. Paragraph 3.2.2.6 - Changed the description of "Targeting Services" to align with recent changes in doctrine.
- 73. Paragraph 3.2.4 - Renamed "Battlespace Information Services" to "Operations Information Services".
- 74. Paragraph 3.2.4.3 - Renamed "Track Services" to "Track Management Services". Changed the description for clarification.
- 75. Paragraph 3.2.4.4 - Added "Track Distribution Services".
- 76. Paragraph 3.2.4.5 - Moved "Data Exchange Monitoring Services" from "COI-Enabling SMC Services".
- 77. Paragraph 3.2.5 - Merged "Modeling and Simulation Services" from "Modeling and Simulation Services" and "Modeling and Simulation Enabling Services". Changed the description for clarification.
- 78. Paragraph 3.2.5.2 - Added "Model Repository Services".
- 79. Paragraph 3.2.5.4 - Added "Information Registry Services".
- 80. Paragraph 3.2.5.5 - Added "Simulation Control Services".

NATO UNCLASSIFIED
Releasable to NORTH MACEDONIA

- 81. Paragraph 3.2.5.6 - Added "Simulation Composition Services".
- 82. Paragraph 3.2.5.7 - Moved "Battlespace Simulation Services" from Modeling and Simulation Enabling Services".
- 83. Paragraph 3.2.5.8 - Moved "Ground Truth Battlespace Objects Services" from Modeling and Simulation Enabling Services".
- 84. Paragraph 3.2.5.9 - Moved "Ground Truth Battlespace Events Services" from Modeling and Simulation Enabling Services".

Business Support Services

- 85. Paragraph 4.1.1 - In "Business Support CIS Security Services" changed "CIS Security policies" to "CIS Security measures".
- 86. Paragraph 4.1.1.1 - In "Business Support Guard Services" changed "security policy" to "information security and management policies" and changed "security domains" to "information domains".
- 87. Paragraph 4.1.2.3 - Moved "Call Management Services" from "COI-Specific SMC Services".
- 88. Paragraph 4.1.2.4 - Moved "VTC Management Services" from "COI-Specific SMC Services".
- 89. Paragraph 4.1.3 - Renamed "Unified Communication and Collaboration Services" to "Communication and Collaboration Services".
- 90. Paragraph 4.1.6.2 - Renamed "Military Messaging Services" to "Formal Messaging Services", moved from "Unified Communication and Collaboration Services". Changed the description for clarification.
- 91. Paragraph 4.1.6.4 - Added "Unit Conversion Services".
- 92. Paragraph 4.1.6.5 - Renamed "Distributed Search Services" to "Search Services".
- 93. Paragraph 4.1.6.7 - Added "Archiving Services".
- 94. Paragraph 4.1.7 - Added "Data Science Services".
- 95. Paragraph 4.1.7.1 - Added "Reporting Services".
- 96. Paragraph 4.1.7.2 - Added "Data Ingest Services".
- 97. Paragraph 4.1.7.3 - Added "Data Processing Services".

NATO UNCLASSIFIED
Releasable to NORTH MACEDONIA

98. Paragraph 4.1.7.4 - Moved "Analytics Services" from "Information Management Services". Changed the description to include reporting functionality.

99. Paragraph 4.1.7.5 - Added "Statistical Analysis Services".

100. Paragraph 4.1.7.6 - Added "Machine Learning Services".

Platform Services

101. Paragraph 4.2 - Renamed "SOA Platform Services" to "Platform Services".

102. Paragraph 4.2.1 - Renamed "SOA Platform CIS Security Services" to "Platform CIS Security Services". Changed "CIS Security policies" to "CIS Security measures".

103. Paragraph 4.2.1.1 - Renamed "SOA Platform Guard Services" to "Platform Guard Services". Changed "security policy" to "information security and management policies".

104. Paragraph 4.2.1.5 - In "Information Labeling Services" changed "security policy" to "information security and management policies".

105. Paragraph 4.2.2 - Renamed "SOA Platform SMC Services" to "Platform SMC Services".

106. Paragraph 4.2.2.1 - Renamed "SOA SMC Policy Enforcement Services" to "SMC Policy Enforcement Services".

107. Paragraph 4.2.2.3 - Renamed "SOA Platform Logging Services" to "Platform Logging Services".

108. Paragraph 4.2.2.4 - Renamed "SOA Platform Monitoring Services" to "Platform Monitoring Services".

109. Paragraph 4.2.2.5 - Renamed "SOA Platform Metering Services" to "Platform Metering Services".

110. Paragraph 4.2.3.4 - Changed the description of "Message Proxying Services" to include security features and relation with "Message Caching Services".

111. Paragraph 4.2.5.3 - Changed the description of "Information Aggregation Services" for clarification.

112. Paragraph 4.2.6 - Added "Database Services".

113. Paragraph 4.2.6.1 - Renamed "Directory Storage Services" to "Directory Services", moved from "Infrastructure Storage Services".

114. Paragraph 4.2.6.2 - Renamed "Non-relational Structured Storage Services" to "Non-relational Database Services", moved from "Infrastructure Storage Services".

NATO UNCLASSIFIED
Releasable to NORTH MACEDONIA

115. Paragraph 4.2.6.3 - Renamed "Relational Database Storage Services" to "Relational Database Services", moved from "Infrastructure Storage Services".

Infrastructure Services

116. Paragraph 4.3.1 - In "Infrastructure CIS Security Services" changed "CIS Security policies" to "CIS Security measures".

117. Paragraph 4.3.1.3 - In "Authentication Services" changed "security domains" to "information domains".

118. Paragraph 4.3.1.5 - In "Authorization and Access Services" changed "security policies" to "information security and management policies".

119. Paragraph 4.3.1.7 - In "Intrusion Detection Services" changed "security policy" to "relevant policy" and the second instance, to "information security and management policies". Changed the description for clarification.

120. Paragraph 4.3.1.9 - In "Infrastructure Guard Services" changed "security policy" to "information domains".

121. Paragraph 4.3.2.5 - Added "Time Zone Data Distribution Services".

122. Paragraph 4.3.3.3 - Added "Distributed Processing Services".

123. Paragraph 4.3.4 - Changed the description of "Infrastructure Storage Services" to focus on data rather than information.

124. Paragraph 4.3.5.1 - Renaming "Web Caching Services" to "Caching Services" moved from "Web Platform Services".

125. Paragraph 4.3.5.2 - Renaming "Web Proxying Services" to "Proxying Services" moved from "Web Platform Services".

126. Paragraph 4.3.5.3 - Added "Virtualized Networking Services".

127. Paragraph 4.3.5.9 - Added "Location Awareness Services".

Communications Access Services

128. Paragraph 5.1.1. - In "Communications Access CIS Security Services" changed "CIS Security policies" to "CIS Security measures".

Transport Services

129. Paragraph 5.2.1. - In "Transport CIS Security Services" changed "CIS Security policies" to "CIS Security measures".

Transmission Services

130. Paragraph 5.3.1. - In "Transmission CIS Security Services" changed "CIS Security policies" to "CIS Security measures".

REGISTER OF DELETIONS

131. The following services are part of Baseline 2.0 of the C3 Technical Services Taxonomy and do not return in Baseline 3.1 because they were deleted or subsumed into other services:

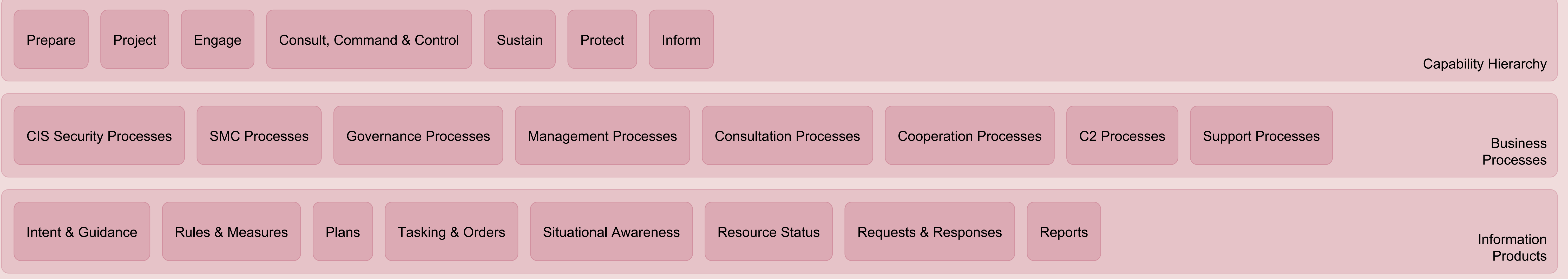
- a. CIS Security Audit Analysis Services;
- b. COI-Enabling CIS Security Services;
- c. COI-Enabling SMC Services;
- d. COI-Specific CIS Security Services;
- e. COI-Specific SMC Services;
- f. Cyber Threat Detection Services;
- g. Document Sharing Services;
- h. JISR Collection and Exploitation Plans Services;
- i. JISR Imagery and Video Services;
- j. JISR Reporting Services;
- k. JISR Sensor Services;
- l. Radio Simulation Services;
- m. Report Generation Services;
- n. Sonar Prediction Services;
- o. Spectrum Usage Information Services; and
- p. Water Space Management Services.

Operational Context

Missions and Operations

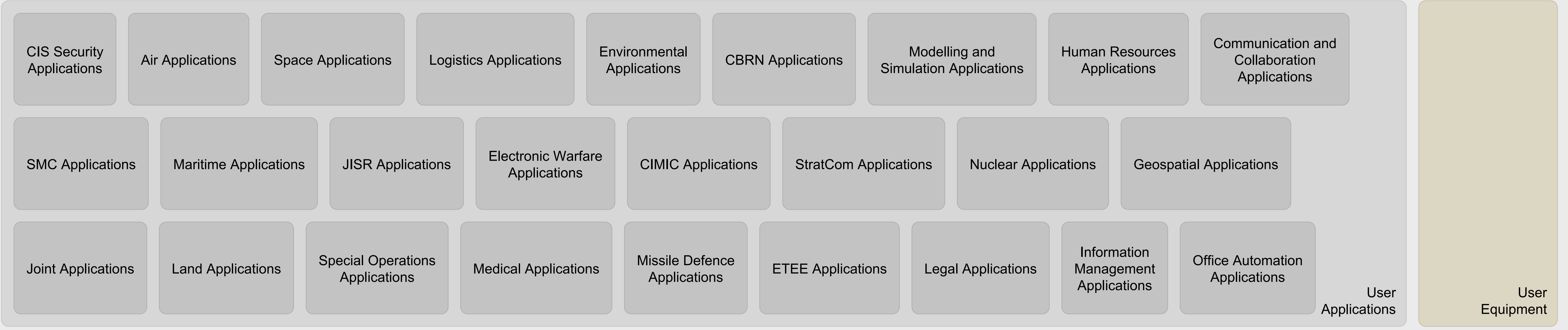


Operational Capabilities



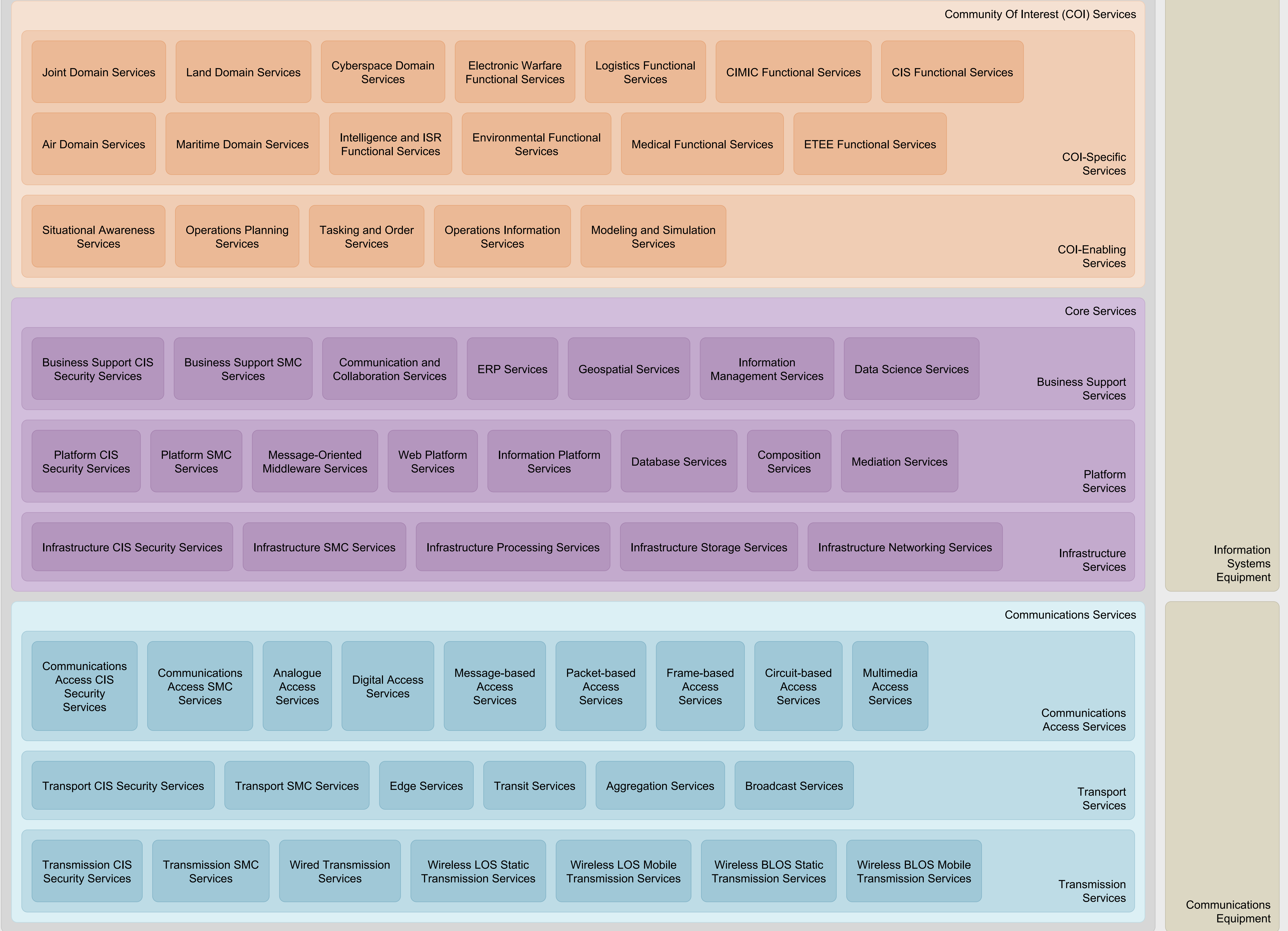
Communication and Information Systems (CIS) Capabilities

User-Facing Capabilities



Back-End Capabilities

Technical Services





C3 Taxonomy Report

Table of Contents

1 Introduction	6
2 Background	7
3 C3 Taxonomy	8
4 Operational Context	9
4.1 Missions and Operations	10
4.1.1 Policy and Guidance	10
4.1.1.1 Strategic Concept	10
4.1.1.2 Political Guidance	10
4.1.1.3 Military Guidance	11
4.1.1.4 Allied Publications	11
4.1.1.5 Policies and Directives	11
4.1.2 Mission Types and Tasks	11
4.1.2.1 Mission Type - Collective Defence (CD)	11
4.1.2.2 Mission Type - Consequence Management (CM)	11
4.1.2.3 Mission Type - Counter Insurgency (COIN)	11
4.1.2.4 Mission Type - Counter Terrorism (CT)	12
4.1.2.5 Mission Type - Peacekeeping (PK)	12
4.1.2.6 Mission Type - Peace Enforcement (PE)	12
4.1.2.7 Mission Type - Conflict Prevention (CP)	12
4.1.2.8 Mission Type - Peacemaking (PM)	12
4.1.2.9 Mission Type - Peacebuilding (PB)	13
4.1.2.10 Mission Type - Support to Humanitarian Assistance (SHA)	13
4.1.2.11 Mission Type - Support to Disaster Relief (DR)	13
4.1.2.12 Mission Type - Support of Non-Combatant Evacuation Operations (NEO)	13
4.1.2.13 Mission Type - Extraction Operation (EOP)	13
4.1.2.14 Mission Type - Military Aid/Support to Civil Authorities (SCA)	14
4.1.2.15 Mission Type - Enforcement of Sanctions and Embargoes (ESE)	14
4.1.2.16 Mission Type - Permanent Tasks	14
4.2 Operational Capabilities	15
4.2.1 Capability Hierarchy	15
4.2.1.1 Capability Area R - Prepare	15
4.2.1.2 Capability Area D - Project	16
4.2.1.3 Capability Area E - Engage	16
4.2.1.4 Capability Area C - Consult, Command and Control	16
4.2.1.5 Capability Area L - Sustain	16
4.2.1.6 Capability Area P - Protect	16
4.2.1.7 Capability Area I - Inform	16
4.2.2 Business Processes	16
4.2.2.1 CIS Security Processes	16
4.2.2.2 SMC Processes	16
4.2.2.3 Governance Processes	17
4.2.2.4 Management Processes	17

4.2.2.5 Consultation Processes	17
4.2.2.6 Cooperation Processes	17
4.2.2.7 C2 Processes	17
4.2.2.8 Support Processes	17
4.2.3 Information Products	17
4.2.3.1 Intent and Guidance	17
4.2.3.2 Rules and Measures	18
4.2.3.3 Plans	18
4.2.3.4 Tasking and Orders	18
4.2.3.5 Situational Awareness	18
4.2.3.6 Resource Status	18
4.2.3.7 Requests and Responses	18
4.2.3.8 Reports	18
5 CIS Capabilities	19
5.1 User-Facing Capabilities	20
5.1.1 User Applications	21
5.1.1.1 CIS Security Applications	21
5.1.1.2 SMC Applications	21
5.1.1.3 Joint Applications	22
5.1.1.4 Air Applications	22
5.1.1.5 Land Applications	22
5.1.1.6 Maritime Applications	22
5.1.1.7 Space Applications	22
5.1.1.8 Special Operations Applications	22
5.1.1.9 JISR Applications	22
5.1.1.10 Logistics Applications	22
5.1.1.11 Medical Applications	23
5.1.1.12 Electronic Warfare Applications	23
5.1.1.13 Environmental Applications	23
5.1.1.14 Missile Defence Applications	23
5.1.1.15 CIMIC Applications	23
5.1.1.16 CBRN Applications	23
5.1.1.17 ETEE Applications	23
5.1.1.18 StratCom Applications	24
5.1.1.19 Modelling and Simulation Applications	24
5.1.1.20 Legal Applications	24
5.1.1.21 Nuclear Applications	24
5.1.1.22 Human Resources Applications	24
5.1.1.23 Information Management Applications	24
5.1.1.24 Geospatial Applications	24
5.1.1.25 Office Automation Applications	24
5.1.1.26 Communication and Collaboration Applications	25
5.1.2 User Equipment	26
5.2 Back-End Capabilities	27

5.2.1 Technical Services	28
5.2.1.1 Community Of Interest (COI) Services	29
5.2.1.1.1 COI-Specific Services	29
5.2.1.1.1.1 Joint Domain Services	29
5.2.1.1.1.2 Air Domain Services	29
5.2.1.1.1.3 Maritime Domain Services	29
5.2.1.1.1.4 Land Domain Services	30
5.2.1.1.1.5 Cyberspace Domain Services	30
5.2.1.1.1.6 Intelligence and ISR Functional Services	30
5.2.1.1.1.7 Electronic Warfare Functional Services	30
5.2.1.1.1.8 Environmental Functional Services	30
5.2.1.1.1.9 Logistics Functional Services	30
5.2.1.1.1.10 Medical Functional Services	30
5.2.1.1.1.11 CIMIC Functional Services	30
5.2.1.1.1.12 ETEE Functional Services	31
5.2.1.1.1.13 CIS Functional Services	31
5.2.1.1.2 COI-Enabling Services	31
5.2.1.1.2.1 Situational Awareness Services	31
5.2.1.1.2.2 Operations Planning Services	31
5.2.1.1.2.3 Tasking and Order Services	31
5.2.1.1.2.4 Operations Information Services	31
5.2.1.1.2.5 Modeling and Simulation Services	31
5.2.1.2 Core Services	32
5.2.1.2.1 Business Support Services	32
5.2.1.2.1.1 Business Support CIS Security Services	32
5.2.1.2.1.2 Business Support SMC Services	32
5.2.1.2.1.3 Communication and Collaboration Services	32
5.2.1.2.1.4 ERP Services	33
5.2.1.2.1.5 Geospatial Services	33
5.2.1.2.1.6 Information Management Services	33
5.2.1.2.1.7 Data Science Services	33
5.2.1.2.2 Platform Services	33
5.2.1.2.2.1 Platform CIS Security Services	33
5.2.1.2.2.2 Platform SMC Services	33
5.2.1.2.2.3 Message-Oriented Middleware Services	33
5.2.1.2.2.4 Web Platform Services	34
5.2.1.2.2.5 Information Platform Services	34
5.2.1.2.2.6 Database Services	34
5.2.1.2.2.7 Composition Services	34
5.2.1.2.2.8 Mediation Services	34
5.2.1.2.3 Infrastructure Services	34
5.2.1.2.3.1 Infrastructure CIS Security Services	34
5.2.1.2.3.2 Infrastructure SMC Services	34
5.2.1.2.3.3 Infrastructure Processing Services	35

5.2.1.2.3.4 Infrastructure Storage Services	35
5.2.1.2.3.5 Infrastructure Networking Services	35
5.2.1.3 Communications Services	36
5.2.1.3.1 Communications Access Services	37
5.2.1.3.1.1 Communications Access CIS Security Services	37
5.2.1.3.1.2 Communications Access SMC Services	37
5.2.1.3.1.3 Analogue Access Services	37
5.2.1.3.1.4 Digital Access Services	37
5.2.1.3.1.5 Message-based Access Services	37
5.2.1.3.1.6 Packet-based Access Services	37
5.2.1.3.1.7 Frame-based Access Services	37
5.2.1.3.1.8 Circuit-based Access Services	38
5.2.1.3.1.9 Multimedia Access Services	38
5.2.1.3.2 Transport Services	38
5.2.1.3.2.1 Transport CIS Security Services	38
5.2.1.3.2.2 Transport SMC Services	38
5.2.1.3.2.3 Edge Services	38
5.2.1.3.2.4 Transit Services	38
5.2.1.3.2.5 Aggregation Services	39
5.2.1.3.2.6 Broadcast Services	39
5.2.1.3.3 Transmission Services	39
5.2.1.3.3.1 Transmission CIS Security Services	40
5.2.1.3.3.2 Transmission SMC Services	40
5.2.1.3.3.3 Wired Transmission Services	40
5.2.1.3.3.4 Wireless LOS Static Transmission Services	40
5.2.1.3.3.5 Wireless LOS Mobile Transmission Services	40
5.2.1.3.3.6 Wireless BLOS Static Transmission Services	40
5.2.1.3.3.7 Wireless BLOS Mobile Transmission Services	41
5.2.2 Information Systems Equipment	42
5.2.3 Communications Equipment	43

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 categorization, 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 the Requirements Division in Allied Command Transformation (ACT). The 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 Enterprise Mapping 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).

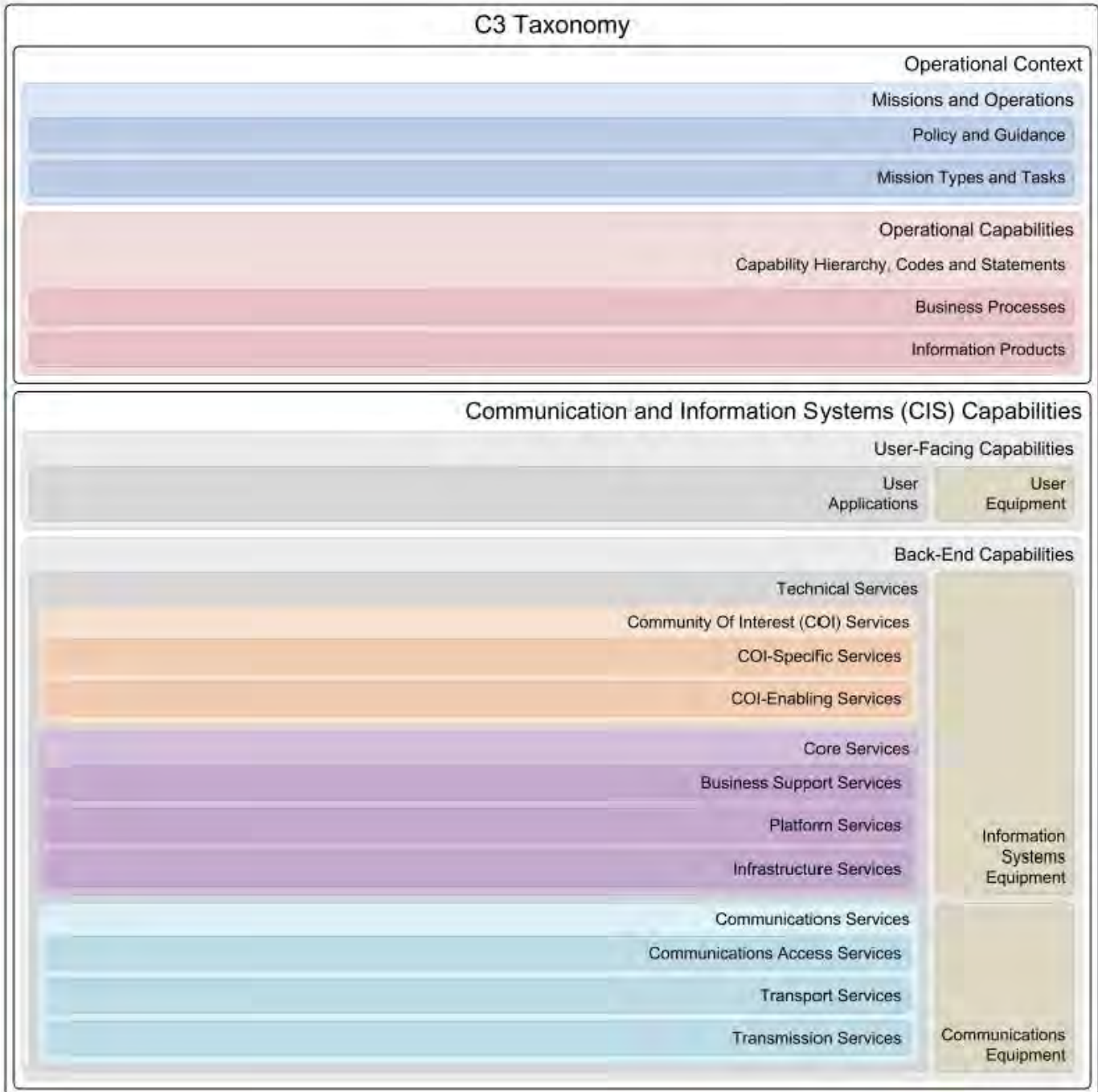
It is NATO's intent that the approach for deriving C3 requirements is through "service provision". This entails specifying the "requester" for a task to be performed and a "provider" who commits to performing the task. An example of a requester may be a headquarter and the provider may be a subordinate 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 (NEC), there is a need to reflect multiple perspectives on relationships between processes, requirements, standards, architectures and implementations that will help program, capability and project managers gain a better understanding of the complete environment.

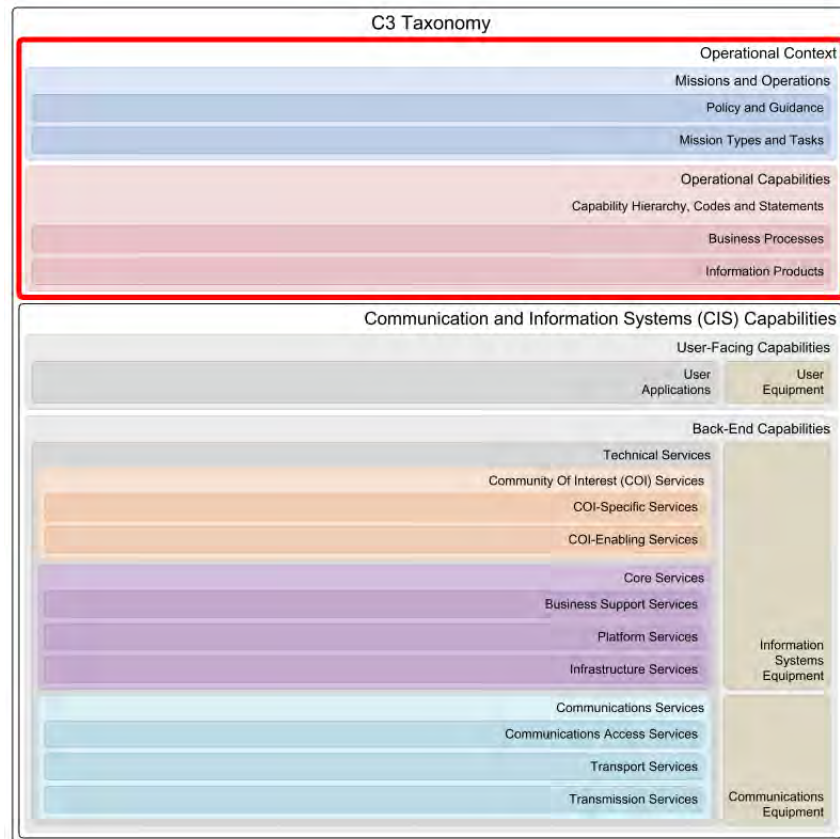
In a complex and federated enterprise like NATO there is a need for a generic structure or framework that can be used to align and synchronize various activities and projects that are on-going in parallel, when the organisation's CIS infrastructure transforms towards a network-enabled capability. The C3 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 categorization 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 Wiki on the calendar date shown at the bottom of the page.



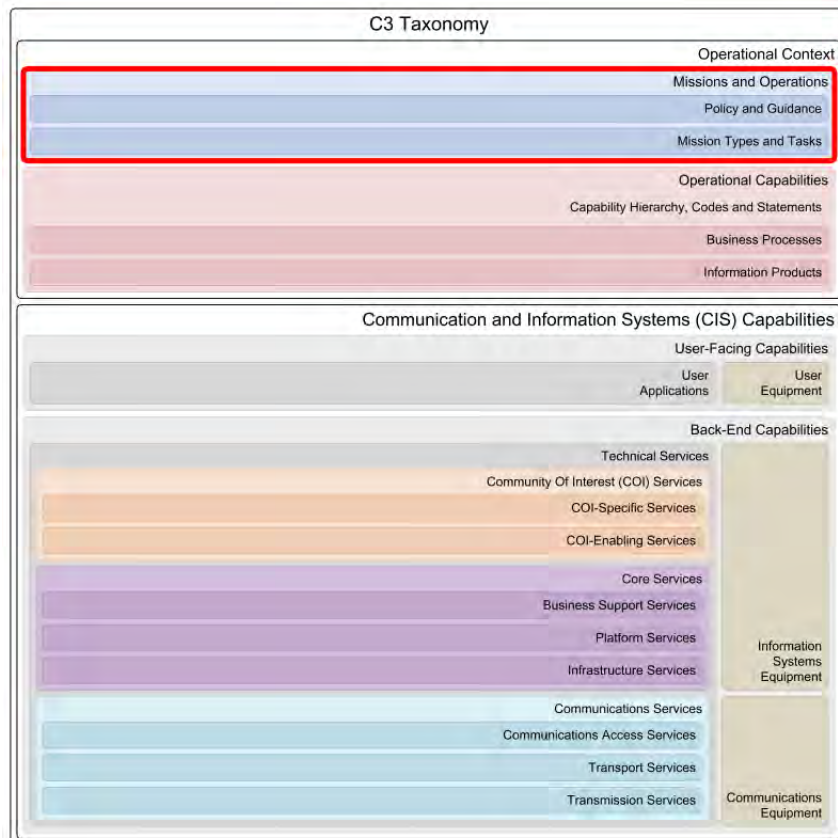
4 Operational Context



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 through 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 - 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.

4.1.2.3 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.

4.1.2.4 Mission Type - Counter Terrorism (CT)

The Counterterrorism (CT) mission type consists of activities 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, they may 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 without the assistance of the local government.

4.1.2.5 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.

4.1.2.6 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.

4.1.2.7 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.

4.1.2.8 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.

4.1.2.9 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.

4.1.2.10 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 governmental 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.

4.1.2.11 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 be conducted 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).

4.1.2.12 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) noncombatants 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.

4.1.2.13 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.

4.1.2.14 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 civil authorities and support to humanitarian 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 security will 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 their tasks. This assistance will normally be provided by multinational specialized units (MSUs) or, in special circumstances, other forces.

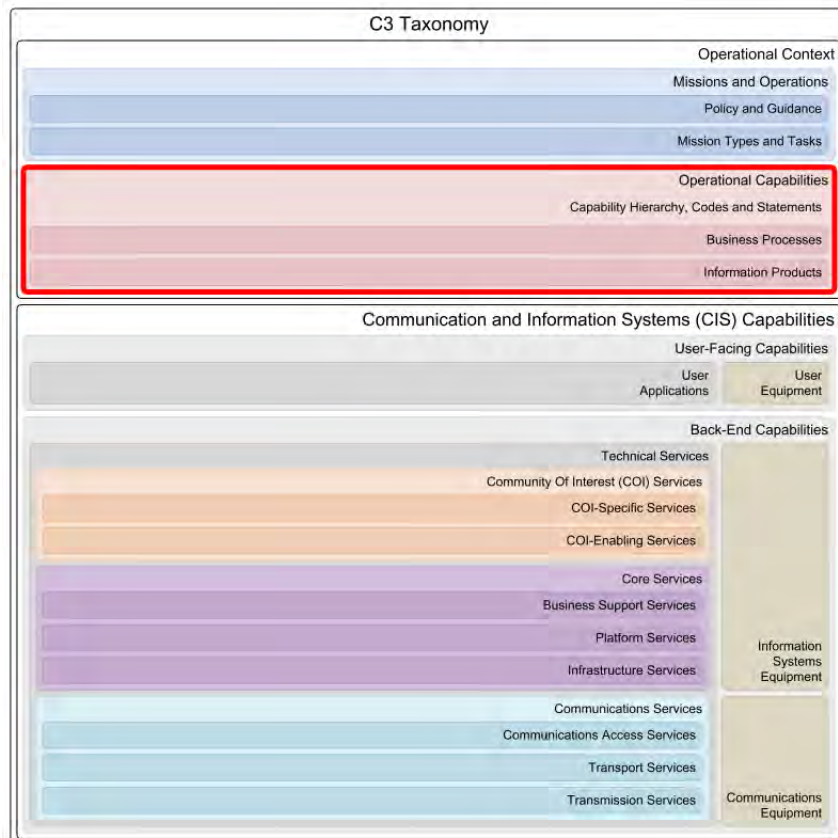
4.1.2.15 Mission Type - Enforcement of Sanctions and Embargoes (ESE)

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).

4.1.2.16 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 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

The "Capability Hierarchy" taxonomy layer represents the agreed means by which NATO groups and organizes its capabilities. It describes a functional breakdown of capabilities and is used as a framework to support the expression of capability requirements at differing levels of detail.

The Capability Hierarchy is used primarily within the NATO Defence Planning Process (NDPP) to provide a coherent structure to support the expression of the Minimum Capability Requirement (MCR) and for the aggregation of shortfalls. In addition, the CH is also used as a structural framework to support the expression of ACO Force Standards (AFS) and by the International Staff to structure the Step 5 Capability Reports. The hierarchy provides an agreed NATO capability taxonomy, which is exploited as a tool for use in areas beyond NDPP.

The Capability Hierarchy encompasses the full spectrum of capabilities to meet all aspects of NATO's Strategic Concept (Article 5 Collective Defence, Non-Article 5 Crisis response and Cooperative Security). Full spectrum comprises military and non-military capabilities to cover all phases of NATO operations including preparation, deployment, implementation with sustainment, and re-deployment/withdrawal.

4.2.1.1 Capability Area R - Prepare

The capabilities to establish, prepare and sustain sufficient and effective presence at the right time, including the ability to build up forces, through appropriate and graduated readiness, to meet any requirements, keeping sufficient flexibility to adapt to possible changes in the strategic environment. These also include the capabilities to contribute to Deterrence and Defence, Resilience and Projecting Stability.

4.2.1.2 Capability Area D - Project

The capabilities to conduct strategic deployment of headquarters (both for the NATO Force Structure and at a national level), forces and capabilities in support of any Alliance mission. These also include the capabilities to contribute to deterrence.

4.2.1.3 Capability Area E - Engage

The capabilities to perform the tasks which contribute directly to the achievement of mission goals within the context of collective defence, crisis management, and cooperative security. It includes all capabilities required to defeat, if necessary, adversaries as well as other capabilities such as, inter alia, those necessary to evacuate non-combatants, prevent the use of force by opponents, train local security forces and participate in stabilization and reconstruction.

4.2.1.4 Capability Area C - Consult, Command and Control

The capabilities of commanders to exercise authority over and direct full spectrum of assigned and attached forces in the accomplishment of the mission. Include the capability to communicate and coordinate with other actors which are present or involved in the operational area and effective information exchange with the political and military leadership; capability to plan, employ and coordinate civilian activities with other actors and organizations; capability for nuclear planning and political consultation that allow the rapid development of nuclear employment options in crisis and war, should circumstances so dictate.

4.2.1.5 Capability Area L - Sustain

The capabilities to plan and execute the timely support and sustainment of forces, including essential military infrastructure, movement and transportation, military engineering support, contracting, supply/maintenance/services management, basing support and health and medical support.

4.2.1.6 Capability Area P - Protect

The capabilities to minimize through a common multinational and holistic approach of Force Protection the vulnerability of personnel, facilities, materiel and activities to any threat and in all situations, to include towards the effects of WMD, whilst ensuring the Allies freedom of action and contributing to mission success. During deployed operations, it includes lines of communication and lines of supply and cyber space.

4.2.1.7 Capability Area I - Inform

The capabilities to establish and maintain the situational awareness and level of knowledge required to allow commanders at all levels to make timely and informed decisions.

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 in support of the security objectives that are implemented and executed to guarantee adequate levels of confidentiality, integrity and availability of information. These processes enable a secure environment to meet these 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 Communications 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 a compilation of related, structured information collections that can be regarded as the formal output of a business process and/or can be used as an input to other business processes. These information products can be seen as any communication or representation of knowledge such as facts, data, or opinions in any medium or form. Their definition is linked with activities in related business processes and with automation needs (applications and their respective functions).

Information Products have the capacity to be delivered in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. They may be uniformly consumed by more than one person in more than one business process.

4.2.3.1 Intent and Guidance

The "Intent & Guidance" information products 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.

4.2.3.2 Rules and Measures

The "Rules & Measures" information products 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.

4.2.3.3 Plans

The "Plans" information products 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.

4.2.3.4 Tasking and Orders

The "Tasking & Orders" information products 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.

4.2.3.5 Situational Awareness

The "Situational Awareness" information products are processed and created to provide critical information to decision-makers in complex, dynamic areas such as military command and control.

Situation Awareness (SA) is the perception of environmental elements with respect to time and/or space, the comprehension of their meaning, and the projection of their status, affecting the safe, expedient and effective conduct of the mission. It involves being aware of what is happening in the vicinity to understand how information, events, and actions (both own and others) might impact goals and objectives, both immediately and in the near future.

4.2.3.6 Resource Status

The "Resource Status" information products 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.

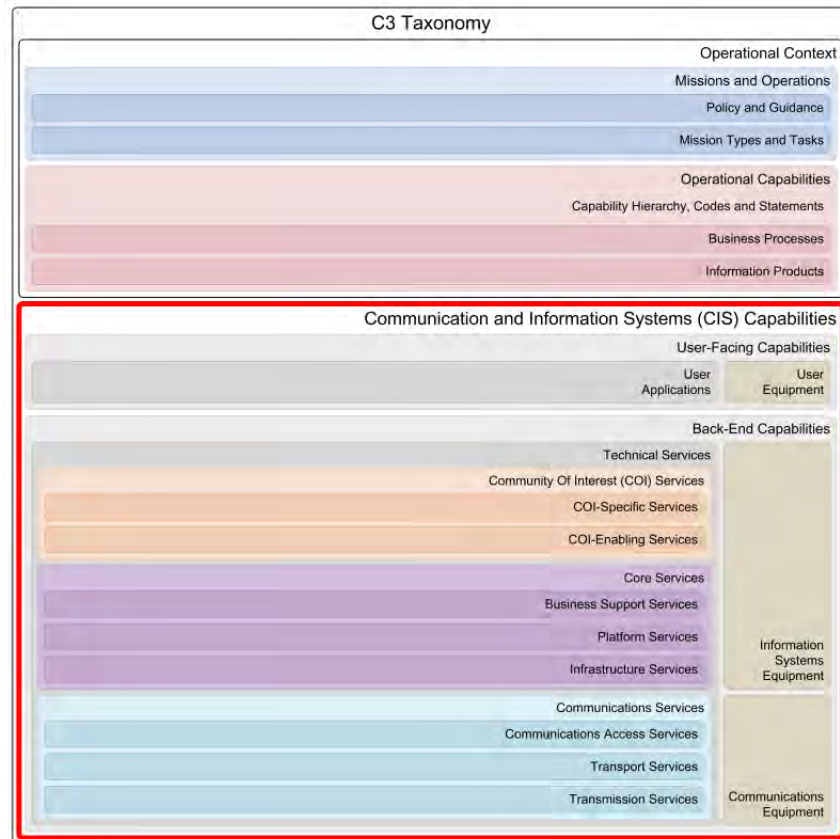
4.2.3.7 Requests and Responses

The "Requests & Responses" information products 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.

4.2.3.8 Reports

The "Reports" information products 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

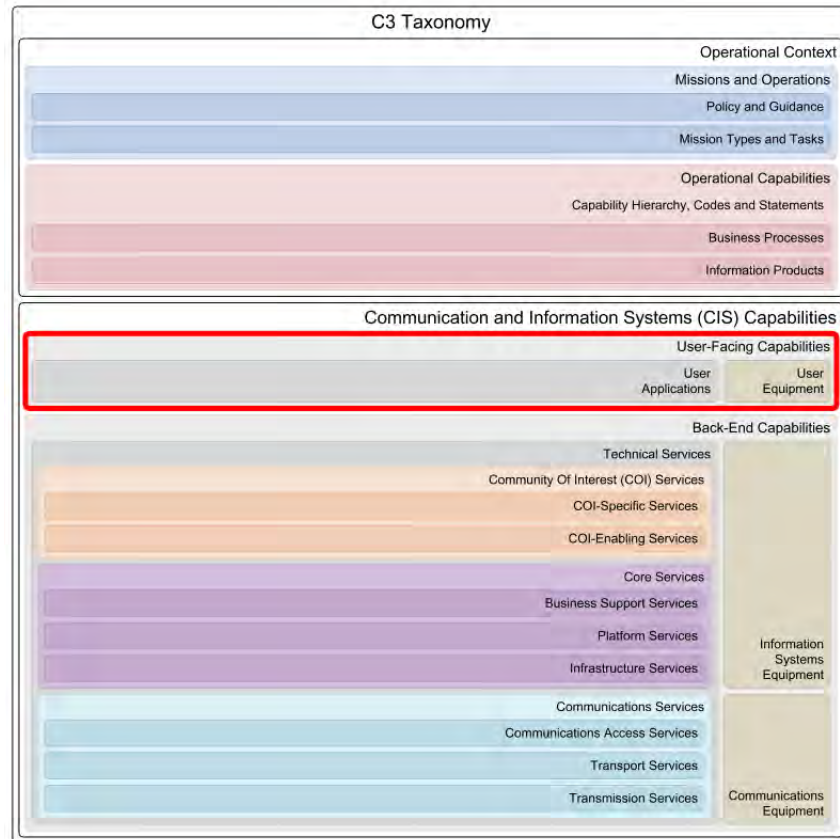


The C3 Taxonomy layer for the "Communication and Information System (CIS) Capabilities" represents the logical components of the capabilities required to meet NATO's information system and communication needs in support of Missions and Operations.

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.

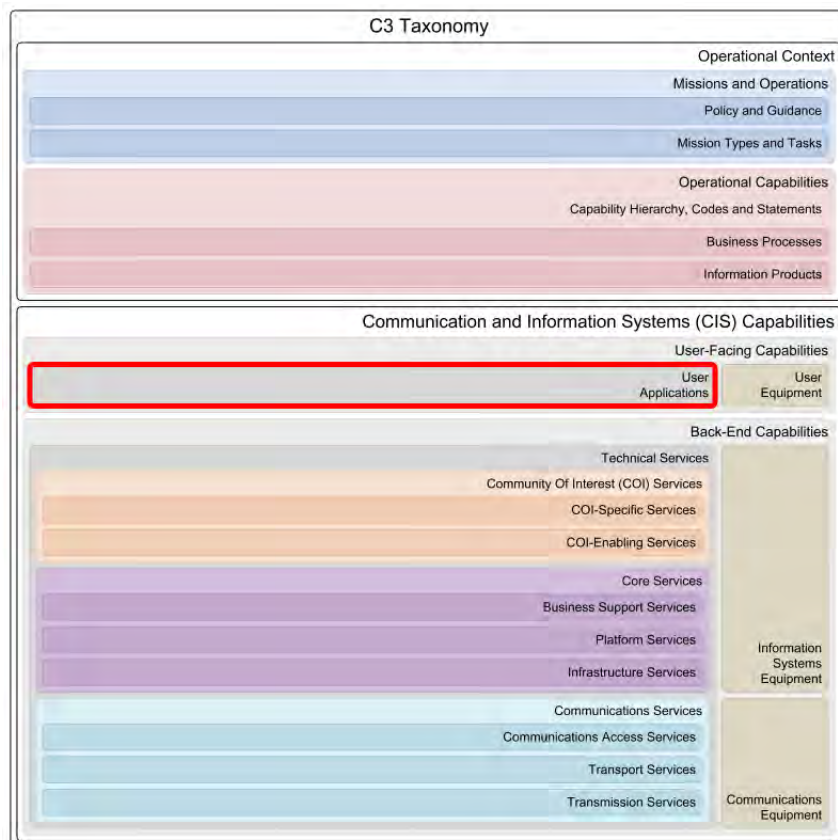
5.1 User-Facing Capabilities



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 constraints 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 measures.

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 Medical Applications

The Medical Applications enable users to provide Medical Situational Awareness (may include medical capabilities, requirements determination and medical sustainability assessment) input to the Common Operational Picture (COP) by automation and standardisation of the information exchange between NATO and national/other systems, and will ensure the timely provision, exchange and management of data required to enable: Medical Planning; Medical Management; Medical Intelligence; Health Surveillance; and Clinical Support.

5.1.1.12 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.

5.1.1.13 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.

5.1.1.14 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.

5.1.1.15 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.

5.1.1.16 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.

5.1.1.17 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.

5.1.1.18 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).

5.1.1.19 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.

5.1.1.20 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.

5.1.1.21 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.

5.1.1.22 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.

5.1.1.23 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.

5.1.1.24 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.

5.1.1.25 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.

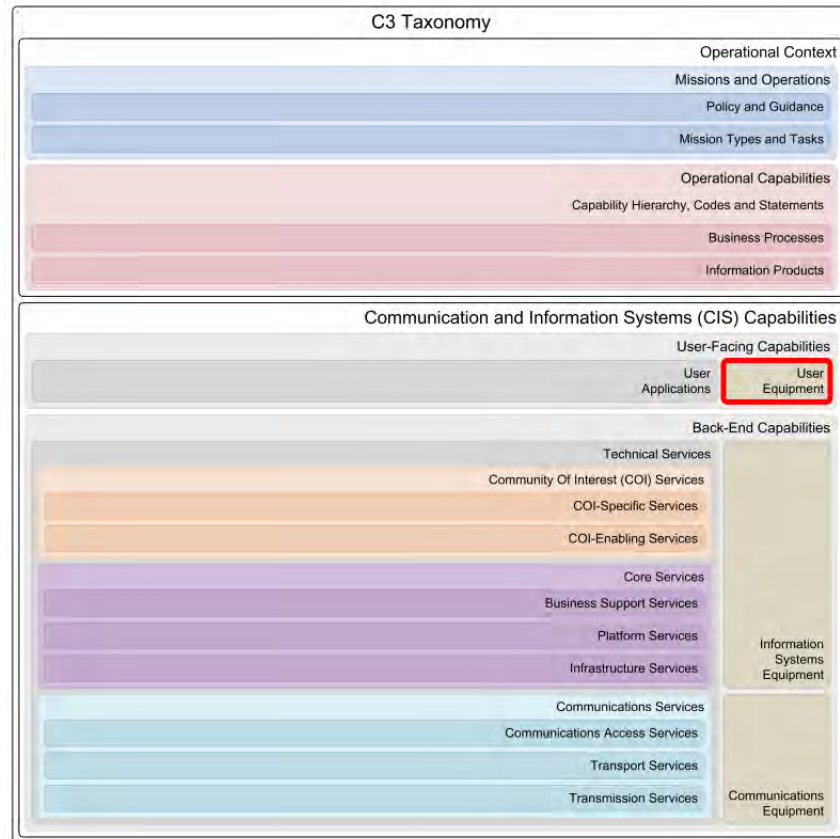
5.1.1.26 Communication and Collaboration Applications

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.

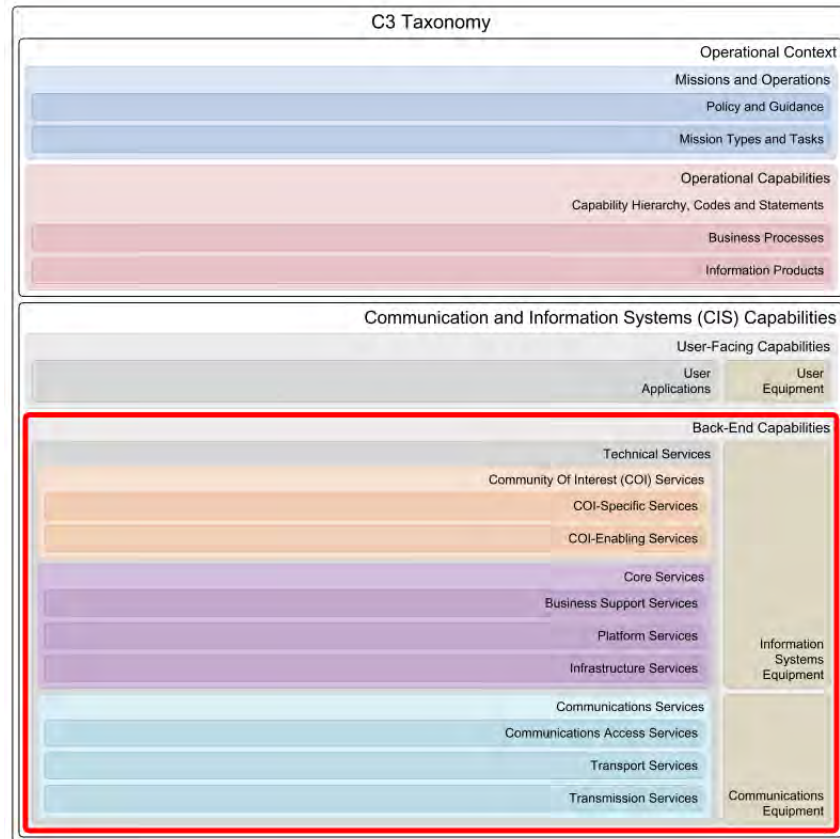
5.1.2 User Equipment



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.

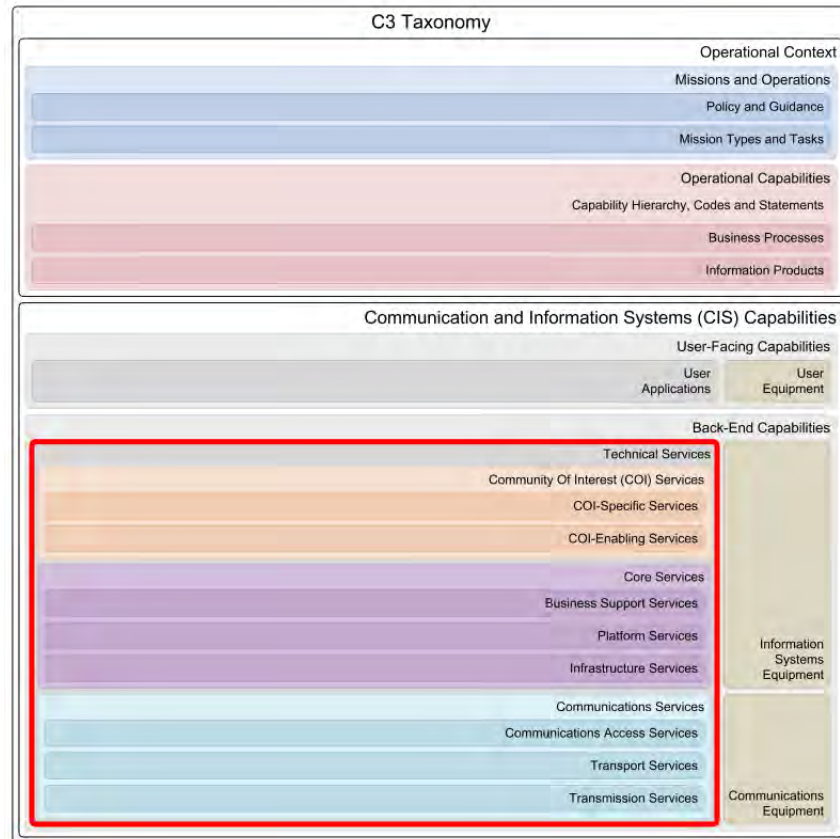
Examples of User Equipment are telephones, computers, laptops, tablets and peripherals (I/O units) including: terminals, card readers, optical character readers, magnetic tape units, mass storage devices, card punches, printers, video display units, data entry devices, teletypes, teleprinters, plotters, 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

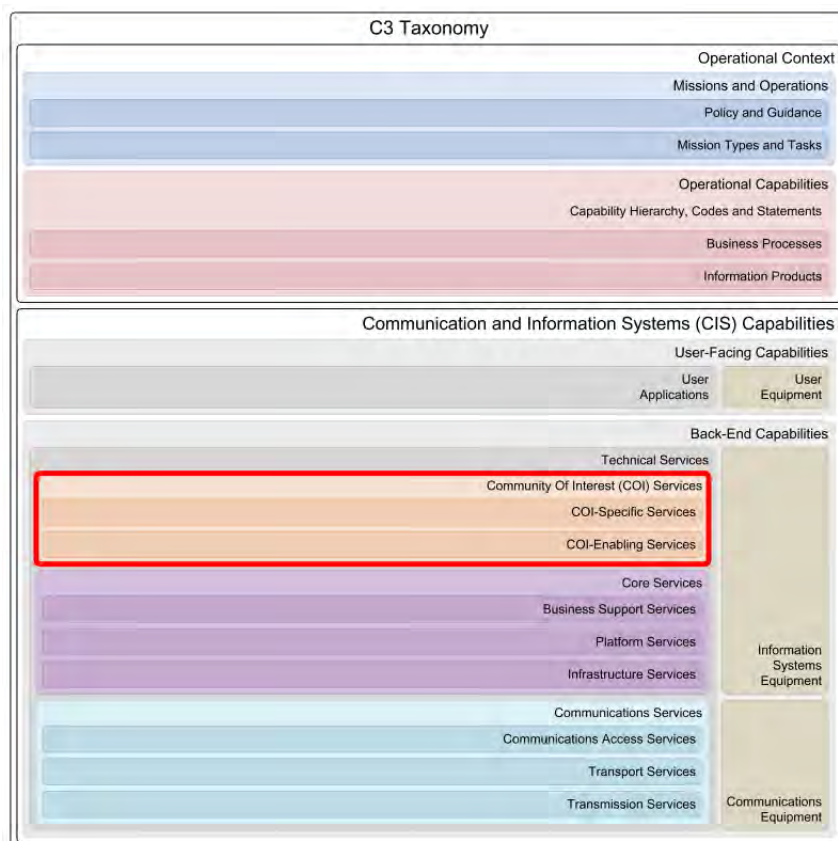


The "Technical Services" taxonomy layer represents the collection of services with requirements for software and hardware functionalities that can be reused for different purposes, together with the policies that should control their usage. These requirements are derived from the operational needs expressed 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 Joint Domain Services

The Joint Domain Services provide unique computing and information services in support of Joint Operations. It supports the set of military activities in which elements of at least two services participate as Joint Forces. When Joint Operations are carried out by military forces of two or more nations, they are known as Combined Joint Operations.

5.2.1.1.1.2 Air Domain Services

The Air Domain Services provide unique computing and information services in support of Air Operations. It supports 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.

5.2.1.1.1.3 Maritime Domain Services

The Maritime Domain Services provide unique computing and information services in support of Maritime Operations. It supports 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.

5.2.1.1.1.4 Land Domain Services

The Land Domain Services provide unique computing and information services in support of Land Operations. It supports 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.

5.2.1.1.1.5 Cyberspace Domain Services

The Cyberspace Domain Services provide unique computing and information services in support of Cyberspace Operations (CO). Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace capabilities are integrated into the joint force commander's plans and synchronized with other operations across the range of military operations. Whilst some military objectives may be achieved by CO alone, typically commanders conduct CO to obtain or retain freedom of maneuver in cyberspace, accomplish joint force commander's objectives, deny freedom of action to the threat, and enable other operational activities. Cyberspace is the global domain created by communication, information and other electronic systems, their interaction and the information that is stored, processed or transmitted in these systems.

5.2.1.1.1.6 Intelligence and ISR Functional Services

The Intelligence and Intelligence, Surveillance and Reconnaissance (ISR) Functional Services provide unique computing and information services for intelligence and ISR support to operations. It supports 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.

5.2.1.1.1.7 Electronic Warfare Functional Services

The Electronic Warfare (EW) Functional 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. It supports 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.

5.2.1.1.1.8 Environmental Functional 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.

5.2.1.1.1.9 Logistics Functional Services

The Logistics Functional Services provide unique computing and information services for logistics support to operations. It supports the set of (military) activities that are undertaken for the planning and execution of the movement, sustainment, and maintenance of forces.

5.2.1.1.1.10 Medical Functional Services

The Medical Functional Services provide the means to collect and disseminate accurate, complete and timely information on medical issues and actions, some of which may be sensitive and involve legal liability. The management of medical data and information is a fundamental aspect of medical support. Adequate documentation of medical care given, health status and location of personnel and environmental threats is part of a continuum of patient treatment and care, and is therefore, a medical responsibility.

The services deliver unique computing and information services: to support medical command and control; to serve as an interface for the exchange of health information between different mission participants, and to allow clinical health data to be transmitted between mission participants.

5.2.1.1.1.11 CIMIC Functional Services

The Civil-Military Cooperation (CIMIC) Functional Services provide unique computing and information services for CIMIC support to operations. It supports the set of (military) activities that are undertaken to coordinate and cooperate, in support of the mission, between force 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 Functional Services

The Education, Training, Exercises and Evaluation (ETEE) Functional 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 CIS Functional Services

The Communications and Information Systems (CIS) Functional Services delivers a collection of Service Management and Control (SMC), CIS Security and Cyber Defence Services that provides the means to implement and enforce SMC and CIS Security measures and standards.

5.2.1.1.2 COI-Enabling Services

The Community of Interest (COI)-Enabling Services provide COI-dependant functionality required by more than one community of interest. They are similar to Business Support Services in that they provide building blocks for domain-specific service development. The distinction between the two is that Business 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 Business Support Services tend to be more generic and can be used by any business or enterprise.

5.2.1.1.2.1 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.

5.2.1.1.2.2 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.

5.2.1.1.2.3 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.

5.2.1.1.2.4 Operations Information Services

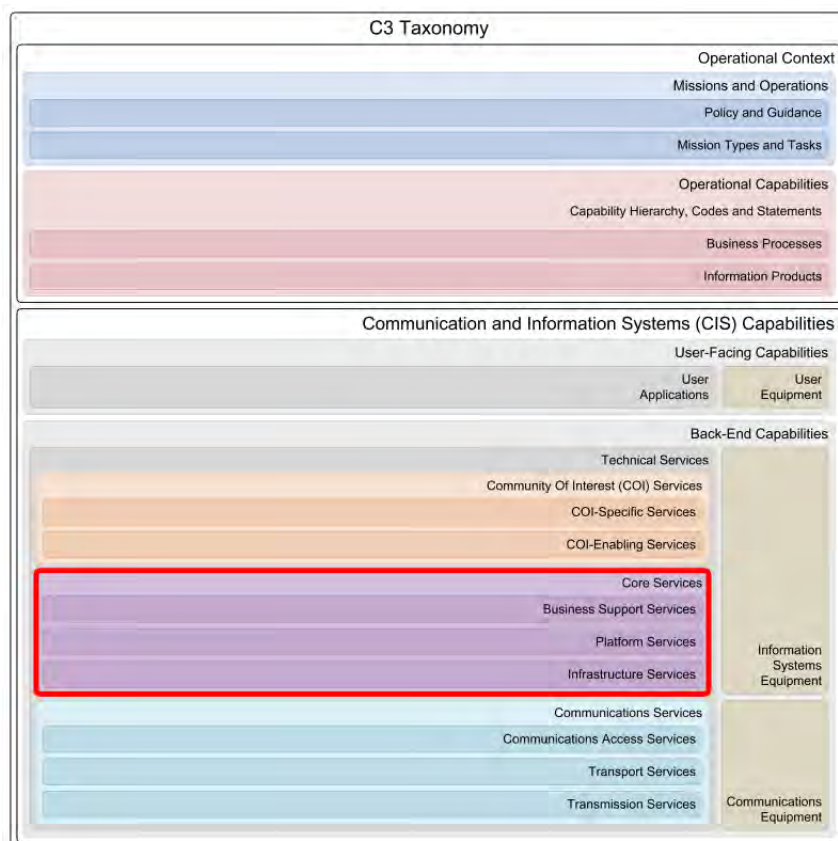
The Operations Information Services provides the means to discover, identify, access and disseminate operationally relevant information and data. This information includes, but is not limited to, Battlespace Objects, Battlespace Events and Tracks.

5.2.1.1.2.5 Modeling and Simulation Services

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

Each simulation requires well-defined models, information resources, rules, behaviours and constraints, which are authoritative and managed. One or more simulations are executed and controlled to achieve the outputs required by follow on simulations, processes and/or decision makers. The simulation environment allows for the modeling of multiple entities, their behaviours and interactions to determine the likely results.

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 measures 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 Communication and Collaboration Services

The 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 fulfill alliance's and coalition's operational requirements. These services enable real-time situational updates to time-critical planning activities between coalition partners, communities of interest, and (NATO and National) agencies. Levels of collaboration include awareness, shared information, coordination and joint product development.

5.2.1.2.1.4 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.

5.2.1.2.1.5 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.

5.2.1.2.1.6 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.

5.2.1.2.1.7 Data Science Services

The Data Science Services provide the means to collect, aggregate, manage, curate and control information resources and analytical services required for conducting operations research and other data analysis activities. Whilst each analytical task is unique there are common technical requirements with respect to collection of large volumes of unstructured and structured data, management of data excerpts, normalization, visualization, analytical and statistical processing, big-data analytics, optimization algorithms etc.

The major steps involved in a data analysis are:

- Ingestion: Extract, transform and store data extracts;
- Curation: Validate, store and manage data in multidimensional databases;
- Analysis: Provide data access to operational analysts using application software; and
- Presentation: Present analyzed data in easily understandable forms, such as graphs.

5.2.1.2.2 Platform Services

The Platform Services provide a foundation to implement services in a loosely coupled environment, where flexible and agile service orchestration is a requirement. They offer generic building blocks for 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 Platform CIS Security Services

The 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 measures at the platform level.

5.2.1.2.2.2 Platform SMC Services

The Platform Service Management and Control (SMC) Services provide a suite of capabilities needed to ensure that platform 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 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 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 Database Services

The Database Services provide access to shared, structured virtual storage components for data and information persistence as part of the platform environment.

5.2.1.2.2.7 Composition Services

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

5.2.1.2.2.8 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 measures 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, 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.

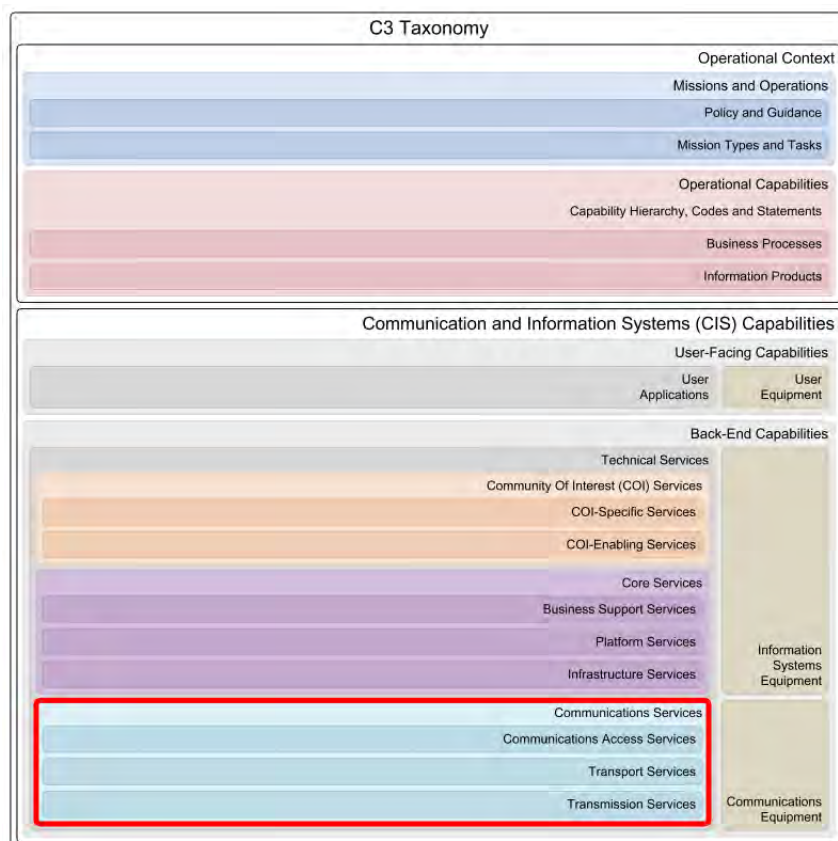
5.2.1.2.3.4 Infrastructure Storage Services

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

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 providers (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 measures 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 measures 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 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 measures 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.

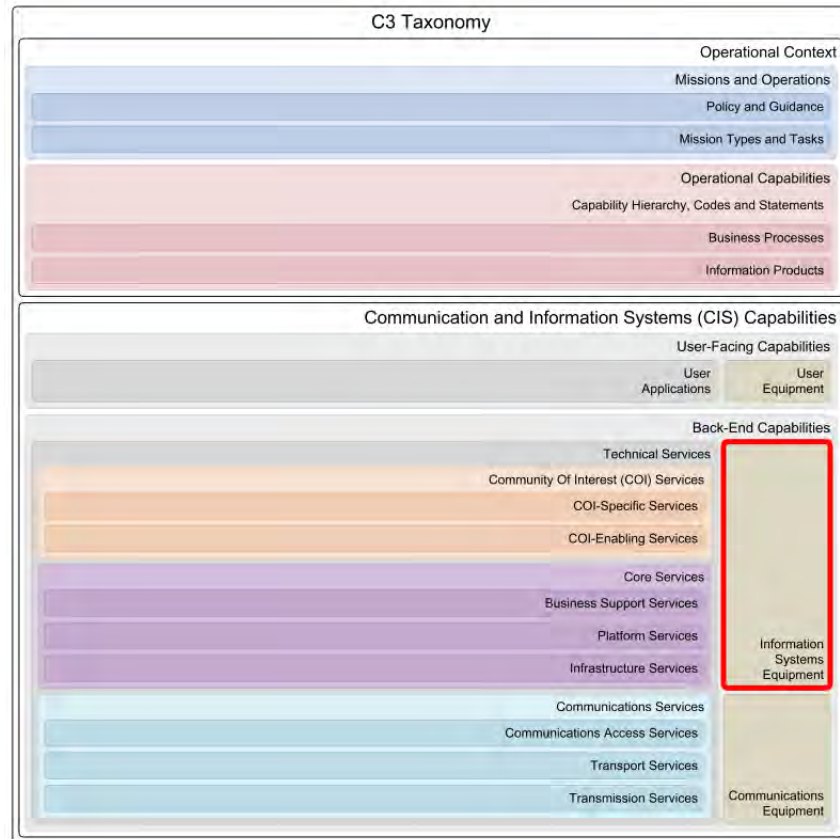
In the context of these services, the wireless transmission path between the static nodes can be established passively (i.e. wireless signal is refracted back to earth by different atmospheric layers) or actively (i.e. wireless signal is transmitted back to earth via a transponder). In the case when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

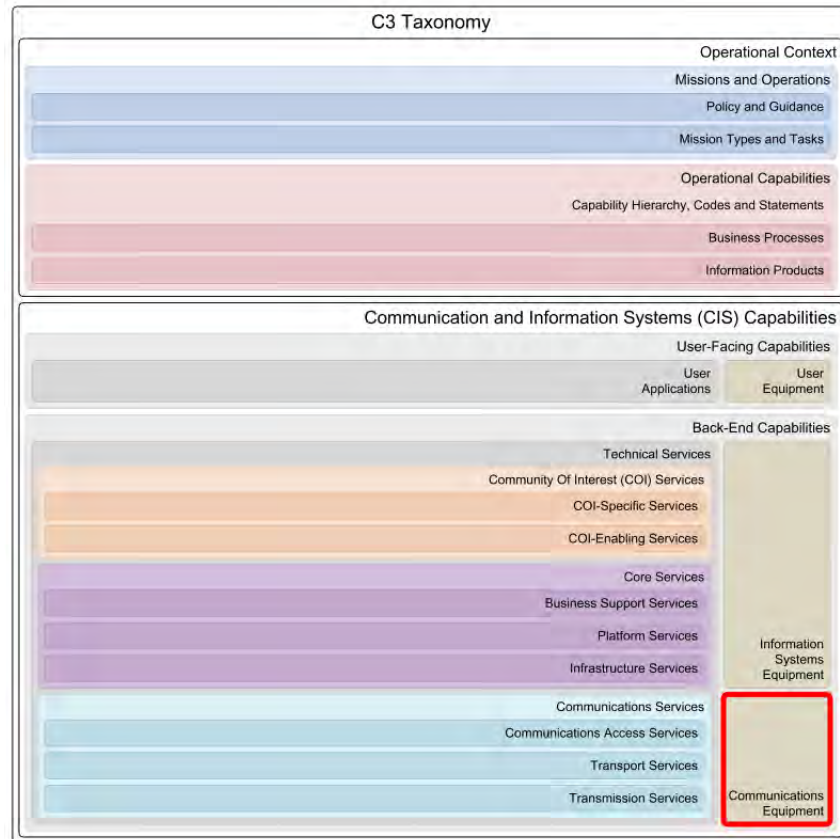
5.2.2 Information Systems Equipment



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.

C3 Technical Services Taxonomy

Community Of Interest (COI) Services

COI-Specific Services

Joint Domain Services

Air Domain Services

Maritime Domain Services

Land Domain Services

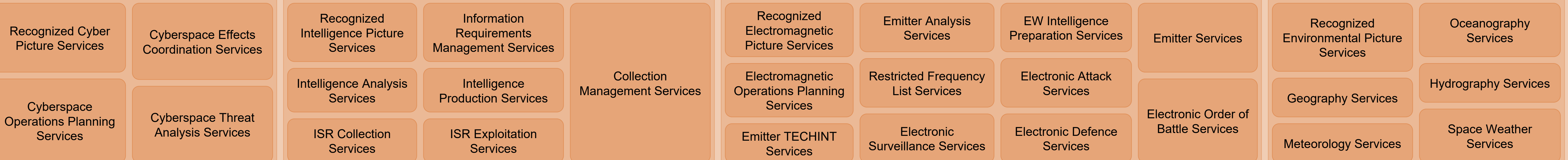


Cyberspace Domain Services

Intelligence and ISR Functional Services

Electronic Warfare Functional Services

Environmental Functional Services



Logistics Functional Services

Medical Functional Services

CIMIC Functional Services

ETEE Functional Services

CIS Functional Services



COI-Enabling Services

Situational Awareness Services

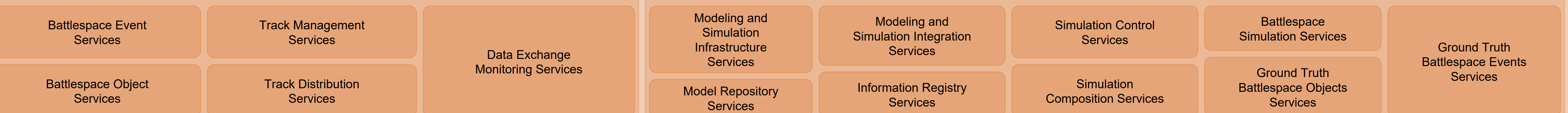
Operations Planning Services

Tasking and Order Services



Operations Information Services

Modeling and Simulation Services



Core Services

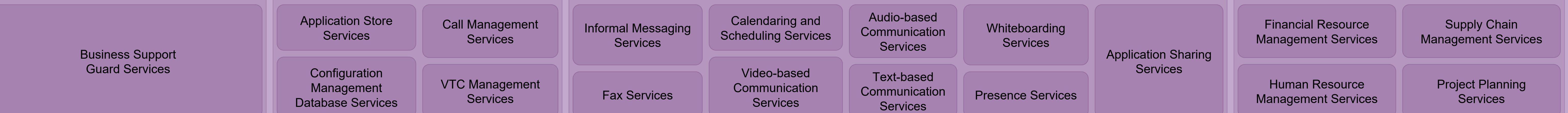
Business Support Services

Business Support CIS Security Services

Business Support SMC Services

Communication and Collaboration Services

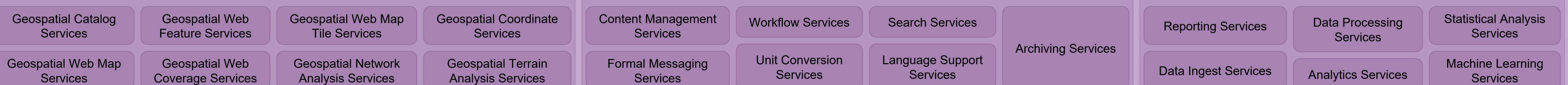
ERP Services



Geospatial Services

Information Management Services

Data Science Services



Platform CIS Security Services

Platform SMC Services

Message-Oriented Middleware Services

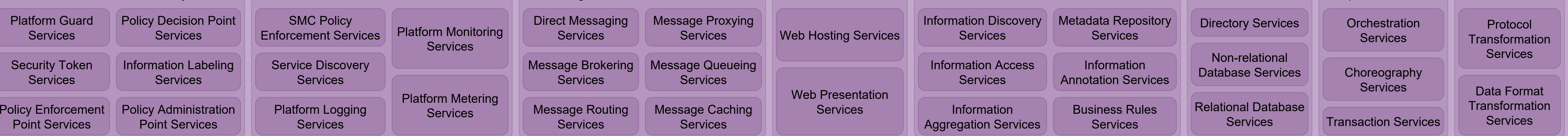
Web Platform Services

Information Platform Services

Database Services

Composition Services

Mediation Services



Infrastructure Services

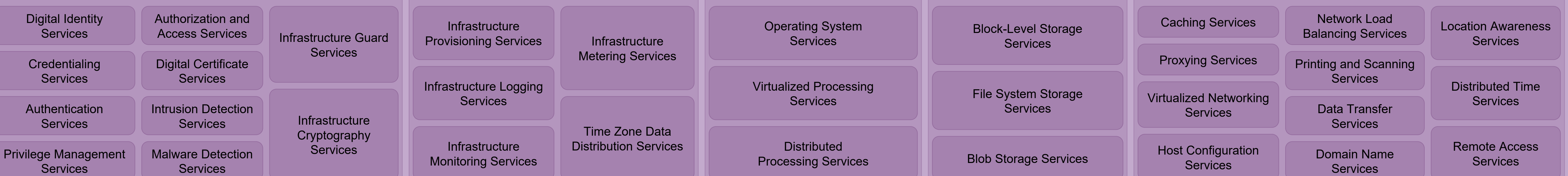
Infrastructure CIS Security Services

Infrastructure SMC Services

Infrastructure Processing Services

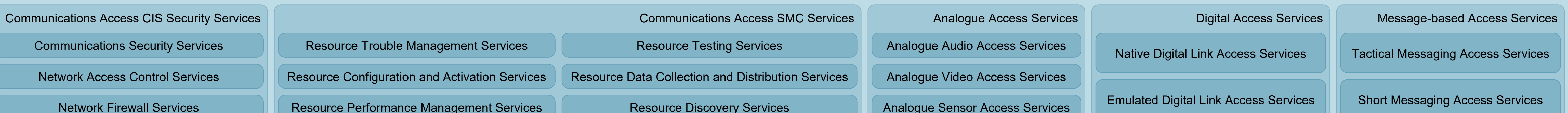
Infrastructure Storage Services

Infrastructure Networking Services



Communications Services

Communications Access Services



Packet-based Access Services

Frame-based Access Services

Circuit-based Access Services

Multimedia Access Services



Transport CIS Security Services

Transport SMC Services

Edge Services

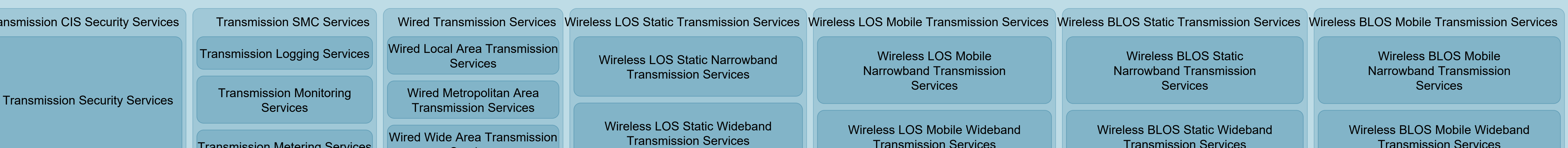
Transit Services

Aggregation Services

Broadcast Services



Transmission Services





C3 Technical Services Taxonomy Report

Table of Contents

1 Introduction	10
2 Overarching Context	11
2.1 C3 Taxonomy	11
2.2 CIS Capabilities	12
2.3 Back-End Capabilities	12
2.4 Technical Services	12
3 Community Of Interest (COI) Services	13
3.1 COI-Specific Services	14
3.1.1 Joint Domain Services	14
3.1.1.1 Surface Area Management Services	14
3.1.1.2 Force Generation and Activation Services	14
3.1.1.3 Crisis Response Measures Services	15
3.1.1.4 CONOPS Development Services	15
3.1.2 Air Domain Services	15
3.1.2.1 Recognized Air Picture Services	15
3.1.2.2 Aeronautical Information Services	15
3.1.2.3 ACO Services	15
3.1.2.4 Air Asset List Services	16
3.1.2.5 ATO Services	16
3.1.2.6 Airspace Management Services	16
3.1.2.7 Airspace Structure Management Services	16
3.1.2.8 Airlift Services	16
3.1.2.9 Air Threat Analysis Services	16
3.1.2.10 Air Weapon Matching Services	16
3.1.2.11 Air Mobility Analysis Services	16
3.1.3 Maritime Domain Services	16
3.1.3.1 Recognized Maritime Picture Services	16
3.1.3.2 Maritime Reference Object Management Services	17
3.1.3.3 Maritime Anomaly Detection Services	17
3.1.3.4 Amphibious Warfare Services	17
3.1.3.5 Subsurface Warfare Services	17
3.1.3.6 Naval Mine Warfare Services	17
3.1.3.7 Maritime Vessel Management Services	17
3.1.4 Land Domain Services	17
3.1.4.1 Recognized Ground Picture Services	17
3.1.4.2 Manoeuver Planning Services	17
3.1.4.3 Task Time Location Management Services	18
3.1.4.4 Terrain Analyzer Services	18
3.1.4.5 Task Classifier Services	18
3.1.4.6 Force Comparison Services	18
3.1.5 Cyberspace Domain Services	18
3.1.5.1 Recognized Cyber Picture Services	18

3.1.5.2 Cyberspace Operations Planning Services	18
3.1.5.3 Cyberspace Effects Coordination Services	18
3.1.5.4 Cyberspace Threat Analysis Services	19
3.1.6 Intelligence and ISR Functional Services	19
3.1.6.1 Recognized Intelligence Picture Services	19
3.1.6.2 Intelligence Analysis Services	19
3.1.6.3 ISR Collection Services	19
3.1.6.4 Information Requirements Management Services	19
3.1.6.5 Intelligence Production Services	19
3.1.6.6 ISR Exploitation Services	19
3.1.6.7 Collection Management Services	19
3.1.7 Electronic Warfare Functional Services	20
3.1.7.1 Recognized Electromagnetic Picture Services	20
3.1.7.2 Electromagnetic Operations Planning Services	20
3.1.7.3 Emitter TECHINT Services	20
3.1.7.4 Emitter Analysis Services	20
3.1.7.5 Restricted Frequency List Services	20
3.1.7.6 Electronic Surveillance Services	20
3.1.7.7 EW Intelligence Preparation Services	20
3.1.7.8 Electronic Attack Services	20
3.1.7.9 Electronic Defence Services	20
3.1.7.10 Emitter Services	21
3.1.7.11 Electronic Order of Battle Services	21
3.1.8 Environmental Functional Services	21
3.1.8.1 Recognized Environmental Picture Services	21
3.1.8.2 Geography Services	21
3.1.8.3 Meteorology Services	21
3.1.8.4 Oceanography Services	21
3.1.8.5 Hydrography Services	21
3.1.8.6 Space Weather Services	21
3.1.9 Logistics Functional Services	21
3.1.9.1 Recognized Logistic Picture Services	22
3.1.9.2 Logistics Planning Services	22
3.1.9.3 Movement Services	22
3.1.9.4 Asset Tracking Services	22
3.1.10 Medical Functional Services	22
3.1.10.1 Recognized Medical Picture Services	22
3.1.10.2 Medical Regulating Services	22
3.1.10.3 Teleconsultation Services	23
3.1.10.4 Casualty Rate Estimation Services	23
3.1.10.5 Epidemiology Services	23
3.1.10.6 Medical Documentation Services	23
3.1.10.7 Trauma Registry Services	23
3.1.11 CIMIC Functional Services	24

3.1.11.1 Behaviour Analysis Services	24
3.1.11.2 Pattern Analysis Services	24
3.1.12 ETEE Functional Services	24
3.1.12.1 Objectives Management Services	24
3.1.12.2 MEL MIL Management Services	24
3.1.13 CIS Functional Services	24
3.1.13.1 Recognized CIS Picture Services	24
3.1.13.2 Cyber Defence Services	24
3.1.13.3 ITSM Services	24
3.1.13.4 Change Management Services	25
3.1.13.5 Spectrum Management Services	25
3.1.13.6 Advanced Threat Management Services	25
3.1.13.7 Electronic Key Management Services	25
3.1.13.8 Security Information and Event Management Services	25
3.2 COI-Enabling Services	26
3.2.1 Situational Awareness Services	26
3.2.1.1 Recognized Picture Services	26
3.2.1.2 Overlay Services	26
3.2.1.3 Symbology Services	27
3.2.2 Operations Planning Services	27
3.2.2.1 Deployment Plan Services	27
3.2.2.2 Courses of Action Services	27
3.2.2.3 Synchronisation Matrix Services	27
3.2.2.4 Order of Battle Services	27
3.2.2.5 Operation Plan Development Services	27
3.2.2.6 Targeting Services	27
3.2.3 Tasking and Order Services	27
3.2.3.1 Resource Allocation Services	27
3.2.3.2 Resource Request Services	28
3.2.3.3 Operations Estimation Services	28
3.2.3.4 Operations Assessment Services	28
3.2.3.5 Operations Order Services	28
3.2.3.6 Tasking Services	28
3.2.4 Operations Information Services	28
3.2.4.1 Battlespace Event Services	28
3.2.4.2 Battlespace Object Services	28
3.2.4.3 Track Management Services	28
3.2.4.4 Track Distribution Services	28
3.2.4.5 Data Exchange Monitoring Services	29
3.2.5 Modeling and Simulation Services	29
3.2.5.1 Modeling and Simulation Infrastructure Services	29
3.2.5.2 Model Repository Services	29
3.2.5.3 Modeling and Simulation Integration Services	29
3.2.5.4 Information Registry Services	29

3.2.5.5 Simulation Control Services	29
3.2.5.6 Simulation Composition Services	29
3.2.5.7 Battlespace Simulation Services	29
3.2.5.8 Ground Truth Battlespace Objects Services	30
3.2.5.9 Ground Truth Battlespace Events Services	30
4 Core Services	31
4.1 Business Support Services	32
4.1.1 Business Support CIS Security Services	32
4.1.1.1 Business Support Guard Services	32
4.1.2 Business Support SMC Services	32
4.1.2.1 Application Store Services	32
4.1.2.2 Configuration Management Database Services	33
4.1.2.3 Call Management Services	33
4.1.2.4 VTC Management Services	33
4.1.3 Communication and Collaboration Services	33
4.1.3.1 Informal Messaging Services	33
4.1.3.2 Fax Services	33
4.1.3.3 Calendaring and Scheduling Services	33
4.1.3.4 Video-based Communication Services	33
4.1.3.5 Audio-based Communication Services	34
4.1.3.6 Text-based Communication Services	34
4.1.3.7 Whiteboarding Services	34
4.1.3.8 Presence Services	34
4.1.3.9 Application Sharing Services	34
4.1.4 ERP Services	34
4.1.4.1 Financial Resource Management Services	34
4.1.4.2 Human Resource Management Services	34
4.1.4.3 Supply Chain Management Services	35
4.1.4.4 Project Planning Services	35
4.1.5 Geospatial Services	35
4.1.5.1 Geospatial Catalog Services	35
4.1.5.2 Geospatial Web Map Services	35
4.1.5.3 Geospatial Web Feature Services	35
4.1.5.4 Geospatial Web Coverage Services	35
4.1.5.5 Geospatial Web Map Tile Services	35
4.1.5.6 Geospatial Network Analysis Services	36
4.1.5.7 Geospatial Coordinate Services	36
4.1.5.8 Geospatial Terrain Analysis Services	36
4.1.6 Information Management Services	36
4.1.6.1 Content Management Services	36
4.1.6.2 Formal Messaging Services	36
4.1.6.3 Workflow Services	36
4.1.6.4 Unit Conversion Services	36
4.1.6.5 Search Services	36

4.1.6.6 Language Support Services	37
4.1.6.7 Archiving Services	37
4.1.7 Data Science Services	37
4.1.7.1 Reporting Services	37
4.1.7.2 Data Ingest Services	37
4.1.7.3 Data Processing Services	37
4.1.7.4 Analytics Services	37
4.1.7.5 Statistical Analysis Services	37
4.1.7.6 Machine Learning Services	37
4.2 Platform Services	39
4.2.1 Platform CIS Security Services	39
4.2.1.1 Platform Guard Services	39
4.2.1.2 Security Token Services	39
4.2.1.3 Policy Enforcement Point Services	39
4.2.1.4 Policy Decision Point Services	40
4.2.1.5 Information Labeling Services	40
4.2.1.6 Policy Administration Point Services	40
4.2.2 Platform SMC Services	40
4.2.2.1 SMC Policy Enforcement Services	40
4.2.2.2 Service Discovery Services	40
4.2.2.3 Platform Logging Services	40
4.2.2.4 Platform Monitoring Services	40
4.2.2.5 Platform Metering Services	41
4.2.3 Message-Oriented Middleware Services	41
4.2.3.1 Direct Messaging Services	41
4.2.3.2 Message Brokering Services	41
4.2.3.3 Message Routing Services	41
4.2.3.4 Message Proxying Services	41
4.2.3.5 Message Queueing Services	42
4.2.3.6 Message Caching Services	42
4.2.4 Web Platform Services	42
4.2.4.1 Web Hosting Services	42
4.2.4.2 Web Presentation Services	42
4.2.5 Information Platform Services	42
4.2.5.1 Information Discovery Services	42
4.2.5.2 Information Access Services	42
4.2.5.3 Information Aggregation Services	42
4.2.5.4 Metadata Repository Services	42
4.2.5.5 Information Annotation Services	43
4.2.5.6 Business Rules Services	43
4.2.6 Database Services	43
4.2.6.1 Directory Services	43
4.2.6.2 Non-relational Database Services	43
4.2.6.3 Relational Database Services	44

4.2.7 Composition Services	44
4.2.7.1 Orchestration Services	44
4.2.7.2 Choreography Services	44
4.2.7.3 Transaction Services	45
4.2.8 Mediation Services	45
4.2.8.1 Protocol Transformation Services	45
4.2.8.2 Data Format Transformation Services	45
4.3 Infrastructure Services	46
4.3.1 Infrastructure CIS Security Services	46
4.3.1.1 Digital Identity Services	46
4.3.1.2 Credentialing Services	46
4.3.1.3 Authentication Services	46
4.3.1.4 Privilege Management Services	47
4.3.1.5 Authorization and Access Services	47
4.3.1.6 Digital Certificate Services	47
4.3.1.7 Intrusion Detection Services	47
4.3.1.8 Malware Detection Services	47
4.3.1.9 Infrastructure Guard Services	47
4.3.1.10 Infrastructure Cryptography Services	47
4.3.2 Infrastructure SMC Services	47
4.3.2.1 Infrastructure Provisioning Services	47
4.3.2.2 Infrastructure Logging Services	48
4.3.2.3 Infrastructure Monitoring Services	48
4.3.2.4 Infrastructure Metering Services	48
4.3.2.5 Time Zone Data Distribution Services	48
4.3.3 Infrastructure Processing Services	48
4.3.3.1 Operating System Services	48
4.3.3.2 Virtualized Processing Services	48
4.3.3.3 Distributed Processing Services	48
4.3.4 Infrastructure Storage Services	48
4.3.4.1 Block-Level Storage Services	48
4.3.4.2 File System Storage Services	49
4.3.4.3 Blob Storage Services	49
4.3.5 Infrastructure Networking Services	49
4.3.5.1 Caching Services	49
4.3.5.2 Proxying Services	49
4.3.5.3 Virtualized Networking Services	49
4.3.5.4 Host Configuration Services	50
4.3.5.5 Network Load Balancing Services	50
4.3.5.6 Printing and Scanning Services	50
4.3.5.7 Data Transfer Services	50
4.3.5.8 Domain Name Services	50
4.3.5.9 Location Awareness Services	50
4.3.5.10 Distributed Time Services	51

4.3.5.11 Remote Access Services	51
5 Communications Services	52
5.1 Communications Access Services	54
5.1.1 Communications Access CIS Security Services	54
5.1.1.1 Communications Security Services	54
5.1.1.2 Network Access Control Services	54
5.1.1.3 Network Firewall Services	55
5.1.2 Communications Access SMC Services	55
5.1.2.1 Resource Trouble Management Services	55
5.1.2.2 Resource Configuration and Activation Services	55
5.1.2.3 Resource Performance Management Services	55
5.1.2.4 Resource Testing Services	55
5.1.2.5 Resource Data Collection and Distribution Services	56
5.1.2.6 Resource Discovery Services	56
5.1.3 Analogue Access Services	56
5.1.3.1 Analogue Audio Access Services	56
5.1.3.2 Analogue Video Access Services	56
5.1.3.3 Analogue Sensor Access Services	56
5.1.4 Digital Access Services	56
5.1.4.1 Native Digital Link Access Services	56
5.1.4.2 Emulated Digital Link Access Services	56
5.1.5 Message-based Access Services	56
5.1.5.1 Tactical Messaging Access Services	56
5.1.5.2 Short Messaging Access Services	57
5.1.6 Packet-based Access Services	57
5.1.6.1 IPv4 Routed Access Services	57
5.1.6.2 IPv6 Routed Access Services	57
5.1.6.3 VPN Access Services	57
5.1.7 Frame-based Access Services	57
5.1.7.1 Native Frame-based Access Services	57
5.1.7.2 Emulated Frame-based Access Services	57
5.1.8 Circuit-based Access Services	58
5.1.8.1 Native Circuit-based Access Services	58
5.1.8.2 Emulated Circuit-based Access Services	58
5.1.9 Multimedia Access Services	58
5.1.9.1 Voice Access Services	58
5.1.9.2 Video Access Services	58
5.1.9.3 VTC Access Services	58
5.2 Transport Services	59
5.2.1 Transport CIS Security Services	59
5.2.1.1 Transport Cryptography Services	59
5.2.2 Transport SMC Services	59
5.2.2.1 Transport Logging Services	60
5.2.2.2 Transport Monitoring Services	60

5.2.2.3 Transport Metering Services	60
5.2.3 Edge Services	60
5.2.3.1 Packet-based Transport Services	60
5.2.3.2 Frame-based Transport Services	60
5.2.3.3 Circuit-based Transport Services	61
5.2.3.4 Link Emulation Transport Services	61
5.2.4 Transit Services	61
5.2.4.1 Packet Routing Services	61
5.2.4.2 Frame Switching Services	61
5.2.4.3 Link Switching Services	62
5.2.5 Aggregation Services	62
5.2.5.1 Packet-based Aggregation Services	62
5.2.5.2 Frame-based Aggregation Services	62
5.2.5.3 Circuit-based Aggregation Services	63
5.2.5.4 Link-based Aggregation Services	63
5.2.6 Broadcast Services	63
5.2.6.1 Packet-based Broadcast Services	63
5.2.6.2 Frame-based Broadcast Services	63
5.2.6.3 Link-based Broadcast Services	63
5.3 Transmission Services	64
5.3.1 Transmission CIS Security Services	64
5.3.1.1 Transmission Security Services	64
5.3.2 Transmission SMC Services	65
5.3.2.1 Transmission Logging Services	65
5.3.2.2 Transmission Monitoring Services	65
5.3.2.3 Transmission Metering Services	65
5.3.3 Wired Transmission Services	65
5.3.3.1 Wired Local Area Transmission Services	65
5.3.3.2 Wired Metropolitan Area Transmission Services	65
5.3.3.3 Wired Wide Area Transmission Services	65
5.3.4 Wireless LOS Static Transmission Services	66
5.3.4.1 Wireless LOS Static Narrowband Transmission Services	66
5.3.4.2 Wireless LOS Static Wideband Transmission Services	66
5.3.5 Wireless LOS Mobile Transmission Services	66
5.3.5.1 Wireless LOS Mobile Narrowband Transmission Services	66
5.3.5.2 Wireless LOS Mobile Wideband Transmission Services	67
5.3.6 Wireless BLOS Static Transmission Services	67
5.3.6.1 Wireless BLOS Static Narrowband Transmission Services	67
5.3.6.2 Wireless BLOS Static Wideband Transmission Services	67
5.3.7 Wireless BLOS Mobile Transmission Services	67
5.3.7.1 Wireless BLOS Mobile Narrowband Transmission Services	68
5.3.7.2 Wireless BLOS Mobile Wideband Transmission Services	68

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.

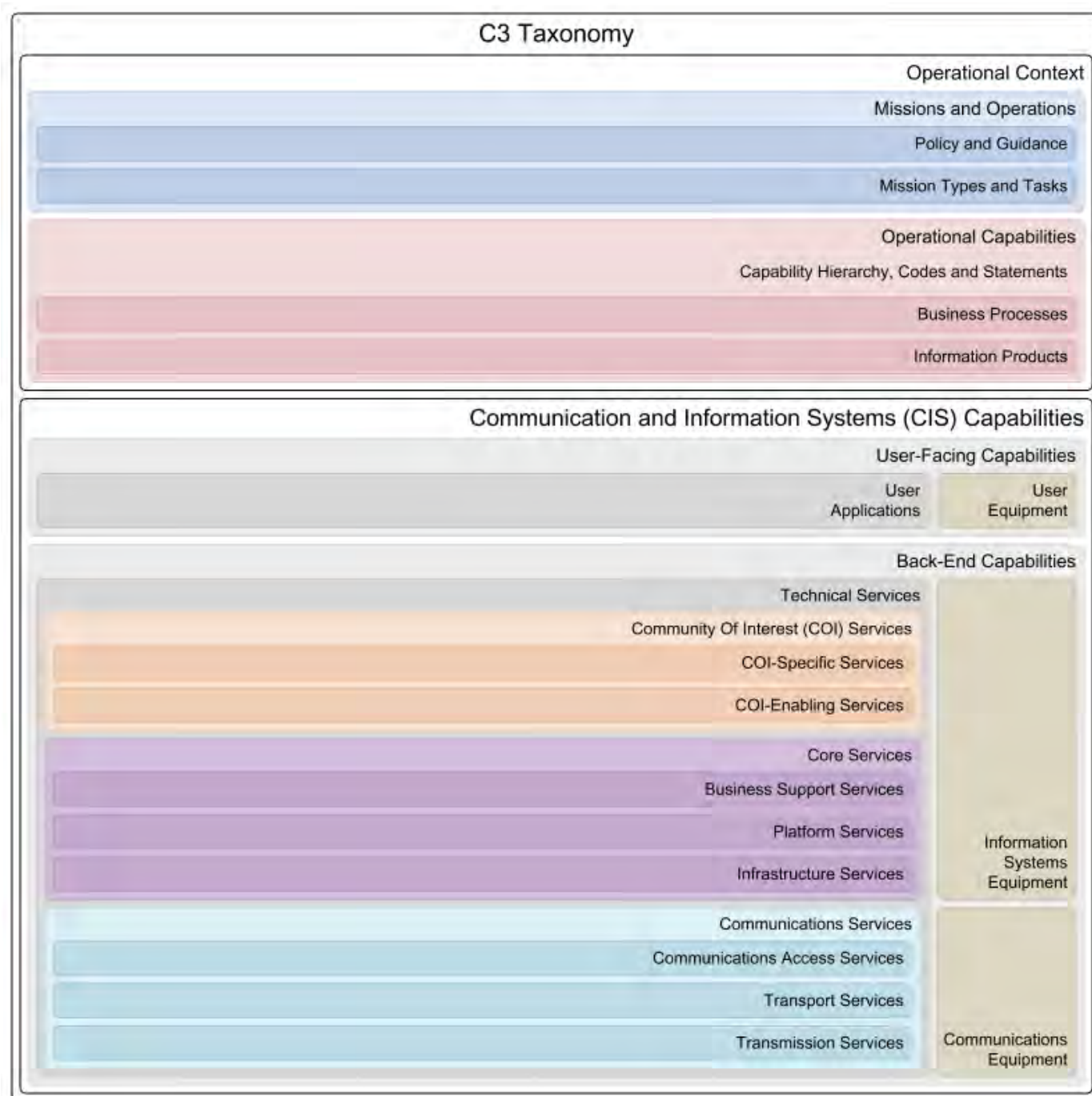
Technical Services are implemented in a federated model that allows NATO and the Nations to jointly provide a robust and secure platform on top of which powerful User Applications can be run. Thus the Technical Services provide the foundation for the NATO Network Enabled Capability (NNEC). They must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

This document contains a report for the C3 Technical Services Taxonomy that is complemented by the C3 Technical Services Taxonomy poster. The data for the C3 Technical Services Taxonomy is registered, processed and maintained on the Enterprise Mapping (EM) Wiki, a protected internet-facing website run by the Requirements Division in Allied Command Transformation (ACT). 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 the "NNEC Services Framework" (NSF).

For the purpose of this document, a "taxonomy" is defined as a particular categorization arranged in a hierarchical structure organized by supertype-subtype relationships. Lower levels in the taxonomy as well as linkage between the taxonomy items and Programs Of Work (POWs), Implementation programs (Capability Packages, Crisis Response Operations (CRO) Urgent Requirements), Standards and Fielded Capabilities can be found on the ACT Enterprise Mapping 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 categorization, 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 Enterprise Mapping 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.

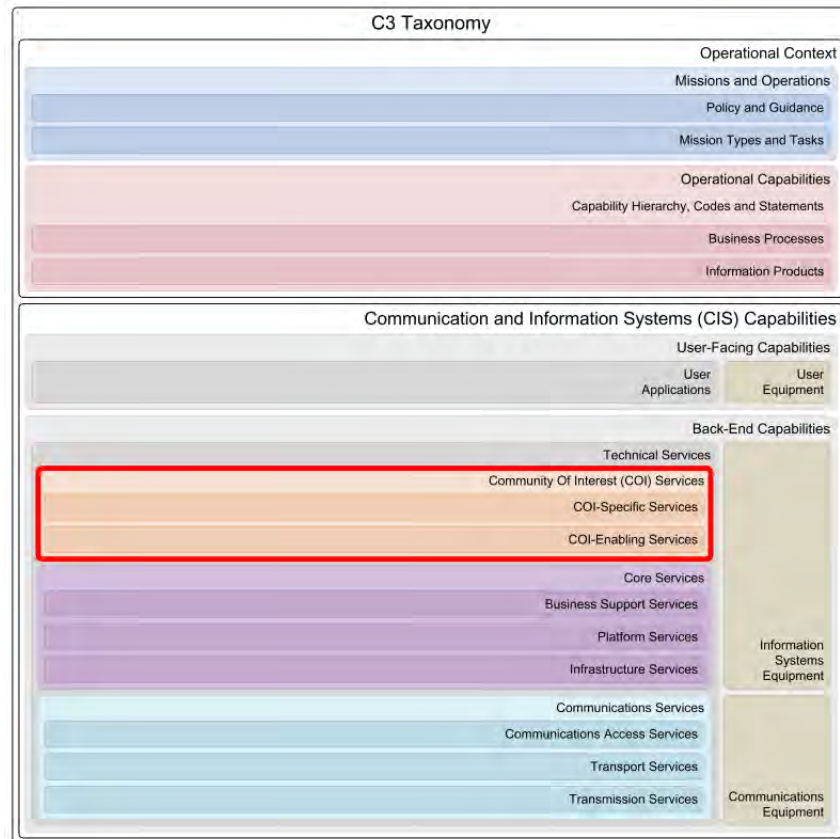
2.4 Technical Services

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.

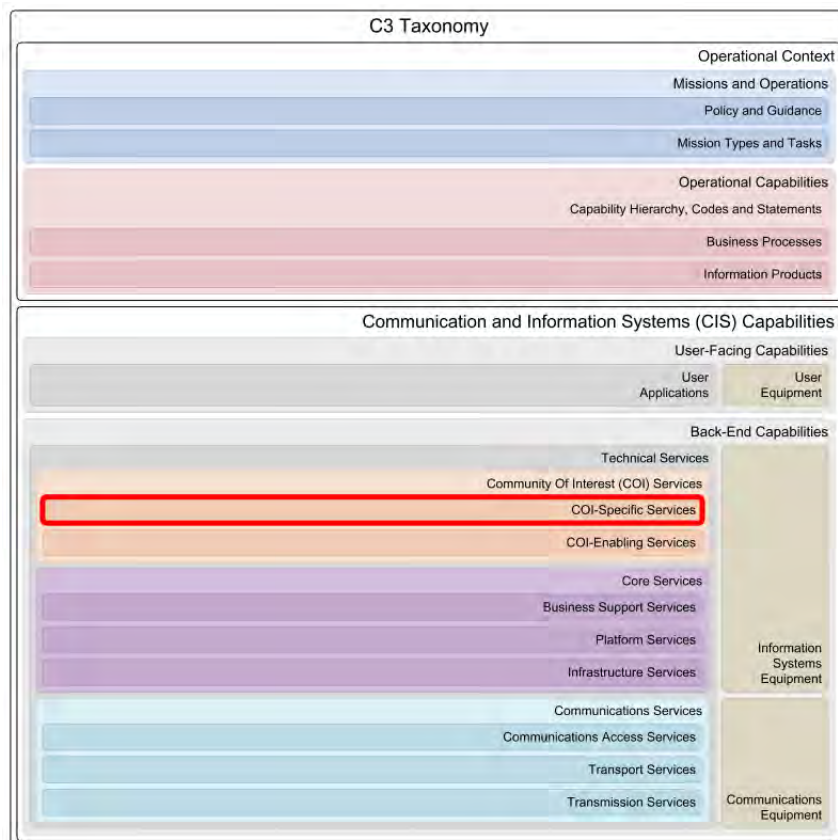
The complete collection of Technical Services is sometimes referred to as the "Technical Services Framework" (TSF) or "NNEC Services Framework" (NSF).

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 Joint Domain Services

The Joint Domain Services provide unique computing and information services in support of Joint Operations. It supports the set of military activities in which elements of at least two services participate as Joint Forces. When Joint Operations are carried out by military forces of two or more nations, they are known as Combined Joint Operations.

3.1.1.1 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.

3.1.1.2 Force Generation and Activation Services

The Force Generation and Activation Services provide unique computing and information services supporting the Force Generation and Activation Processes, such as managing Crisis Response Measures (CRMs) requests, recording responses from potential Troop Contributing Nations, and tracking their implementation.

Force Generation and Activation Services manage the established force package for operations based on confirmed contributions and support planners in the assessment of strategic and operational risks resulting from shortfalls in critical capabilities. Force Generation and Activation Services also support the management of information concerning the lines of communications, entry points, arrival sequence, timings, final destination and Transfer of Authority for each element of a force package entering the theatre.

3.1.1.3 Crisis Response Measures Services

Crisis Response Measures Services provide supporting functionalities for planning applications, specifically with regards to the planning or responses to crisis situations and operations.

3.1.1.4 CONOPS Development Services

The Concept of Operations (CONOPS) Development Services provide the means to facilitate the collaborative planning and the structured development of products for the concept of operations.

CONOPS Development Services support the following areas and associated information products:

- Missions and objectives for Subordinate Commanders
- Critical Timings and Events
- CRM requirements
- Commanders Critical Information Requirements, Priority Intelligence Requirements (PIRs) and Essential Elements of Friendly Information (EEFI)
- Targeting Guidance
- Rules of Engagement
- StratCom Guidance
- civil-military interaction
- Force Protection
- Partner Involvement
- Operations assessment guidance
- Exit Criteria
- Service Support
- Military Police
- Command and Signal
- Communications and Information Concept

3.1.2 Air Domain Services

The Air Domain Services provide unique computing and information services in support of Air Operations. It supports 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.

3.1.2.1 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.

3.1.2.2 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.

3.1.2.3 ACO Services

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

3.1.2.4 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 limited to: the Critical Asset List (CAL), Joint Prioritized Critical Asset List (JPCAL) and Joint Prioritized Defended Asset List (JPDAL).

3.1.2.5 ATO Services

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

3.1.2.6 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).

3.1.2.7 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 categorization. In uncontrolled airspace, all aircraft do their own separation according to general rules.

3.1.2.8 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.

3.1.2.9 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.

3.1.2.10 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.

3.1.2.11 Air Mobility Analysis Services

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

3.1.3 Maritime Domain Services

The Maritime Domain Services provide unique computing and information services in support of Maritime Operations. It supports 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.

3.1.3.1 Recognized Maritime Picture Services

The Recognized Maritime Picture (RMP) Services provide the means to create, manage and disseminate the Recognized 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. It also provides data on the current and historical information of object data, e.g. tracks, vessels, figures, ports and special points.

The information related to both combatant and non-combatant vessels builds the Maritime Operational Picture (MOP), in the broadest sense, which consists of all kinds of maritime operational objects available. MOP is the overall collection of Military Picture (MP), which is the collection of all recognized combatant tracks, vessels and relevant reference objects, White Picture (WP), which is the collection of civilian maritime tracks and vessels from a non-combatant category (merchant, fishing, pleasure, research, government etc.) and relevant reference objects, and any unknown and pending tracks with any other available supportive information.

3.1.3.2 Maritime Reference Object Management Services

The Maritime Reference Object Management Services support maritime control measures (reference points, special points, lines and areas) under "Reference Objects". It provides world-wide management of Reference Objects as well as within Maritime Operations, which are identified uniquely in the system context.

3.1.3.3 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.

3.1.3.4 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.

3.1.3.5 Subsurface Warfare Services

The Subsurface Warfare Services perform computational analysis related to Water Space Management (WSM) and Prevention of Mutual Interference (PMI) of subsurface vessels. When WSM/PMI Area is created, the authorised user can initiate an Interference Check. The checking process compares the areas and reports all conflicts between areas, tracks, grid assignments, and area sequences for surface and subsurface operations.

3.1.3.6 Naval Mine Warfare Services

The Naval Mine Warfare (NMW) Services provide the means to support management of various types of NMW data such as mines, intelligence information, NMW areas and plans. These services also include functions related to Mine Countermeasures (MCM) planning, evaluation, and risk assessment. Additionally, the support for mine hunting SONAR is provided to estimate probability of detection and categorization of echoes.

3.1.3.7 Maritime Vessel Management Services

The Maritime Vessel Management Services provides the means to manage data related to all naval units, merchant vessels, fishing vessels, pleasure crafts and government ships like coastguard, police, customs and research. The services provide the facilities to maintain the Vessel Database.

The Vessel Database accumulates the information from various data sources such as Nation reports, intelligence reports and data links. It enables the analysis and correlation of data, and the association of available tracks with vessels in the Vessel Database. The database provides detailed, static information for those Tracks and stores the history. Authorized users can update the static attributes of Vessels, such as its activity, status, capabilities, and image.

3.1.4 Land Domain Services

The Land Domain Services provide unique computing and information services in support of Land Operations. It supports 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.

3.1.4.1 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.

3.1.4.2 Manoeuvre Planning Services

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

3.1.4.3 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.

3.1.4.4 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.

3.1.4.5 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.

3.1.4.6 Force Comparison Services

The Force Comparison Services provide the means to support the quantitative and qualitative comparison of forces and the specification of the Measures of Effectiveness (MOEs) and Measures of Effectiveness (MOPs) for force component combinations.

3.1.5 Cyberspace Domain Services

The Cyberspace Domain Services provide unique computing and information services in support of Cyberspace Operations (CO). Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace capabilities are integrated into the joint force commander's plans and synchronized with other operations across the range of military operations. Whilst some military objectives may be achieved by CO alone, typically commanders conduct CO to obtain or retain freedom of maneuver in cyberspace, accomplish joint force commander's objectives, deny freedom of action to the threat, and enable other operational activities. Cyberspace is the global domain created by communication, information and other electronic systems, their interaction and the information that is stored, processed or transmitted in these systems.

3.1.5.1 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).

There are basically three main components contributing to Cyber Situational Awareness:

- Status of the own or friendly cyber terrain (own CIS), this is supported by the RCISP
- Intelligence regarding adversaries, vulnerabilities, intent etc., this is supported by the RIP
- Cyberspace information of specific interest to the mission.

While many elements of cyberspace can be mapped geographically, a full understanding of an adversary's disposition and capabilities in cyberspace involves understanding the target, not only at the underlying physical network layer but also at the logical network layer and cyber-persona layer, including profiles of system users and administrators and their relationship to adversary critical factors.

3.1.5.2 Cyberspace Operations Planning Services

The Cyberspace Operations Planning Services provide unique computing and information services for integrating cyberspace aspects into the strategic and operational planning process, addressing the Commander's need to maintain Command and Control (C2) of the operation and ensure that effects delivered in or through different domains are orchestrated. By themselves, these services are not unique to cyberspace. Rather, by recognizing cyberspace as a domain, cyber should be fully integrated into existing processes and operations planning services.

3.1.5.3 Cyberspace Effects Coordination Services

The Cyberspace Effects Coordination Services provide unique computing and information services in support of Cyberspace Operations (CO). Activities in cyberspace must be optimized and de-conflicted to maximize the effectiveness of operations conducted by Nations in Cyberspace. Cyberspace Effects Coordination Services enable Commanders to request specific Cyberspace Effects for defined planning periods. The services enable providers of those effects a means for sharing of restrictions and other utilization guidance for the use of cyberspace .

3.1.5.4 Cyberspace Threat Analysis Services

The Cyberspace Threat Analysis Services provide unique computing and information services for supporting systematic, continuous process of analyzing the threat and environment in cyberspace, the "Intelligence Preparation of the Cyber Environment". This process typically consists three steps (1) Defining the operational environment, (2) Evaluating threats and adversaries, and (4) Determining threat/adversary courses of action (COAs).

3.1.6 Intelligence and ISR Functional Services

The Intelligence and Intelligence, Surveillance and Reconnaissance (ISR) Functional Services provide unique computing and information services for intelligence and ISR support to operations. It supports 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.

3.1.6.1 Recognized Intelligence Picture Services

The Recognized Intelligence Picture (RIP) Services provide the means to produce, manage and disseminate the Recognized Intelligence Picture (RIP). The RIP is the compilation of validated data relating to a defined area of interest that is disseminated to enable situational awareness and support decision making at all levels. Most intelligence is derived from a single source. However, there are significant advantages to be derived from the deliberate application of two or more discrete but supporting intelligence disciplines (e.g. Geospatial Intelligence (GEOINT), Human Intelligence (HUMINT) or Signals Intelligence (SIGINT)) seeking to improve the quality of the Recognized Intelligence Picture. The RIP Services will support the development of the RIP through the collection, aggregation, correlation and fusion of intelligence from multiple sources.

3.1.6.2 Intelligence Analysis Services

The Intelligence Analysis Services support Joint Intelligence Preparation of the Operating Environment (JIPOE) and Targeting (Joint Effects) processes. During the JIPOE process, new intelligence requirements are identified and entered into the Intelligence Cycle. For Joint Effects process the Intelligence Analysis Services provide information for targeting the threat's forces and systems with direct and indirect lethal and nonlethal fires.

3.1.6.3 ISR Collection Services

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

3.1.6.4 Information Requirements Management Services

The Information Requirements Management Services provide the means to access and manage information requirements, related information objects, their status and relationship to decision making. The Information 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 requirements, and related information objects, throughout the intelligence cycle (direction, collection, processing, analysis, dissemination and feedback).

3.1.6.5 Intelligence Production Services

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

3.1.6.6 ISR Exploitation Services

The Intelligence, Surveillance and Reconnaissance (ISR) Exploitation Services provide the means to exploit collected ISR data. The services will provide the means to analyse and verify the collected data against the intelligence requirements. In support of analysis, the ISR Exploitation Services will support functions for the transformation, categorization, and matching of collected data.

3.1.6.7 Collection Management Services

The Collection Management Services provide the means to facilitate close collaboration with both Intelligence, Surveillance and Reconnaissance (ISR) and command staff to optimize the use of ISR collection assets.

3.1.7 Electronic Warfare Functional Services

The Electronic Warfare (EW) Functional 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. It supports 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.

3.1.7.1 Recognized Electromagnetic Picture Services

The Recognized Electromagnetic Picture (REMP) Services provide the means to produce, manage and disseminate the REMP. These services will generate a de-conflicted and agreed picture of the Electromagnetic Environment through the collection, aggregation, correlation and fusion of information from multiple sources.

3.1.7.2 Electromagnetic Operations Planning Services

The Electromagnetic Operations (EMO) Planning Service will permit assessment of EW threat, coordination of force deployment, creation of operational reporting and dissemination of tasking orders.

3.1.7.3 Emitter TECHINT Services

The Emitter Technical Intelligence (TECHINT) Services provide the means to accumulate and manage the information lifecycle of Technical Intelligence held on known emitters. It focuses on foreign technological developments, and the performance and operational capabilities of foreign materiel, which have or may eventually have a practical application for military purposes.

3.1.7.4 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.

3.1.7.5 Restricted Frequency List Services

The Restricted Frequency List Services provide the means to create, manage and share a list of restricted frequencies and related metadata for the purpose of Electronic Warfare.

3.1.7.6 Electronic Surveillance Services

The Electronic Surveillance Service Provides the means to permit the exploitation of electromagnetic (EM) energy, either for communications or any other EM emission data to enhance situational awareness, using alerts and indicators to report any change in operational activity.

3.1.7.7 EW Intelligence Preparation Services

The Electronic Warfare (EW) Intelligence Preparation Services provides the means to develop the EW aspects in the Joint Intelligence Preparation of the Operational Environment (JIPOE). It permits creation of workflow, collaboration, product life cycle management, re-use of products, archiving, building of knowledge base and reporting in the Electromagnetic Environment (EME), integrated with the Operational Planning Process, management of the Intelligence Cycle, CCIRM, co-ordination of targeting and integration with related ISR services.

3.1.7.8 Electronic Attack Services

The Electronic Attack (EA) Services support assessment of the enemy capabilities alongside determining optimal timing to degrade, disrupt, deceive, destroy or deny the enemy C2 capabilities and diminish their opportunities to shape or exploit the operational environment.

3.1.7.9 Electronic Defence Services

The Electronic Defence (ED) Services provide the means to permit the detection of electromagnetic (EM) energy, using alerts of incoming Radio Frequency (RF), Infra Red (IR) and laser guided weapons to protect resources and ensure effective friendly use of the EM spectrum.

3.1.7.10 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).

3.1.7.11 Electronic Order of Battle Services

The Electronic Order of Battle (EOB) Services provide the means to produce, manage and disseminate the Electronic Order of Battle, either Initial EOB (I-EOB), Theatre Specific EOB (TS-EOB), Nation EOB or other EOB types. The services permit the versioning, assigning of metadata and storage.

3.1.8 Environmental Functional 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.

3.1.8.1 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.

3.1.8.2 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.

3.1.8.3 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.

3.1.8.4 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.

3.1.8.5 Hydrography Services

The Hydrography Services provide access to high-level and value-added information, and related computational 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.

3.1.8.6 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.

3.1.9 Logistics Functional Services

The Logistics Functional Services provide unique computing and information services for logistics support to operations. It supports the set of (military) activities that are undertaken for the planning and execution of the movement, sustainment, and maintenance of forces.

3.1.9.1 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.

The elements comprising the RLP typically include, but are not limited to, the following: stock levels, including standard days of supply, by classes of supply in combined joint force and HNS (on which visibility has been granted); transportation capabilities; mission essential equipment; and status of the Joint Logistic Support Network (JLSN).

3.1.9.2 Logistics Planning Services

The Logistics Functional Services deliver functionality to automatically access, process and disseminate information related to threat environment; identified available logistic nodes; available infrastructure and its suitability for logistic operations; host-nation support capabilities and capacity; military interoperability and cooperation agreements; environmental protection; climate; and terrain.

During each planning activity, logistic opportunities and limitations will be clear drivers when developing different COAs. It is vital that the impact of logistic support on the proposed conduct of operations is clearly understood.

3.1.9.3 Movement Services

The Movement Services deliver functionality to automatically access, process and disseminate information to coordinate and control movements to/from and within the theater of operations. This also includes reception, staging and onward movement (RSOM)/ rearward movement, staging and dispatch (RMSD) operations.

3.1.9.4 Asset Tracking Services

The Asset Tracking Services deliver functionality to automatically access, process and disseminate asset information pertaining to location, status, and condition of products, vehicles, and other assets. In addition, as the military has to deal with volatile supply chains which can be affected by adversaries, unpredictable events including adverse weather, natural disasters, geopolitical events, and many other factors.

3.1.10 Medical Functional Services

The Medical Functional Services provide the means to collect and disseminate accurate, complete and timely information on medical issues and actions, some of which may be sensitive and involve legal liability. The management of medical data and information is a fundamental aspect of medical support. Adequate documentation of medical care given, health status and location of personnel and environmental threats is part of a continuum of patient treatment and care, and is therefore, a medical responsibility.

The services deliver unique computing and information services: to support medical command and control; to serve as an interface for the exchange of health information between different mission participants, and to allow clinical health data to be transmitted between mission participants.

3.1.10.1 Recognized Medical Picture Services

The Recognized Medical Picture (RMedP) Services provide the means to create, manage and disseminate the Recognised Medical Picture. Medical decision-making is dependent on the efficient, speedy processing of environmental, tactical, and casualty data. Such information is of fundamental importance in specialties such as epidemiology to enable early detection of disease outbreaks including the use of biological warfare agents (disease surveillance). RMedP 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.

3.1.10.2 Medical Regulating Services

The Medical Regulating Services provide unique computing and information services supporting control and coordination processes that ensure patients are evacuated from point of wounding or onset of disease through successive medical treatment facilities which are best capable of providing the required treatment. Medical Regulating Services include managing of resources such as evacuation means and medical treatment facilities and also the tracking of patients as they are being moved through the medical evacuation and treatment chain.

3.1.10.3 Teleconsultation Services

The Teleconsultation Services support provisioning of clinical health care from a distance, by facilitating the provisioning of offsite specialist medical advice and services (e.g., dental, mental health, cardiology, dermatology) and provides mechanism for exchange of medical specialty-specific data sets (e.g., heart and lung sounds, electrocardiograms, video and still images and electronic health records) between referring physician and remote specialists. Teleconsultation Services supplement common collaboration and communications services such as VTC, chat and email.

Teleconsultation Services can be used in critical care and emergency situations when specialist medical healthcare is not available on-site.

3.1.10.4 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.

3.1.10.5 Epidemiology Services

The Epidemiology Services provide the means for automated data management in support of health and disease surveillance, including the collection and management of health surveillance data summaries, final reports and investigations prepared for analysis and repository center.

The Epidemiology Services support:

- the data collection points (e.g. deployed task force medical advisor office, medical coordination cells, medical national headquarters, civilian centres, etc.),
- the collection and storage of data, data summaries, reports and investigations,
- the provision of analytical tools, search functionalities ,
- the monitoring, collection and evaluation of illness/injury data on all coalition force's personnel who report for medical treatment support, both on an outpatient and inpatient basis.
- the integration with geographic information system to provide near real-time visualization for situational awareness;
- the continuous monitoring of current incidence of disease symptom complexes;
- the automated reporting and early warnings in case of statistical anomalies and an emergency/critical event/input.

3.1.10.6 Medical Documentation Services

The Medical Documentation Services provide the means for the secure electronic exchange of Electronic Clinical records - also known as Electronic health records (EHR), or electronic medical records (EMR) - across different medical stakeholders such as Medical Treatment Facilities to supports continuity of care. It supports the systematized collection of patient and population electronically-stored health information in a digital format.

Clinical Records may include a range of data, including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal statistics like age and weight, and billing information. The minimum standardized data set of medical information must include the data elements relevant for patient regulating.

3.1.10.7 Trauma Registry Services

The Trauma Registry Services provide the means for recording, management and retrieval of information about patients who have received treatment for trauma injuries for the purpose of deriving lessons learned and improving of patient treatment.

Trauma injuries are sudden injuries caused by blunt force trauma to the body that require immediate medical attention, such as injuries sustained in explosions, car accidents, falls, and sports collisions or gun shots.

Information managed by Trauma Registry Services typically includes:

- The demographics of the patient.
- The specific type of injury of the patient.
- The treatment the patient received.
- The length of hospitalization.
- The outcome of the treatments.

3.1.11 CIMIC Functional Services

The Civil-Military Cooperation (CIMIC) Functional Services provide unique computing and information services for CIMIC support to operations. It supports the set of (military) activities that are undertaken to coordinate and cooperate, in support of the mission, between force 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 perform 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 Functional Services

The Education, Training, Exercises and Evaluation (ETEE) Functional 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 CIS Functional Services

The Communications and Information Systems (CIS) Functional Services delivers a collection of Service Management and Control (SMC), CIS Security and Cyber Defence Services that provides the means to implement and enforce SMC and CIS Security measures and standards.

3.1.13.1 Recognized CIS Picture Services

The Recognized CIS Picture (RCISP) Services provide the means to produce, manage and disseminate the Recognized CIS Picture through the collection, aggregation, correlation and fusion of CIS information from multiple sources. It supports the delivery of a joint CIS information product, compiled by the Mission Network Service Management Authority (i.e. CJ6) in coordination with all involved Service Providers participating in a Mission Network.

3.1.13.2 Cyber Defence Services

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

3.1.13.3 ITSM Services

The Information Technology Service Management (ITSM) Services provide a standardized interface to manage design, plan, deliver, operate and control information technology (IT) services offered to customers. It aggregates a functions of User Management, Incident Management, Service Management, Service Catalog Management, Ordering, Inventory, Customer Management, and Problem Management.

3.1.13.4 Change Management Services

The Change Management Services provide the means for the response to changing business requirements while maximizing value and reducing incidents, disruption and network. It supports IT Service Management to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure and Network, in order to minimize the number and impact of any related incidents upon service. Change Management Services delivers the standard integration capabilities between external applications and the Change Management Application.

3.1.13.5 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.

3.1.13.6 Advanced Threat Management Services

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

3.1.13.7 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.

3.1.13.8 Security Information and Event Management Services

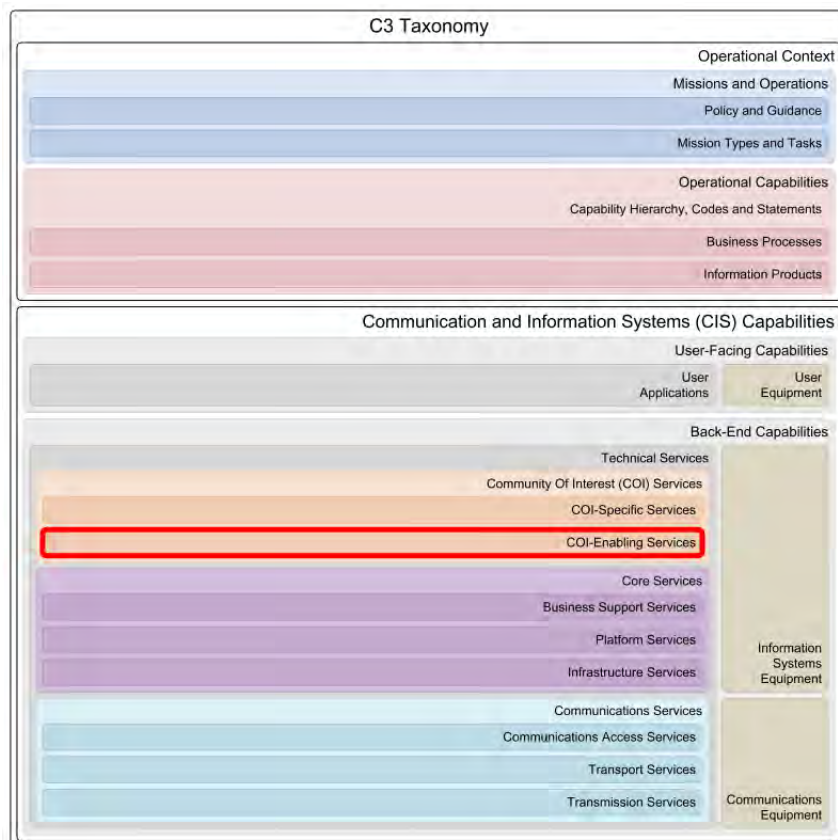
The Security Information and Event Management (SIEM) Services combines support of security information management and security event management to provide real-time analysis of security alerts generated by service assets (e.g. user applications, IT Services and communications equipment), to identify security threats, detect and prevent breaches, and provide forensic analysis. SIEM Services also support logging and analysis of security data and generation of reports for compliance purposes.

The likely sources of logs that SIEM Services ingest include:

- Intrusion detection systems/intrusion prevention systems (IDS/IPS)
- Data Loss Prevention (DLP) systems
- Anti-virus and other endpoint security software
- Firewalls
- Unified Threat Management (UTM) systems
- VPN concentrators
- Web filters
- Honeypot or deception systems
- Routers and switches
- Domain controllers
- Wireless access points
- Application servers, intranet application and databases

The SIEM Service also provide functionality to periodically and systematically review the application of CIS security during operations by collecting information related to policy compliance and risk management in order to gather evidence of undesirable behaviors and effects. With this the services support the presentation of findings to the appropriate authorities for the purpose of accountability.

3.2 COI-Enabling Services



The Community of Interest (COI)-Enabling Services provide COI-dependant functionality required by more than one community of interest. They are similar to Business Support Services in that they provide building blocks for domain-specific service development. The distinction between the two is that Business 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 Business Support Services tend to be more generic and can be used by any business or enterprise.

3.2.1 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.

3.2.1.1 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.

3.2.1.2 Overlay Services

The Overlay services provide the means to collect battlespace information from multiple sources for the purpose of geographic visualization, including annotation of maps and images. Geographic visualization includes not only the presentation of graphical data on the globe/map, but also allow drilling down from rendered battlespace information to more detailed content not available in the overlay data itself. To share overlays dynamically, they must be published as services.

The Overlay Services provide the exchange protocols and business rules required for effective information exchange of battlespace information so that it can be unambiguously rendered by command and control (C2) and Situational Awareness

(SA) applications, and understood by humans.

3.2.1.3 Symbology Services

The Symbology Services provide the means to render standard military or mission specific symbology sets and to disseminate the rendered images as overlays on maps or as standalone illustrations.

3.2.2 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.

3.2.2.1 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.

3.2.2.2 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.

3.2.2.3 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.

3.2.2.4 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.

3.2.2.5 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).

3.2.2.6 Targeting Services

The Targeting Services provide the means to select and prioritize targets, while matching the appropriate target response. It supports information about entities and objects considered for possible engagement or action. This may be an area, structure, object, person or group of people against which lethal or non-lethal capability can be employed to create specific psychological or physical effects to support the Commander's objectives, guidance, and intent.

3.2.3 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.

3.2.3.1 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.

3.2.3.2 Resource Request Services

The Resource Request Services enable the development, dissemination 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.

3.2.3.3 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.

3.2.3.4 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.

3.2.3.5 Operations Order Services

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

3.2.3.6 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 Operations Information Services

The Operations Information Services provides the means to discover, identify, access and disseminate operationally relevant information and data. This information includes, but is not limited to, Battlespace Objects, Battlespace Events and Tracks.

3.2.4.1 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 maintain 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).

3.2.4.2 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.

3.2.4.3 Track Management Services

The Track Management Services provide the means to collect and monitor the position, course, speed and general characteristics of relevant entities in near-real time to enhance Situational Awareness (SA) and Command and Control (C2). The services allow for the combination identification, correlation, processing and dissemination of all tracks. It supports the management of tracks received from available sensors or other sources while allowing for consumer-driven filters to be applied when required.

3.2.4.4 Track Distribution Services

The Track Distribution Services provide functionality for machine-to-machine dissemination of track data. Track Distribution Services aims to enable scalable, near-real-time, dependable, high-performance and interoperable data exchanges. A *track* is the representation of a moving object in terms of its position, course, speed and general characteristics. Track information generally comes from external sources or sensors.

3.2.4.5 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.

3.2.5 Modeling and Simulation Services

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

Each simulation requires well-defined models, information resources, rules, behaviours and constraints, which are authoritative and managed. One or more simulations are executed and controlled to achieve the outputs required by follow on simulations, processes and/or decision makers. The simulation environment allows for the modeling of multiple entities, their behaviours and interactions to determine the likely results.

3.2.5.1 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.

3.2.5.2 Model Repository Services

The Model Repository Services provides the means to store, retrieve and manage models used for simulation purposes. The Model Repository Services supports all models required for simulation, independent of type and purpose. Each model has well-defined parameters, including: inputs, outputs, rules, behaviours and constraints. Each model has associated metadata detailing its provenance, problem domain, and information and parameter requirements. Through Model Repository Services, authoritative models can be discovered, including their metadata, and retrieved for execution.

3.2.5.3 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.

3.2.5.4 Information Registry Services

The Information Registry Services provides the means to store, manage and retrieve references to authoritative information required for execution of simulation models. The Information Registry Services facilitates the retrieval of metadata associated with the authoritative information reference, including the provenance, semantics, structure and the means to retrieve the information. The Information Registry Services allows the outputs of a simulation model to be registered and utilized as the inputs for future simulations. The authoritative information may not come from a single source, but instead be the result of aggregation, correlation, mediation and/or orchestration.

3.2.5.5 Simulation Control Services

The Simulation Control Services provide the means to apply a set of parameters and information to a given model and calculate the output. The input information can be either static or dynamic, with the dynamic information being the result of other processes, systems or simulations. The Simulation Control Service provides control over the execution of the model as required by the consumer. The outputs of the model execution are provided to the consumer.

3.2.5.6 Simulation Composition Services

The Simulation Composition Services provide the means to define and execute complex simulations composed of an orchestration of multiple simulations working cooperatively to provide a required output. The orchestration of simulations can include both concurrent and sequential execution of simulations. The outputs of one simulation may provide the input to another for both concurrent and sequentially running simulations. The results, whether discrete or continuous, are provided to the consumer as required.

3.2.5.7 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.

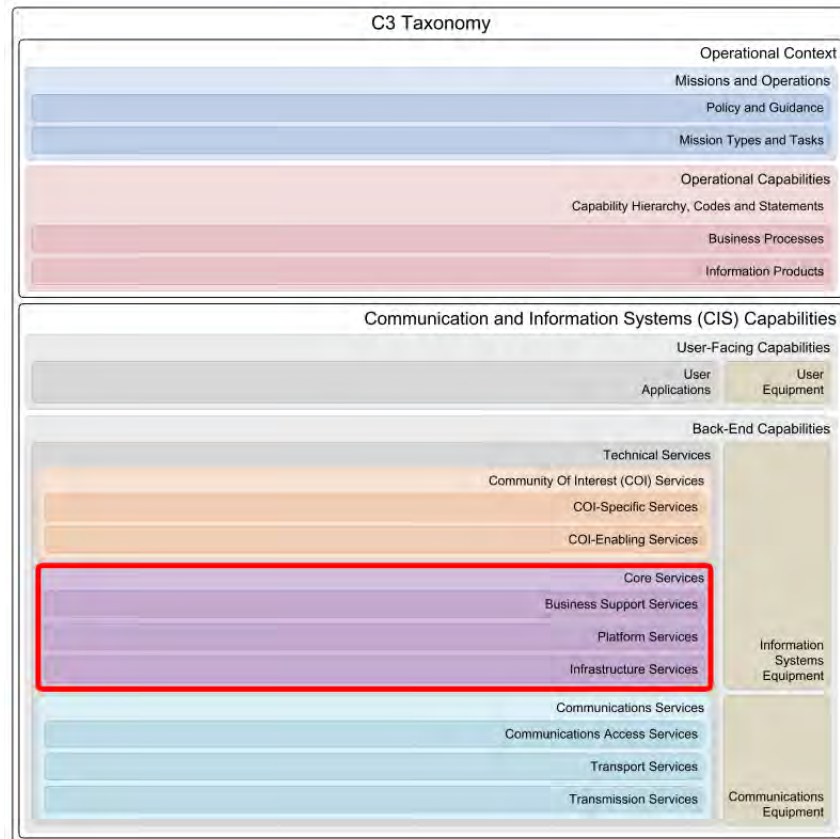
3.2.5.8 Ground Truth Battlespace Objects Services

The Ground Truth Battlespace Objects Services provide the means to discover, exchange, access and modify Ground Truth Battlespace Objects (BSOs) which are generated as input to simulations. The services enable the stimulated development of perceived truth BSOs by Battlespace Object Services.

3.2.5.9 Ground Truth Battlespace Events Services

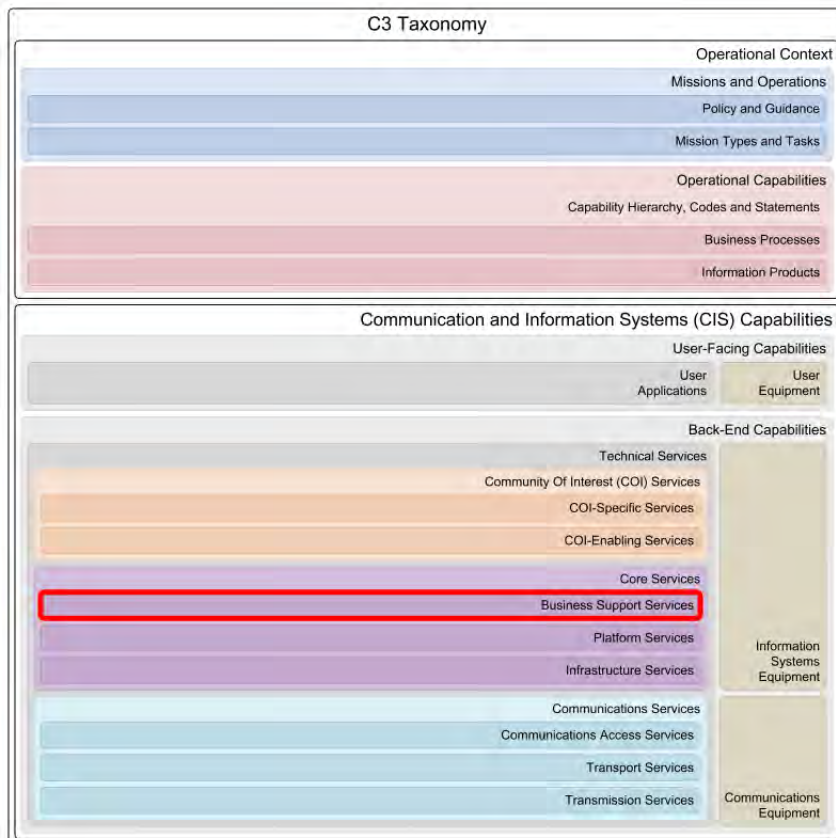
The Ground Truth Battlespace Events Services provide the means to discover, exchange, access and modify Ground Truth Battlespace Events and Incidents which are generated as input to simulations. The services enable the stimulated development of perceived truth events by Battlespace Events Services.

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 measures at the enterprise support level.

4.1.1.1 Business Support Guard Services

The Business Support Guard Services connect networks of different information security and management policies 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.

4.1.2.3 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.

4.1.2.4 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.

4.1.3 Communication and Collaboration Services

The 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 fulfill alliance's and coalition's operational requirements. These services enable real-time situational updates to time-critical planning activities between coalition partners, communities of interest, and (NATO and National) agencies. Levels of collaboration include awareness, shared information, coordination and joint product development.

4.1.3.1 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.

4.1.3.2 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.

4.1.3.3 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.

4.1.3.4 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.

4.1.3.5 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 (translating and transcoding), and features such as Continuous Presence, in which multiple parties can be seen onscreen at once.

4.1.3.6 Text-based Communication Services

The Text-based Communication Services provide the ability to exchange relatively brief text messages, in near real-time, between network addressable entities. Text-based Communication 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.

4.1.3.7 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.

4.1.3.8 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.

4.1.3.9 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 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.

4.1.4.1 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.

4.1.4.2 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.

4.1.4.3 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).

4.1.4.4 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 Applications and tools typically model and enforce best practices that facilitate reliable and consistent project planning, launch and delivery across the enterprise or federation.

4.1.5 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.

4.1.5.1 Geospatial Catalog Services

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

4.1.5.2 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.

4.1.5.3 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.

4.1.5.4 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.

4.1.5.5 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.

4.1.5.6 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.

4.1.5.7 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.

4.1.5.8 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.

4.1.6 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.

4.1.6.1 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.

4.1.6.2 Formal Messaging Services

The Formal Messaging Services - also known as Military Messaging Services - provide the means for a reliable, store and forward message transfer for both users and applications in support of organizational messaging (messaging between organizations and organizational units). It 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. It also supports different qualities of service for different message priorities to honour the precedence of the military messages.

4.1.6.3 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.

4.1.6.4 Unit Conversion Services

The Unit Conversion Services perform conversion of a given value in a selected unit to another selected unit. The areas include Distance (Nautical Mile, Statute Mile, Data Mile, Yard, Feet, Metre, Kilometre), Wind speed and force (e.g. Beaufort to km/h), Speed (knots, Data Mile per hour, km/h, m/s, mph), Weight/Mass, Length, Area, Volume, Temperature, Density/Pressure.

4.1.6.5 Search Services

The 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.

4.1.6.6 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.

4.1.6.7 Archiving Services

The Archiving Services provide the means to archive an organization's electronic data and to manage archives. In general, archives of any individual or organization consist of records which have been especially selected for permanent or long-term preservation, due to their enduring value. Archival records are normally unpublished and almost always unique, unlike books or magazines, in which many identical copies exist.

4.1.7 Data Science Services

The Data Science Services provide the means to collect, aggregate, manage, curate and control information resources and analytical services required for conducting operations research and other data analysis activities. Whilst each analytical task is unique there are common technical requirements with respect to collection of large volumes of unstructured and structured data, management of data excerpts, normalization, visualization, analytical and statistical processing, big-data analytics, optimization algorithms etc.

The major steps involved in a data analysis are:

- Ingestion: Extract, transform and store data extracts;
- Curation: Validate, store and manage data in multidimensional databases;
- Analysis: Provide data access to operational analysts using application software; and
- Presentation: Present analyzed data in easily understandable forms, such as graphs.

4.1.7.1 Reporting Services

The Reporting Services transforms data from a various sources source such as a database, XML stream or a spreadsheet, and use it to produce a document in a format which satisfies a particular human readership. The information provided by this service shall be Timely, Accurate and Relevant. Report generation targets the final requirement by making sure that the information delivered is presented in the way most readily understood by the target reader.

4.1.7.2 Data Ingest Services

The Data Ingest Services automatically collect unstructured and structured data from various sources.

4.1.7.3 Data Processing Services

The Data Processing Services automatically transform, aggregate unstructured and structured data ingested from various sources, and tag, store and manage those data extracts for further exploitation.

4.1.7.4 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. The Analytics 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.

4.1.7.5 Statistical Analysis Services

The Statistical Analysis Services are part of a wider data analytics toolset. The Statistical Analysis Services support data exploration, with the help of visualization and description techniques, and the analysis of data sets with descriptive and inferential statistical methods.

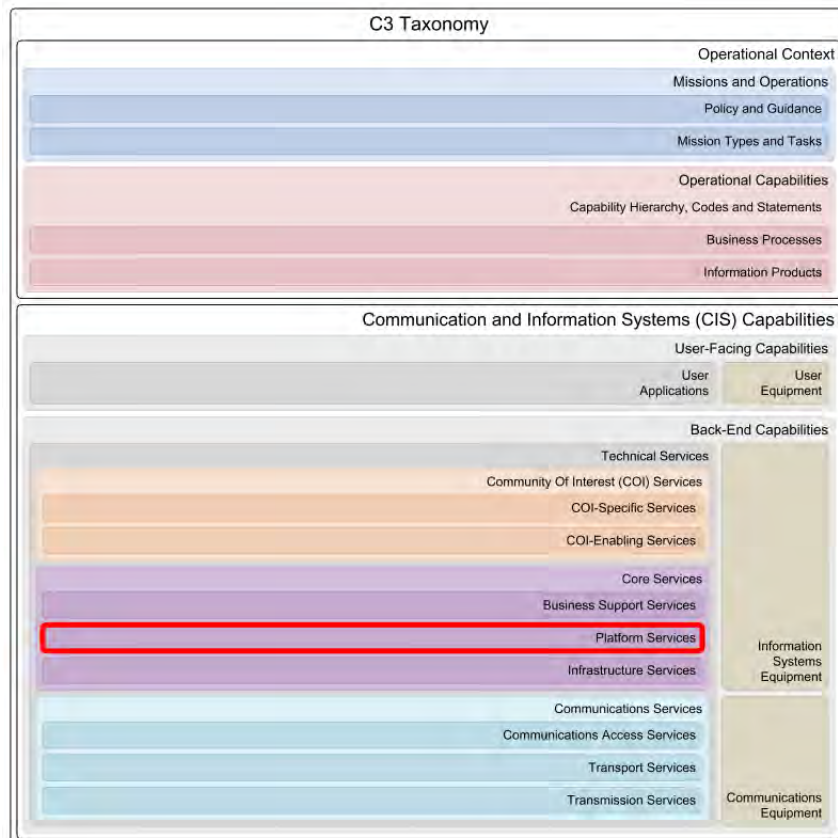
4.1.7.6 Machine Learning Services

The Machine Learning Services simplify and accelerate the building, training, and deployment of machine learning models. Machine learning facilitates the continuous advancement of computing through exposure to new scenarios, testing and adaptation, while employing pattern and trend detection for improved decisions. Machine Learning Services support multiple stat methods that address categorization (binary and multi-class), clustering, anomaly detection, regression,

recommendation, and cognitive analysis such as:

- Vision: Image-processing algorithms to smartly identify, caption, index, and moderate pictures and videos.
- Knowledge: Mapping complex information and data in order to conduct semantic searches.
- Language: Processing natural language and evaluating sentiment.
- Speech: Converting spoken audio into text. Recognizing voices of individual speakers.

4.2 Platform Services



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

4.2.1 Platform CIS Security Services

The 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 measures at the platform level.

4.2.1.1 Platform Guard Services

The Platform Guard Services provide the means to connect networks of different information security and management policies and usage areas to control traffic flow in-between the networks following a set of predefined rules for platform services. The intended function is to allow automated data exchange between two network enclaves that belong to different information domains. The services enable a cross-domain information exchange by mediating traffic flows, while offering sufficient protection against the unintended leakage of confidential information and possible degradation of integrity of resources by enforcing an appropriate access control policy.

4.2.1.2 Security Token Services

The Security Token Services (STS) provide the means to identify providers responsible for issuing security tokens, which may or may not be structured as XML. These 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 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" information security and management policies.

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.

4.2.1.6 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.

4.2.2 Platform SMC Services

The Platform Service Management and Control (SMC) Services provide a suite of capabilities needed to ensure that platform 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 platform level.

4.2.2.1 SMC Policy Enforcement Services

The 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. SMC Policy Enforcement Services act as effectors that enforce policies at run-time.

SMC Policy Enforcement Services enforce policies on services hosted within the Platform. Depending on implementation, the 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 Platform Logging Services

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

4.2.2.4 Platform Monitoring Services

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

The Platform Metering Services measures levels of 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 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. A number of security features may be activated, such as content checking, authentication and authorisation, auditing and anonymity (as the identity of the client machine can be hidden).

The 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.

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 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).

4.2.5 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 pull together related information from multiple (often heterogeneous) sources and present it as a single information set. This allows the easy integration of the aggregated information into other contexts, such as business processes, mash-ups, gadgets and business intelligence applications.

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 Database Services

The Database Services provide access to shared, structured virtual storage components for data and information persistence as part of the platform environment.

4.2.6.1 Directory 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.

4.2.6.2 Non-relational Database Services

The Non-relational Database 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).

4.2.6.3 Relational Database Services

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

4.2.7 Composition Services

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

4.2.7.1 Orchestration Services

The Orchestration Services provide the means to coordinate 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 aggregation 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.

4.2.7.2 Choreography Services

The Choreography Services provide the means to model the compositions of multiple technical services into so called choreographies and to specify the 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.

4.2.7.3 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.

4.2.8 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.

4.2.8.1 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.

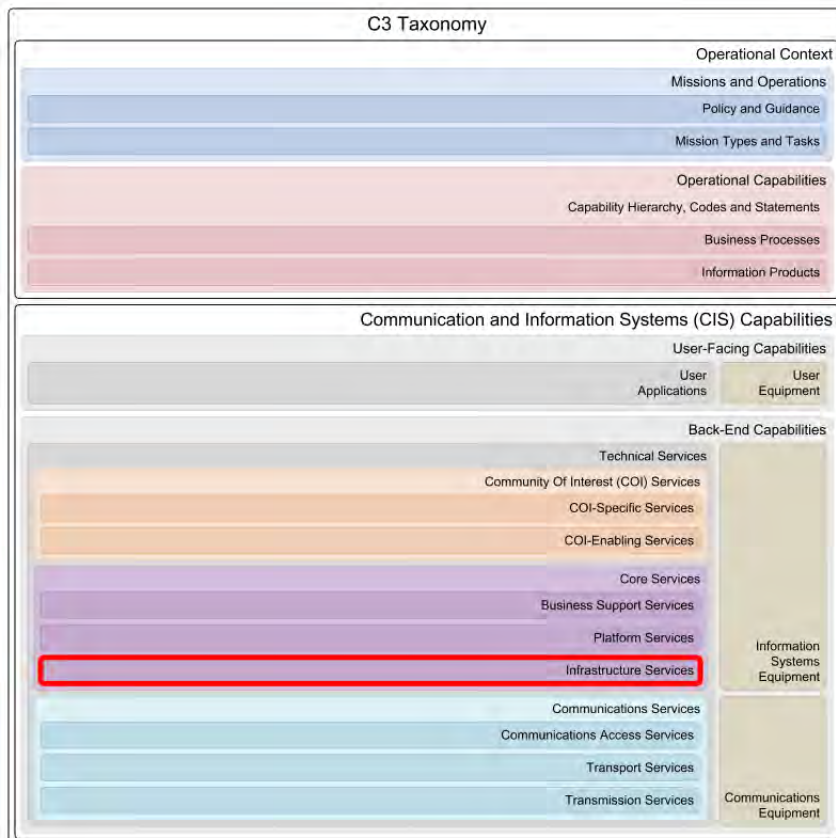
4.2.8.2 Data Format Transformation Services

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 measures 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 information 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 information security and management policies 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 provide the means to gather information on malicious activity and/or relevant policy violations. They focus on the identification of possible incidents and intrusive events, on the registration and logging of corresponding activities and system behavior, and the generation of reports. The main objective is to identify problems with information security and management policies, document existing threats, and deter individuals from violations.

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 information domains 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 cryptographic 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, 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.

4.3.2.5 Time Zone Data Distribution Services

Time Zone Data Distribution Services allow reliable, secure, and fast delivery of time zone data and leap-second rules to client systems such as calendaring and scheduling applications or operating systems. Time Zone Data Distribution Services provide data for the set of time zones known to servers and expected to be used by clients. This is a key service to ensure server-to-server and client-to-server content interoperability. If such a service is not available, all participants would need to agree up front to configure their systems with a common timezone reference datasource, e.g.

<https://www.iana.org/time-zones>.

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.

4.3.3.3 Distributed Processing Services

The Distributed Processing Services supports task dispatching, scheduling and execution across a cluster of nodes.

4.3.4 Infrastructure Storage Services

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

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 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.

4.3.4.3 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.

4.3.5 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 Caching Services

The 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. 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. Caching Services are often used by Proxy Services, and are indeed often colocated with them. However, they are separate, and an entire caching infrastructure can be built independent of proxy services.

4.3.5.2 Proxying Services

The 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 Proxying Services:

- Forward Proxy - in this case, the user's client (which may be an Internet Browser or 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.

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).

4.3.5.3 Virtualized Networking Services

The Virtualized Networking Services Network virtualization allow IT managers to consolidate multiple physical networks, divide a network into multiple segments or create software-only networks between virtual machines (VMs). The goal of network virtualization is to improve the agility to direct appropriate network resources to VMs in data center environments and the ability to consolidate or segment networks. Virtual networks can be created in two ways -- inside or outside the server. External software uses switches, adapters and the network to aggregate physical local area networks (LANs) into a single logical LAN, or to break a physical LAN into multiple virtual LANs (VLANs). Internal software allows virtual machines (VMs) to exchange data on a host without an external network.

4.3.5.4 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.

4.3.5.5 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.

4.3.5.6 Printing and Scanning Services

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

4.3.5.7 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

4.3.5.8 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.

4.3.5.9 Location Awareness Services

The Location Awareness Services provide access to geographic and/or network location data of a device that have been acquired through multiple sources including network carriers, Wi-Fi, IP addresses and landlines. Location data provided through Location Awareness Services can be used to realize greater operational efficiencies, optimize information management and increase security. Location awareness services are typically actively supported by devices using positioning systems, without the active participation of the device "non-cooperative locating" or detection mechanisms can be used.

Location Services in the context of networking relates to locating network nodes. These include:

- ITU switched line access addressing according to International Telecommunications Union Q-Series standards, Telecommunications Signaling System#7 (SS7) and mirroring ANSI Standards T1.110—General Information and subsequent standards.
- IEEE media access addressing according to MAC International standard ISO/IEC 10038 with ISO/IEC 11802 and ANSI/IEEE edition.
- ISO procedure call addressing according to URN/UUID International standards ISO/IEC 11578 and ISO/IEC 9834 and IETF RFC 4122.

Location Services in the context of geography relates to coordinates and altitude/elevation that are either relative to either a standardized system of coordinates, e.g. WGS84, or a fixed object such as a building plan.

- Global navigation satellite systems (GNSS) such as the United States' GPS or the European Union's Galileo use satellites to provide autonomous geo-spatial positioning. It allows small electronic receivers to determine their location (longitude, latitude, and altitude/elevation).
- Indoor positioning systems (IPS) are systems that can locate devices inside a building using lights, radio waves, magnetic fields, acoustic signals, or other sensory information. There are several commercial systems on the market, but there are

no agreed standard for IPS systems. Indoor positioning systems use different technologies, including distance measurement to nearby anchor nodes (nodes with known fixed positions, e.g. WiFi / LiFi access points or Bluetooth beacons), magnetic positioning, dead reckoning.

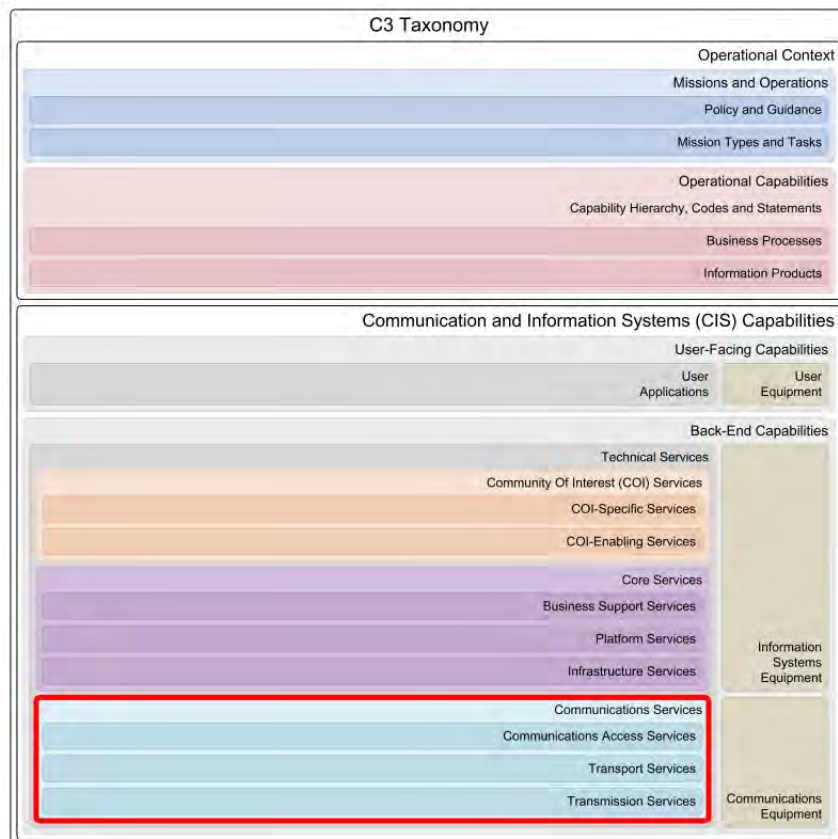
4.3.5.10 Distributed Time Services

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

4.3.5.11 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.

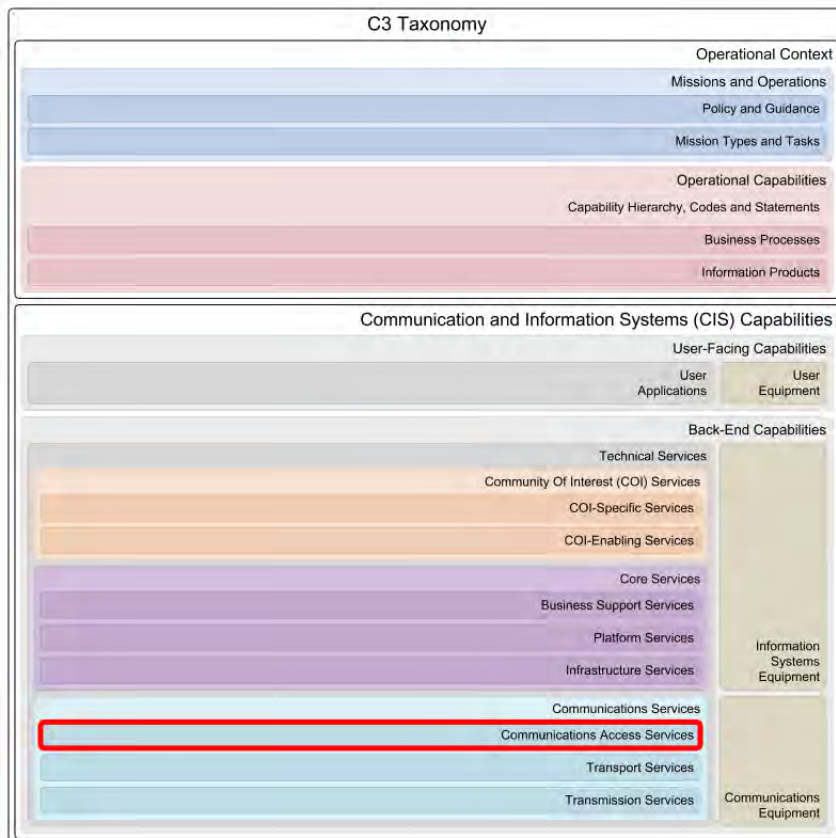
The required granularity is achieved by defining elementary service blocks. These are building blocks in complex end-to-end services, as those formulated in the NSOVs of the relevant reference architectures and derived target architectures. Elementary service blocks are agnostic to the resources and 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 providers/providers (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 measures 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 services 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 Native 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.

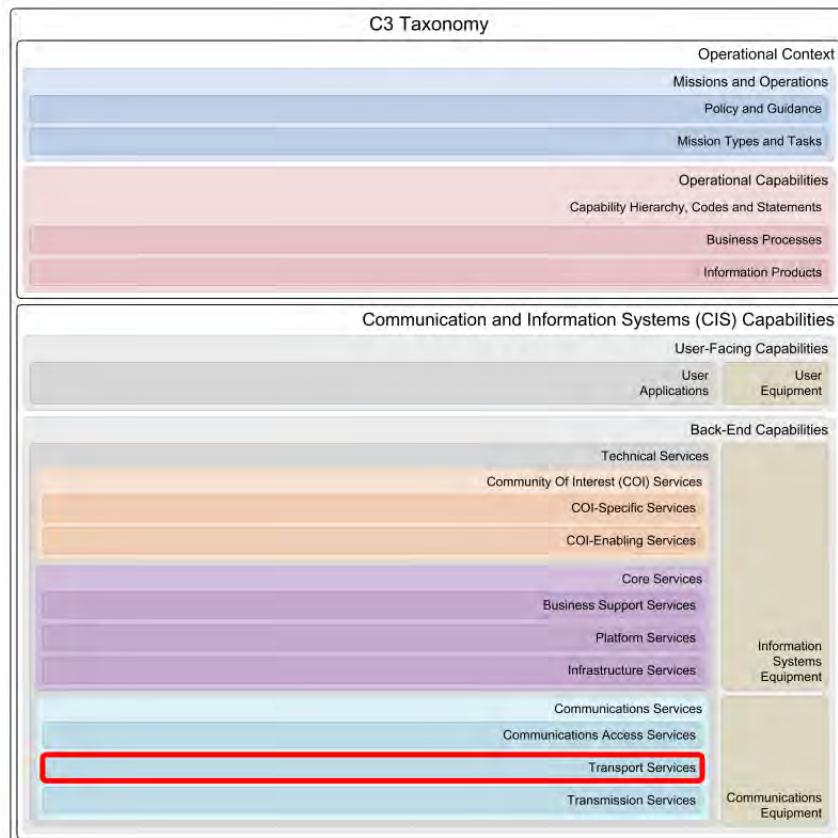
5.1.9.2 Video Access Services

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-to-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 measures 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 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 Switching 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.

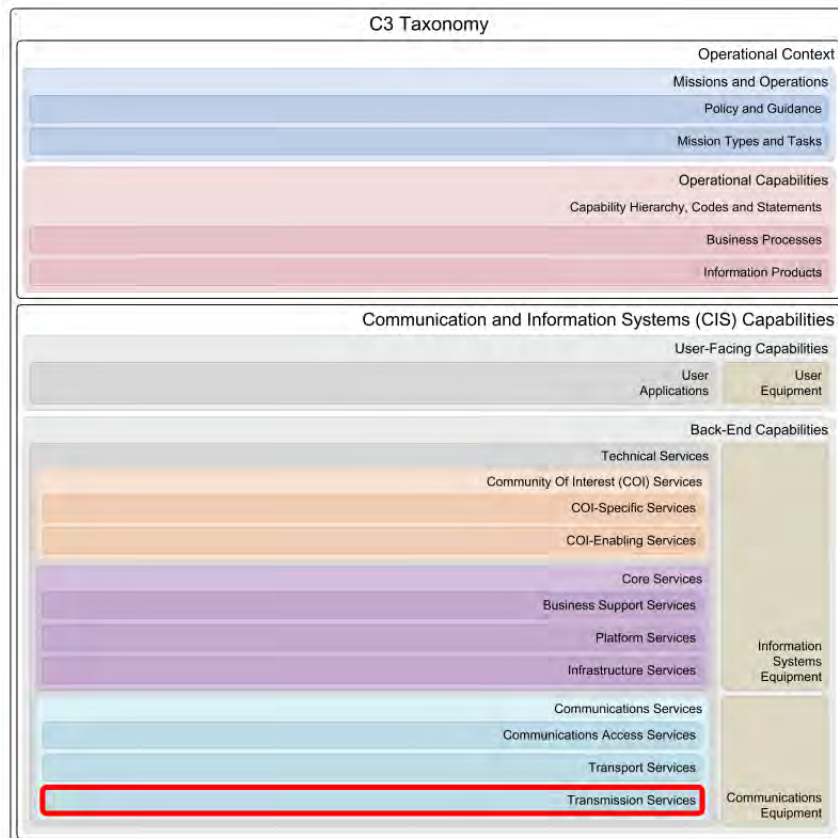
5.2.6.2 Frame-based Broadcast Services

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 measures 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 achieve 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 Services

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.



NATO UNCLASSIFIED
Releasable to North Macedonia

10 September 2019

DOCUMENT
AC/322-D(2019)0038 (INV)

CONSULTATION, COMMAND AND CONTROL BOARD (C3B)

**CIS Security Technical and Implementation Directive
for the Security of Web Applications**

Note by the Secretary

References:

A. AC/322-D(2019)0038 (INV) CIS Security Technical and Implementation Directive for the Security of Web Applications, 9 September 2019.

1. On 9 September 2019, C3B approved under silence, the Draft CIS Security Technical and Implementation Directive for the Security of Web Applications (Reference A).
2. A clean version of this document is now issued at Annex 1 for future reference.

(Signed) S. NDAGIJIMANA-MUNEZERO

Annex 1: CIS Security Technical and Implementation Directive for the Security of Web Applications

1 Annex

Action Officer: Mrs. J. Arthur, Ext. 5385
Original: English



**CIS SECURITY TECHNICAL AND IMPLEMENTATION
DIRECTIVE FOR THE SECURITY OF WEB
APPLICATIONS**

Table of Contents

INTRODUCTION	4
SCOPE	4
WEB APPLICATION SECURITY PROCESS	5
Determine the Security Requirements	5
Design and Implement Security Requirements	7
Security Testing, Validation and Accreditation	7
Operate while Maintaining Web Application Security	7
MINIMUM SECURITY REQUIREMENTS FOR WEB APPLICATIONS	7
PROCEDURAL SECURITY REQUIREMENTS	8
Web Application Planning	8
Web Application Operation	8
TECHNICAL SECURITY REQUIREMENTS	9
Authentication	9
Session Management	11
Access Control	12
Input Validation	12
Cryptography	14
Error Handling and Logging	14
Data Protection	15
Communications Security	16
HTTP Security	16
Business Logic	17
Files and Resources	17
Web Services	18
Configuration	18
Miscellaneous	19
TESTING AND TASKS	19

REFERENCES:

- A. AC/322-D/0048-REV2, INFOSEC Technical & Implementation Directive for Computer and Local Area Network (LAN) Security, 14 Nov 2011
- B. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997
- C. C-M(2007)0118, The NATO Information Management Policy, 11 Dec 2007
- D. C-M(2002)60, The Management of Non-Classified Information, 11 Jul 2002
- E. C-M(2002)49-COR1-12, Security within the North Atlantic Treaty Organisation, 14 Sep 2015
- F. CD PO(2014)0358, Enhanced NATO Policy on Cyber Defence, 27 May 2014
- G. AC/35-D/2004-REV3 Primary Directive on CIS Security, 15 Nov 2015
- H. AC/35-D/2005-REV3 Management Directive on CIS Security, 12 Oct 2015
- I. AC/35-D/1019, Guidelines for the Security Evaluation and Certification of CIS, 12 Dec 2008
- J. AC/35-D/1021-REV3, Guidelines for the Security Accreditation of CIS, 31 Jan 2012
- K. AC/35-N(2012)0022 (CISS) Rules of Engagement for Security Audits of NATO CIS, 20 Oct 2015
- L. AC/322-D(2017)0044-REV1, CIS Security Technical and Implementation Directive on the Procurement and Use of Commercial PKI Certificates for Internet Facing NATO Websites, 18 Jan 2018
- M. AC/35-D/1050, AC/322-D(2019)0001, Supporting Document for the Protection of NATO Information within Public Cloud-Based CIS, 3 January 2019
- N. AC/322-D/0047-REV2, INFOSEC Technical and Implementation Directive for Cryptographic Security and Cryptographic Mechanisms, 11 Mar 2019.

INTRODUCTION

1. This C3 Board CIS Security Directive complements Reference A, Computer and LAN Security Directive, by providing a comprehensive set of security measures for the protection of NATO's web applications¹. The included set of security measures will be selected for each web application based upon the assessment process described within the Web Application Security Process section of this Directive. The Directive provides a methodology to determine the security level of a web application and mandates security measures applicable for each security level.
2. This Directive uses key words from RFC 2119, Reference B.
 - A "SHALL" statement is an absolute requirement.
 - A "SHALL NOT" statement is an absolute prohibition.
 - A "SHOULD" statement is advisory and there may exist valid reasons in particular circumstances to ignore a particular security measure, but the full implications must be understood and carefully weighed before choosing a different course.
 - Likewise, a "SHOULD NOT" statement is advisory and there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications must be understood and carefully weighed before implementing any behaviour described with this label.
 - "MAY" or the adjective "OPTIONAL" means that an item is optional².
3. This Directive is published in support of security requirements detailed in the NATO Information Management Policy (Reference C), Management of Non-Classified Information (Reference D), Security within the North Atlantic Treaty Organisation (Reference E), the NATO Policy on Cyber Defence (Reference F), and the Primary Directive on CIS Security (Reference G) as well as the Management Directive on CIS Security (Reference H).

SCOPE

4. This Directive shall be used by CIS Planning and Implementation Authorities (CISPIA) and CIS Providers (CISP) in developing and operating secure web applications handling NATO information. This Directive shall also be utilized by NATO Security Accreditation Authorities (SAAs), CIS Operational Authorities (CISOAs), and security management staffs in ensuring the security of web applications.

¹ The term web application refers to any resource that is offered by a web server. This includes web applications which use a browser as a client; web service applications that expose resources for consumption; as well as, websites serving content from particular domains. Web applications, web service applications and web sites will inclusively be referred to as web applications throughout this document when the topic is generalizable; when specificity is required, they will be referred to accordingly.

² Optional is defined as available to be chosen but not obligatory.

5. This Directive shall be applicable to web applications hosted on NATO CIS or when it has been outsourced to a third party to be hosted on their infrastructure. This Directive and the security measures it describes are focused on the web application itself and not the underlying infrastructural platform. The security of the underlying infrastructure is addressed in References A and G. The applicability of each security measure shall be further assessed by the CISOA in coordination with the SAA for certain commercial off the shelf (COTS) and cloud solutions (e.g., Software as a Service (SaaS)).

WEB APPLICATION SECURITY PROCESS

6. The Web application security process to be followed for the entire lifecycle of NATO web applications is detailed below.

Determine the Security Requirements

7. The CISP, in coordination with the CISOA and subject to approval by the SAA, shall conduct an assessment to determine the web application security level requirements for each web application and any additional security measures. The security level shall be determined based on an assessment of the level of threat the web application will face and the level of impact suffered if the web application is compromised.

8. This Directive defines three security levels: Standard, Enhanced and High. Each security level has a minimum set of associated security measures. Each level increases the provided security, but with additional cost and effort.

- Standard is applicable for all web applications.
- Enhanced is applicable for web applications that require additional security measures as indicated by a significant threat and/or impact level, as described in Table 3 below.
- High is for the most critical web applications. High implies that the web application requires the most amount of security measures to ensure its protection.

9. The threat level is determined by a joint consideration of where the web application resides within the CIS and the requirements for accessibility to the web application, as identified in Table 1 below. The CISP shall use the table to determine the threat level, but the CISP, in coordination with the CISOA and subject to approval by the SAA may adjust the level based on the specific circumstance of the web application. The CISP shall also take into consideration the insider threat, both to their CIS and to the CIS which they are interconnected.

Table 1 – Threat Level

Threat Level	Description
High	The web application is required to be accessible from the Internet, and is therefore highly exposed to being attacked by adversaries.
Medium	The web application is located in an environment where attacks have less likelihood of occurrence. Such web applications may be on CIS connected to the Internet, but are designed for internal use, thus blocked from internet access by boundary protection services. Or such web applications are on isolated networks (e.g. by cryptography), but the web

Threat Level	Description
	applications are required to be accessible by users on interconnected CIS (e.g. BICES, or a FMN instance).
Low	The web application is located in an environment where attacks are unlikely to occur, for example an isolated network which is not interconnected to other CIS.

10. The impact level is determined by the consequences if the web application is breached, as identified in Table 2 below. The CISP shall use the table to determine the impact level, but the CISP may adjust the level based on the specific circumstance of the web application. The impact shall take into consideration the loss of confidentiality, integrity, or availability of the data handled by the web application as well as the reputational risk NATO would suffer if a web application were compromised.

Table 2 – Impact Level

Impact Level	Description
High	<p>The compromise of the web application will cause damage to NATO including, but not limited to:</p> <ul style="list-style-type: none"> • Result in the unauthorised disclosure of NATO classified information with severely damaging results; • Allow unauthorized access to industrial control systems with the potential to cause serious damage; • Cause severe damage to NATO's reputation, for example, exposing the effect of a compromise to a world-wide audience (e.g. by defacing www.nato.int).
Medium	<p>The compromise of the web application will cause damage to NATO including, but not limited to:</p> <ul style="list-style-type: none"> • Result in the unauthorised disclosure of NATO classified information which would cause damage to NATO; • Allow unauthorized access to industrial control systems with the potential to cause damage; • Cause damage to NATO's reputation, for example, exposing a considerable amount of NU information with administrative markings (e.g. personal, medical, commercial) to the public.
Low	<p>The compromise of the web application will cause damage to NATO including, but not limited to:</p> <ul style="list-style-type: none"> • Result in the unauthorised disclosure of NATO classified information which would be detrimental to the interests or effectiveness of NATO; • Allow unauthorized access to industrial control systems with the potential to cause minimal damage or nuisance; • Cause detrimental damage to NATO's reputation by, for example, exposing to the public a limited amount of NU information with administrative markings (e.g. personal, medical, commercial).

11. Table 3 defines how the security level is determined based on the threat level and the impact level.

Table 3 - Security Level Relationship to Threat and Impact Level

		Threat Level		
		<i>High</i>	<i>Medium</i>	<i>Low</i>
Impact Level	<i>High</i>	High	Enhanced	Enhanced
	<i>Medium</i>	Enhanced	Enhanced	Standard
	<i>Low</i>	Enhanced	Standard	Standard

Design and Implement Security Requirements

12. The identified set of security requirements shall be accounted for in the design, implementation, and future enhancements of the web application solution, given the specific technology chosen.

Security Testing, Validation and Accreditation

13. Security testing, validation and accreditation shall be conducted in accordance with References G and H, and shall consider the guidance of References I, J, and K.

Operate while Maintaining Web Application Security

14. The CISP shall operate the web application and supporting infrastructure as per References A, G, and H to ensure security is upheld.

MINIMUM SECURITY REQUIREMENTS FOR WEB APPLICATIONS

15. This section describes a list of detailed, minimum security requirements for each security level (*Standard, Enhanced, and High*) for web applications handling NATO information. The list is based on international standards, and takes into consideration current NATO policies. The security requirements are sorted in two areas:

- Procedural security requirements:
 - Web application planning
 - Web application operation
- Technical Security Requirements:
 - Authentication
 - Session Management
 - Access Control
 - Input Validation
 - Cryptography

- Error Handling and Logging
- Data Protection
- Communication Security
- HTTP Security
- Business Logic
- Files and resources
- Web Services
- Miscellaneous requirements

PROCEDURAL SECURITY REQUIREMENTS

16. The security measures identified within the following tables are applicable to all web applications according to the determined security level, including those hosted within cloud environments. In the particular case of public cloud environments, the applicability of these security measures will require some additional considerations based on a shared responsibility model, as described in the Supporting Document for the Protection of NATO Information within Public Cloud-Based CIS (Reference M).

Web Application Planning

ID	Requirement	Standard	Enhanced	High
WP1	The required security level for the protection of the web application shall be identified based on an assessment. (Refer to Web Application Security Process section above.)	X	X	X
WP2	The results of the assessment and the required security level shall be approved by the SAA.	X	X	X
WP3	Requirements for security baselines, configuration management and change control shall be identified.	X	X	X
WP4	Requirements for business continuity shall be identified.	X	X	X
WP5	Requirement for security logs retention shall be identified.	X	X	X

Web Application Operation

ID	Requirement	Standard	Enhanced	High
WO1	A CIS Operational Authority shall be identified.	X	X	X
WO2	The Senior User responsible for the web application content shall be identified.	X	X	X
WO3	Security patches shall be applied to web application components in order to mitigate vulnerabilities, in accordance with the timelines to be determined in coordination with the SAA.	X	X	X
WO4	Relevant security recommendations issued by the appropriate NATO entities regarding security patches, system upgrades, and configuration changes shall be taken into account and applied to the highest extent possible.	X	X	X

ID	Requirement	Standard	Enhanced	High
WO5	A Type 3 Security Audit ³ (Vulnerability Assessment) shall be performed prior to initial fielding (going live), if the web application has undergone major changes ⁴ , or within the following timeframes:	biennial ⁵	annual	annual
WO6	A Type 4 Security Audit (Penetration Test) shall be performed prior to initial fielding (going live), if the web application has undergone major changes ⁶ , or within the following timeframes:	biennial	biennial	annual
WO7	A code review shall be performed together with a Type 4 Security Audit, unless evidence is provided to the SAA ensuring that a Secure Software Development Life Cycle (S-SDLC) process is followed (e.g. by compliance certifications such as SOC II, FedRamp, PCI-DSS, or similar, which also audits S-SDLC aspects of an application).	X	X	X
WO8	Web application operation statistics and report on usage and operability issues shall be stored (and maintained as mandated by NATO data retention policies).		X	X
WO9	The web applications shall be subject to continuous security monitoring (e.g. to detect defacements, DDoS attacks, etc.), as determined in coordination with the SAA.		X	X
WO10	Internet-facing websites shall use https.	X	X	X
WO11	PKI Certificates used by Internet-facing websites for TLS (https) shall comply with the requirements of Reference L.		X	X

TECHNICAL SECURITY REQUIREMENTS

Authentication

ID	Requirement	Standard	Enhanced	High
A1	All pages and resources by default shall require authentication except those specifically intended to be public.	X	X	X
A2	Forms containing credentials shall not be filled in by the web application. Pre-filling by the web application implies that credentials are stored in plaintext or a reversible format, which is explicitly prohibited.	X	X	X
A3	Automatic population of credential fields via 'autofill-like' mechanisms shall be disabled on the client side (i.e. client browser).			X
A4	All authentication controls shall be enforced on the server side.	X	X	X
A5	All authentication controls shall fail securely to ensure attackers cannot log in.	X	X	X

³ AC/35-D/2005-REV3 Management Directive on CIS Security, 12 Oct 2015, Reference H.

⁴ The relevant change management authority will determine whether the change impacts the previous security determination enough to necessitate a Type 3 Security Audit.

⁵ Once every two years

⁶ The relevant change management authority will determine whether the change impacts the previous security determination enough to necessitate a Type 4 Security Audit.

ID	Requirement	Standard	Enhanced	High
A6	Password entry fields shall allow, or encourage, the use of passphrases, and shall not prevent password managers, long passphrases or highly complex passwords being entered.	X	X	X
A7	All account identity authentication functions (such as update profile, forgot password, disabled / lost token, help desk or IVR) that might allow a user to regain access to the account shall be at least as resistant to attack as the primary authentication mechanism.	X	X	X
A8	All authentication decisions shall be logged, without storing sensitive session identifiers or passwords. This shall include login, logout, session expiration, lockout and requests with relevant metadata needed for security investigations, to ensure a user remains accountable.	X	X	X
A9	The changing password functionality shall include the old password, the new password, and a password confirmation.	X	X	X
A10	Account passwords shall be one way hashed with a salt, and there shall be sufficient work factor to deter brute force and password hash recovery attacks.	X	X	X
A11	Credentials shall be transported using a suitable encrypted link and all pages/functions that require a user to enter credentials shall be done so using an encrypted link.	X	X	X
A12	Forgotten password function and other recovery paths shall not reveal the current password and the new password shall not be sent in clear text to the user.	X	X	X
A13	Information enumeration shall not be possible via login, password reset, or forgot account functionality.	X	X	X
A14	No default passwords shall be in use for the application framework or any components used by the application (such as "admin/password").	X	X	X
A15	Measures shall be in place to block the use of commonly chosen passwords and weak passphrases.	X	X	X
A16	Anti-automation shall be in place to prevent breached credential testing, brute forcing, and account lockout attacks.	X	X	X
A17	All service authentication credentials for accessing services or interfaces, internal or external to the application, shall be encrypted and stored in a protected location.		X	X
A18	Account lockout shall be divided into soft and hard lock status, and these are not mutually exclusive. If an account is temporarily soft locked out due to a brute force attack, this shall not reset the hard lock status.		X	X
A19	Risk based re-authentication, two factor or transaction signing shall be in place for high value			X

ID	Requirement	Standard	Enhanced	High
	transactions, to be determined in coordination with the SAA.			
A20	All authentication challenges, whether successful or failed, shall respond in the same average response time.			X
A21	API keys, passwords and other similar secrets shall not be included in the source code, or online source code repositories.	X	X	X
A22	Administrative interfaces shall not be accessible to non-privileged users.	X	X	X
A23	When passwords are assigned by the application for the user's first login, there shall be controls in place to force the user to immediately change their password after first login.	X	X	X

Session Management

ID	Requirement	Standard	Enhanced	High
SM1	No custom session manager shall be used, or the custom session manager shall be resistant against all common session management attacks.	X	X	X
SM2	Sessions shall be invalidated when the user logs out.	X	X	X
SM3	Sessions shall timeout after a specified period of inactivity.	X	X	X
SM4	Sessions shall timeout after an administratively-configurable maximum time period regardless of activity (an absolute timeout).		X	X
SM5	All pages that require authentication shall have easy and visible access to logout functionality.	X	X	X
SM6	Session ids, session information and cookie content shall never be disclosed in URLs, error messages, or logs. The application shall not support URL rewriting of session cookies.	X	X	X
SM7	All successful authentication and re-authentication shall generate a new session and session id.	X	X	X
SM8	Only session ids generated by the application framework, that are not expired, shall be recognized as active by the application.	X	X	X
SM9	Session ids shall be sufficiently long, random and unique across the correct active session base.	X	X	X
SM10	Session ids stored in cookies shall have their path set to an appropriately restrictive value for the application, and authentication session tokens shall additionally set appropriate security flags (e.g. "HttpOnly" and "secure").	X	X	X
SM11	The application shall limit the number of active concurrent sessions.	X	X	X
SM12	An active session list should be displayed in the account profile or similar of each user. The user shall be able to terminate any active session.	X	X	X
SM13	Users should be prompted with the option to terminate all other active sessions after a successful change password process.	X	X	X

Access Control

ID	Requirement	Standard	Enhanced	High
AC1	The principle of least privilege shall exist - users shall only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This includes protection against spoofing and elevation of privilege.	X	X	X
AC2	Access to sensitive records shall be protected, such that only authorized objects or data is accessible to each user (for example, protect against users tampering with a parameter to see or alter another user's account).	X	X	X
AC3	Directory browsing shall be disabled unless deliberately desired by the application developer. Additionally, applications shall not allow discovery or disclosure of file or directory metadata, such as "Thumbs.db", ".DS_Store", ".git" or ".svn" folders.	X	X	X
AC4	Access controls shall fail securely.	X	X	X
AC5	The same access control rules enforced by the presentation layer shall be enforced on the server side.	X	X	X
AC6	All user and data attributes and policy information used by access controls shall not be tamperable by end users		X	X
AC7	All access control decisions shall be logged.		X	X
AC8	The application or framework shall use strong random anti-Cross-Site Request Forgery (CSRF) tokens or shall have another transaction protection mechanism.	X	X	X
AC9	The application shall correctly enforce context-sensitive authorisation, so as to not allow unauthorised manipulation by means of parameter tampering.	X	X	X

Input Validation

ID	Requirement	Standard	Enhanced	High
IV1	The runtime environment shall not be susceptible to buffer overflows, or security controls shall prevent buffer overflows.	X	X	X
IV2	Server side input validation failures shall result in request rejection and shall be logged.	X	X	X
IV3	Input validation routines shall be enforced on the server side.	X	X	X
IV4	All queries, stored procedures, and calling of stored procedures shall be protected by the use of prepared statements or query parameterization, and thus not susceptible to injections (independently of the querying language, e.g. SQL, NOSQL, HQL, OSQL, etc.).	X	X	X
IV5	The application shall not be susceptible to LDAP Injection, or security controls shall prevent LDAP Injection, by not passing untrusted user supplied input directly to parsers and execution methods.	X	X	X

ID	Requirement	Standard	Enhanced	High
IV6	The application shall not be susceptible to OS Command Injection, or security controls shall prevent OS Command Injection, by not passing untrusted user supplied input directly to parsers and execution methods.	X	X	X
IV7	The application shall not be susceptible to Remote File Inclusion (RFI) or Local File Inclusion (LFI), by not passing untrusted user supplied input directly to parsers and execution methods.	X	X	X
IV8	The application shall not be susceptible to common XML attacks, such as XPath query tampering, XML External Entity attacks, and XML injection attacks.	X	X	X
IV9	All string variables placed into HTML or other web client code shall either be properly contextually encoded manually, or shall utilize templates that automatically encode contextually to ensure the application is not susceptible to reflected, stored and DOM Cross-Site Scripting (XSS) attacks.	X	X	X
IV10	If the application framework allows automatic mass parameter assignment (also called automatic variable binding) from the inbound request to a model, security sensitive fields such as "role" or "password" shall be protected from malicious automatic binding.		X	X
IV11	The application shall have defences against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.)		X	X
IV12	All input data shall be validated, not only HTML form fields but all sources of input such as REST calls, query parameters, HTTP headers, cookies, batch files, RSS feeds, etc.; using positive validation (whitelisting), then lesser forms of validation such as greylisting (eliminating known bad strings), or rejecting bad inputs (blacklisting).	X	X	X
IV13	Structured data shall be strongly typed ⁷ and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers or telephone, or validating that two related fields are reasonable, such as validating zip or post codes match).		X	X
IV14	Unstructured data shall be sanitized to enforce generic safety measures such as allowed characters and length, and characters potentially harmful in given context shall be escaped (e.g. natural names with Unicode or apostrophes).		X	X
IV15	Untrusted HTML from What You See is What You Get (WYSIWYG) editors or similar shall be properly sanitized with an HTML sanitizer and shall be appropriately handled according to the input validation task and encoding task.	X	X	X

⁷ In this context, strongly typed means the data containers/variables are explicitly defined in the code so that the type is not ambiguous or decided at compile-time or later.

ID	Requirement	Standard	Enhanced	High
IV16	Data transferred from one DOM context to another shall use safe JavaScript methods, such as ".innerText" and ".val".		X	X
IV17	When parsing JSON in browsers, JSON.parse shall be used to parse JSON on the client. Eval() shall not be used to parse JSON on the client.		X	X
IV18	Authenticated data shall be cleared from client storage, such as the browser DOM, after the session is terminated.		X	X

Cryptography

ID	Requirement	Standard	Enhanced	High
CY1	Refer to AC/322-D/0047 ⁸ for any cryptographic requirements.	X	X	X

Error Handling and Logging

ID	Requirement	Standard	Enhanced	High
EH1	The application shall not output error messages or stack traces containing data that could assist an attacker, including session identifiers, software/framework versions, NATO and/or personal information.	X	X	X
EH2	Error handling logic in security controls shall deny access by default.	X	X	X
EH3	Security logging controls shall provide the ability to log success and particularly failure events that are identified as security-relevant.	X	X	X
EH4	Each log event shall include necessary information that would allow for a detailed investigation of the timeline when an event happens.	X	X	X
EH5	All events that include untrusted data shall not execute as code in the intended log viewing software.	X	X	X
EH6	Security logs are protected from unauthorized access and modification.	X	X	X
EH7	The application shall not log data that could assist an attacker such as user's session identifiers, passwords, hashes, or API tokens.	X	X	X
EH8	The application shall not log NATO information unless logs are protected in line with the highest classification level of the information they contain	X	X	X
EH9	All non-printable symbols and field separators shall be properly encoded in log entries, to prevent log injection.	X	X	X
EH10	Log fields from trusted and untrusted sources shall be distinguishable in log entries.			X
EH11	An audit log shall ensure the non-repudiation of all logged users' activities.	X	X	X

⁸ AC/322-D/0047-REV2, INFOSEC Technical and Implementation Directive for Cryptographic Security and Cryptographic Mechanisms, 11 Mar 2019.

ID	Requirement	Standard	Enhanced	High
EH12	Security logs shall have some form of integrity checking or controls to prevent unauthorized modification.	X	X	X
EH13	Logs shall be stored on a different partition than the one from the application is running, and leverage proper log rotation.			X
EH14	Time sources shall be synchronized to ensure uniformity when it comes to logs entries timestamps.	X	X	X

Data Protection

ID	Requirement	Standard	Enhanced	High
DP1	All forms containing sensitive data ⁹ shall have client side caching disabled, including autocomplete features.	X	X	X
DP2	The security classification level and marking of information processed by the application shall be identified, and security requirements defined in line with relevant NATO policies and directives (References D, E and G) to protect information while processed, stored, and transmitted by the application.		X	X
DP3	All sensitive data shall be sent to the server in the HTTP message body or headers (i.e., URL parameters are never used to send sensitive data).	X	X	X
DP4	The application shall set appropriate anti-caching headers as per the risk of the application.	X	X	X
DP5	On the server, all cached or temporary copies of sensitive data stored shall be protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data.	X	X	X
DP6	There shall be a method to remove each type of sensitive data from the application at the end of the required retention policy.	X	X	X
DP7	The application shall minimize the number of parameters in a request, such as hidden fields, Ajax variables, cookies and header values.		X	X
DP8	Data stored in client side storage (such as HTML5 local storage, session storage, IndexedDB, regular cookies or Flash cookies) shall not contain sensitive data.	X	X	X
DP9	All access to NATO Information and all administrative actions shall be logged in line with relevant NATO policies and supporting directives.	X	X	X
DP10	Sensitive data maintained in memory shall be overwritten with zeros as soon as it is no longer required, to mitigate memory dumping attacks.		X	X

⁹ Sensitive data, in this context, includes NATO information, credentials, and any information that can ease an attacker in probing and eventually compromise an application.

Communications Security

ID	Requirement	Standard	Enhanced	High
CS1	Each Transport Layer Security (TLS) server certificate shall be issued by a trusted certificate authority (CA) and each server certificate shall be valid.	X	X	X
CS2	TLS shall be used for all connections (including both external and backend remote connections) that are authenticated or that involve sensitive data or functions, and shall not fall back to insecure or unencrypted protocols.	X	X	X
CS3	Backend TLS connection failures shall be logged.			X
CS4	Certificate paths shall be built and verified for all client certificates using configured trust anchors and revocation information.	X	X	X
CS5	All connections to external systems that involve sensitive data shall be authenticated.		X	X
CS6	There shall be a single standard TLS implementation used by the application, configured to operate in a secure mode of operation.			X
CS7	HTTP Strict Transport Security headers shall be included on all requests and for all subdomains.	X	X	X
CS8	Forward secrecy ciphers shall be used to mitigate passive attackers recording traffic.	X	X	X
CS9	Proper certification revocation, such as Online Certificate Status Protocol (OCSP) Stapling, shall be enabled and configured.	X	X	X
CS10	Only strong algorithms, ciphers, and protocols shall be used, as per C3B policy through the complete certificate hierarchy, including the root certificates.	X	X	X
CS11	TLS settings shall be kept updated from a security perspective ¹⁰ , particularly as common configurations, ciphers, and algorithms become insecure.	X	X	X

HTTP Security

ID	Requirement	Standard	Enhanced	High
H1	The application shall only accept a defined set of required HTTP request methods (e.g. GET and POST), and unused methods (e.g. TRACE, PUT, and DELETE) are explicitly blocked.	X	X	X
H2	Every HTTP response shall contain a content type header specifying a safe character set (e.g., UTF-8, ISO 8859-1).	X	X	X
H3	HTTP headers added by a trusted proxy or Single Sign On (SSO) devices, such as a bearer token, shall be authenticated by the application.		X	X

¹⁰ E.g. in accordance with RFC 8446. New implementations of web applications shall use TLS version 1.3. Legacy applications utilizing TLS version 1.2 shall adhere to the new requirements identified within RFC 8446 specifically for TLS version 1.2.

ID	Requirement	Standard	Enhanced	High
H4	A suitable X-FRAME-OPTIONS header shall be used for sites where content shall not be viewed in a 3rd-party iframe.		X	X
H5	HTTP headers or any part of the HTTP response shall not expose detailed version information of system components.	X	X	X
H6	All API responses shall contain proper X-Content-Type-Options and Content-Disposition header declarations with filenames appropriate for the content type.	X	X	X
H7	Verify that the latest versions of a Content Security Policy (CSP) is in place that helps mitigate common DOM, XSS, JSON, and JavaScript injection vulnerabilities (e.g. Content-Security-Policy: default-src 'self' 'unsafe-eval' shall never be used, and usage of 'unsafe-inline' should be limited to the minimum and whitelisting of the scripts shall be implemented).	X	X	X
H8	The reflected cross-site scripting browser filter protection header (i.e. X-XSS-Protection: 1; mode=block) shall be implemented for all HTTP responses.	X	X	X

Business Logic

ID	Requirement	Standard	Enhanced	High
BL1	The application shall only process business logic flows in sequential step order, with all steps being processed in realistic human time, and not process out of order, skipped steps, process steps from another user, or too quickly submitted transactions.		X	X
BL2	The application shall have business limits and correctly enforces on a per user basis, with configurable alerting and automated reactions to automated or unusual application traffic.		X	X

Files and Resources

ID	Requirement	Standard	Enhanced	High
FR1	URL redirects and forwards shall only allow whitelisted destinations.	X	X	X
FR2	Untrusted file data submitted to the application shall not be used directly with file I/O commands (i.e. file content and filename shall be validated to protect against path traversal, local file include, file mime type, and OS command injection vulnerabilities).	X	X	X
FR3	Files obtained from untrusted sources shall be validated to be of expected type and scanned by antivirus scanners to prevent upload and download of known malicious content.	X	X	X
FR4	Untrusted data shall not be used within inclusion, class loader, or reflection capabilities (i.e. file content and filename shall be validated to prevent remote/local file inclusion vulnerabilities).	X	X	X

ID	Requirement	Standard	Enhanced	High
FR5	Untrusted data shall be validated prior to use within cross-origin resource sharing (CORS) to protect against arbitrary remote content.	X	X	X
FR6	Application code shall not execute uploaded data obtained from untrusted sources.	X	X	X
FR7	Files obtained from untrusted sources shall be stored outside the web application root, with limited permissions, and validation of file contents and filename.		X	X
FR8	Web or application servers shall be configured to deny access by default to remote resources or systems outside the web or application server.		X	X

Web Services

ID	Requirement	Standard	Enhanced	High
WS1	The same encoding style shall be used between the client and the server.	X	X	X
WS2	Access to administration and management functions within the Web Service Application shall be limited to web service administrators.	X	X	X
WS3	Applicable schemas (e.g. XML or JSON) shall be in place and verified prior to accepting input.	X	X	X
WS4	All input shall be limited to an appropriate size limit according to the application's functional requirements.	X	X	X
WS5	SOAP based web services shall, at a minimum, be compliant with Web Services-Interoperability (WS-I) Basic Profile. This includes the employment of TLS encryption.	X	X	X
WS6	Session-based authentication and authorization shall be used.	X	X	X
WS7	REST services and administrative tasks shall be protected from Cross-Site Request Forgery attacks by using CSRF nonces (i.e. randomly generated) or other similar anti-CSRF mechanisms	X	X	X
WS8	REST services shall explicitly check that the incoming Content-Type (e.g. application/xml or application/json) is appropriate for the application's functionality.		X	X

Configuration

ID	Requirement	Standard	Enhanced	High
C1	All components shall be the most current tested versions and have proper up to date security configuration(s) applied. This includes the removal of unneeded configurations and folders such as sample applications, platform documentation, and default or example users.	X	X	X
C2	All communications between components, such as between the application server and the database server shall be authenticated using an account with the least necessary privileges.	X	X	X

ID	Requirement	Standard	Enhanced	High
C3	Application deployments shall be adequately sandboxed, containerized or isolated to delay and deter attackers from attacking other applications.		X	X
C4	Authorised administrators shall have the capability to verify the integrity of all security-relevant configurations to ensure that they have not been tampered with.			X
C5	All application components shall be signed.			X
C6	All third party components shall come from trusted repositories.	X	X	X
C7	All build processes for system level languages shall have all security flags enabled, such as ASLR, DEP, and security checks.			X
C8	All application assets (e.g. JavaScript libraries, CSS stylesheets and web fonts) shall be hosted by the application rather than on a CDN or external provider.	X	X	X

Miscellaneous

ID	Requirement	Standard	Enhanced	High
M1	Client-based applications shall not have secret keys or passwords hard-coded in the executable.	X	X	X
M2	Unique identifiers shall never be used as security controls (e.g. Unique device ID (UDID) or MAC addresses).	X	X	X
M3	Client-based applications shall not request more permissions or access to resources than those strictly required for its correct operation.	X	X	X
M4	Files with unrestricted permissions shall never be generated.	X	X	X
M5	Unless specifically required, client-based applications shall be configured to run in a restricted sandbox, with no direct access to OS resources, such as the file system or native libraries.		X	X
M6	The management interface shall not be exposed to the Internet ¹¹ .		X	X
M7	The client-based application binary shall be obfuscated and stripped of debugging symbols.			X

TESTING AND TASKS

This section describes testing tools and tasks that can be executed during the lifecycle of the software development of a web application to ensure that security considerations are addressed during the design, development, deployment, maintenance, operation and

¹¹ There are technologies available to mitigate exposure (e.g., VPN). These technologies are to be determined in coordination with the SAA.

deprecation of the site. The tools and task used for each project will depend on the security level assigned to the web application based on a risk assessment.

Testing tool/task	Description	Standard	Enhanced	High
Review security level	Assess that the site has been assigned to the correct security level based on its risk assessment.	X	X	X
Review design and architecture	Revision of the documented design and architecture to ensure that security considerations have been addressed.	X	X	X
Configuration management testing	Testing the deployment and security of the underlying infrastructure.	X	X	X
Vulnerability assessments	Scanning and analysis of the site using automatic and manual tools, security configuration baselines, and other checklist items to identify vulnerabilities, which may potentially be exploited.	X	X	X
Health checks	Periodic verification that the application and infrastructure are still operationally secure.	X	X	X
Application penetration testing	Testing beyond identification of potential vulnerabilities, in order to assess the possible extent of compromise, and to provide an accurate assessment of the business risk posed by the verified vulnerabilities.	X	X	X
Code reviews	Detailed search for code defects.	X	X	X
Create and review UML models	Use UML models to ensure exact understanding about how the application works.			X
Create and review threat models	Develop threat scenarios and analyse the design and architecture to ensure that the threats have been considered.	X	X	X

SUPREME HEADQUARTERS
ALLIED POWERS EUROPE
B-7010 SHAPE BELGIUM



GRAND QUARTIER GÉNÉRAL
DES PUISSANCES ALLIÉES
EN EUROPE
B-7010 SHAPE - BELGIQUE

SHJ3/JOS/JO/AH/07 - 203466

TO: See Distribution

SUBJECT: ACO Recognised Ground Picture Directive 80-84

DATE: 10 January 2008

1. The emerging roles of NATO operations, including the NATO Response Force (NRF), have changed fundamentally the need for improved flow of information, in both timeliness and granularity, from the tactical level to the operational and strategic levels. This requires the capability to develop and transfer data automatically between the different levels of command. This capability dictates national systems capable of compiling land force data and significant improvements in interoperability and connectivity between national C2 systems and NATO. Finally, the NATO chain of command requires a means to process and display the land force information that is passed from the national, tactical level in a Recognised Ground Picture (RGP).
2. The purpose of the ACO RGP is to provide land battle space data to a NATO Common Operational Picture (COP) to enable NATO-led forces to share a common view of the land battle space, to support common understanding to improve situational awareness, and to support the decision-making process.
3. Enclosed, you will find the ACO RGP Directive 80-84, which is to be implemented immediately.
4. The SHAPE point of contact is LTC Anders Henriksen, J3, NCN 254-3245.

FOR THE SUPREME ALLIED COMMANDER, EUROPE:

A handwritten signature in black ink, appearing to read 'K-H. Lather'.

Karl-Heinz Lather
General, DEU A
Chief of Staff

ENCLOSURE:

1. ACO Directive 80-84 NATO Recognised Ground Picture.

DISTRIBUTION:

External -

Action:

COS HQ SACT
COS JFC HQ Brunssum
COS JFC HQ Naples
COS Joint HQ Lisbon
JALLC
CC-Land HQ Heidelberg
CC-Land HQ Madrid
NCSA
NC3A

Information:

JWC
JALLC
JFTC
CC-Air HQ Ramstein
CC-Air HQ Izmir
CC-Mar HQ Naples
CC-Mar HQ Northwood
1 DEU/NLD Corps
ARRC
EUROCORPS
MNC NE
NDC Greece
NRDC Spain
NRDC Italy
NRDC Turkey
FRRC

Internal -

Action:

ACOS J2
ACOS J3
ACOS J4
ACOS J6

Information:

DCOS OPS
DCOS SPT
ACOS J1
ACOS J5
ACOS J7
ACOS J8
ACOS J9
DOS

SUPREME HEADQUARTERS
ALLIED POWERS EUROPE
B-7010 SHAPE BELGIUM



GRAND QUARTIER GÉNÉRAL
DES PUISSANCES ALLIÉES
EN EUROPE
B-7010 SHAPE - BELGIQUE

ACO DIRECTIVE
NUMBER 80-84

TT 203466
14 January 2008

NATO RECOGNISED GROUND PICTURE (RGP)

This is a new Allied Command Operations (ACO) Directive.

- REFERENCES:
- A. NATO Land Focused Working Group, Land Recognised Ground Picture (RGP) Operational Requirements, SHAPE letter, dated 18 Oct 01.
 - B. Maritime Command and Control Information System (MCCIS) Standard Operating Procedures, dated 08 Nov 05.
 - C. MC 400/2 Military Committee Guidance for the Military Implementation of Alliance Strategy, dated 23 May 00.
 - D. MC 477 Military Concept for the NATO Response Force, dated 18 Jun 03.
 - E. MCM 159-02 NATO Response Force, dated 30 Oct 02.
 - F. Bi-SC Concept of Operations for the NATO Common Operational Picture, dated 02 Jan 01.

1. **Applicability.** This directive is applicable to all NATO-led operations.
2. **Supplementation.** Supplementation is not authorised.
3. **Interim Changes.** Interim changes are authorised when approved by the Deputy Chief of Staff, Operations (DCOS OPS).
4. **Purpose.** The aim of this directive is to provide directions and guidance for development of a Recognised Ground Picture (RGP) for all NATO-led operations, to define the NATO RGP, and to identify responsibilities for development, maintenance, and dissemination of the RGP. This directive does not attempt to address specific operational situations, nor does it meet every RGP Manager's specific requirements. Each RGP Manager is directed to tailor this standing guidance to accommodate specific operational or training scenarios as necessary.
5. **Table of Contents**

	Page	Paragraph
CHAPTER 1 – INTRODUCTION		
Introduction	1-1	1-1
CHAPTER 2 – PURPOSE AND DEFINITION		
Purpose	2-1	2-1
Definition	2-1	2-2
Attributes of the RGP	2-1	2-3
Elements of the RGP	2-2	2-4
CHAPTER 3 – RESPONSIBILITIES		
RGP Manager	3-1	3-1
Common Operational Picture (COP) Manager	3-2	3-2
Higher HQ	3-2	3-3
Local RGP Manager (User Level)	3-2	3-4
CHAPTER 4 – RGP MANAGEMENT PROCESS		
RGP Development and Depiction	4-1	4-1
RGP Management	4-1	4-2

AD 80-84

CHAPTER 1**INTRODUCTION****1-1. Introduction**

- a. The emerging roles of NATO operations, especially the NATO Response Force (NRF) operations, have changed fundamentally the need for improved flow of information, in both timeliness and granularity, amongst the tactical, operational and strategic levels. This requires the capability to collect, process, and exchange data between the different levels of command without loss of time. This capability dictates national and NATO Command and Control Information Systems (C2IS) to improve interoperability and connectivity. For land forces under NATO command, all operationally relevant tactical information will be summed up in the RGP.
- b. Relevant, timely and correct knowledge of the joint battlespace in NATO military operations are pre-requisite for planning and conducting military operations. NRF missions, complementing traditional NATO missions, result in an intertwining of the relationships between the strategic, operational and tactical command level tasks and decision making. Tactical-level information may have an enormous impact on the strategic level and possibly also on the geo-political level.
- c. Current technological developments will allow NATO forces to use information from an evolving and increasing number of sensors and C2IS, enabling commanders at all levels to decide on the basis of the most topical information derived from multiple sources.
- d. NATO is pursuing the incremental development of a NATO Common Operational Picture (COP), which will facilitate improved situational awareness of the joint battlespace, required to conduct effective operations with minimised risk of collateral damage and fratricide. The RGP is one of the indispensable contributions to the COP.

AD 80-84

CHAPTER 2

PURPOSE AND DEFINITION

2-1. **Purpose.** The purpose of the NATO RGP is to provide land battlefield data to the NATO COP to enable NATO-led forces to share a common view of the land battlefield, to support common understanding in order to improve situational awareness, and to support the decision-making process.

2-2. **Definition**

a. Despite the term "picture", the NATO RGP does not only refer to the graphical presentation of the situation but, extensively, also to all relevant information that is required to fulfil the Land Commander's needs for his situational awareness and the information needs on ground forces to manage the COP.

b. Therefore, **"The NATO 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"**.

(1) The RGP will be displayed to the most possible extent in a geographic presentation of processed, all source information and data known at a given time of activities in the land operating environment. This includes force, contact, geographic, environmental-industrial hazards, health, and other operational, as well as tactical information. The NATO RGP is compiled in accordance with operational directives and tasking to support decision makers in the conduct of Command and Control of land forces and operations. The NATO RGP is an operational picture, not a tactical plot, and is not intended to be used to directly support weapon systems, target acquisition, or engagements.

2-3. **Attributes of the NATO RGP**

a. A distinct RGP will be developed, managed, and disseminated for each area of operation and support development of the COP for that operation. Operational and Strategic-level commands may desire to combine the RGP and/or COP for more than one operation to develop a wider view of NATO operations.

b. The RGP, as defined, is based on a synchronised, distributed common set of validated land-relevant data, from all levels, that each Commander draws upon to depict the land battlefield in a manner which best supports his situational awareness needs and decision-making process. This common set of validated land-relevant data is made available to all levels of command within the NATO operational structure, and supports the capability to selectively depict the battlefield in whatever format, and at whatever level is relevant to each particular commander. The RGP makes all land-relevant

AD 80-84

data available to all levels, all of the time, and each commander determines the depiction of the data that he wants to see.

c. The RGP data should be as close to real-time and as accurate as possible, based on available sensors and reporting and information exchange mechanisms. Moving or changing objects should be depicted in near-real time, while the static environment may be updated as changes occur.

d. The RGP will consist of both near-real time and non-real time data, and users of the data must be aware of the latency of all data.

e. Data should be processed and exchanged automatically, where possible, to avoid processing delays and minimise the risks associated with human data entry errors. This may dictate the need to exchange data between national and NATO networks and across security domains.

f. All land battlefield related data must be shared and available to all levels of command. A principle that is fundamental to developing a complete and accurate RGP is full and open sharing of information throughout the theatre command structure, while accommodating national information disclosure policies. Withholding of data to prevent command interference or micromanagement by higher headquarters will result in incomplete data, degraded situational awareness, and possibly reduced information superiority and mission effectiveness.

2-4. Elements of the RGP

a. The RGP includes all land battlefield data that is necessary to support the development of the NATO COP and fulfil the situational awareness requirements of commanders at the tactical and operational levels of a NATO-led operation. In accordance with Allied Joint Publication 2.1, battlespace situational awareness is the requirement that focuses on three overlapping and complementary components: the adversary, the operational environment, and the friendly forces. Intelligence staffs are responsible for providing information and intelligence on the first two components. Operations staffs provide the third. In addition, neutral parties and elements should also be included and may be provided by both the intelligence and operations staffs. The elements of the RGP are independent of the systems or methods of displaying the data.

b. **Geography.** The geography of the area of operation will be included in the RGP, to include standard geographic (GEO) products (maps, elevation data, vector graphics), based on an agreed upon geographic reference. Also included will be the Battlefield Area Analysis (i.e., knowledge on geography, climate and Political, Military, Social, Economic, Infrastructure and Information (PMSEII-factors) of the area of operation and their impact on GROUND operations.

- c. **Operating area features.** Within the area of interest, military graphics which are needed for the battlefield management from all levels of command will be available as part of the RGP.
- d. **Civil and Military Infrastructure.** The civil and military infrastructure in the area of operation will be included in the RGP. This includes political boundaries, cities, bridges, roads, railroads, airfields, medical treatment facilities, and other significant infrastructure. Additionally, the status of the infrastructure and its usability, including impact on operations of availability or non-availability should be included. Civil - Military Cooperation (CIMIC) sites of interest should be included such as restricted sites or areas, protected sites, civil administration, civil infrastructure, hazardous industries, as well as civilian agencies, Displaced Persons and Refugees (DPRE) camps, and ethnic enclaves. Also to be included are humanitarian, International Organisations (IO)/Non-Governmental Organisations (NGO), civil authority, and local population activities, incidents or movement. The situational awareness of CIMIC-related information is of increasing importance during non Crisis Response Operation (CRO) missions, particularly humanitarian assistance and peacekeeping, and must be available within the RGP. Engineering information affecting NATO operations or civil operations to include minefields, fortifications, towers, other obstacles, and environmental incidents should be available. The validated status of significant obstacles, including a mobility-hindrance rating or impact on operations assessment, should be included.
- e. **Land Military Units.** A major element of the RGP is the current situation of friendly land forces (organisation, unit identification, unit location, unit type, unit size, nationality, function, operational status, equipment and weapons holdings, etc.); land force organic air forces; and chemical, biological, radiological and nuclear (CBRN) forces. Friendly units under NATO Operational control (OPCON) and other friendly military units (such as host nation, coalition or UN forces not under NATO OPCON) may be included. Neutral military units may be included. The level of detail of units in the RGP dataset should be the lowest level possible, with the depiction at each command level filtered and tailored dependent on the Commander's needs at a particular time and dependent on the operational situation. Special Operation Force (SOF) unit current situation should be available, but access may be restricted based on the need to know and level of access.
- f. **Intelligence information.** Intelligence information reaches across the Joint spectrum, but is critical in the land battlefield. Intelligence data, and threat locations, including disease risks and health threats, as well as significant events are to be included in the RGP. These include threat unit or cell locations, type, size, direction of movement, area of influence, and capabilities and intentions. Weapon effective ranges, including for systems such as artillery and air defence, should also be available for overlay of geographic features. The location of intelligence related incidents or events,

AD 80-84

such as suspicious observations and threat warnings, epidemic and endemic disease of operational significance, and environmental-industrial hazards should be included in the intelligence information provided to the RGP. Intelligence collection timings and areas should also be included.

g. **Operational documents.** Operational documents pertaining to land operations, such as Operation and Fragmentary Orders, directives, and procedures, as well as Commander's intent and battle plans will be included in the RGP.

AD 80-84

CHAPTER 3**RESPONSIBILITIES**

3-1. **RGP Manager.** The RGP Manager is the Land Commander for an operation and is responsible for the production of the RGP, including data collection, management, and dissemination. Developing the RGP requires aggregating data from numerous sources into a coherent collection of information for dissemination and depiction at the user commands. Data is shared from the lowest tactical level through the chain of command, aggregated with other data, and the RGP Manager incorporates it into the RGP. Relevant data may enter at any level in the command structure, including the strategic level. The final aggregation of data takes place at the Land Commander level and is disseminated as the RGP, both up and down the chain of command.

a. RGP management functions shall be performed at each RGP generation location. The management tasks are to be flexibly implemented to meet the flexible nature of the NATO force and command organisation for each operation. Overall, RGP management includes responsibilities for:

(1) Information management, with the responsibility to collect, exchange, filter, validate and disseminate information that is included in the RGP. Data will come from a variety of sources, but the Land Commander and its subordinate units are the primary sources. Information may also come in from other functional areas at the Operational level or above and be added to the RGP dataset. The RGP only contains information that has been evaluated and validated at some level prior to inclusion.

(2) Information source management, with responsibility to control allocated information sources and sensors.

(3) Information exchange and reporting requirements, with responsibility to ensure that all relevant data is provided to the RGP.

(4) *Ambiguity management* (multiple reports from different sources for the same unit or event), with responsibility for identifying and resolving possible reporting errors and inconsistencies among RGP contributions in case there is overlapping of reporting sources.

b. RGP management shall be executed in accordance with this directive and as further defined by specific RGP management procedures. The RGP management procedures should provide the capability for specific organisations or commands to have responsibility for managing certain types of data, such as G3 managing the Blue land force data or G9 managing the CIMIC data.

AD 80-84

3-2. **COP Manager.** (NATO Joint Commander Deployable Joint Task Force/Combined Joint Task Force (DJTF/CJTF)). The Joint (NATO) Commander, as the COP Manager for an operation, is a primary stakeholder in the RGP and has a vested interest in its completeness, accuracy, and timeliness. The NATO Commander may direct specific information requirements to be included in the RGP beyond those described in the previous chapter.

a. **NATO COP.** Land battlefield data from the RGP is an essential element of developing and presenting a NATO COP for an operation area, in addition to data from the Recognised Air Picture (RAP), Recognised Maritime Picture (RMP), and the recognised pictures provided by other functional areas. The RGP Manager shall disseminate RGP data to the NATO COP Manager for incorporation. The level of land battlefield data in the COP should be comparable to the RGP, with appropriate filtering and display manipulation capabilities available, to tailor the display to meet the needs of the user. The COP Manager will disseminate the NATO COP to the Component Commanders and other users.

3-3. **Higher HQs.** The RGP Manager provides the RGP to all higher, adjacent and subordinate headquarters, according to the operational chain of command, to support reach-back capabilities and Commanders' situational awareness of the operation.

3-4. **Local RGP Manager (user level).** The local RGP Manager (at user sites in all levels of command) is responsible for the local management of RGP data and its appropriate depiction. This includes the Local RGP Manager at the Joint Command level (CJTF/DJTF). Within each organisation and command that contributes to the RGP, the Local RGP Manager must ensure that contributions to the RGP are valid, current, and properly managed. The Local RGP Manager is responsible for the accuracy and timeliness of the track data/force element and database information they contribute.

AD 80-84

CHAPTER 4**RGP MANAGEMENT PROCESS**

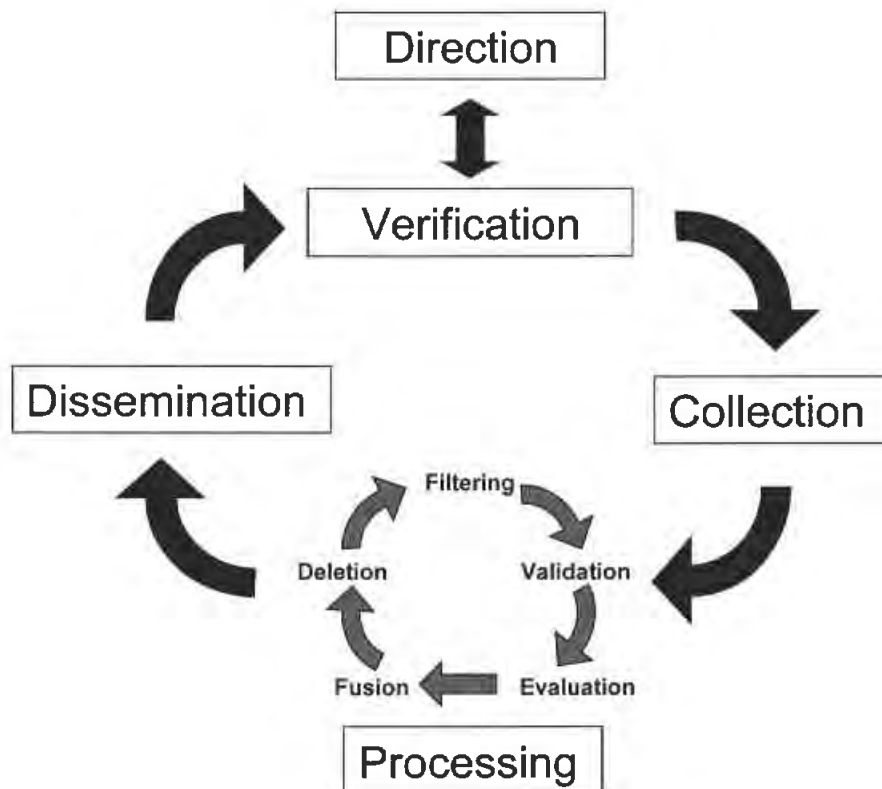
4-1. **RGP Development and Depiction.** The process of developing or building the RGP is one of collecting and aggregating data from a variety of sources that is either pushed to the RGP Manager or pulled from the source. Flow of information should be automated to the maximum extent possible to reduce time delays and potential for human-induced errors. The depiction of land-relevant data can take many forms and formats. From paper maps and pushpins, to sophisticated C2IS, there are many means of depiction of RGP data available to support the situational awareness needs of the Commander. The process for building the RGP dataset is similar for all methods of depiction, and only the mechanics of building the depiction differ.

4-2. **RGP Management.** The RGP management process is interactive and continuous in nature and can be conducted on different levels. Understanding and executing this process is the most effective means of ensuring standardisation and consistency among users involved in RGP management. This process ensures that the data is properly entered into the RGP track database. The RGP management process consists of five distinct elements:

- a. Direction.
- b. Collection.
- c. Processing.
- d. Dissemination.
- e. Verification.

(1) **Direction.** The Operational Commander will promulgate Operational Directives (e.g. OPDIR RGP) to the assigned RGP Manager for an operation. The RGP Manager will implement the Operational Directive by promulgating their OPTASK RGP and SUPPLEMENTS as required to units and forces in their RGP Operation Area.

(2) **Collection.** Data collection involves the accumulation of data reports from multiple sources in a variety of reporting formats. The RGP Manager will monitor the receipt of incoming data and, if problems occur involving data exchange, initiate troubleshooting procedures to resolve the problem. The RGP Manager ensures that all received data is entered into the RGP Management process. Normally, this data will be provided to the RGP Manager electronically through appropriate communication channels and may come from any level of command.



RGP Management Process

(3) **Processing.** Processing of collected data consists of:

- (a) Filtering.
- (b) Validation.
- (c) Evaluation.
- (d) Fusion.
- (e) Deletion.

Data Processing is a continuous operation described through the five sub-processes above and shall seek to keep the RGP as updated, unambiguous, user friendly, and adjusted to the operational objective as possible.

- (a) **Filtering.** The RGP Manager filters data upon receipt, so that only information applicable to that Operation Area is inserted into the RGP.
- (b) **Validation.** Data validation is the process of identifying data of interest to the operational commander.

AD 80-84

(c) **Evaluation.** Data evaluation involves assessing the reliability of a source and data against the existing RGP information.

(d) **Fusion.** Data fusion is the iterative process of merging evaluated and validated data into a single, coherent data set. The data fusion process includes:

- 1/ Removing duplicate information.
- 2/ Resolving ambiguous data.
- 3/ Correlating reports from different sources.
- 4/ Adding new information.

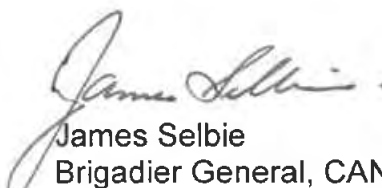
(4) **Deletion.** Deletion is the process of removing data no longer contributing to situational awareness from the RGP.

(5) **Dissemination.** Dissemination is the process of providing the RGP to:

- a. NATO Commands.
- b. National Commands.
- c. Other RGP users.

(6) **Verification.** The process by which the disseminated RGP is confirmed by the reporting source in order to ensure any possible errors are resolved in a timely manner.

FOR THE SUPREME ALLIED COMMANDER, EUROPE:


James Selbie
Brigadier General, CAN Army
Director of Staff

ANNEX:

A. Acronyms and Abbreviations.

DISTRIBUTION:

External –

AD 80-84

Action:

COS JFC HQ Brunssum
COS JFC HQ Naples
COS Joint HQ Lisbon
CC-Land HQ Heidelberg
CC-Land HQ Madrid
NRDC Italy
NRDC Turkey
NRDC Spain
ARRC
EUROCORPS
1 DEU/NLD Corps
Multinational Corps Northeast
NDC Greece
FRRC
JWC
JFTC

Information:

COS HQ SACT
JALLC

Internal –

Action:

SDC
ACOS J3
ACOS J6

Information:

DCOS SPT

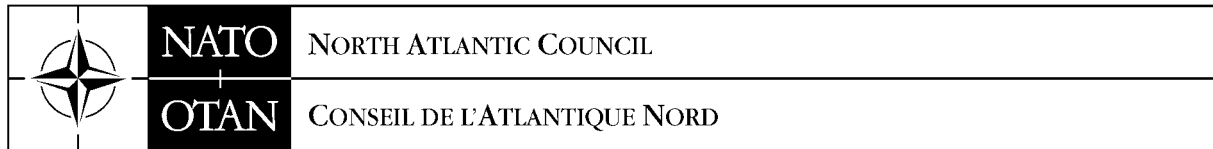
AMENDMENTS/COMMENTS

Users of this directive are invited to send comments, amendments and suggested improvements to ACO/J3

Acronyms and Abbreviations

ACC	Air Component Command
ACO	Allied Command Operations
ACT	Allied Command Transformation
AOI	Area of Interest
AOR	Area of Responsibility
BICC	BICES Initial Core Capability
BICES	Battlefield Information Collection & Exploitation System
C2	Command and Control
C2IS	Command and Control Information System/Service
CBRN	Chemical, Biological, Radiological and Nuclear
CIMIC	Civil-military Cooperation
CJOC	Combined Joint Operations Centre
CJTF	Combined Joint Task Force
CONOPS	Concept of Operations
COP	Common Operational Picture
DCOS	Deputy Chief of Staff
DJTF	Deployable Joint Task Force
DPRE	Displaced Persons and Refugees
GEO	Geographic
JFC	Joint Force Command
JOC	Joint Operations Centre
JOIIS	Joint Operations/Intelligence Information System
LC2IS	Land Command and Control Information Services
LCC	Land Component Command
MCC	Maritime Component Command
NRF	NATO Response Force
OPCON	Operational Control
OPDIR	Operational Directive
OPLAN	Operation Plan
OPTASK	Operational Task
PMSEII	Political, Military, Social, Economic, Infrastructure and Information
RAP	Recognised Air Picture
RMP	Recognised Maritime Picture
SA	Situational Awareness
SACEUR	Supreme Allied Commander Europe
SIGINT	Signals Intelligence
SOF	Special Operations Force
SOP	Standing Operating Procedures
UN	United Nations

INSERTED INTO
DOCUMENT.



NATO UNCLASSIFIED

09 April 2010

DOCUMENT
C-M(2002)49-COR8

**SECURITY WITHIN THE
NORTH ATLANTIC TREATY ORGANISATION**

**Corrigendum to C-M(2002)49 dated 17 June 2002
Amendment 8**

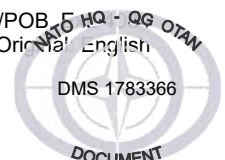
1. This document is the result of a review of Enclosures "B" and "E" to C-M(2002)49 by the NATO Security Committee and has been approved by Council¹ under the silence period. These amendments concern the handling and protection of NATO signals intelligence marked COSMIC TOP SECRET – BOHEMIA. They are reflected in paragraph 8 of Enclosure "B" and in paragraph 13 of Enclosure "E".
2. Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosures "B" and "E" and destroy the previous versions.
3. This amendment bears serial number 8. Holders of C-M(2002)49 are therefore requested to strike out number 8 on the "Record of Amendments" which can be found on the opposite side of the cover page.

¹ C-M(2010)0033 refers

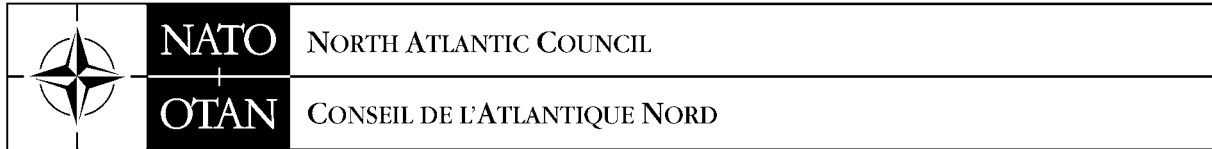
Annexes: Enclosure "B"
Enclosure "E"

Action Officer: Robert Keil, NOS/POB, 5 HQ - QG OTAN
Original: English

NATO UNCLASSIFIED



INSERTED INTO
DOCUMENT.



NATO UNCLASSIFIED

19 August 2009

DOCUMENT
C-M(2002)49-COR7

**SECURITY WITHIN THE
NORTH ATLANTIC TREATY ORGANISATION**

**Corrigendum to C-M(2002)49 dated 17 June 2002
Amendment 7**

1. This document is the result of a review of Enclosure "B" by the NATO Security Committee and has been approved by Council¹ under the silence period. This amendment of Enclosure "B" introduces under paragraph 23 the necessity to establish specific security provisions and guidance applicable in circumstances where NATO Operations, Training, Exercise, Transformation and Cooperation activities involve Non-NATO Entities.
2. Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosure "B" and destroy the previous version.
3. This amendment bears serial number 7. Holders of C-M(2002)49 are therefore requested to strike out number 7 on the "Record of Amendments" which can be found on the opposite side of the cover page.

¹ C-M(2009)0112-COR1 refers

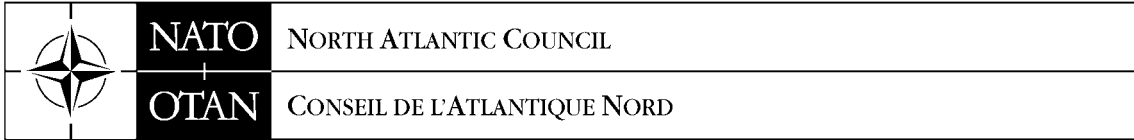
Annex: Enclosure "B"

Action Officer: Robert Keil, NOS/POB, 5 HQ - QG OTAN
Original: English

NATO UNCLASSIFIED



INSERTED INTO
DOCUMENT.



NATO UNCLASSIFIED

09 December 2008

DOCUMENT
C-M(2002)49-COR6

**SECURITY WITHIN THE
NORTH ATLANTIC TREATY ORGANISATION**

**Corrigendum to C-M(2002)49 dated 17 June 2002
Amendment 6**

1. This document is the result of a review of Enclosures "B" and "F" by the NATO Security Committee and has been approved by Council¹ under the silence period. The revision of Enclosure "B" emphasizes the necessity for NATO Nations and NATO Civil and Military bodies to establish appropriate Security Awareness and Training Programmes. The revision of Enclosure "F" reflects the need to include text with respect to the cryptographic protection of information classified NATO CONFIDENTIAL or NATO RESTRICTED transmitted between NATO and non-NATO nations / international organisations (NNN/IO) systems.
2. Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosures "B" and "F" and destroy the previous version.
3. This amendment bears serial number 6. Holders of C-M(2002)49 are therefore requested to strike out number 6 on the "Record of Amendments" which can be found on the opposite side of the cover page.

Annexes: Enclosures "B" and "F"

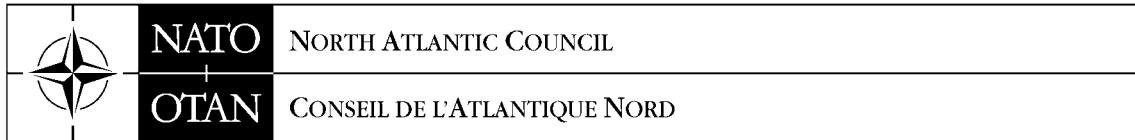
Action Officer: Robert Keil, NOS/POB, Ext. 4084
Original: English

¹ C-M(2008)0121 and C-M(2008)0067 refer

NATO UNCLASSIFIED



INSERTED INTO
DOCUMENT



NATO UNCLASSIFIED

03 July 2007

DOCUMENT
C-M(2002)49-COR5

**SECURITY WITHIN THE
NORTH ATLANTIC TREATY ORGANISATION**

**Corrigendum to C-M(2002)49 dated 17 June 2002
Amendment 5**

1. This document is the result of a review by the NATO Security Committee of NATO Security Policy and has been approved by Council¹ under the silence period. This revision reflects approved changes concerning the extension of the regular inspection interval for CTS holdings from 18 to 24 months.
2. Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosure "B" and destroy the previous version.
3. This amendment bears serial number 5. Holders of C-M(2002)49 are therefore requested to strike out number 5 on the "Record of Amendments" which can be found on the opposite side of the cover page.

Annex : Enclosure "B"

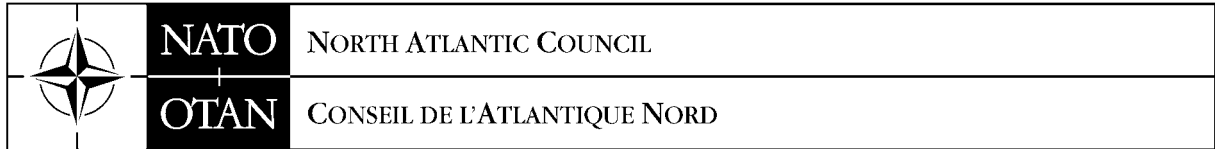
Action Officer: Robert Keil, NOS/POB, Ext. 4084
Original: English

¹ C-M(2007)0050-COR1

NATO UNCLASSIFIED



INSERTED INTO
DOCUMENT



NATO UNCLASSIFIED

5 December 2006

DOCUMENT
C-M(2002)49-COR4

**SECURITY WITHIN THE
NORTH ATLANTIC TREATY ORGANISATION**

**Corrigendum to C-M(2002)49 dated 17 June 2002
Amendment 4**

1. This document is the result of a review by the NATO Security Committee of NATO INFOSEC Policy and has been approved by Council¹.
2. Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosure "F" and destroy the old one.
3. This amendment bears serial number 4. Holders of C-M(2002)49 are therefore requested to strike out number 4 on the "Record of Amendments" which can be found on the opposite side of the cover page.

Annex : Enclosure "F"

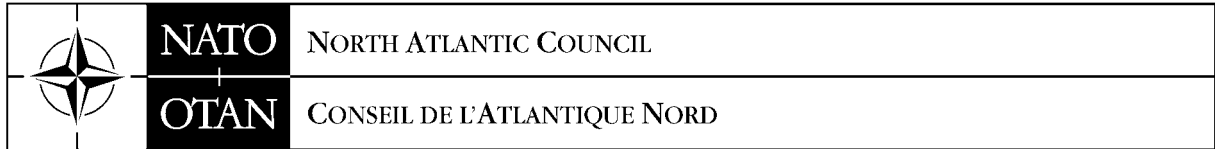
Original: English

¹ C-M(2006)0113

NATO UNCLASSIFIED



INSERTED INTO
DOCUMENT



NATO UNCLASSIFIED

5 December 2006

DOCUMENT
C-M(2002)49-COR3

**SECURITY WITHIN THE
NORTH ATLANTIC TREATY ORGANISATION**

**Corrigendum to C-M(2002)49 dated 17 June 2002
Amendment 3**

1. Council has approved text¹ with respect to the following :
 - (a) the updated responsibilities of the NATO Office of Security;
 - (b) NATO classified contracting involving non-NATO nations;
 - (c) release procedures for NATO classified information; and
 - (d) partners' integration into NATO civil and military bodies.
2. Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosures "B", "C", "D", "E" and "G" and destroy the old ones.
3. This amendment bears serial number 3. Holders of C-M(2002)49 are therefore requested to strike out number 3 on the "Record of Amendments" which can be found on the opposite side of the cover page.

Annexes : Enclosure "B"
Enclosure "C"
Enclosure "D"
Enclosure "E"
Enclosure "G"

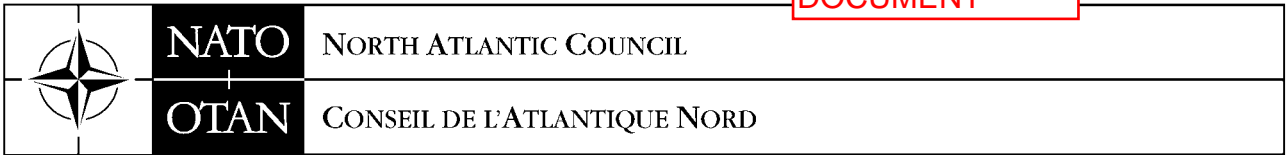
Original: English

¹ C-M(2006)0112

NATO UNCLASSIFIED



INSERTED INTO
DOCUMENT



NATO UNCLASSIFIED

11 May 2005

DOCUMENT
C-M(2002)49-COR2

**SECURITY WITHIN THE
NORTH ATLANTIC TREATY ORGANISATION**

**Corrigendum to C-M(2002)49 dated 17 June 2002
Amendment 2**

1. Council has approved a text¹ with respect to the revised Terms of Reference (TORs) for the NATO Security Committee (NSC) which is included at paragraphs 33 and 34 in the attached revised Enclosure "B" to C-M(2002)49. In addition, it is also required in paragraph 36(f) to change "SACLANT" to "HQ SACT". Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosure "B" and destroy the old one.
2. This amendment bears serial number 2. Holders of C-M(2002)49 are therefore kindly requested to strike out number 2 on the "Record of Amendments" which can be found on the opposite of the cover page.

Annex : Enclosure "B"

Original: English

¹ C-M(2005)0025

NATO UNCLASSIFIED



NATO UNCLASSIFIED

9 January 2004

DOCUMENT
C-M(2002)49-COR1

**SECURITY WITHIN THE
NORTH ATLANTIC TREATY ORGANISATION (NATO)**

**Corrigendum to C-M(2002)49 dated 17 June 2002
Amendment 1**

1. Council has approved a text¹ with respect to the rules for the protection of Signals Intelligence (SIGINT) information which is included as paragraph 8 in the attached revised Enclosure "B" to C-M(2002)49. Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosure "B" and destroy the old one.
2. This amendment bears serial number 1. Holders of C-M(2002)49 are therefore kindly requested to strike out number 1 on the Record of Amendments which can be found on the opposite side of the cover page.

Annex: Enclosure "B"

Action Officer: N. Janssens, NOS/Adm. Officer, Ext. 4526
Original: English/French

¹ C-M(2003)25

NATO UNCLASSIFIED





17 June 2002

DOCUMENT
C-M(2002)49

**SECURITY WITHIN THE
NORTH ATLANTIC TREATY ORGANISATION (NATO)**

Note by the Secretary General

Reference: C-M(2002)23 and its Action Sheet

1. This document is the result of a Fundamental Review by the NATO Security Committee (NSC) and it was approved by Council under the silence procedure on 26th March 2002 (reference refers).

2. This present document, in conjunction with C-M(2002)50, "Protection Measures for NATO Civil and Military Bodies, deployed NATO Forces and Installations (Assets) against Terrorist Threats", supersedes C-M(55)15(Final). With the exception of Enclosure "A", the "Security Agreement by the Parties to the North Atlantic Treaty" which is still valid for those nations which have not yet ratified the "Agreement between the Parties to the North Atlantic Treaty for the Security of Information", all previous versions of C-M(55)15(Final) should now be destroyed.

3. The following Directives support this present document:

AC/35-D/2000	Directive on Personnel Security
AC/35-D/2001	Directive on Physical Security
AC/35-D/2002	Directive on Security of Information
AC/35-D/2003	Directive on Industrial Security
AC/35-D/2004	Primary Directive on INFOSEC
AC/35-D/2005	INFOSEC Management Directive for CIS

(The first four directives (AC/35-D/2000-2003) were approved by Council (reference refers) and the remaining two AC/35-D/2004 and D/2005) were approved by the NATO Security Committee (NSC) and the NATO C3 Board.

4. For ease of reference, a compendium, containing the two security policy documents (C-M(2002)49 and C-M(2002)50) and the above-mentioned supporting directives, will be distributed in the near future to all current holders of C-M(55)15(Final).

(Signed) George Robertson

Original: English

RECORD OF AMENDEMENTS

Strike out corresponding number
as each amemdment is inserted

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

TABLE OF CONTENTS

Note by the Secretary General

Record of Amendments

Table of Contents

Enclosure "A" - Security Agreement

Enclosure "B" - Basic Principles of Security

Enclosure "C" - Personnel Security

Enclosure "D" - Physical Security

Enclosure "E" - Security of Information

Enclosure "F" - INFOSEC

Enclosure "G" - Industrial Security

Glossary

ENCLOSURE "A"
AGREEMENT BETWEEN THE PARTIES TO THE NORTH ATLANTIC TREATY FOR THE SECURITY OF INFORMATION ¹

The Parties to the North Atlantic Treaty, signed at Washington on 4th April, 1949;

Reaffirming that effective political consultation, cooperation and planning for defence in achieving the objectives of the Treaty entail the exchange of classified information among the Parties;

Considering that provisions between the Governments of the Parties to the North Atlantic Treaty for the mutual protection and safeguarding of the classified information they may interchange are necessary;

Realising that a general framework for security standards and procedures is required;

Acting on their own behalf and on behalf of the North Atlantic Treaty Organization, have agreed as follows:

ARTICLE 1

The Parties shall:

- (i) protect and safeguard:
 - (a) classified information (see ANNEX 1), marked as such, which is originated by NATO (see ANNEX 2) or which is submitted to NATO by a member state;
 - (b) classified information, marked as such, of the member states submitted to another member state in support of a NATO programme, project, or contract,

¹ This agreement is currently awaiting ratification by the Governments of the following NATO member nations : Belgium, Iceland, Italy, Luxembourg, Norway, Portugal, Spain and UK. The "Security Agreement by the Parties to the North Atlantic Treaty Organisation" contained in "Enclosure "A" to C-M(55)15(Final) remains valid for those nations who have not yet ratified.

- (ii) maintain the security classification of information as defined under (i) above and make every effort to safeguard it accordingly;
- (iii) not use classified information as defined under (i) above for purposes other than those laid down in the North Atlantic Treaty and the decisions and resolutions pertaining to that Treaty;
- (iv) not disclose such information as defined under (i) above to non-NATO Parties without the consent of the originator.

ARTICLE 2

Pursuant to Article 1 of this Agreement, the Parties shall ensure the establishment of a National Security Authority for NATO activities which shall implement protective security measures. The Parties shall establish and implement security standards which shall ensure a common degree of protection for classified information.

ARTICLE 3

- (1) The Parties shall ensure that all persons of their respective nationality who, in the conduct of their official duties, require or may have access to information classified CONFIDENTIAL and above are appropriately cleared before they take up their duties.
- (2) Security clearance procedures shall be designed to determine whether an individual can, taking into account his or her loyalty and trustworthiness, have access to classified information without constituting an unacceptable risk to security.
- (3) Upon request, each of the Parties shall cooperate with the other Parties in carrying out their respective security clearance procedures.

ARTICLE 4

The Secretary General shall ensure that the relevant provisions of this Agreement are applied by NATO (see ANNEX 3).

ARTICLE 5

The present Agreement in no way prevents the Parties from making other Agreements relating to the exchange of classified information originated by them and not affecting the scope of the present Agreement.

ARTICLE 6

(a) This Agreement shall be open for signature by the Parties to the North Atlantic Treaty and shall be subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Government of the United States of America;

(b) This Agreement shall enter into force thirty days after the date of deposit by two signatory States of their instruments of ratification, acceptance or approval. It shall enter into force for each other signatory State thirty days after the deposit of its instrument of ratification, acceptance or approval.

(c) This Agreement shall with respect to the Parties for which it entered into force supersede the "Security Agreement by the Parties to the North Atlantic Treaty Organization" approved by the North Atlantic Council in Annex A (paragraph 1) to Appendix to Enclosure to D.C. 2/7, on 19th April, 1952, and subsequently incorporated in Enclosure "A" (paragraph 1) to C-M(55)15(Final), approved by the North Atlantic Council on 2nd March, 1955.

ARTICLE 7

This Agreement shall remain open for accession by any new Party to the North Atlantic Treaty, in accordance with its own constitutional procedures. Its instrument of accession shall be deposited with the government of the United States of America. It shall enter into force in respect of each acceding State thirty days after the day of the deposit of its instrument of accession.

ARTICLE 8

The Government of the United States of America shall inform the Governments of the other Parties of the deposit of each instrument of ratification, acceptance, approval or accession.

ARTICLE 9

This Agreement may be denounced by written notice of denunciation by any Party given to the depository which shall inform all the other Parties of such notice. Such denunciation shall take effect one year after receipt of notification by the depository, but shall not affect obligations already contracted and the rights or prerogatives previously acquired by the Parties under the provisions of this Agreement.

NATO UNCLASSIFIED

ENCLOSURE "A" to
C-M(2002)49

In witness whereof the undersigned, duly authorized to this effect by their respective Governments, have signed this Agreement.

Done in Brussels, this day of xxxx in a single copy in the English and French languages, each text being equally authoritative, which shall be deposited in the archives of the Government of the United States of America and of which certified copies shall be transmitted by that Government to each of the other signatories.

NATO UNCLASSIFIED

ANNEX 1

This Annex forms an integral part of the Agreement.

NATO classified information is defined as follows:

- (a) information means knowledge that can be communicated in any form;
- (b) classified information means information or material determined to require protection against unauthorized disclosure which has been so designated by security classification;
- (c) the word "material" includes documents and also any item of machinery or equipment or weapons either manufactured or in the process of manufacture;
- (d) the word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

ANNEX 2

This Annex forms an integral part of the Agreement.

For the purposes of the present Agreement, the term "NATO" denotes the North Atlantic Treaty Organization and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organization, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.

NATO UNCLASSIFIED

ENCLOSURE "A" to
C-M(2002)49

ANNEX 3

This Annex forms an integral part of the Agreement.

Consultation takes place with military commanders in order to respect their prerogatives.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "B" to
C-M(2002)49

ENCLOSURE "B"
BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY

INTRODUCTION

1. This C-M establishes the basic principles and minimum standards of security to be applied by NATO nations and NATO civil and military bodies in order to ensure that a common degree of protection is given to classified information exchanged among the parties. NATO security procedures only operate to the best advantage when they are based upon and supported by a national security system having the characteristics set out in this Enclosure. This Enclosure also addresses security responsibilities in NATO.

AIMS AND OBJECTIVES

2. NATO nations and NATO civil and military bodies shall ensure that the basic principles and minimum standards of security set forth in this C-M are applied to safeguard classified information from loss of confidentiality, integrity and availability.

3. NATO nations and NATO civil and military bodies shall establish security programmes that meet these basic principles and minimum standards to ensure a common degree of protection for classified information.

APPLICABILITY

4. These basic principles and minimum standards shall be applied to:
- (a) classified information originated by NATO, originated by a member nation and submitted to NATO or submitted by a member nation to another member nation in support of a NATO programme, project or contract;
 - (b) classified information received by NATO from non-NATO sources; and
 - (c) classified information entrusted to individuals and organisations outside a government (or a NATO civil or military body), e.g., consultants, industry, universities, which shall protect it according to the same standards applied by the government or NATO civil or military body.

NATO UNCLASSIFIED

ENCLOSURE "B" to
C-M(2002)49

5. Access to, and the protection of, ATOMAL information are subject to the Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding Atomic Information – C-M(64)39. The Administrative Arrangements to implement the Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding ATOMAL Information – the current version of C-M(68)41 – shall be applied to control access to, to handle and protect such information.

6. Access to, and protection of, US-SIOP information are subject to the provisions of C-M(71)27(Revised), "Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information within NATO".

7. The sensitive nature of cryptographic information, measures, and products requires the application of stringent security precautions, often beyond those set forth in this C-M. Therefore, access to, and protection of, cryptographic information, measures and products that are nationally- or NAMILCOM-approved, shall be in accordance with Enclosure "F", supporting directives and procedures established by the appropriate authority.

8. The sensitive nature of Signals Intelligence (SIGINT) information, operations, sources and methods require the application of stringent security regulations and procedures often beyond those set forth in this C-M. Therefore, access to and protection of, SIGINT information, operations, sources and methods are subject to national regulations and the provisions laid down in MC 101 (NATO Signals Intelligence Policy) and its companion Allied Joint Publication (AJP).

AUTHORITY

9. The North Atlantic Council (NAC) has approved this document which implements the Agreement Between the Parties to the North Atlantic Treaty for the Security of Information (reproduced at Enclosure "A"), and thereby establishes NATO Security Policy.

BASIC PRINCIPLES

10. The following basic principles shall apply :

- (a) NATO nations and NATO civil and military bodies shall ensure that the agreed minimum standards set forth in this C-M are applied to ensure a common degree of protection for classified information exchanged among the parties;
- (b) classified information shall be disseminated solely on the basis of the principle of need-to-know to individuals who have been briefed on the relevant security procedures; in addition, only security cleared individuals shall have access to information classified CONFIDENTIAL and above;

April 2010
Amdt. n° 8

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "B" to
C-M(2002)49

- (c) security risk management shall be mandatory within NATO civil and military bodies. Its application within NATO nations shall be optional;
 - (d) classified information shall be safeguarded by a balanced set of security measures, including personnel, physical, security of information and INFOSEC, which shall extend to all individuals having access to classified information, all media-carrying information, and to all premises containing such information;
 - (e) NATO Nations and NATO Civil and Military Bodies shall establish Security Awareness and Training Programmes related to all security aspects as described in paragraph 10 (d) above;
 - (f) all suspected breaches of security shall be reported immediately to the appropriate security authority. Reports shall be evaluated by appropriate officials to assess the resulting damage to NATO and to take appropriate action. Enclosure "E" provides details;
 - (g) originators release classified information to NATO and to NATO nations in support of a NATO programme, project or contract on the understanding that it will be managed and protected in accordance with the NATO Information Management Policy (NIMP) and NATO Security Policy;
 - (h) classified information shall be subject to originator control;
 - (i) the release of classified information shall be in accordance with the requirements of Enclosure "E" to this C-M, and supporting directives; and
 - (j) subject to the consent of the originator and in accordance with Enclosure "E" to this C-M, NATO classified information shall only be released to non-NATO nations and organisations that have either signed a Security Agreement with NATO or that have provided a Security Assurance to NATO, either directly or through the NATO nation or NATO civil or military body sponsoring the release. In all cases, a degree of protection, no less stringent than that specified in this C-M, shall be required for any NATO classified information released.
11. The foundations of sound national security are :
- (a) a security organisation responsible for :
 - (i) the collection and recording of intelligence information regarding espionage, terrorist, sabotage and subversive threats; and
 - (ii) the centralisation of such information so that it can be applied to any situation relating to the employment of individuals in government departments and agencies and by contractors; and

April 2010
Amdt. n° 8

NATO UNCLASSIFIED

- (iii) the provision of information and advice to governments on the nature of the threats to security and the means of protection against them; and
- (b) the regular collaboration among government departments and agencies to :
 - (i) identify classified information that needs to be protected; and
 - (ii) establish and apply common degrees of protection as set forth in this C-M.

Personnel Security

12. Personnel security procedures shall be designed to assess whether an individual can, taking into account his loyalty, trustworthiness and reliability, be authorised to have initial and continued access to classified information without constituting an unacceptable risk to security. All individuals, civilian and military, who require access to, or whose duties or functions may afford access to information classified CONFIDENTIAL or above, shall be appropriately cleared and briefed before such access is authorised. Individuals shall only have access to NATO classified information for which they have a need-to-know.

13. A security clearance is not required for access to RESTRICTED information; individuals shall be briefed about their responsibilities for the protection of RESTRICTED information.

14. Personnel security is addressed further at Enclosure "C" of this C-M and in the supporting personnel security directive.

Physical Security

15. Physical security is the application of physical protective measures to sites, buildings or facilities that contain information requiring protection against loss or compromise. Physical security programmes, consisting of active and passive security measures, shall be established to provide levels of physical security consistent with the threat, security classification and quantity of the information to be protected.

16. Physical security is addressed further at Enclosure "D" of this C-M and in the supporting physical security directive.

Security of Information

17. Security of information is the application of general protective measures and procedures to prevent, detect and recover from the loss or compromise of information. Classified information shall be protected throughout its life cycle to a level commensurate with its level of classification. It shall be managed to ensure that it is appropriately classified, is clearly identified as classified and remains classified only as long as this is necessary.

NATO UNCLASSIFIED

ENCLOSURE "B" to
C-M(2002)49

18. Security classifications shall be applied to information to indicate the possible damage to the security of NATO and/or its member nations if the information is subjected to unauthorised disclosure. NATO security classifications shall be applied in accordance with Enclosure "E" to this C-M. It is the prerogative of the originator of the information to determine or modify the security classification.

19. NATO security classifications and their significance are :

- (a) COSMIC TOP SECRET (CTS) – unauthorised disclosure would result in exceptionally grave damage to NATO;
- (b) NATO SECRET (NS) – unauthorised disclosure would result in grave damage to NATO;
- (c) NATO CONFIDENTIAL (NC) – unauthorised disclosure would be damaging to NATO; and
- (d) NATO RESTRICTED (NR) – unauthorised disclosure would be detrimental to the interests or effectiveness of NATO.

20. When classifying information, the originator shall take account of the damage if the information is subjected to unauthorised disclosure, and shall indicate, where possible, whether their information can be downgraded or declassified on a certain date or event.

21. NATO UNCLASSIFIED information – policy and procedures for the management and protection of non-classified information marked NATO UNCLASSIFIED are contained in the NATO Information Management Policy (NIMP).

22. Security of Information is addressed further at Enclosure "E" of this C-M and in the supporting security of information directive.

23. The planning, preparation, execution and support relating to NATO Operations, Training, Exercises, Transformation and Cooperation (OTETC) may require specific additional security aspects to be addressed; the Supporting Document on Information and Intelligence Sharing with Non-NATO Entities (NNEs) contains security provisions and guidance applicable in these circumstances.

INFOSEC

24. INFOSEC is the application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves. In order to achieve the security objectives of confidentiality, integrity and availability for classified information stored, processed or transmitted in communication, information and other electronic systems, a balanced set of security measures (physical, personnel, security of information and INFOSEC) shall be implemented to create a secure environment in which to operate a communication, information or other electronic system.

April 2010
Amdt. n° 8

NATO UNCLASSIFIED

25. INFOSEC is addressed further at Enclosure "F" of this C-M and in supporting INFOSEC Management and INFOSEC Technical and Implementation directives.

Industrial Security

26. Industrial security is the application of protective measures and procedures to prevent, detect and recover from the loss or compromise of classified information handled by industry in contracts. NATO classified information disseminated to industry, generated as a result of a contract with industry, and classified contracts with industry shall be protected in accordance with NATO Security Policy and supporting directives.

27. Before a facility or its employees, managers or owners can have access to classified information or be invited to bid, negotiate or perform on a classified contract or work on a classified study involving access to information classified CONFIDENTIAL or above, the facility shall be granted a facility security clearance issued by the National Security Authority (NSA) (or, if appropriate, the Designated Security Authority (DSA)) of its nation of origin, that is to say, the nation in which the facility is located and incorporated to do business.

28. Facilities shall be required to protect classified information in accordance with the basic principles and minimum standards contained in this C-M. NSAs shall ensure that they have the means to make their industrial security requirements binding upon industry and that they have the right to inspect and approve the measures taken in industry for the protection of classified information.

29. Industrial security is addressed further at Enclosure "G" of this C-M and in the supporting industrial security directive.

PROTECTION OF INFORMATION ON KEY POINTS

30. The publication of information about civilian installations (defence supplies, energy supply, etc.) of military significance in times of tension or war may assist bombing, sabotage or terrorist attack by allowing potential enemies to compile a key points list, and to identify points vulnerable to sabotage or terrorism within individual key points. Policy should be designed to hamper the compilation by potential enemies of a Key Points List, to allow the invocation of security exemptions from publication of relevant data, and to encourage awareness of the risks among installation owners and operators.

SECURITY RESPONSIBILITIES

National Security Authority (NSA)

31. Each member nation shall establish a National Security Authority (NSA) responsible for the security of NATO classified information.

NATO UNCLASSIFIED

ENCLOSURE "B" to
C-M(2002)49

32. The NSA is responsible for :
- (a) the maintenance of security of NATO classified information in national agencies and elements, military or civil, at home or abroad;
 - (b) ensuring that periodic and appropriate inspections are made of security arrangements for the protection of NATO classified information in all national organisations at all levels, both military and civil, to determine that such arrangements are adequate and in accordance with current NATO security regulations. In the case of organisations holding CTS or ATOMAL information, security inspections shall be made at least every 24 months, unless, during that period, they are carried out by the NOS;
 - (c) ensuring that a security determination of eligibility has been made in respect of all nationals who are required to have access to information classified NC and above, in accordance with NATO Security Policy;
 - (d) ensuring that such national emergency security plans as are necessary to prevent NATO classified information from falling into unauthorised or hostile hands have been prepared; and
 - (e) authorising the establishment (or dis-establishment) of national Cosmic Central Registries. The establishment (or dis-establishment) of Cosmic Central Registries shall be notified to the NOS.

Designated Security Authority (DSA)

33. Each member nation may designate one or more DSAs responsible to the NSA. In this case the DSA of a NATO nation is responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some nations, the functions of a DSA may be carried out by the NSA.

NATO Security Committee (NSC)

34. The NSC is established by the NAC and is composed of representatives from each member nation's National Security Authorities (NSAs) supported, where required, by additional member nation security staff. Representatives of the International Military Staff, Strategic Commands and NATO C3 Board shall be present at the meetings of the NSC. Representatives of NATO civil and military bodies may also be present when matters of interest to them are addressed.

35. The NSC is responsible directly to the NAC for :

- (a) reviewing NATO Security Policy (as set forth in C-M(2002)49 and C-M(2002)50) and making recommendations for change / endorsement to the NAC;

April 2010
Amdt. n° 8

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "B" to
C-M(2002)49

- (b) examining questions concerning NATO Security Policy;
- (c) reviewing and approving the supporting directives and guidance documents published by the NSC in the areas of personnel security, physical security, security of information, industrial security and INFOSEC (Note: a nation may request that a supporting directive also be approved by the NAC); and
- (d) considering security matters referred to it by the NAC, a member nation, the Secretary General, the Military Committee, the NATO C3 Board or the heads of NATO civil and military bodies and preparing appropriate recommendations thereon.

NATO Office of Security (NOS)

36. The NOS is established within the NATO International Staff. It is composed of personnel experienced in security matters in both military and civil spheres. The Office maintains close liaison with the NSA of each member nation, and with NATO civil and military bodies. The Office may also, as required, request member nations and NATO civil and military bodies to provide additional security experts to assist it for limited periods of time when full-time additions to the Office would not be justified. The Director, NOS, serves as Chairman to the NSC.

37. The NOS is responsible for :

- (a) the examination of any questions affecting NATO security;
- (b) identifying means whereby NATO security might be improved;
- (c) the overall co-ordination of security for NATO among member nations and NATO civil and military bodies;
- (d) ensuring the implementation of NATO security decisions, including the provision of such advice as may be requested by member nations and NATO civil and military bodies either in their application of the basic principles and the standards of security described in this Enclosure, or in the implementation of the specific security requirements;
- (e) informing, as appropriate, the NSC, the Secretary General and the Chairman of the Military Committee of the state of security within NATO, and the progress made in implementing NAC decisions regarding security;
- (f) carrying out periodic surveys of security systems for the protection of NATO classified information in member nations, NATO civil bodies, and SHAPE and SACT;
- (g) carrying out periodic surveys of security systems for the protection of released NATO classified information in non-NATO nations and international organisations with whom NATO has signed a Security Agreement;

April 2010
Amdt. n° 8

NATO UNCLASSIFIED

- (h) co-ordinating, with NSAs and NATO civil and military bodies, the investigation into cases of lost, compromised or possibly compromised NATO classified information;
- (i) informing NSAs of any adverse information which comes to light concerning their nationals;
- (j) devising security measures for the protection of the NATO Headquarters, Brussels and ensuring their correct implementation; and
- (k) carrying out, under the direction and on behalf of the Secretary General, acting in the name of the NAC and under its authority, responsibilities for supervising the application of the NATO security programme for the protection of ATOMAL information under the provisions of the Agreement and supporting Administrative Arrangements referenced at paragraph 5 above.

NATO Military Committee and NATO Military Bodies

38. As the highest military authority in NATO, the NAMILCOM is responsible for the overall conduct of military affairs. The NAMILCOM is consequently responsible for all security matters within the NATO military structure including centralised overall cognisance of measures necessary to assure the adequacy of cryptographic techniques and materials used for transmitting NATO classified information, including the security approval of NATO funded cryptographic equipment as defined in Enclosure "F". In accordance with previously agreed policy and in compliance with its Terms of Reference in paragraph 36 above, the NOS carries out the executive functions for security within the NATO military structure and keeps the Chairman of the NAMILCOM informed.

39. The Heads of NATO military bodies established under the aegis of the NAMILCOM are responsible for all security matters within their establishment. This includes responsibility for ensuring that a security organisation is set up, that security programmes are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases of organisations holding COSMIC TOP SECRET (CTS) or ATOMAL information, security inspections are to be made at least every 24 months, unless, during that period, an inspection has been carried out by the NOS.

NATO Civil Bodies

40. The NATO International Staff and NATO civil agencies are responsible to the NAC for the maintenance of security within their establishment. This includes responsibility for ensuring that a security organisation is set up, that security programmes are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases of organisations holding COSMIC TOP SECRET (CTS) or ATOMAL information, security inspections are to be made at least every 24 months, unless, during that period, an inspection has been carried out by the NOS.

NATO UNCLASSIFIED

ENCLOSURE "B" to
C-M(2002)49

INFOSEC

41. Principal organisations with responsibilities for INFOSEC (for example, the NC3B, NCSAs and NDAs) are described in Enclosure "F".

SECURITY CO-ORDINATION

42. Any NATO security problem necessitating co-ordination between NSAs of member nations, and NATO civil and military bodies, shall be referred to the NATO Office of Security (NOS). In cases where such reference is by military authorities, this shall be made through command channels. Any unresolved differences arising in the course of such co-ordination shall be submitted by the NOS to the NATO Security Committee (NSC) for consideration.

43. Any proposals by member nations and NATO civil and military bodies involving modification of NATO security procedures shall be referred in the first instance to the NOS. Any proposals made by the military authorities shall be transmitted through command channels. If the NATO security problems giving rise to such proposals cannot be resolved except by modification of NATO Security Policy, the proposals shall be referred to the NSC, and if necessary, by it to the NAC.

ENCLOSURE "C"
PERSONNEL SECURITY

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for personnel security. Amplifying details are found in the supporting directive on personnel security.
2. There shall be an agreed standard of confidence about the loyalty, trustworthiness and reliability of all individuals granted access to, or whose duties or functions may afford access to, NATO classified information. All individuals, civilian and military, whose duties require access to information classified NC and above shall be sufficiently investigated to give a satisfactory level of confidence as to their eligibility for access to such information.
3. Individuals authorised to have access to information classified NC and above shall have been granted an appropriate personnel security clearance (PSC), granted by their NSA or other competent authority, valid for the duration of the authorised access, and have a need-to-know. The extent of security clearance procedures shall be determined by the classification of the NATO information to which the individual is to have access. Security clearance procedures shall be in accordance with NATO security policy and supporting directives.
4. Individuals who require access to information classified NC and above shall have been granted an appropriate personnel security clearance (PSC) , shall have been briefed on NATO security procedures, shall have acknowledged their responsibilities, and shall have a need-to-know. Individuals who require access to only information classified NR shall have been briefed on their security responsibilities, and shall have a need-to-know. Unless specifically required by national security rules and regulations, a security clearance is not required for access to information classified NR.
5. The granting of a PSC should not be considered as a final step in the personnel security process; there is a requirement to ensure an individual's continuing eligibility for access to NATO classified information. This should be achieved through continuous evaluation by security authorities and managers; and through security education and awareness programmes which remind individuals of their security responsibilities and of the need to report, to their managers or security staffs, information which may affect their security status.

APPLICATION OF THE "NEED TO KNOW" PRINCIPLE

6. Individuals in NATO nations and in NATO civil and military bodies shall only have access to NATO classified information for which they have a need-to-know. No individual is entitled solely by virtue of rank or appointment or PSC to have access to NATO classified information.

PERSONNEL SECURITY CLEARANCES (PSCs)

Responsibilities

7. The PSC responsibilities of NSAs, or other competent national authorities, NATO nations and the Heads of a NATO civil or military body are set out in the supporting personnel security directive.

8. Individuals shall be made aware of their responsibilities to comply with security regulations, and act in the interests of security.

Personnel Security Directive

9. The supporting personnel security directive sets out the following :

- (a) the requirements for identifying positions requiring an appropriate PSC;
- (b) the criteria for assessing the loyalty, trustworthiness and reliability of an individual in order for him to be granted and to retain a PSC;
- (c) the investigative requirements for NATO CONFIDENTIAL, NATO SECRET and COSMIC TOP SECRET clearances;
- (d) the requirements for the provision of PSCs for employees of NATO civil and military bodies;
- (e) the requirements for revalidation of PSCs;
- (f) the procedures for addressing adverse information about an individual holding a PSC; and
- (g) the requirements for maintaining records of PSCs granted to individuals.

SECURITY AWARENESS AND BRIEFING OF INDIVIDUALS

10. All individuals employed in positions where they have access to NR information, or hold a clearance for access to NC or above, shall be briefed on security procedures and their security obligations. All cleared individuals shall acknowledge that they fully understand

NATO UNCLASSIFIED

ENCLOSURE "C" to
C-M(2002)49

their responsibilities and the consequences which the law or administrative or executive order of their nation provides when classified information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement shall be maintained by the NATO nation or NATO civil or military body authorising access to NATO classified information.

11. All individuals who are authorised access to, or required to handle NATO classified information, shall initially be made aware, and periodically reminded of the dangers to security arising from indiscreet conversation with persons having no need-to-know, their relationship with the media, and the threat presented by the activities of intelligence services which target NATO and its member nations. Individuals shall be thoroughly briefed on these dangers and must report immediately to the appropriate security authorities any approach or manoeuvre which they consider suspicious or unusual.

AUTHORISING ACCESS TO NATO CLASSIFIED INFORMATION

ACCESS BY NATO NATIONALS

12. An individual shall only be authorised access to NATO classified information after he has been granted the appropriate personnel security clearance, a determination of his need-to-know has been made, and he has been briefed on NATO security procedures and has acknowledged his security obligations.

Exceptional Circumstances

13. However, circumstances may arise when, for example for urgent mission purposes, some of the requirements in paragraph 12 above cannot be met. Details in respect to provisional appointments, one-time access, emergency access, and attendance at conferences and meetings are set out in the supporting personnel security directive.

ACCESS BY NON-NATO NATIONALS

14. Non-NATO nationals serving as integrated members of the Armed Forces of NATO member nations may be authorised access up to and including information classified CTS. In the case of such nationals it shall be incumbent upon the NSA to satisfy itself that the conditions for access stipulated in paragraphs 12 or 13 above are fulfilled.

15. Individuals who are nationals¹ of non-NATO nations may be granted access to NATO classified information on a case-by-case basis, provided that :

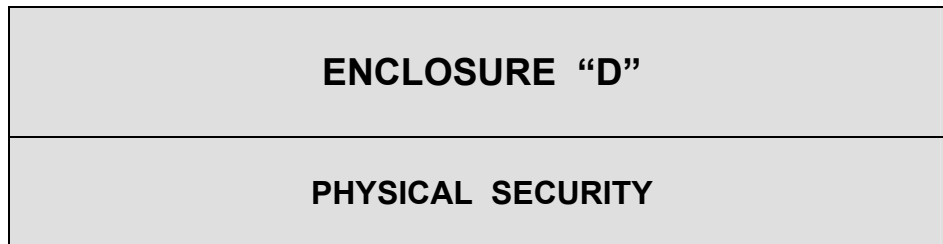
1 Nationals of non-NATO nations includes "nationals of a Kingdom", "citizens of a State", and "landed immigrants in Canada". "Landed immigrants in Canada" are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.

NATO UNCLASSIFIED

ENCLOSURE "C" to
C-M(2002)49

- (a) access is necessary in support of a specified NATO programme, project, contract, operation, or related task;
- (b) the individual is granted a NATO Personnel Security Clearance (PSC) based on a clearance procedure no less rigorous than that required for a NATO national in accordance with NATO security policy and supporting directives; noting that a NATO PSC is not required for access to NR information;
- (c) the prior written consent of the NATO nation or NATO civil or military body that originated the information is obtained; and
- (d) the non-NATO individual in question shall have clearly understood and undertaken, by means of personally undersigning an acknowledgement of responsibilities, that NATO information that he might have access to in the context of a specified NATO programme, project, contract, operation, or related task, shall strictly and solely be used for the purposes of the entrusted task and shall not be shared with or transmitted to third persons, bodies, organisations or governments.

16. As an exception to the requirement for originator control in sub-paragraph 15(c) above, NSAs of NATO nations may approve access to NATO classified information by nationals of certain non-NATO nations who are employed by the Government of the NATO nation, or by a contractor that is located and incorporated in the NATO nation, provided that, in addition to those criteria set out in sub-paragraphs 15(a), 15(b) and 15(d) above, the criteria set out in the equivalent section of the supporting personnel security directive are applied.



INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for physical security measures for the protection of NATO classified information. Amplifying details are found in the supporting directive on physical security.
2. NATO nations and NATO civil and military bodies shall establish physical security programmes that meet these minimum standards. Such programmes, which consist of active and passive security measures, shall provide a common degree of protection consistent with the security classification of the NATO information to be protected.

SECURITY REQUIREMENTS

3. All premises, buildings, offices, rooms, and other areas in which NATO classified information and material is stored and/or handled shall be protected by appropriate physical security measures. In deciding what degree of physical security protection is necessary, account shall be taken of all relevant factors, such as:
 - (a) the level of classification and category of information;
 - (b) the quantity and form of the information (hard copy/computer storage media) held;
 - (c) the security clearance and need-to-know of the staff;
 - (d) the locally-assessed threat from intelligence services which target NATO and/or its member nations, sabotage, terrorist, subversive or other criminal activities; and
 - (e) how the information will be stored.
4. Physical security measures shall be designed to:
 - (a) deny surreptitious or forced entry by an intruder;

- (b) deter, impede and detect actions by disloyal personnel (the spy within);
- (c) allow for segregation of personnel in their access to NATO classified information in accordance with the need-to-know principle; and
- (d) detect and act upon all security breaches as soon as possible.

PHYSICAL SECURITY MEASURES

5. Physical measures represent only one aspect of protective security and shall be supported by sound personnel security, security of information, and INFOSEC measures, details of which will be found respectively in Enclosures "C", "E" and "F". Sensible management of security risks will involve establishing the most efficient and cost-effective methods of countering the threats and compensating for vulnerabilities by a combination of protective measures from these areas. Such efficiency and cost-effectiveness is best achieved by defining physical security requirements as part of the planning and design of facilities, thereby reducing the need for costly renovations.

6. Physical security programmes shall be based on the principle of "defence in depth", and although physical security measures are site-specific, the following general principles shall apply. It is first necessary to identify the locations that require protection. This is followed by the creation of layered security measures to provide "defence in depth" and delaying factors. The outermost physical security measures shall define the protected area and deter unauthorised access. The next level of measures shall detect unauthorised or attempted access and alert the guard force. The innermost level of measures shall sufficiently delay intruders until they can be detained by the guard force. Consequently, there is an interrelationship between the reaction time of the guard force and the physical security measures designed to delay intruders.

7. Regular maintenance of security systems is necessary to ensure that equipments operate at optimum performance. It is also necessary to periodically re-evaluate the effectiveness of individual security measures and the complete security system. This is particularly important if there is a change in use of the site or elements of the security system. This can be achieved by exercising incident response plans.

Security Areas

8. Areas in which information classified NC and above is handled and stored shall be organised and structured so as to correspond to one of the following:

- (a) **NATO Class I Security Area:** an area in which information classified NC and above is handled and stored in such a way that entry into the area constitutes, for all practical purposes, access to classified information. Such an area requires:

- (i) a clearly defined and protected perimeter through which all entry and exit is controlled;
 - (ii) an entry control system which admits only those individuals appropriately cleared and specifically authorised to enter the area;
 - (iii) specification of the level of classification and the category of the information normally held in the area, i.e. the information to which entry gives access;
- (b) **NATO Class II Security Area:** an area in which information classified NC and above is handled and stored in such a way that it can be protected from access by unauthorised individuals by controls established internally. Such an area requires:
- (i) a clearly defined and protected perimeter through which all entry and exit is controlled;
 - (ii) an entry control system which admits unescorted access only to those individuals who are security cleared and specifically authorised to enter the area. For all other individuals, provision shall be made for escorts or equivalent controls, to prevent unauthorised access to NATO classified information and uncontrolled entry to areas subject to technical security inspection.

9. Those areas which are not occupied by duty personnel on a 24-hour basis shall be inspected immediately after normal working hours to ensure that NATO classified information is properly secured.

Administrative Zones

10. An Administrative Zone may be established around or leading up to NATO Class I or Class II security areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified up to and including NR shall be handled and stored in Administrative Zones.

Access to NATO Class II Security Areas by Individuals from Non-NATO Nations / International Organisations

11. Individuals from non-NATO nations / International Organisations who, because of their assignment and official duties, need regular interface with NATO staffs may be granted unescorted access to a NATO Class II Security Area. Such individuals may also be assigned office space within a NATO Class II Security Area in order to fulfil their assignment and official duties. The granting of unescorted access and/or the assignment of office space shall be handled on a case-by-case basis, and shall be in accordance with the criteria set out in the supporting Directive on Physical Security.

Specific Measures

12. The following measures are identified to indicate examples of physical security measures that can be implemented :

- (a) perimeter fence - a perimeter fence will form a useful physical barrier and will identify the boundary of an area requiring security protection. The effectiveness of any security perimeter will depend, to a large extent, on the level of security at the points of access;
- (b) intruder detection system (IDS) – IDS may be used on perimeters to enhance the level of security offered by the fence, or may be used in rooms and buildings in place of, or to assist, guards;
- (c) control of access – control of access may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. The control may be electronic, electro-mechanical, by a guard or receptionist, or physical;
- (d) guards – the employment of appropriately cleared, trained and supervised guards can provide a valuable deterrent to individuals who might plan covert intrusion;
- (e) closed circuit television (CCTV) - CCTV is a valuable aid to security guards in verifying incidents and IDS alarms on large sites or perimeters; and
- (f) security lighting - security lighting can offer a high degree of deterrence to a potential intruder, in addition to providing the illumination necessary for effective surveillance either directly by the guards or indirectly through a CCTV system.

Entry and Exit Searches

13. NATO establishments shall undertake random entry and exit searches which are designed to act as a deterrent to the unauthorised introduction of material into, or the unauthorised removal of NATO classified information from a site or building.

Access Control

14. A pass or personal recognition system governing the regular staff shall control entry into Class I or II security areas. Visitors shall be permitted escorted or unescorted access to a NATO establishment based upon checks on the individual and their access requirements.

MINIMUM STANDARDS FOR THE STORAGE OF NATO CLASSIFIED INFORMATION

15. NATO classified information shall be stored only under conditions designed to deter and detect unauthorised access to the information.

16. **COSMIC TOP SECRET (CTS)**. CTS information shall be stored within a class I or II security area under one of the following conditions :

- (a) in an IDS-equipped vault, or in a nationally-approved security container in an area which is subject to continuous protection or periodic inspection; or
- (b) an IDS-protected open storage area constructed in accordance with the supporting physical security directive.

17. **NATO SECRET (NS)**. NS information shall be stored within a class I or II security area under one of the following conditions :

- (a) in the same manner as prescribed for CTS information; or
- (b) in a nationally-approved security container or vault; or
- (c) an open storage area, which is IDS-protected, or subject to continuous protection or periodic inspection.

18. **NATO CONFIDENTIAL (NC)**. NC information shall be stored in the same manner as prescribed for CTS or NS information except that supplemental controls, as described in the supporting physical security directive, are not required.

19. **NATO RESTRICTED (NR)**. NR information shall be stored in a locked container.

20. Amplifying details for the storage of NATO classified information are set out in the supporting directive on physical security.

PROTECTION AGAINST TECHNICAL ATTACKS

Eavesdropping

21. Offices or areas in which information classified NS and above is regularly discussed shall be protected against passive and active eavesdropping attacks, by means of sound physical security measures and access control, where the risk warrants it. The responsibility for determining the risk shall be coordinated with technical specialists and decided by the appropriate security authority.

Technically Secure Areas

22. Areas to be protected against audio eavesdropping shall be designated as technically secure areas and entry to them shall be specially controlled. Rooms shall be locked and /or guarded in accordance with physical security standards when not occupied and any keys treated as security keys. Such areas shall be subject to regular physical and/or technical inspections in accordance with the requirements of the appropriate security authority, and shall also be undertaken following any unauthorised entry or suspicion of such and entry by external personnel for maintenance work or redecoration.

PHYSICAL SECURITY FOR COMMUNICATION AND INFORMATION SYSTEMS (CIS)

23. Areas in which NATO classified information is presented or handled using information technology, or where potential access to such information is possible, shall be established such that the aggregate requirement for confidentiality, integrity and availability is met. Areas in which CIS are used to display, store, process, or transmit information classified NC and above, or where potential access to such information is possible, shall be established as NATO Class I or Class II security areas or the national equivalent. Areas in which CIS are used to display, store, process or transmit information classified NR, or where potential access to such information is possible, may be established as Administrative Zones.

APPROVED EQUIPMENT

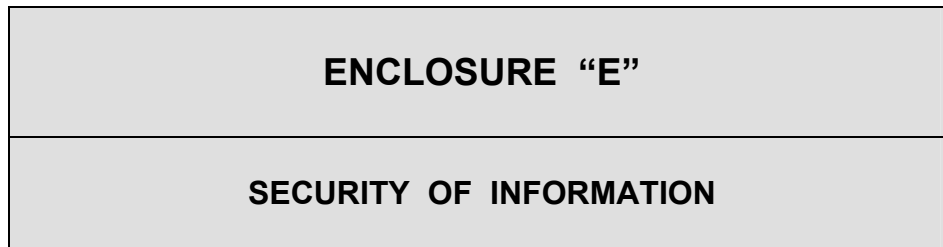
24. NSAs shall maintain lists of equipment which they or other NATO nations have approved for the protection of NATO classified information under various specified circumstances and conditions. NATO civil and military bodies shall ensure that any equipment purchased complies with the regulations of a NATO member nation(s).

OTHER PHYSICAL SECURITY MEASURES

25. Detailed requirements are set out in the supporting physical security directive, addressing, for example, rooms and locks, keys and combinations, and containers and locks.

NATO UNCLASSIFIED

ENCLOSURE "E" to
C-M(2002)49



INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the security of NATO classified information. Amplifying details are found in the supporting security of information directive.
2. NATO classified information requires protection throughout its life-cycle. It shall be managed to ensure that it is appropriately classified, clearly identified as classified information, and remains classified only for as long as this is necessary. Security of information measures shall be complemented by personnel, physical and INFOSEC safeguards to ensure a balanced set of measures for the protection of NATO classified information.

CLASSIFICATION and MARKINGS

General

3. The originator is responsible for determining the security classification and initial dissemination of information. The classification level of NATO information shall not be changed, downgraded or declassified without the consent of the originator. At the time of its creation, originators shall indicate, where possible, whether their information can be downgraded or declassified on a certain date or event.
4. The classification assigned determines the physical security given to the information in storage and transmission, its circulation, destruction and the personnel security clearance required for access. Therefore both over-classification and under-classification should be avoided in the interests of effective security as well as efficiency.
5. NATO nations and NATO civil and military bodies shall introduce measures to ensure that information created by, or provided to NATO is assigned the correct security classification, and protected in accordance with the requirements of the supporting security of information directive.

NATO UNCLASSIFIED

ENCLOSURE "E" to
C-M(2002)49

6. Each NATO civil or military body shall establish a system to ensure that CTS information which it has originated is reviewed no less frequently than every five years to ascertain whether the CTS classification still applies. Such a review is not necessary in those instances where the originator has predetermined that specific CTS information shall be automatically downgraded after two years and the information has been so marked.

7. The overall security classification of a document shall be at least as high as that of its most highly classified component. Component parts of documents classified NC and above shall, where possible, be classified (including by paragraph) by the originator to facilitate decisions on further dissemination of appropriate sections. Covering documents shall be marked with the security classification of the information contained therein when they are separated from the information they accompany.

8. When information from various sources is collated, the product shall be reviewed for overall security classification since it may warrant a higher classification than its component parts. Original security classification caveats must be retained when information is used to prepare composite documents.

Qualifying Markings

9. The terms COSMIC and NATO are qualifying markings which, when applied to classified information, signify that the information shall be protected in accordance with NATO Security Policy.

Special Category Designators

10. The term "ATOMAL" is a marking applied to special category information signifying that the information shall be protected in accordance with the Agreement and supporting Administrative Arrangements referenced in Enclosure "B", paragraph 5.

11. The term "SIOP" is a marking applied to special category information signifying that the information shall be protected in accordance with the reference cited in Enclosure "B", paragraph 6.

12. The term "CRYPTO" is a marking and a special category designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying NATO security-related information; signifying that the information shall be protected in accordance with the appropriate cryptographic security instructions.

13. The term "BOHEMIA" is a marking applied to special category information derived from or pertaining to Communications Intelligence (COMINT). All information marked COSMIC TOP SECRET - BOHEMIA will be protected in strict accordance with MC 101 (NATO Signals Intelligence Policy) and its companion Allied Joint Publication (AJP) which covers doctrinal and procedural issues.

April 2010
Amdt. n° 8

NATO UNCLASSIFIED

Dissemination Limitation Markings

14. As an additional marking to further limit the dissemination of NATO classified information, a Dissemination Limitation Marking may be applied by the originator.

CONTROL AND HANDLING

Objectives of Accountability

15. The primary objective of accountability is to provide sufficient information to be able to investigate a deliberate or accidental compromise of accountable information and assess the damage arising from the compromise. The requirement for accountability serves to impose a discipline on the handling of, and control of access to, accountable information.

16. Subordinate objectives are :

- (a) to keep track of access to accountable information – who has, or potentially has, had access to accountable information; and who has attempted to access accountable information;
- (b) to know the location of accountable information; and
- (c) to keep track of the movement of accountable information within the NATO and national domains.

17. CTS and NS and ATOMAL information shall be accountable, controlled and handled in accordance with the requirements of this Enclosure and the supporting security of information directive. Where required by National rules and regulations, information bearing other classification or special category markings may be considered as accountable information.

The Registry System

18. There shall be a Registry System which is responsible for the receipt, accounting, handling, distribution and destruction of accountable information. Such a responsibility may be fulfilled either within a single registry system, in which case strict compartmentalisation of CTS information shall be maintained at all times, or by establishing separate registries and control points.

19. Each NATO member nation and NATO civil or military body shall establish a Central Registry(s) for CTS, which acts as the main receiving and despatching authority for the nation or body within which it has been established. The Central Registry(s) may also act as a registry(s) for other accountable information.

20. Registries and control points shall act as the responsible organisation for the internal distribution of CTS and NS information and for keeping records of all accountable documents held on that registry's or control point's charge; they may be

NATO UNCLASSIFIED

ENCLOSURE "E" to
C-M(2002)49

established at ministry, department, or command levels. NC and NR information is not required to be processed through the Registry System unless specified by National security rules and regulations.

21. With regard to NATO accountable information, registries and control points shall be able at all times to establish its location. Infrequent and temporary access to such information does not necessarily require the establishment of a registry or control point, provided procedures are in place to ensure that the information remains under the control of the Registry System.

22. The dissemination of information classified CTS shall be through COSMIC registry channels. At least annually, each registry shall carry out an inventory of all information classified CTS for which it is accountable, in accordance with the requirements of the supporting security of information directive. Regardless of the type of registry organisation, those that handle information classified CTS shall appoint a "COSMIC Control Officer" (CCO).

23. The supporting security of information directive sets out, inter alia, the responsibilities of the CCO, the detailed registry system handling processes for CTS and NS information, the procedures for reproductions, translations and extracts, the requirements for the dissemination of transmission of information, and the requirements for the disposal and destruction of information.

24. The NAMILCOM has established a separate system for the accountability, control and distribution of cryptographic material. Material being transferred through this system do not require accountability in the Registry System.

CONTINGENCY PLANNING

25. NATO nations and NATO civil and military bodies shall prepare contingency plans for the protection or destruction, during emergency situations, of NATO classified information to prevent unauthorised access and disclosure and loss of availability. These plans shall give highest priority to the most sensitive, and mission- or time-critical information.

SECURITY INFRACTIONS, BREACHES AND COMPROMISES

26. The protection of NATO classified information depends on the design of appropriate security regulations to give effect to approved security policy, directives and guidance, and on the effective implementation of these regulations by education and supervision backed up by disciplinary and, in extreme cases, legal sanctions.

27. All breaches of security shall be reported immediately to the appropriate security authority. Each reported breach of security shall be investigated by individuals who have security, investigative and, where appropriate, counterintelligence experience, and who are independent of those individuals immediately concerned with the breach.

April 2010
Amdt. n° 8

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "E" to
C-M(2002)49

28. The main purpose of reporting compromises of NATO classified information is to enable the originating NATO component to assess the resulting damage to NATO and to take whatever action is desirable or practicable to minimize the damage. Reports of the damage assessment and minimising action taken shall be forwarded to the NOS.

29. When a compromise of NATO classified information has to be reported to the NOS, the report shall be forwarded through the NSA or the Head of the NATO civil or military body concerned. Where possible, the reporting authority should inform the originating NATO component at the same time as the NOS, but the latter may be requested to do this when the originator is difficult to identify. The timing of the reports depends on the sensitivity of the information and the circumstances.

30. The Secretary General of NATO may request the appropriate authorities to make further investigations and to report.

31. The supporting security of information directive sets out the detailed actions, records and reporting requirements for breaches and compromises of security.

32. Separate provisions relating to the compromise of cryptographic material have been issued by the NAMILCOM to communications security authorities of member nations and NATO civil and military bodies.

SECURITY ARRANGEMENTS FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO NATIONS AND INTERNATIONAL ORGANISATIONS

Introduction

33. Classified information entrusted to or generated by NATO in order to enable it to perform its missions is disseminated and protected in accordance with NATO Security Policy, directives and procedures. This section sets out the policy for the release of NATO classified information to non-NATO nations and international organisations including such nations (hereinafter referred to as non-NATO recipients). This section also covers information contained in documents issued by the NAC, or by any other NATO committee or NATO civil or military body (hereinafter referred to as NATO bodies).

34. The release of NATO classified information to non-NATO recipients shall take place in the context of NATO cooperative activities approved by the NAC. Any request for the release of NATO classified information to non-NATO recipients outside such cooperative activities shall be examined and approved on a case-by-case basis.

35. ATOMAL information of any classification may not be released to any nation/organisation which is not a party to the current versions of C-M(64)39 and C-M(68)41.

April 2010
Amdt. n° 8

NATO UNCLASSIFIED

Principles for Authorising the Release of NATO Classified Information to Non-NATO Nations and International Organisations

36. Authorisation to release shall always be subject to the consent of the originator(s). Additionally, the following shall apply :

- (a) for NATO classified information to be released under NAC-approved NATO cooperative activities, where the non-NATO participants to that activity have been endorsed by the NAC on a case-by-case basis :
 - (i) release decisions can either concern clearly identified information or a general category of information;
 - (ii) the subject matter shall be included in the general work plan or the OPLAN for the activity or in the practical measures established for cooperation;
 - (iii) the release of NATO classified information shall be necessary to initiate cooperation on a specific subject, and to continue cooperation within the approved activity;
 - (iv) a Security Agreement, signed by the Secretary General on behalf of NATO and by a representative duly mandated² by the non-NATO recipient, shall have been concluded. In the absence of a Security Agreement and in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC (for example, in support of force protection, and the exchange of intelligence information), a Security Assurance from the non-NATO recipient, signed by a representative duly mandated¹ by the non-NATO recipient that any information received will be protected in accordance with its national laws and regulations and to a degree no less stringent than NATO minimum standards, shall have been provided to the NATO Office of Security;
 - (v) where a Security Agreement is in force with an international organisation, the release of information to its non-NATO members shall be in accordance with the relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities;
 - (vi) the Security Assurance provided by the non-NATO recipient shall also identify the NATO security classifications and the equivalent security classifications of the non-NATO recipient. The Security Assurance shall be forwarded to the relevant committee responsible

² A "representative duly mandated" is an officially authorised representative who is either the direct recipient of released information or is a senior representative responsible for ensuring the protection of information released in support of a co-operative activity.

NATO UNCLASSIFIED

ENCLOSURE "E" to
C-M(2002)49

for the approval of the release. Copies of the written Security Assurances shall be provided to the NATO Office of Security who shall maintain a database of Security Assurances;

- (vii) only information classified up to and including NC may be released through Security Assurances. However, in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC, NS information may be released; and
 - (viii) where there is a requirement to release NS information to a non-NATO nation which has signed a Security Agreement / Arrangement with a NATO sponsor, the NATO sponsor shall provide the necessary assurance that the appropriate security system is in place for the protection of such released information, and shall seek the agreement of the relevant committee responsible for the approval of the release prior to its release; and
- (b) for NATO classified information to be released on special request from NATO member nations (the Sponsor) to non-NATO recipients outside NAC-approved cooperative activities :
- (i) release decisions shall be taken on a case-by-case basis and can only concern clearly identified information;
 - (ii) a bilateral Security Agreement / Arrangement shall exist between the NATO member nation sponsoring the release and the non-NATO recipient;
 - (iii) the Sponsor shall be responsible for providing a written Security Assurance, signed by a representative duly mandated³ by the non-NATO recipient, to NATO from the non-NATO recipient. The Security Assurance provided by the non-NATO recipient shall oblige the non-NATO recipient to protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement / Arrangement for the protection of the Sponsor's classified information. The NATO security classifications shall be identified with their equivalents to the national classifications cited in the bilateral Security Agreement / Arrangement;

³ A "representative duly mandated" is an officially authorised representative who is either the direct recipient of released information or is a senior representative responsible for ensuring the protection of information released in support of a co-operative activity.

NATO UNCLASSIFIED

ENCLOSURE "E" to
C-M(2002)49

- (iv) the Sponsor shall forward this written Security Assurance to the relevant committee, together with the release request. Copies of written Security Assurances shall also be provided to the NATO Office of Security;
- (v) the request shall demonstrate the advantage which would accrue to NATO. Justifications for release shall be specific, avoiding general statements;
- (vi) where a Security Agreement is in force with an international organisation, the release of information to its non-NATO members shall be in accordance with the relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities; and
- (vii) only information classified up to and including NC may be released through Security Assurances in this case. Where there is a requirement to release NS information to a non-NATO nation which has signed a Security Agreement / Arrangement with a NATO sponsor, the NATO sponsor shall provide the necessary assurance that the appropriate security system is in place for the protection of such released information, and shall seek the agreement of the relevant committee responsible for the approval of the release prior to its release.

Release Authority

37. The NAC is the ultimate authority for the release of NATO classified information to non-NATO recipients. This authority adheres to the principle of originator consent and is delegated, taking into account the principles for authorising the release identified in paragraph 36 above, to :

- (a) the appropriate subject-matter committee for information classified up to and including NS which has been originated by that committee and/or bodies subordinate to it. For NR, the appropriate subject-matter committee may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staffs to that committee;
- (b) the NAMILCOM for information classified up to and including NS which has been originated by the NAMILCOM and/or bodies subordinate to it. For NR, the NAMILCOM may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staffs to the NAMILCOM;
- (c) SACEUR or D/SACEUR for information classified up to and including NS which is identified as being releasable to xFOR, or is classified NATO/xFOR SECRET (mission SECRET), under the following conditions :

April 2010
Amdt. n° 8

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "E" to
C-M(2002)49

- (i) the information is limited to NATO classified information necessary for the effective participation of non-NATO Troop Contributing Nations (NNTCN) in operations and exercises, as approved on a case-by-case by the NAC;
 - (ii) the information to be released is only that NATO classified information originating from within Allied Command Operations (ACO) and is directly related to specific operations and exercises where the participation of non-NATO nations to that activity has also been endorsed by the NAC on a case-by-case basis; and
 - (iii) the ACO Security Authority (SHAPE J2) shall implement an authoritative and auditable process for the release of classified information;
- (d) the Mission Commander for an operation involving non-NATO Troop Contributing Nations, as endorsed by the NAC, for information classified up to and including NS that has already been determined as releasable to the mission (xFOR), under the following conditions :
- (i) the information shall be related specifically to the Mission;
 - (ii) the information shall be limited to tactical information related to an ongoing operation and deemed necessary for the successful conduct of the ongoing operation;
 - (iii) the Mission Security Authority shall implement an authoritative and auditable process for the release of classified information; and
 - (iv) the NOS, in close co-ordination with SHAPE J2, reserves the right to conduct inspections of the security arrangements in place; and
- (e) the NPLO, for NATO classified information originated by and belonging to one or more of the nations participating in the NPLO.

38. Authority for release shall only be delegated to an appropriate subject-matter committee on which the originator(s) is/are represented. If the originator(s) cannot be established, the appropriate subject-matter committee shall assume the responsibility of the originator. Authority for release may be delegated to the lowest committee level best suited to evaluate the importance of the classified information.

39. With the exceptions applying to NR information stated in paragraphs 37(a) and (b) above, delegated release authorities cannot further delegate their powers, although they can entrust subordinate bodies with the implementation of the release decision.

40. NATO civil and military bodies shall keep control records of information classified CONFIDENTIAL and above which they have released to non-NATO recipients. These records shall be subject to inspection by the appropriate NATO security authority (for example, NOS, SHAPE J2).

Administrative Arrangements for the Implementation of a Security Agreement

41. The completion of the administrative arrangements shall be confirmed by a security survey carried out by the NOS of the relevant agencies of the non-NATO recipient. The security survey shall establish the ability of the non-NATO recipient to comply with the provisions of the Security Agreement and with the minimum standards.

42. The NOS shall produce a report of the survey and transmit a copy to the Security Authority of the non-NATO recipient. The original report shall be filed in the NOS and made available, upon request, to NATO member nations. The NATO Security Committee shall be provided with a written summary of the results of the NOS survey. The conclusion drawn from the survey as to the ability of the non-NATO recipient to protect NATO classified information shall be communicated by the NOS to the relevant NATO bodies and to NATO member nations.

43. The NOS shall carry out periodic security surveys, at least once every two years, of the relevant agencies of the non-NATO recipients to ensure that the non-NATO recipient continues to be compliant with the provisions of the Security Agreement and with the minimum standards.

44. Where a Security Assurance has been provided to NATO in respect to the protection of released classified information, an annual re-validation of that Security Assurance shall be provided, as appropriate, in accordance with the assessed continued need to receive information. The NOS shall also assess whether or not it would be more appropriate to negotiate a Security Agreement in lieu of the Security Assurance. The NOS shall keep the record of validated Security Assurances, which shall also comprise the grounds for such re-validation. The NATO member nations, on request, shall be provided with a copy of this record.

Supporting Directive on the Security of Information

45. The supporting security of information directive contains, inter alia, the :

- (a) procedures for the release of NATO classified information to non-NATO recipients;
- (b) specific release procedures for NATO Production and Logistics Organisations (NPLOs), international organisations and Combined Joint Task Forces (CJTFs);

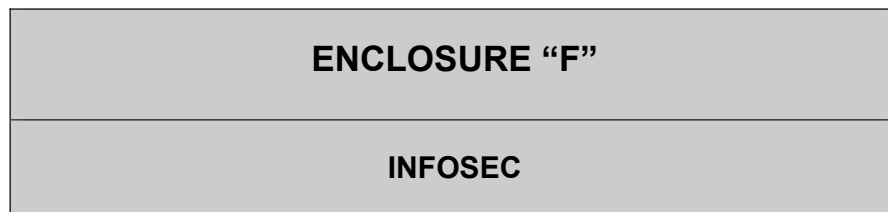
NATO UNCLASSIFIED

ENCLOSURE "E" to
C-M(2002)49

- (c) minimum standards required for the handling and protection of NATO classified information released to non-NATO recipients. The minimum standards apply to any non-NATO recipient, regardless of whether a Security Agreement has been concluded with NATO or a Security Assurance provided to NATO;
- (d) detailed administrative arrangements to be implemented by all non-NATO recipients; and
- (e) samples of the Security Assurance, the Personnel Security Clearance Certificate and the Certificate of Security Clearance.

NATO UNCLASSIFIED

ENCLOSURE "F" to
C-M(2002)49



INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the protection of NATO classified information, and supporting system services and resources¹ in communication, information and other electronic systems (hereafter referred to within this Enclosure as *systems*) storing, processing or transmitting (hereafter referred to within this Enclosure as handling) NATO classified information.

2. The "Primary Directive on INFOSEC", which is published by the NSC and the NC3B in support of this policy, addresses the INFOSEC activities in the *system* life-cycle, and the INFOSEC responsibilities of committees, and NATO civil and military bodies. The "Primary Directive on INFOSEC" is supported by directives addressing INFOSEC management (including security risk management, security approval, security-related documentation, and security review / inspection) and INFOSEC technical and implementation aspects (including computer and local area network (LAN) security, interconnection of networks security, cryptographic security, transmission security, and emission security).

SECURITY OBJECTIVES

3. To achieve adequate security protection of NATO classified information handled in *systems*, a balanced set of security measures (physical, personnel, information and INFOSEC) shall be identified and implemented to create a secure environment in which a *system* operates, and to meet the following security objectives :

- (a) to ensure the confidentiality of information by controlling the disclosure of, and access to, NATO classified information, and supporting system services and resources;
- (b) to ensure the integrity of NATO classified information, and supporting system services and resources; and

¹ Supporting System Services and Resources - those services and resources required to ensure that the security objectives of the *systems* are achieved; to include, for example, cryptographic products and mechanisms, COMSEC materials, directory services, and environmental facilities and controls.

December 2008
Amdt. n°6

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "F" to
C-M(2002)49

- (c) to ensure the availability of NATO classified information, and supporting system services and resources.

4. The integrity and availability of NATO classified information, and of supporting system services and resources, shall be protected by a minimum set of measures aimed at ensuring general protection against commonly encountered problems (whether accidental or intentional) known to affect all *systems* and supporting system services and resources. Additional measures shall be taken, appropriate to the circumstances, where a security risk assessment has established that NATO classified information and/or supporting system services and resources are subject to increased risks from specific threats and vulnerabilities.

5. Independent of the security classification of the NATO information being handled, NATO security authorities shall assess the risks and the level of damage done to NATO if the measures to achieve the non-confidentiality security objectives fail. The minimum set of measures for non-confidentiality shall be determined in accordance with directives supporting this policy.

SECURITY APPROVAL or ACCREDITATION

6. The extent to which the security objectives are to be met, and the extent to which INFOSEC measures are to be relied upon for the protection of NATO classified information and supporting system services and resources shall be determined during the process of establishing the security requirement. The security approval or accreditation process shall determine that an adequate level of protection has been achieved, and is being maintained.

7. All *systems* handling NATO classified information shall be subject to a security approval or accreditation process, addressing the security objectives of confidentiality, integrity and availability.

PERSONNEL SECURITY

8. Individuals authorised access to NATO classified information in any form shall be security cleared, to the appropriate level, taking account of their aggregate responsibility for maintaining the confidentiality, integrity and availability of the information and the supporting system services and resources. This includes individuals who are authorised access to supporting system services and resources, or who are responsible for their protection, even if they are not authorised access to the information handled by the *system*.

PHYSICAL SECURITY

9. Areas in which NATO classified information is presented or handled using information technology, or where potential access to such information is possible, shall be established such that the aggregate requirement for confidentiality, integrity and availability is met.

December 2008
Amdt. n°6

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "F" to
C-M(2002)49

SECURITY of INFORMATION

10. All classified computer storage media shall be properly identified, stored and protected in a manner commensurate with the highest classification of the stored information.

11. NATO classified information recorded on re-usable computer storage media, shall only be erased in accordance with procedures approved by the appropriate security authority.

12. Approved security measures (confidentiality and non-confidentiality), implemented in accordance with directives supporting this policy, may be used to protect NATO classified information in computer storage media in such a manner as to reduce the physical security requirements commensurate with a lower classification level.

ACCOUNTABILITY

13. There shall be a means to provide sufficient information to be able to investigate a deliberate or accidental compromise of the confidentiality of accountable information and, commensurate with the damage that would be caused, a deliberate or accidental compromise of the integrity and/or availability of NATO classified information and supporting system services and resources.

SECURITY MEASURES

14. For all *systems* handling NATO classified information, a consistent set of security measures shall be applied to meet the security objectives, and to protect information and supporting system services and resources. The security measures shall include, where appropriate, the following :

- (a) a means to reliably identify and authenticate persons authorised access. Information and material which controls access to a *system* shall be controlled and protected under arrangements commensurate with the information to which it may give access;
- (b) a means to control disclosure of, and access to, information and supporting system services and resources, based upon the need-to-know principle;
- (c) a means to verify the integrity and origin of information, and supporting system services and resources;
- (d) a means to maintain the integrity of NATO classified information and supporting system services and resources;

December 2008
Amdt. n°6

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "F" to
C-M(2002)49

- (e) a means to maintain the availability of NATO classified information and supporting system services and resources;
- (f) a means to control the connection of *systems* handling NATO classified information;
- (g) a determination of the confidence to be placed in the INFOSEC protection mechanisms;
- (h) a means to assess and verify the proper functioning of the INFOSEC protection mechanisms over the life-cycle of the *system*;
- (i) a means to investigate user and *system* activity;
- (j) a means to provide non-repudiation assurances that the sender of information is provided with proof of delivery and the recipient is provided proof of the sender's identity; and
- (k) a means to protect stored NATO classified information where the physical security measures do not meet the minimum standards.

15. Security management mechanisms and procedures shall be in place to deter, prevent, detect, and recover from, the impacts of incidents affecting the confidentiality, integrity and availability of NATO classified information and supporting system services and resources, including the reporting of security incidents.

16. The security measures shall be managed and implemented in accordance with directives supporting this policy.

SECURITY RISK MANAGEMENT

17. *Systems* handling NATO classified information, in NATO civil and military bodies, shall be subject to security risk assessment and risk management in accordance with the requirements of directives supporting this policy.

ELECTROMAGNETIC TRANSMISSION ² of NATO CLASSIFIED INFORMATION

18. When NATO classified information is transmitted electromagnetically, special measures shall be implemented to protect the confidentiality, integrity and availability of such transmissions. NATO authorities shall determine the requirements for protecting transmissions from detection, interception or exploitation. The information being transmitted

² The term "electromagnetic transmission" covers transmission having both an electrical and magnetic character or properties, and includes, inter alia, visible light, radio waves, microwave, and infrared radiation.

NATO UNCLASSIFIED

ENCLOSURE "F" to
C-M(2002)49

in a communication system shall be protected based upon the requirements for confidentiality, integrity and availability.

19. When cryptographic products or mechanisms are required to provide confidentiality, integrity and availability protection, such products or mechanisms shall be specifically approved for the purpose.

20. During transmission, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

21. During transmission, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms approved by either the NAMILCOM or a NATO member nation.

22. During transmission, the integrity and availability of classified information shall be assured in accordance with the communications system's operational requirement. The evaluation requirements and approval authority, for integrity and availability mechanisms based on cryptography, shall be identified and agreed in conjunction with the specification of such mechanisms in the operational requirement, as agreed in technical directives.

23. Under exceptional operational circumstances, information classified NR, NC and NS may be transmitted in clear text provided each occasion is properly authorised. The exceptional circumstances are as follows :

- (a) during impending or actual crisis, conflict, or war situations; and
- (b) when speed of delivery is of paramount importance, or means of encryption are not available, and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations.

NATO and non-NATO Nations / International Organisations

24. During transmission between NATO and non-NATO nations / International Organisations (NNN/IO) *systems*, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

25. During transmission within NNN/IO *systems*, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

26. Where the requirements of paragraphs 24 and 25 above cannot be met, NATO and an IO may reach agreement on the mutual acceptance of each others' evaluation, selection and approval processes for cryptographic products or mechanisms authorised for

December 2008
Amdt. n°6

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "F" to
C-M(2002)49

the protection in transmission of NS information or IO information of the equivalent classification level. The conditions for such acceptance are set out in paragraph 28 below.

27. In exceptional circumstances, in order to support specific operational requirements, and where the requirements of paragraphs 24 and 25 above cannot be met, NATO may agree the NNN's evaluation, selection and approval processes for cryptographic products or mechanisms authorised for the protection in transmission of NS information or NNN information of the equivalent classification level. The conditions for such agreement are set out in paragraph 28 below.

28. The following conditions are applicable in respect to the scenarios described at paragraphs 26 and 27 above :

- (a) the NNN/IO shall have a Security Agreement with NATO and be certified by the NOS that they can appropriately protect released NATO classified information;
- (b) each NNN/IO shall be treated on a case-by-case basis; and the basis of any acceptance / agreement shall be set out in the security arrangements supporting the Security Agreement between NATO and the NNN/IO;
- (c) the terms of any such acceptance / agreement shall be approved by the NAMILCOM on the basis of an objective assessment carried out by the NATO Office of Security (NOS), working in conjunction with the NAMILCOM Communications and Information Systems Security and Evaluation Agency (SECAN), the NC3B INFOSEC Sub-committee and the NATO HQ C3 Staff (INFOSEC Branch), of the capability of the NNN/IO to perform cryptographic evaluations that meet requirements equivalent to those used within NATO for the cryptographic protection of NS information; and
- (d) the NOS, in conjunction with SECAN and the NATO HQ C3 Staff, shall satisfy themselves, through verification and periodic re-verification, that the NNN/IO has in place appropriate structures, rules and procedures for the evaluation, selection, approval and control of cryptographic products and mechanisms, and that those structures, rules and procedures are being effectively and securely applied in practice.

29. Where acceptance / agreement is reached in accordance with the conditions set out in paragraph 28 above, the confidentiality of information classified NS may be protected by either cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM) or cryptographic products or mechanisms approved by the NCSA (or equivalent authority) of the NNN/IO for the protection of the equivalent classification level.

30. During transmission between NATO and NNN/IO *systems*, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms approved by either the NAMILCOM or a NATO member nation.

December 2008
Amdt. n°6

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "F" to
C-M(2002)49

31. During transmission within NNN/IO *systems*, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms evaluated and approved by an appropriate authority. The appropriate authority may be the NAMILCOM, the NCSA of a NATO member nation or the equivalent authority of the NNN/IO, provided that the NNN/IO has appropriate structures, rules and procedures in place for the evaluation, selection, approval and control of such products or mechanisms, and that those structures, rules and procedures are being effectively and securely applied in practice. The structures, rules and procedures shall be agreed between the NAMILCOM and the NNN/IO.

The SECURITY of CRYPTOGRAPHIC PRODUCTS, MECHANISMS, and INFORMATION

32. The sensitive nature of the cryptographic products, mechanisms and information used to protect the confidentiality, integrity and availability of NATO classified information necessitates the application of special security precautions beyond those required for the protection of other NATO classified information.

33. The protection which shall be afforded to cryptographic products, mechanisms and information shall be commensurate with the damage that may be caused should that protection fail. There shall be positive means to assess and verify the protection and proper functioning of the cryptographic products and mechanisms, and the protection and control of cryptographic information.

34. In recognition of the particular sensitivity of cryptographic information, special regulations and bodies shall exist within NATO and within each member nation to govern the receipt, control and dissemination of NATO cryptographic information to specially certified persons.

35. Special procedures shall also be followed which regulate the sharing of technical information, and which regulate the selection, production and procurement of cryptographic products and mechanisms.

EMISSION SECURITY

36. Security measures shall be implemented to protect against the compromise of information classified NC and above through unintentional electromagnetic emissions. The measures shall be commensurate with the risk of exploitation and the sensitivity of the information.

SPECIFIC INFOSEC RESPONSIBILITIES

NATO Military Committee (NAMILCOM)

37. The NAMILCOM's INFOSEC responsibilities include the security approval of cryptographic equipment and participating in the evaluation and selection of cryptographic products and mechanisms for standard NATO use. The four nationally manned agencies of

December 2008
Amdt. n°6

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "F" to
C-M(2002)49

the Military Committee (SECAN, DACAN, EUSEC and EUDAC) provide INFOSEC advice and support to the NAMILCOM, to the NSC, to the NC3B and, as appropriate, to their sub-committees, to member nations and to other NATO organisations.

NATO C3 Board (NC3B)

38. As the senior Consultation, Command and Control (C3) policy committee within the Alliance, the NC3B supports the NAMILCOM and the NATO political authorities in their validation process for C3 capabilities and projects by reviewing operational C3 requirements. The NC3B is responsible for the provision of secure and interoperable NATO-wide C3 *systems*. Staff support to the NC3B is provided by the NATO HQ C3 Staff (NHQC3S).

National Communications Security Authority (NCSA)

39. Each NATO nation shall identify an NCSA, which may be established as an agency in the national security infrastructure. The primary roles of the NCSA are the following :

- (a) to control cryptographic technical information related to the protection of NATO information within their nation;
- (b) to ensure that cryptographic systems, products and mechanisms for protecting NATO information are effectively and efficiently selected, operated and maintained; and
- (c) to communicate on NATO communications security and related technical INFOSEC matters, both civil and military, with appropriate NATO and national bodies.

40. NCSAs work in co-ordination with their NSA(s).

National Distribution Authority (NDA)

41. Each NATO nation shall identify an NDA, which may be established as an agency in the national security infrastructure, which is responsible for the management of NATO cryptomaterial within their nation and shall ensure that appropriate procedures are enforced and channels established for the comprehensive accounting, secure handling, storage and distribution of all cryptomaterial.

42. NDAs work in co-ordination with their NSA(s).

NATO UNCLASSIFIED

ENCLOSURE "F" to
C-M(2002)49

Security Approval or Accreditation Authority(s)

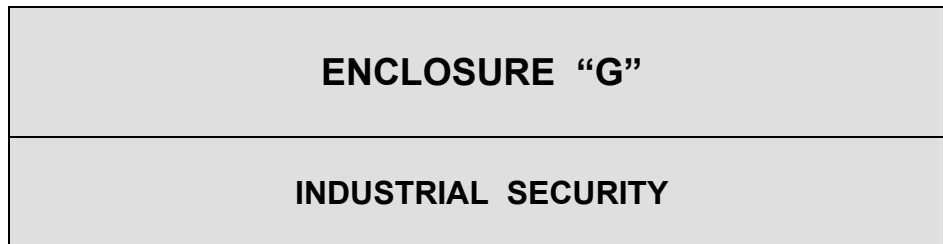
43. Each NATO nation shall identify a security approval or accreditation authority(s) which is responsible for the security approval or accreditation of the following :

- (a) national communication and information systems (CIS) handling NATO classified information; and
- (b) NATO CIS operating within national bodies / organisations.

44. Where a NATO civil or military body is established within a NATO nation, the NATO CIS shall be subject to security accreditation by a NATO SAA (see paragraph 45 below). In this case, the security accreditation may be co-ordinated with the appropriate national security approval or accreditation authority.

NATO Security Accreditation Authority (SAA)

45. NATO HQ and each Strategic Command shall identify a SAA which is responsible for the security approval or accreditation of NATO CIS handling NATO classified information. The SAA shall be the Director, NATO Office of Security or a Strategic Commander, or their delegated / nominated representative(s), dependent upon the CIS to be accredited.



INTRODUCTION

1. This Enclosure deals with security aspects of industrial operations that are unique to the negotiation and letting of NATO classified contracts and their performance by industry, including the release of NATO classified information during pre-contract negotiations. This Enclosure sets out the security policy for :

- (a) the negotiation and the letting of NATO classified contracts;
- (b) the security requirements for NATO classified contracts;
- (c) the release of NATO classified information in contracting;
- (d) Facility Security Clearances (FSCs) for NATO contracts;
- (e) the international transportation of NATO classified material;
- (f) international visits;
- (g) personnel on loan within a NATO project / programme; and
- (h) NATO classified contracts involving non-NATO nations.

2. This Enclosure is supported by an industrial security directive which sets out the detailed requirements and procedures. The directive includes the requirements for the negotiation and letting of NATO classified contracts, the security requirements for NATO classified contracts, National authorities for granting FSCs and PSCs, the authorities for international transport, the authorities for international visits, a list of the various entities that typically are involved in NATO classified contracts, and their responsibilities, and a list of NATO Programmes/Projects, Participating Nations and NATO Agencies.

NEGOTIATION AND LETTING OF NATO CLASSIFIED CONTRACTS

3. The prime contract for a NATO programme/project shall be negotiated and awarded by a NATO Programme / Project Agency / Office (NPA/NPO). A FSC shall be required for all

NATO UNCLASSIFIED

ENCLOSURE "G" to
C-M(2002)49

contractors involved in contracts classified NC and above. For contracts classified NR, a FSC is not required unless specifically required by National security rules and regulations.

4. The NPA/NPO who negotiates the contract shall ensure that, for contracts classified NC and above, contractor representatives involved in the negotiations hold appropriate Personal Security Clearance (PSC), and only receive access to NATO classified information needed for the negotiation of the contract.

5. After a prime contract has been let, a prime contractor may negotiate sub-contracts with other contractors, i.e., sub-contractors. These sub-contractors may also negotiate sub-contracts with other sub-contractors. If a potential sub-contractor is located and incorporated in a non-NATO nation permission to negotiate a sub-contract shall be obtained from the NPA/NPO (c.f. Enclosure "E", paragraphs 29-33). If the NPA/NPO has placed restrictions on the award of contracts to NATO-nations that are not participants in a programme/project, the NPA/NPO shall give permission prior to contract discussion with contractors from those nations.

6. Upon letting the prime contract, the NPA/NPO shall notify the NSA/DSA of the prime contractor, and ensure that the Security Aspect Letter (SAL) and/or the Project Security Instruction (PSI), as applicable, is provided to the prime contractor, with the contract (see paragraphs 8 and 9, below).

SECURITY REQUIREMENTS FOR NATO CLASSIFIED CONTRACTS

7. The prime contractor and sub-contractors shall be contractually required, under penalty of termination of their contract, to take all measures prescribed by the NSAs/DSAs for safeguarding all NATO classified information generated by or entrusted to the contractor, or embodied in articles manufactured by the contractor.

8. NATO classified contracts for Major Programme/Projects shall contain a PSI as an annex; a "Project Security Classification Guide" shall be a part of the PSI. All other NATO classified contracts shall include, as a minimum, a SAL, which may be a PSI that is reduced in scope. In the latter case, the Programme/Project Security Classification Guide may be referred to as a "Security Classification Checklist". The PSI and/or SAL, depending on the scope of the programme/project, shall be the single source document for the programme/project, and shall be used to standardise programme/project security procedures among the participating nations and NATO bodies, and their contractors.

9. The responsibility for applying a security classification to elements of a programme/project dealing with a product wherein all elements are clearly defined and their classification pre-determined, rests with the NPA/NPO of the contract, acting in collaboration with the NSAs/DSAs of the participating NATO nations.

10. The classification for programme/project elements of information associated with possible sub-contracts shall be based on the Programme/Project Security Classification Guide.

December 2006
Amdt. n°3

NATO UNCLASSIFIED

RELEASE OF NATO CLASSIFIED INFORMATION IN CONTRACTING

11. The release of NATO classified information shall be with the consent of the originator and in accordance with other applicable enclosures to the NATO Security Policy and the supporting industrial security directive.

INDUSTRIAL SECURITY CLEARANCES FOR NATO CONTRACTS

General

12. The policy described in subsequent paragraphs for facilities and individuals apply to contracts or sub-contracts.

Facility Security Clearances (FSC)

13. The NSA/DSA of each NATO nation is responsible for ensuring that any facility located and incorporated in that nation which will require access to information classified NC and above in order to enter into pre-contractual negotiations or bid on a NATO classified contract, has adopted the protective security measures necessary to qualify for a FSC. Moreover, the facility's employees who require access to NATO classified information shall have been properly cleared and briefed before furnishing a Facility Security Clearance Certificate (FSCC). The clearances shall be based upon the classification level of the information, its volume and nature, and the number of individuals who will require access to it in the course of preparing bids or negotiations.

14. A contractor may participate in pre-contractual negotiations, bid on, or perform on a NATO classified contract provided the NSA/DSA of the nation in which the contractor is located and incorporated to do business has given the contractor facility the requisite level of FSC.

15. The assessment to be made prior to issuing a FSC shall be in accordance with the requirements and criteria set out in the supporting industrial security directive.

16. Lack of a FSC, or PSCs for facility employees, shall not prevent the contractor bidding for a contract or sub-contract classified NR. A nation which, under its National security rules and regulations, requires a FSC for a contract or sub-contract classified NR shall not discriminate against a contractor from a nation not requiring a FSC, but shall ensure that the contractor has been informed of its responsibilities in respect to the protection of the information, and obtains an acknowledgement of those responsibilities.

Personnel Security Clearances for Facility Employees

17. The issuing of PSCs shall be in accordance with Enclosure "C", Personnel Security, to NATO Security Policy, and the supporting personnel and industrial security directives.

18. Applications for the security clearance for employees of contractor facilities shall be made to the NSA/DSA which is responsible for the facility. In submitting the request for verification or initiation of a PSC, the facility shall include :

- (a) the identity and security classification of the NATO contract or sub-contract; and
- (b) the level of NATO classified information to which the employee will have access.

19. If a facility wishes to employ a national of a non-NATO nation in a position that requires access to NATO classified information, it is the responsibility of the NSA/DSA of the nation in which the hiring facility is located and incorporated, to carry out the security clearance procedure prescribed herein, and determine that the individual can be granted access in accordance with the requirements of Enclosure "C" and the supporting personnel and industrial security directives.

INTERNATIONAL TRANSPORTATION OF NATO CLASSIFIED MATERIAL

Security Principles Applicable to all Forms of Transportation

20. The following principles shall be enforced when examining proposed security arrangements for the international transportation of consignments of classified material:

- (a) security shall be assured at all stages during the transportation and under all circumstances, from the point of origin to the ultimate destination;
- (b) the degree of protection accorded to a consignment shall be determined by the highest classification level of material contained within it;
- (c) an FSC shall be obtained, where appropriate, for companies providing transportation. In such cases, personnel handling the consignment shall be cleared in compliance with the provisions of this Enclosure;
- (d) journeys shall be point-to-point to the extent possible, and shall be completed as quickly as circumstances permit; and
- (e) care shall be exercised to arrange routes only through NATO nations. Routes through non-NATO nations should only be undertaken when authorised by the NSA/DSA of the consignor's nation of origin and in accordance with the supporting security of information directive.

21. Arrangements for consignments of classified material shall be stipulated for each programme/project. However, such arrangements shall ensure that there is no likelihood of unauthorized access to classified material.

22. The security standards for the international transportation of NATO classified material can be found in the supporting security of information directive. The detailed requirements for the hand carriage of NATO classified material, the transportation of classified material by commercial carriers as freight, security guards and escorts, and the transportation of explosives, propellants or other dangerous substances are set out in the supporting industrial security directive.

INTERNATIONAL VISITS

General

23. The arrangements described in this section relate to international visits by military and civilian representatives of NATO nations, NATO civil and military bodies, and NATO contractors and sub-contractors who need to visit the following locations on approved NATO-related activities :

- (a) a government department or establishment of another NATO member nation;
- (b) the facility of a contractor or sub-contractor of another NATO member nation; or
- (c) a NATO civil or military body.

24. Visits referred to in paragraph 23 (a) and (b) above shall be approved by the NSA/DSA of the member nation in which the visit(s) will occur, taking into consideration the following :

- (a) the visit has an official purpose related to a NATO programme or project; and
- (b) all visitors hold an appropriate PSC and have a need-to-know for the information related to the NATO Project or Programme or activity.

25. Government departments and establishments, contractors and sub-contractors, and NATO civil and military bodies receiving visitors shall ensure that :

- (a) visits meet the requirements of paragraph 24 above;
- (b) visitors are given access only to NATO classified information related to the purpose of the visit; and
- (c) records are kept of all visitors, including their name, the organisation they represent, the date(s) of the visit(s) and the name(s) of the person(s) visited. Such records are to be retained in accordance with national requirements.

NATO UNCLASSIFIED

ENCLOSURE "G" to
C-M(2002)49

26. Government departments and establishments and contractors and sub-contractors which intend to send personnel on international visits, shall submit to the NSA/DSA of the facility to be visited, through their NSA/DSA or the agreed official channels, an international visit request in accordance with the procedures set out in the industrial security directive. The international visit request shall provide an assurance that each visitor holds a valid personnel security clearance, as appropriate.

27. Where permitted by National security rules and regulations, NR and NU visits may be arranged directly between the Security Office for the visitor and the Security Office of the facility to be visited.

PERSONNEL ON LOAN WITHIN A NATO PROJECT/ PROGRAMME

28. When an individual who has been cleared for access to NATO classified information is to be loaned from one facility to another in the same NATO programme/project, but in a different NATO nation, the individual's parent facility shall request its NSA/DSA to provide a NATO Personnel Security Clearance Certificate for the individual to the NSA/DSA of the facility to which he is to be loaned. The individual on loan shall be assigned using the international visit request procedures set out in the industrial security directive, and in accordance with National security rules and regulations.

NATO CLASSIFIED CONTRACTS INVOLVING NON-NATO NATIONS

29. The policy described in subsequent paragraphs applies to the following scenarios involving NATO classified contracts / sub-contracts :

- (a) a NATO body negotiating with, or awarding to, industry which is located and incorporated in a non-NATO nation;
- (b) a contractor in a NATO nation negotiating with, or awarding to, industry which is located and incorporated in a non-NATO nation;
- (c) a contractor in a non-NATO nation negotiating with, or awarding to, industry which is located and incorporated in a NATO nation;
- (d) a contractor in a non-NATO nation negotiating with, or awarding to, industry which is located and incorporated in the same or another non-NATO nation;
- (e) a contractor in a non-NATO nation negotiating with, or awarding to, a NATO body.

30. NATO contracts / sub-contracts classified NC and above shall only be negotiated with, or awarded to, industry which is located and incorporated in :

December 2006
Amdt. n°3

NATO UNCLASSIFIED

NATO UNCLASSIFIED

ENCLOSURE "G" to
C-M(2002)49

- (a) a NATO nation; or
- (b) in a non-NATO nation that has signed a Security Agreement with NATO; or
- (c) in a non-NATO nation with whom the contracting NATO nation has a bilateral Security Agreement / Arrangement (see paragraph 32 below).

31. NATO contracts / sub-contracts classified NR shall only be negotiated with, or awarded to, industry which is located and incorporated in :

- (a) a NATO nation; or
- (b) in a non-NATO nation that has signed a Security Agreement with NATO; or
- (c) in a non-NATO nation with whom the contracting NATO nation has a bilateral Security Agreement / Arrangement (see paragraph 32 below); or
- (d) in a non-NATO nation that has provided a Security Assurance to NATO (either directly or through a NATO nation or the NATO Programme / Project Agency / Office (NPA/NPO)).

32. In the case of a bilateral Security Agreement / Arrangement (see paragraphs 30(c) and 31(c) above), in accordance with the requirements of Enclosure "E" to this C-M, the NATO nation shall provide a written assurance to NATO based upon a separate exchange of letters of understanding agreed between the NATO nation and the non-NATO nation requiring the latter to protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement / Arrangement. This understanding shall identify the NATO security classifications as equivalents to the national classifications on which the bilateral Security Agreement / Arrangement is based; and identify that NATO classified information shall not be transferred to a third party without the prior approval of the originator of the information.

33. For non-NATO nations, an appropriate security authority(s) shall be identified that fulfils the equivalent functions of the NSA/DSA in a NATO nation.

Negotiation and Letting of NATO Classified Contracts

34. This subject is addressed by paragraphs 3 to 6 of this Enclosure. All aspects of that section are applicable to the negotiation and letting of NATO classified contracts / sub-contracts involving non-NATO nations, with the following clarifications :

- (a) for contracts / sub-contracts classified NR, a FSC is not required unless specifically required under the security rules and regulations of the NATO parent nation or of the non-NATO parent nation of the contractor / sub-contractor performing the contract; and

*December 2006
Amdt. n°3*

NATO UNCLASSIFIED

- (b) contractor representatives from non-NATO nations shall hold an appropriate PSC, and shall only receive access to NATO classified information authorised for release and needed for the negotiation of the contract / sub-contract.

Security Requirements for NATO Classified Contracts

35. This subject is addressed by paragraphs 7 to 10 of this Enclosure. All aspects of that section are applicable to the security requirements for NATO classified contracts / sub-contracts involving non-NATO nations.

Release of NATO Classified Information in Contracting

36. The release to non-NATO nations of NATO classified information in contracting shall be subject to the requirements of NATO Security Policy and supporting directives, specifically the Directive on the Security of Information.

Industrial Security Clearances for NATO Contracts

37. This subject is addressed by paragraphs 12 to 19 of this Enclosure. All aspects of that section are applicable to industrial security clearances for NATO classified contracts / sub-contracts involving non-NATO nations, with the following clarifications :

- (a) the appropriate security authority from the non-NATO nation is responsible for providing the appropriate FSCs; and
- (b) the appropriate security authority from the non-NATO nation is responsible for issuing the appropriate PSCs .

International Transportation of NATO Classified Material

38. This subject is addressed by paragraphs 20 to 22 of this Enclosure. All aspects of that section are applicable to the international transportation of NATO classified material, noting that routes may originate from non-NATO nations and thus be authorised by the appropriate security authority of the non-NATO nation.

International Visits

39. This subject is addressed by paragraphs 23 to 27 of this Enclosure. All aspects of that section are applicable to international visits by individuals of non-NATO nations in support of NATO classified contracts involving non-NATO nations. The individuals may be from the following :

- (a) a government department or establishment of a non-NATO nation; or
- (b) the facility of a contractor or sub-contractor of a non-NATO nation.

Personnel on Loan Within a NATO Project / Programme

40. This subject is addressed by paragraph 28 of this Enclosure. All aspects of that section are applicable to personnel on loan within a NATO project / programme, with the following clarifications :

- (a) where an individual is to be loaned to a facility in a non-NATO nation, the individual's parent facility shall request its security authority to provide the appropriate PSC to the appropriate security authority of the non-NATO nation; and
- (b) where an individual from a non-NATO nation is to be loaned to a facility in a NATO nation, the individual's parent facility shall request its security authority to provide the appropriate PSC to the NSA/DSA of the facility to which he is to be loaned.

GLOSSARY

Accountable Information	All information classified CTS and NS and all Special Category Information (such as ATOMAL)
Availability	The property of information and material being accessible and usable upon demand by an authorised individual or entity
Breach of security	An act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives, that results in the actual or possible compromise of NATO classified information or supporting services and resources (including, for example, classified information lost while being transported; classified information left in an unsecured area where uncleared persons have unescorted access; an accountable document cannot be found; classified information has been subjected to unauthorised modification; destroyed in an unauthorised manner or, for CIS, there is a denial of service)
Classified Information	Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorised disclosure and which has been so designated by a security classification
Competent Authority	An authority identified by the NSA of a NATO nation which is authorised to carry out personnel security clearances in order to give their nationals access to NATO classified information
Compromise	Compromise denotes a situation when – due to a breach of security or adverse activity (such as espionage, acts of terrorism, sabotage or theft) - NATO classified information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorised individuals (e.g. through espionage or to the media) unauthorised modification, destruction in an unauthorised manner, or denial of service
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or entities

NATO UNCLASSIFIED

GLOSSARY to
C-M(2002)49

Consignee	The contractor, facility or other organisation receiving material from the consignor
Consignor	The contractor, facility or other organisation responsible for organising and dispatching material
Contract	A legally enforceable agreement to provide goods or services
Contractor	An industrial, commercial or other entity that agrees to provide goods or services
Courier	A person officially assigned to hand-carry material
Designated Security Authority (DSA)	An authority responsible to the National Security Authority (NSA) of a NATO nation which is responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some countries, the function of a DSA may be carried out by the NSA
Document	Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media
Escorts	Armed or unarmed national police, military, or other government personnel. Their function is to facilitate the secure movement of the material, but they do not have direct responsibility in matters of the protection of the material itself
Facility	An installation, plant, factory, laboratory, office, university or other educational institution, or commercial undertaking, including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity

NATO UNCLASSIFIED

GLOSSARY to
C-M(2002)49

Facility Security Clearance (FSC)	An administrative determination by a NSA/DSA that, from a security viewpoint, a facility can afford adequate security protection to NATO classified information of a specified classification or below, and its personnel who require access to NATO classified information have been properly cleared and briefed on NATO security requirements necessary to perform on the NATO classified contracts
Guards	Civilian (Government or participating contractor employees) or military personnel who may be armed or unarmed. They may be assigned for security guard duties only or may combine security guard duties with other duties
Host Nation	<u>General</u> : the nation in which a NATO civil or military body is located. <u>Industrial security</u> : the nation designated by an official body of NATO to act as the governmental agency to contract for the performance of a NATO prime contract. Nations in which sub-contracts are performed are not referred to as host nations
Information	Knowledge that can be communicated in any form
INFOSEC	The application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves. Notes. 1. INFOSEC measures include those of computer, transmission, emission and cryptographic security. 2. Such measures also include detection, documentation and countering of threats to information and to the systems.
Infraction	A security infraction is an act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives that does not result in the actual or possible compromise of NATO classified information. (e.g. classified information left unsecured inside a secure facility where all persons are appropriately cleared, failure to double wrap classified information, etc.)

NATO UNCLASSIFIED

GLOSSARY to
C-M(2002)49

Integrity	The property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner
International Visits	Visits made by individuals subject to one NSA/DSA or belonging to a NATO body, to facilities or bodies subject to another NSA/DSA or to NATO, which will require, or may give rise to access to NATO classified information or where, regardless of the level of classification involved, national legislation governing the establishment or body to be visited in support of NATO approved related activities requires that such visits shall be approved by the relevant NSA/DSA. All NATO civil and military bodies fall within the security jurisdiction of NATO
Life-cycle	Life cycle of information encompasses the stages of planning, collection, creation or generation of information; its organisation, retrieval, use, accessibility and transmission; its storage and protection; and, finally, its disposition through transfer to archives or destruction
Major Programme/Project	A programme or project of major significance, normally involving more than two nations and security measures that extend beyond the normal basic requirements described in NATO Security Policy
Material	Material includes documents and also any items of machinery, equipment/components, weapons or tools, either manufactured or in the process of manufacture
Nationals	Nationals includes "nationals of a Kingdom", "citizens of a State", and "landed immigrants in Canada". "Landed immigrants in Canada" are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.
National Security Authority (NSA)	An authority of a NATO nation which is responsible for the maintenance of security of NATO classified information in national agencies and elements, military or civil, at home or abroad

NATO UNCLASSIFIED

GLOSSARY to
C-M(2002)49

NATO	"NATO" denotes the North Atlantic Treaty Organisation and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organisation, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952
NATO Classified Contract	Any contract issued by a NATO civil or military body or a NATO member nation in support of a NATO funded or administered programme/project that will require access to or generate NATO classified information
NATO Classified Information	<p>(a) information means knowledge that can be communicated in any form</p> <p>(b) classified information means information or material determined to require protection against unauthorised disclosure which has been so designated by a security classification</p> <p>(c) the word "material" includes documents and also any items of machinery or equipment or weapons either manufactured or in the process of manufacture</p> <p>(d) the word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media</p>
NATO Military Committee (NAMILCOM)	The highest military authority in NATO; the NAMILCOM is responsible for the overall conduct of military affairs. The NAMILCOM is responsible for endorsing and prioritising from an operational point of view the users' requirements submitted by Strategic Commanders.
NATO Personnel Security Clearance	A determination that an individual is eligible to have access to NATO classified information

NATO UNCLASSIFIED

GLOSSARY to
C-M(2002)49

NATO Production and Logistics Organisation (NPLO)	A subsidiary body, created within the framework of NATO for the implementation of tasks arising from that Treaty, to which North Atlantic Council grants clearly defined organisational, administrative and financial independence. It shall be comprised of a board of directors; and an executive body, composed of a General Manager and staff
NATO Programme	A Council approved programme that is administered by a NATO management /office under NATO regulations
NATO Project	A Council approved project that is administered by a NATO management agency/office under NATO regulations
NATO Project Management Agency	The executive body of a NPLO
Need-to-know	See under "Principle of Need-to-know"
Negotiations	The term encompasses all aspects of awarding a contract or sub-contract from the initial "notification of intention to call for bids" to the final decision to let a contract or sub-contract
Open Storage Area	An area, constructed in accordance with security requirements and authorized by the head of the civil or military body for open storage of classified information
Originator	The nation or international organisation under whose authority information has been produced or introduced into NATO
Parent Nation	The Kingdom of which an individual is a national, or the state of which an individual is a citizen
Parent National Security Authority (NSA)	The NSA of the Kingdom of which an individual is a national, or the state of which an individual is a citizen
Personnel Security Clearance (PSC)	A determination that an individual is eligible to have access to classified information
Prime Contract	The initial contract led by a NATO Project Management / Agency / Office for a Programme/project
Prime Contractor	An industrial, commercial or other entity of a member nation which has contracted with a NATO Project Management Agency/Office to perform a service, or manufacture a product, in the framework of a NATO project, and which, in turn, may subcontract with potential sub-contractors as approved

Principle of Need-to-know	The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services
Programme/Project Security Classification Guide	Part of the program (project) security instructions (PSI) which identifies the elements of the program that are classified, specifying the security classification levels. The security classification guide may be expanded throughout the program life cycle, and the elements of information may be re-classified or downgraded
Programme/Project Security Instruction (PSI)	A compilation of security regulations/procedures, based upon NATO Security Policy and supporting directives, which are applied to a specific project/programme in order to standardise security procedures. The PSI also constitutes an Annex to the main contract, and may be revised throughout the program lifecycle. For sub-contracts let within the program, the PSI constitutes the basis for the SAL
Risk	The likelihood of a vulnerability being successfully exploited by a threat, leading to a compromise of confidentiality, integrity and/or availability and damage being sustained.
Risk management	A systematic approach to determining which security counter-measures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.
Security Aspects Letter (SAL)	A document, issued by the appropriate authority, as part of any NATO classified contract or sub-contract, other than Major Programmes/Projects, identifying the security requirements or those elements thereof requiring security protection
Security Assurance	A guarantee provided to NATO either directly or through a NATO nation or NATO civil or military body sponsoring release, that a non-NATO recipient of NATO classified information will provide the same degree of protection to it as required by NATO Security Policy

Security Classification Check List	Part of a security aspect letter (SAL) which describes the elements of a contract that are classified, specifying the security classification levels. In case of contracts let within a program/project, such elements of information derive from the programme (project) security instructions issued for that programme
Special Category Information	Information such as ATOMAL or Single Integrated Operational Plan (SIOP) to which additional handling/protection procedures are applied
Sub-contract	A contract entered into by a prime contractor with another contractor (i.e., the sub-contractor) for the furnishing of goods or services
Sub-contractor	A contractor to whom a prime contractor lets a sub-contract
Threat	The potential for compromise, loss or theft of NATO classified information or supporting services and resources. A threat may be defined by its source, motivation or result, it may be deliberate or accidental, violent or surreptitious, external or internal
Vulnerability	A weakness, an attribute, or lack of control that would allow or facilitate a threat actuation against NATO classified information or supporting services and resources

NATO UNCLASSIFIED

14 December 2018

DOCUMENT
C-M(2015)0041-REV2
Silence procedure ends:
20 Dec 2018 17:30

ALLIANCE CONSULTATION, COMMAND, AND CONTROL POLICY

Note by the Secretary General

1. The Alliance Consultation, Command, and Control (C3) Policy, is a fundamental mechanism to ensure the Alliance's Core Tasks are implemented coherently with the delivery of interoperable and modern C3 Capabilities and Information, and Communication Technology Services.
2. The C3 Board, in consultation with the relevant senior Committees, is now recommending Council approval of a new revision of that document, which contains three new policies on Green IT, Internet Protocol v6 and Data Management (Annex 11 to 13) and minor updates to extant policies, including a harmonised naming convention.
3. In addition, the C3 Board agreed to render the Alliance C3 Policy releasable to the public.
4. I do not believe this issue requires further discussion. Therefore, **unless I hear to the contrary by 17:30 hours on Thursday, 20 December 2018**, I shall assume that the Council has approved the attached revision of the Alliance C3 Policy.

(Signed) Jens Stoltenberg

- Annex 1: C3 Policy Glossary
- Annex 2: Information and Communications Technology Service Management Policy
- Annex 3: C3 Capabilities and ICT Services Lifecycle Management Policy
- Annex 4: Waveform Policy
- Annex 5: C3 Interoperability Policy
- Annex 6: Federation of Communication Services Policy
- Annex 7: Software Policy
- Annex 8: C3 Capabilities Implementation Policy
- Annex 9: Enterprise Architecture Policy
- Annex 10: Cloud Computing Policy
- Annex 11: Green IT Policy
- Annex 12: Internet Protocol Version 6 (IPV6) Policy
- Annex 13: Data Management Policy

Original: English

NATO UNCLASSIFIED

-1-



C3 POLICY GLOSSARY

#	Term	DEFINITION
1	Access	The right, opportunity, and/or means of finding, using, or retrieving information in all types of media over time.
2	Adoption	The use of an existing application that is owned and operated by NATO or one of the NATO nations. It involves the installation, configuration and maintenance of an instance of the application or service being adopted. Adoption differs from use of a service in that it refers to installing a tangible instance of the adopted application whereas use of a service does not. There are two types of adoption: Adoption from NATO and Adoption from an Allied Nation.
3	Adoption from an Allied Nation	The adoption of an application that is owned and operated by an Allied Nation. Adoptions from Allied Nations' are less likely to be low risk than adoptions from within NATO. These adoptions are more likely to run into Intellectual Property Rights (IPR), export control issues, requirement infusion and other life cycle management issues.
4	Adoption from NATO	The use of an existing application that is already owned, tested, accredited and operated by a NATO entity. Such an adoption will be considered relatively low risk since it will have been accredited and tested previously by a NATO organization. The adopting organization will need to work with the owning organization to ensure IPR and Export controls allow for the adoption of the application or service and that the proper licenses are purchased.
5	Application Architecture	Set of artefacts providing a blueprint for the individual application systems to be deployed, the information which they provide, the interactions between the application systems and their relationships to the core business processes of the organization with the frameworks for services to be exposed as business functions for integration.
6	Architecture	The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution. Architecture is a consistent whole of principles, methods and models that are used in the design and realisation of organisational structure, business processes, information systems, and infrastructure. Source: C-(2008)0113(INV)

#	Term	DEFINITION
7	Architecture Processes	The activities of designing and maintaining a representation (i.e. blueprint) of components of a business (i.e. organisation, processes, information, technology) and their relationships in order to understand where, when and why information is required.
8	Architectures at the Capability Level	Architecture content that supports the delivery of large, multi-phased and multi-project change initiatives (e.g. capability packages).
9	Architectures at the NATO Enterprise Level	Architecture content that forms the foundation for architectural coherence across the entire NATO Enterprise, and beyond.
10	Architectures at the Project Level	The description of the envisioned solution that the project aims to implement.
11	Authentication	<p>1. (in CIS security) The reliable identification and authentication of persons, devices and services accessing CIS handling NATO classified information.</p> <p>2. (in records management) The implementation of recordkeeping procedures that control the creation, receipt, transmission, maintenance, management and use of documents, and that prove that the document is official and protected against unauthorised addition, destruction, deletion, alteration, use or concealment.</p> <p>3. The act of verifying the claimed identity of an entity.</p>
12	Availability	The property of information and material being accessible and usable upon demand by an authorised individual or entity.
13	Binding	A relationship between a data object and its metadata, such as the confidentiality metadata label, that provides an appropriate level of assurance of the integrity of the association between the data object and the metadata.
14	Broad Network Access	<p>Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).</p> <p>Source: "The NIST Definition of Cloud Computing", Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.</p>
15	Business Architecture	Set of artefacts defining the business strategy, management, organization, and key business processes (including process ownership and key decisions) of the organization.
16	Buy	<p>The purchasing of "Commercial Off The Shelf" (COTS) products as solutions to C3 requirements.</p> <p>The COTS products must be offered by industries of a NATO member nation.</p>

#	Term	DEFINITION
17	Categorisation	<p>The process of understanding and differentiating information. Categorisation implies that information is grouped into categories, usually for a specific purpose.</p> <p>Source: C-(2008)0113(INV)</p>
18	Cloud Computing	<p>A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimum management effort or service provider interaction.</p> <p>This cloud model is composed of five essential characteristics, three service models and four deployment models: Characteristics: On-demand self-service; Broad network access; Resource pooling; Rapid elasticity; Measures service. Service Models: Software as a Service (SaaS); Platform as a Service (PaaS); Infrastructure as a Service (IaaS). Deployment Models: Private Cloud; Community Cloud; Public Cloud; Hybrid Cloud.</p> <p>Source: “The NIST Definition of Cloud Computing”, Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.</p>
19	Cloud Infrastructure	<p>The collection of hardware and software that enables the five essential characteristics of cloud computing.</p> <p>The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer.</p> <p>The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components.</p> <p>The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.</p> <p>Source: “The NIST Definition of Cloud Computing”, Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.</p>
20	Communications and Information Systems (CIS)	<p>Collective term for communications systems and information systems. An assembly of equipment, methods and procedures and, if necessary, personnel, organized to accomplish information transfer and processing functions.</p> <p>Source: AAP-6</p>

#	Term	DEFINITION
21	Community Cloud	<p>The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).</p> <p>It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.</p> <p>Source: “The NIST Definition of Cloud Computing”, Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.</p>
22	Community Of Interest (COI)	A collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions or business processes.
23	Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
24	Control	<p>A means of managing a risk, ensuring that a business objective is achieved or that a process is followed. [...]</p> <p>Control also means to manage the utilisation or behaviour of a configuration item, system or IT service.</p> <p>Source: ITIL</p>
25	Controlled Vocabulary	<p>A prescribed set of consistently used and carefully defined terms.</p> <p>A collection of preferred terms that are used to assist in more precise retrieval of content.</p> <p>Controlled vocabulary terms can be used for categorising content, building labelling systems, and creating style guides and database schema.</p> <p>Source: C-(2008)0113(INV)</p>
26	Cost	<p>The amount of money spent on a specific activity, IT service or business unit.</p> <p>Costs consist of real cost (money), notional cost (such as people’s time) and depreciation.</p> <p>Source: ITIL</p>
27	Create	<p>The development of tailored solutions to C3 requirements.</p> <p>The Create option can involve a number of COTS products but also involves custom coding and or hardware modifications.</p>
28	Critical Success Factor	<p>Something that must happen if an IT service, process, plan, project or other activity is to succeed.</p> <p>Key performance indicators are used to measure the achievement of each critical success factor.</p> <p>Source: ITIL</p>

#	Term	DEFINITION
29	Data	The quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded magnetic, optical or mechanical recording media. Facts and statistics collected together for reference or analysis.
30	Data Management	Data management is the development, execution, and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets.
31	Data Steward	Role within the NATO Enterprise responsible for utilising the data related processes, policies, directives, and with responsibilities for administering data in compliance with approved policy. The responsibilities of data stewards shall include the inception of data elements, the extension of data elements across data lifecycle, the population of data repositories, the authorisation for data use and the retirement of data elements. They shall also be responsible for identifying duplication of data elements and taking the corrective actions, and for data quality, security and availability of the data for which he or she is data steward.
32	Disposition	The final action resulting from the evaluation of information, consisting in the transfer to the NATO Archives for permanent retention, or destruction, or selective retention.
33	eXtensible Markup Language	It is a marking language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. Although the design of XML focuses on documents, the language is widely used for the representation of arbitrary data structures.
34	Governance	Governance is the structures and processes for decision-making, accountability, control and behaviour within organisations.
35	Green Defence	Multifaceted endeavour cutting across a wide range of activities, including operational effectiveness, environmental protection and energy efficiency. It involves several domains, including operations, logistics, engineering and defence planning and it includes a wide variety of actors: civilian and military, Allies and partners, international organisations and private sector. Source: PO(2014)0059
36	Green IT	The study and practice of designing, manufacturing, using, and disposing of computers, servers (including data centre cooling), associated subsystems (such as monitors, printers, storage devices, and networking and communications systems) efficiently and effectively with minimal or no impact on the environment.

#	Term	DEFINITION
37	Green Manufacturing	<p>A method for manufacturing that minimises waste and pollution. NCI Agency note: this reduces potential disposal issues. C3S note: the implementation Directive will ensure that criteria for the green manufacturing consider the environmental aspects at all production and supply chain stages.</p> <p>Source: Managing Quality: An Integrative Approach, by S. Thomas Foster, 2001, ISBN: 0-13-875964-2</p>
38	Hybrid Cloud	<p>The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).</p> <p>Source: "The NIST Definition of Cloud Computing", Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.</p>
39	ICT Infrastructure	<p>It refers to all the composite hardware, software, networking resources to allow an organization to deliver ICT solutions to its users.</p>
40	IM Plan	<p>A plan providing a clear and complete view of the information needs and how they are fulfilled. In addition, it sets appropriate timelines, milestones and planning cycles for the implementation of the plan. The IM plan is coordinated with relevant authorities.</p> <p>Source: C-(2008)0113(INV)</p>
41	IM Strategic Plan	<p>A rolling plan outlining the long-term objectives for IM, and the means and timelines to accomplish these objectives.</p> <p>Source: C-(2008)0113(INV)</p>
42	Information	<p>Any communications or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual forms.</p> <p>Within the NIMP, the term 'information' is used to embrace all information, including related data, required in support of NATO's missions, whether such information originates in NATO civil or military bodies or is received from member nations or non-NATO sources. Such information, and the media and resources used to record and process it, shall be managed in accordance with this policy and other relevant NATO agreements and legal obligations.</p>
43	Information Architecture	<p>Set of artefacts defining the structure of an organization's logical and physical information assets and the associated data management resources and linking the information required to the key business processes and decisions.</p>

#	Term	DEFINITION
44	Information Assurance	The principle of Information Assurance is described as the set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, non-electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, non-repudiation and authentication. Source: C-(2008)0113(INV)
45	Information Custodian	The nation or organisation which receives information and makes it visible and is responsible to the information owner for the agreed level of safe-keeping and availability of information
46	Information Domain	The domain where information is created, transformed and shared; where intent is conveyed and where communication for consultation, command and control takes place. Source: C-(2008)0113(INV)
47	Information Management	Information Management is a discipline that directs and supports the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organisation.
48	Information of Permanent Value	All information that is required to document NATO's evolution and missions, consultation and decision making processes. Source: C-(2008)0113(INV)
49	Information Owner	The nation or organisation which creates and maintains content, defines access rules, negotiates and agrees to release constraints, establishes disposition instructions, and is the authority for the life-cycle of information
50	Information Standard	A normative document about an aspect of information management, developed according to consensus procedures, which is approved by a body responsible for the respective aspect. Source: C-(2008)0113(INV)
51	Information Superiority	State of relative advantage in the information domain achieved by getting the right information to the right people at the right time in the right form whilst denying an adversary the ability to do the same.

#	Term	DEFINITION
52	Infrastructure As A Service (IaaS)	<p>The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.</p> <p>The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).</p> <p>Source: “The NIST Definition of Cloud Computing”, Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.</p>
53	Integrity	<p>The property that information (including data) has not been altered or destroyed in an unauthorised manner.</p>
54	Interoperability	<p>The ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives.</p> <p>Source: AAP-6</p>
55	IT Infrastructure Library (ITIL)	<p>A set of best-practice publications for IT service management. Owned by the Cabinet Office (part of HM Government), ITIL gives guidance on the provision of quality IT services and the processes, functions and other capabilities needed to support them.</p> <p>Source: ITIL</p>
56	Key Performance Indicator	<p>A metric that is used to help manage an IT service, process, plan, project or other activity. Key performance indicators are used to measure the achievement of critical success factors.</p> <p>Source: ITIL</p>
57	Knowledge	<p>Facts, information and skills acquired through experience or education; the theoretical or practical understanding of a subject.</p> <p>Within NATO, knowledge may be embedded within the organisation through processes, SOPs, cultural ethics and codes of conduct.</p>
58	Knowledge Management	<p>A business process that formalizes the management of intellectual assets, enabling effective action through their use. KM promotes a collaborative and integrative approach to the creation, capture, organization, and use of intellectual assets – including what is known but not necessarily documented.</p>
59	Labelling	<p>The application of a corresponding digital representation of a marking (such as confidentiality metadata labels) which allows automatic processing of data object or an information item.</p>

#	Term	DEFINITION
60	Life-Cycle	The life-cycle of information encompasses the stages of planning, collection, creation or generation of information; its organisation, retrieval, use, accessibility and transmission; its storage and protection; and, finally, its disposition.
61	Marking	Formatted texts, added to an information item manually by humans, for human interpretation, to enable controlling, routing and protecting of the information item.
62	Measures Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilised service. Source: "The NIST Definition of Cloud Computing", Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145
63	Metadata	Structured information that describes, explains, locates, and otherwise makes it easier to retrieve, use and understand an information resource. Metadata facilitates the association of records within the context of broader business activities and functions.
64	Metadata Management	Metadata management is the development, execution, and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of metadata assets.
65	Metadata Schema	A collection of metadata elements that defines a structure for representing metadata. In general, a metadata schema includes semantic definitions of terms used in the schema, structural constraints and data structure definitions, and bindings to physical description syntax. A core metadata schema defines the metadata elements for capturing basic information about the information resource, including its security classification.
66	Metrics	A quantifiable entity that allows the measurement of the achievement of a process goal. Source: COBIT
		Something that is measured and reported to help manage a process, service or activity. Source: ITIL
67	Missions	NATO operations, projects, programmes, contracts and other related tasks. Source: C-(2008)0113(INV)

#	Term	DEFINITION
68	Monitoring	Repeated observation of a configuration item, IT service or process to detect events and to ensure that the current status is known. Source: ITIL
69	NATO	The term “NATO” denotes the North Atlantic Treaty Organization and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organization, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of the International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952. Source: C-(2008)0113(INV)
70	NATO Network Enabled Capability	The Alliance’s cognitive and technical ability to federate the various components of the operational environment from the strategic level (including NATO HQ) down to the technical, through a networking and information infrastructure. Source: C-(2008)0113(INV)
71	Need-To-Know	The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services.
72	Networking And Information Infrastructure	The federated network of NATO and national information and communications infrastructures. Source: C-(2008)0113(INV)
73	Non-Repudiation	Non-repudiation is the measure of assurance to the recipient that shows that information was sent by a particular person or organisation and to the sender that shows that information has been received by the intended recipient(s).
74	On-Demand Self-Service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. Source: “The NIST Definition of Cloud Computing”, Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.

#	Term	DEFINITION
75	Ontology	<p>An explicit representation of the meaning of terms in a vocabulary, and their relationships.</p> <p>A common vocabulary for describing the concepts that exist in an area of knowledge and the relationships that exist between them.</p> <p>An ontology allows for a more detailed specification of the relationships in a domain than is the case with a thesaurus or taxonomy. The resulting vocabulary can be used by computers as well as understood by humans.</p> <p>Source: C-(2008)0113(INV)</p>
76	Operational Level Agreement	<p>An agreement between an IT service provider and another part of the same organization.</p> <p>It supports the IT service provider's delivery of IT services to customers and defines the goods or services to be provided and the responsibilities of both parties.</p> <p>Source: ITIL</p>
77	Originator	<p>The nation or international organisation under whose authority the information has been produced or introduced into NATO.</p>
78	Platform As A Service (PaaS)	<p>The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.</p> <p>The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.</p> <p>Source: "The NIST Definition of Cloud Computing", Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.</p>
79	Preservation	<p>The processes and procedures required to ensure the technical and intellectual availability, integrity and authenticity of information over time.</p>
80	Private Cloud	<p>The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.</p> <p>Source: "The NIST Definition of Cloud Computing", Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145</p>

#	Term	DEFINITION
81	Public Cloud	<p>The cloud infrastructure is provisioned for open use by the general public.</p> <p>It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them.</p> <p>It exists on the premises of the cloud provider.</p> <p>Source: “The NIST Definition of Cloud Computing”, Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.</p>
82	Rapid Elasticity	<p>Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.</p> <p>To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.</p> <p>Source: “The NIST Definition of Cloud Computing”, Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.</p>
83	Requirement	<p>A formal statement of what is needed – for example, a service level requirement, a project requirement or the required deliverables for a process.</p> <p>Source: ITIL</p>
84	Requirement Holder	<p>The representative of the user community responsible to determine the features of the desired solution by establishing the primary conditions for the solution design and the goals the desired solution should achieve.</p>
85	Resource Pooling	<p>The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.</p> <p>There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or datacentre).</p> <p>Examples of resources include storage, processing, memory, and network bandwidth.</p> <p>Source: “The NIST Definition of Cloud Computing”, Peter Mell and Timothy Grance (September 2011). National Institute of Standards and Technology: US Department of Commerce. Special publication 800-145.</p>
86	Responsibility-To-Share	<p>The individual and collective obligation to make information available, discoverable and accessible for those entities that require the information to perform their official tasks and services</p>

#	Term	DEFINITION
87	Risk	<p>A possible event that could cause harm or loss, or affect the ability to achieve objectives.</p> <p>A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.</p> <p>Risk can also be defined as uncertainty of outcome, and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes.</p> <p>Source: ITIL</p>
88	Service	<p>A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.</p> <p>The service is owned and maintained by a service provider.</p> <p>The service user accesses the service remotely and owns no tangible assets.</p> <p>The service provider is responsible for provisioning user accounts for the user community.</p> <p>A Service Level Agreement is required between the service provider and service user.</p> <p>A service can be owned and operated by a NATO Nation, NATO or a commercial entity within one of the NATO nations.</p> <p>Care must be taken to ensure the service is properly tested and accredited for NATO use.</p> <p>In the context of C3 Policy the “delivered value” is a C3 Capability solution and the reference to “without ownership of specific costs and risks” means that the tangible assets providing the C3 Solutions are not owned by the customer.</p> <p>Source: ITIL</p>
89	Service Catalogue	<p>Structured information on all IT services available to customers.</p> <p>A database or structured document with information about all live IT services, including those available for deployment.</p> <p>Source: COBIT</p>
		<p>The Service Catalogue is part of the service portfolio and contains information about two types of IT service: customer-facing services that are visible to the business; and supporting services required by the service provider to deliver customer-facing services.</p> <p>Source: ITIL</p>
90	Service Contract	<p>A contract to deliver one or more IT services.</p> <p>The term is also used to mean any agreement to deliver IT services, whether this is a legal contract or a service level agreement.</p> <p>See also customer agreement portfolio.</p> <p>Source: ITIL</p>

#	Term	DEFINITION
91	Service Customer	<p>Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees the service level targets. Service Customers are responsible for procuring service resources and for service investment. In the context of C3 Policy the customer of a C3 services is defined as the Investment Committee for all NATO Security Investment Programme funded services.</p> <p>Source: ITIL</p>
92	Service Level Agreement	<p>An agreement between an IT Service Provider and a Service Customer. A Service Level Agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT Service Provider and the customer. A single agreement may cover multiple IT services or multiple customers.</p> <p>Source: ITIL</p>
93	Service Level Target	<p>A commitment that is documented in a service level agreement. Service level targets are based on service level requirements, and are needed to ensure that the IT service is able to meet business objectives. They should be SMART (specific, measurable, accepted, realistic, timely), and are usually based on key performance indicators.</p> <p>Source: ITIL</p>
94	Service Lifecycle	<p>An approach to IT service management that emphasizes the importance of coordination and control across the various functions, processes and systems necessary to manage the full lifecycle of IT services. The service lifecycle approach considers the strategy, design, transition, operation and continual improvement of IT services. Also known as service management lifecycle.</p> <p>Source: ITIL</p>
95	Service Management	<p>A set of specialised organisational capabilities for providing value to customers in the form of services.</p> <p>Source: ITIL</p>
96	Service Portfolio	<p>The complete set of services that is managed by a service provider. The service portfolio is used to manage the entire lifecycle of all services, and includes three categories: service pipeline (proposed or in development), Service Catalogue (live or available for deployment), and retired services.</p> <p>Source: ITIL</p>
97	Service Provider	<p>An organization supplying services to one or more internal or external customers.</p> <p>Source: ITIL</p>