

UNCLASSIFIED

COMBINED FEDERATED BATTLE LABORATORY NETWORK (CFBLNET)



2005 ANNUAL REPORT Version 1.0

UNCLASSIFIED

Executive Summary

The Combined Federated Battle Network (CFBLNet) Executive Group (C-EG), held three CFBLNet Management Meetings (CMMs) in 2005. The CFBLNet was created and is maintained to provide the infrastructure of choice for International Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Research, Development, Trial and Assessments. The CFBLNet is available to the U.S., the other four nations in the CCEB and all NATO nations to explore, promote and confirm Coalition/Combined capabilities for the participants. To accomplish these objectives in 2005, nine nations/organizations maintain permanent connections to CFBLNet with twelve others added as needed to support various initiatives.

The 2005 annual report provides background of the CFBLNet and its governance (including the flag-level Senior Steering Group, the C-EG and the four permanent working groups), and it provides a summary of the significant events and accomplishments.

CFBLNet management focused on numerous issues during 2005. As such, the below list represents CFBLNet 2005 accomplishments:

- C-EG development of a Strategic Plan with supporting Goals and Enabling Objectives
- Significant revision of Publication 1 and associated annexes
- Trial use of Collaborative Planning Tool – Groove
- Development of the CFBLNet Black Backbone
- International test and development environment for the migration from IPv4 to IPv6
- Development of the CFBLNet Unclassified Enclave (CUE)
- Developed a list of general security requirements for Multi-Level Security (MLS)
- Development of a process to facilitate the participation of non-chartered nations/organizations in CFBLNet Initiatives
- Identified and published security procedures for guest nations/organizations to participate in CFBLNet Initiatives
- Sixty CFBLNet sites were operational at some point throughout 2005

Six CFBLNet Initiatives completed execution during 2005 and others conducted testing throughout the year. Reports are prepared for all initiatives completed and are available upon request. Over twenty CFBLNet Initiatives were introduced to the CFBLNet in 2005. Status of these Initiatives range from the “pre-nomination” stage through completed execution.

The CFBLNet Strategic Plan specifies the CFBLNet Goals and Objectives that the C-SSG has endorsed. It further specifies the enablers required to achieve these Goals. During 2006, CFBLNet will focus on:

- Further improvement of the CUE for IPv6 testing and evaluation
- “All Eyes” multi-level security testing
- Refinement and publishing of CFBLNet Management processes
- Continued emphasis on CFBLNet Initiative Execution

The Chairman on behalf of the Combined Federated Battle Laboratory Network (CFBLNet) Executive Group (C-EG) hereby approves the *CFBLNet 2005 Annual Report*.



28 April 2006

LtCol Anthony C. Smith
Joint Staff, J6X
C-EG Chairman/U.S. Representative

(date)

With endorsement from:

Mr. Einar C. Thorsen
NATO C3 Agency
NATO C-EG Representative

Mr. Roger O'Sullivan
CCEB C-EG Representative

Table of Contents

FOREWORD.....5

BACKGROUND.....5

2005 EVENTS.....5

PARTICIPANTS.....6

EXECUTIVE GROUP REVIEW5

SECURITY SUMMARY10

INITIATIVES SUMMARY.....11

DOCUMENTATION SUMMARY14

NETWORKS, SYSTEMS AND SERVICES SUMMARY15

CONCLUSION18

Appendix: Acronyms

Foreword

100. This report reflects the progress and accomplishments of the Combined Federated Battle Laboratory Network (CFBLNet) during the calendar year 2005.

Background

101. In April 1999, the United States made a proposal to the North Atlantic Treaty Organisation (NATO) Consultation, Command and Control (C³) Board to establish a Combined Federated Battle Lab (CFBL). Organizers from the US, NATO and Combined Communications-Electronics Board (CCEB) developed a concept for the CFBL that built on the Coalition Wide Area Network that was established each year for the Joint Warfare Interoperability Demonstration (JWID).

102. The CFBLNet concept called for the establishment of a year-round network for research, development, trials, and assessments that operates at a Secret Releasable accreditation level. The Lab is developing coalition interoperability, doctrine, procedures, and protocols that can be transitioned to operational coalition networks in future contingencies. Accordingly, in August 2002 the CFBLNet Technical Arrangement (Charter) was signed.

103. The sustaining vision of the CFBL is to provide the best choice international Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance (C⁴ISR) research, development, trials, and assessments infrastructure to explore, promote, and confirm Coalition/Combined capabilities and interoperability for the members.

2005 Events

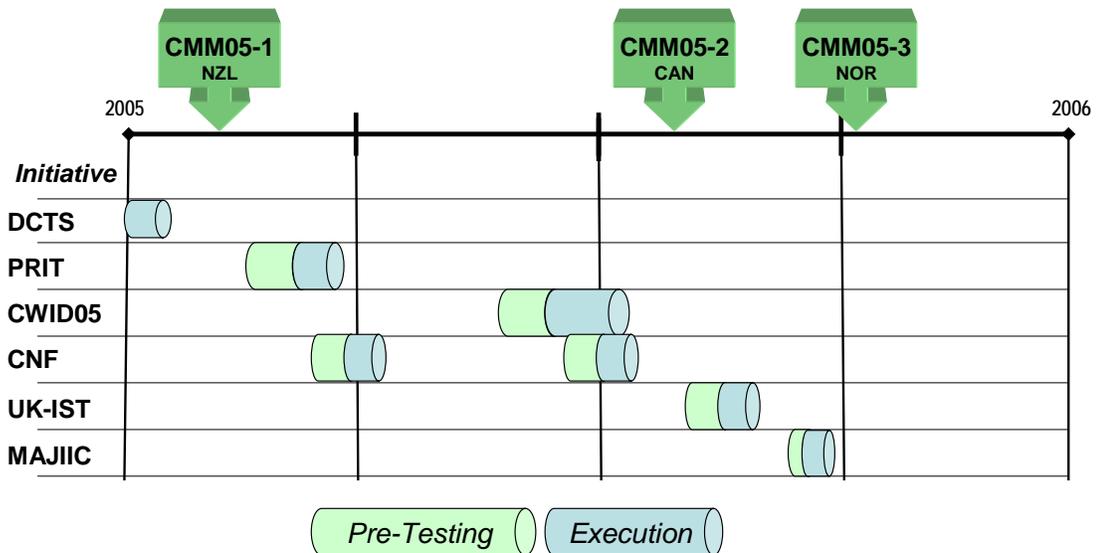
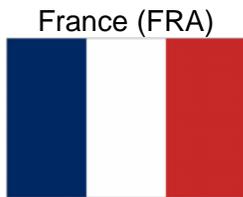


Illustration 1: CFBLNet 2005 Events Time line

Participants

104. Nations and Organizations permanently connected to CFBLNet in 2005 are listed below:



105. In addition, several nations have had temporary connections and/or have participated in CFBLNet Initiatives to include 2 Partnership for Peace Nations.



CFBLNet Executive Group Review

KEY ISSUES IN 2005

106. The CFBLNet management gave particular attention to a number of issues during 2005. These were themes that were highlighted during 2004 and formulated as having strategic importance to enhancing coalition C4ISR capabilities. Most of them were also briefed as such to and endorsed by the CFBLNet Senior Steering Group at the end of 2004.

107. Being somewhat of a victim of its own success, the CFBLNet was challenged to come up with a revised network architecture that could scale to meet the needs of the user community. This scalability was achieved by first introducing a network layer with seamless connectivity to all CFBLNet sites on top of which several protected network enclaves were established in which CFBLNet initiatives were conducted. The implementation of this scalable architecture has progressed very satisfactorily during 2005.

108. The CFBLNet was proposed as the international test and development environment for the migration from IP version 4 to IP version 6. The proposal has been taken forward by dedicating one initiative to prepare a CFBLNet enclave in which such test and development could take place without affecting the CFBLNet's service to other initiatives.

109. One of the biggest challenges in coalition networks is to achieve information sharing across multiple security levels/domains. Consequently, initiatives that addressed various aspects of multi-level security were encouraged and given priority.

110. The growth of CFBLNet activities has led to participation from non-charter nations/organizations. The associated CFBLNet procedures needed to be revised and formalized to provide guidance for initiatives and individuals dealing with these nations/organizations. Good progress was made on this and the relevant parts of Pub 1 were prepared for updates accordingly.

C-EG REPORT

111. The C-EG consists of senior representatives from the Charter Nations/Organizations. The C-EG provides policy and decision-making on behalf of the Senior Steering Group (SSG). The C-EG met in conjunction with the working groups at CFBLNet Management Meetings (CMM) in February, July and October 2005. In addition to providing direction to and oversight of working group activities, key C-EG outcomes and issues included:

- the development of a Strategic Plan with supporting Goals and Enabling Objectives;
- significant revision of Publication 1 and its annexes; and
- investigation into the selection and use of a collaborative planning tool to support the conduct of CFBLNet business.

STRATEGIC PLAN

112. Since its inception, the only formal governance and guidance for CFBLNet activities has been the Technical Arrangement (Charter), originally signed in August 2002 and reviewed and resigned in December 2004. This document is a very high level statement of

intent of the Charter Nations/Organizations (CN/O) to participate in the CFBLNet. During 2005, the C-EG developed a Strategic Plan, which includes Goals and Enabling Objectives that provide clear direction to the CFBLNet organization for current activities and the evolution of the CFBLNet to remain the network of choice for the conduct of RDT&A activities.

113. The Goals included in CFBLNet Strategic Plan are to:

- Provide the most effective and well managed Coalition network environment for the conduct of concurrent Coalition C4ISR RDT&A Initiatives;
- Evolve the CFBLNet to reflect emerging technologies potentially impacting operational networks; and
- Provide the most effective management processes for the conduct of Coalition C4ISR RDT&A Initiatives.

114. The C-EG considered the potential benefits and costs of allowing the CFBLNet to be used for a range of non-RDT&A-related activities, such as training, recognizing the priority of initiatives and subject to CFBLNet scheduling, availability and support implications. There was not consensus that non-RDT&A activities should be conducted on the CFBLNet and therefore this aspect of potential expanded use of the CFBLNet was not pursued.

115. The C-SSG will review the Strategic Plan at its earliest convenience in 2006 for approval. During 2006, the C-EG and the working groups will continue to develop the supporting matrix that includes tasks and activities necessary to achieve the Enabling Objectives identified in the Strategic Plan.

PUBLICATION 1

116. CFBLNet Pub 1 details organizational roles and responsibilities. During 2005, the C-EG has conducted a comprehensive review of Publication 1 and has coordinated a review and refresh of its supporting annexes by the responsible working groups. Pub 1 Version 3 was approved by the C-EG in December 2005. This publication now more accurately reflects the current roles and responsibilities of the CFBLNet organization. Due to the dynamic nature of the CFBLNet infrastructure, which is necessary to support a wide range of initiatives, and because of the evolution of the CFBLNet to reflect emerging technologies, the network and security focused annexes will require continual review and updates. This will be accomplished through the annual review process established to ensure that Pub 1 remains relevant and accurate.

COLLABORATIVE PLANNING TOOL

117. Over the past 18 months, participants in CFBLNet working groups have been experimenting with "Groove" as a tool to assist in collaboration during and between CMM meetings. Groove has proven to be useful in improving real time information sharing, as well as providing a temporary repository for information and issues being addressed within the working groups. The working groups have collectively proposed that Groove be adopted as the preferred collaboration tool for the conduct of CFBLNet business. While the C-EG recognizes the potential benefits of adopting a common collaboration tool, we

also recognize that there are a range of other issues that need to be considered before endorsing its use. These issues include:

- security (including aggregation of information);
- information management;
- resourcing and funding, including acquisition of licenses and provision of (wireless) connectivity and other necessary infrastructure;
- availability to users, which may be subject to national policies (and marginalization of those who are not “Groove-enabled”); and
- training and familiarization of Groove functionality.

SUMMARY

118. During 2006, the C-EG will continue to oversee the operation and evolution of the CFBLNet and will provide guidance and direction to the working groups on behalf of the C-SSG. The key foci of the C-EG during 2006 will be to:

- finalize the Goals, Enabling Objectives and Required Actions so as to provide clear direction and tasking for the working groups;
- improve the governance and processes supporting the conduct of initiatives on the CFBLNet, so as to improve its efficiency and effectiveness for the conduct of RDT&A Initiatives.
- develop an agreed position on the adoption of a collaboration tool to support and improve the conduct of CFBLNet business.

KEY ISSUES FOR 06

119. The CFBLNet Strategic Plan specifies the CFBLNet Goals and Objectives that the Senior Steering Group has endorsed. It further specifies the enablers required to achieve these Goals. The CFBLNet management will focus on identifying and implementing the actions required to establish these enablers and to monitor the effect it has on achieving the related Goals and Objectives.

120. The timely establishment of the CFBLNet Unclassified Enclave (CUE) for IPv6 and “all eyes” multi-level security testing is an essential, but challenging, activity that requires management attention.

121. As lessons are learned by CFBLNet initiatives, in particular related to security procedures and tools for use in multiple security domain environments, such as the CFBLNet itself, those lessons must be taken onboard as the CFBLNet evolves to reflect best practices in this area.

122. Having refined the CFBLNet management processes and having achieved significant progress over the last couple of years, the focus should now be turned towards publishing the related procedures and ensuring that they are followed. In assisting with this, collaboration tools and procedures for CFBLNet management and information sharing will be standardized.

Security Summary

123. During 2005, the security efforts for CFBLNet included the following:
- Major Review of Publication 1, Annex C;
 - Developed security requirements for the CUE and Backbone, including cryptographic procedures, connectivity, border protection and minimum standards;
 - Developed procedures for the inclusion of non-chartered nations/organizations into CFBLNet sites/enclaves;
 - Formalized and improved the relationship between CFBL and MSAB;
 - Requested and received new procedures from MSAB for the accreditation of sites and initiatives;
 - Produced dirty word list for initiative quad charts to assist in keeping them UNCLASSIFIED;
 - Provided security advice to many initiatives, including CWID and MNE;
 - Mandated that Commercial and Non-Military agencies/companies who are CN/O sponsored to connect must adhere to National/Organizational Military Security and Installation standards.
 - Defined the types of boundary protection system requirements for interconnection of Coalition security domains/enclaves.
 - Developed documentation and procedures for the Coalition to support nations/organizations policies, practices and procedures
 - Developed a list of general security requirements for Multi-Level Security (MLS).
 - Provided security procedures for guest nations/organizations to participate in CFBLNet Initiatives.

Initiatives Summary

124. Six CFBLNet Initiatives completed execution in 2005. In addition to the Initiatives listed in this section, other Initiatives conducted testing throughout the year.

<u>Defense Collaboration Tool Suite (DCTS)</u>	
Participants:	AUS, CAN, GBR, NATO, USA
Execution Completed:	January 2005
Objective:	<ul style="list-style-type: none"> - To provide users with the capability to collaborate using audio, video, whiteboard, chat and application sharing.
<u>Ptarmigan Rita Interoperability Tests (PRIT)</u>	
Participants:	FRA, GBR
Execution Completed:	March 2005
Objectives:	<ul style="list-style-type: none"> - To assess interoperability of FR RITA to UK GATE (STANAG 4206); - To assess Phase 1 and 2 – De-risk UK/FR connectivity through CFBLNet by ping tests.
<u>Coalition Warrior Interoperability Demonstration 2005 (CWID05)</u>	
Participants:	AUS, CAN, GBR, NZL, USA, CCEB, NATO, ROK, PfP
Execution Completed:	June 2005
Objectives:	To:
	<ul style="list-style-type: none"> - Improve Mission Assurance planning and execution capabilities and procedures - Provide an enhanced interoperable Situational Awareness capability - Provide solutions to facilitate Information Sharing/Multi-Level Security - Provide solutions that enable Collaborative Information Environment - Provide solutions to permit Intelligence, Surveillance and Reconnaissance Dissemination - Provide solutions to address Wireless Security - Provide improvements to Language Translation - Provide solutions for Integrated Logistics
<u>Coalition Naval Fires (CNF) Interoperability</u>	
Participants:	GBR, USA
Execution Completed:	July 2005
Objective:	To conduct an engineering level experiment to examine interoperability and CONOPS for future phases of the Coalition Naval Fires effort.

UK International Support Team (UK-IST)

Participants: GBR, USA

Execution Completed: September 2005

Objective:

- To experiment with a bilateral connectivity between the USA and GBR with a goal of establishing a permanent link between these two entities.

Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition (MAJIC)

Participants: NATO, FRA, DEU, ITA, NLD, ESP, GBR

Execution Completed: October 2005

Objectives:

- To conduct distributed classified experiments with multiple ISR coalition partners/systems;
- To expand the capability begun with CAESAR project (TIE Oct 2004), leading to broad multi-player operational exercises
- To address a dynamic community of interest and NNEC/NCES Security Services

New Initiatives Interests in 2005

125. The following CFBLNet Initiatives were introduced to the CFBLNet in 2005. The status of these listed Initiatives range from 'pre-nomination' stage through completed execution.

Lead	Initiative Name
AUS	Virtual Battle Experiment-D (VBE-D, TTCP MAR TP-1)
USA	Multinational Experiment 4 (MNE4)
DEU	Internet Protocol Version 6 (IPv6)
GBR	NATO TDL Interoperability Testing (TDLITS)
GBR	Maritime Composite Training System (MCTS)
GBR	Co-operative Engagement Capability (CEC)
USA	Radiant Mercury (Rad-Merc)
GBR	Ground Based Air Defence (GBAD-SE)
DEU	IEG Case B
DEU	Coalition Hostage Rescue Operation with Mobile Environment & QOS (CHROMEQ)
USA	Fleet Synthetic Training – Joint (FST-J)
USA	Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition (MAJIIC)
CAN	MIC Griffin Domain Testing (MGD)
USA	Empire Challenge
USA	UK International Support Team (UK-IST)
USA	Coalition Warrior Interoperability Demonstration 2006 (CWID06)
USA	Coalition Distributed Engineering Plan (CDEP) 'EL16CN'
USA	ACP145 Messaging
USA	Coalition Warfare System Demonstration (CWSD) 'Project Churchill'
USA	CENTRIXS
USA	Coalition Secure Management and Operations Systems (COSMOS)
USA	C2BMC

Table 1: CFBLNet 2005 Initiative Interests

Documentation Summary

126. The first complete version of the CFBLNet Publication 1 was completed in 2003. Changes and updates to this document will be undertaken as CFBLNet continues to evolve with new requirements and direction. A summary of the status of all the Technical Arrangement (Charter) and the Publication 1 and its annexes is contained below.

Technical Arrangement (Charter) <i>Updated: DEC04</i>	Signed & Approved by C-SSG: December 2004
Publication 1: Organization and Responsibilities <i>Version 3.0/DEC05</i>	Signed & Approved by C-EG: December 2005
CFBLNet Publication 1 – Annex A: Glossary <i>Version 3.0/DEC05</i>	Approved by C-EG: December 2005
CFBLNet Publication 1 – Annex B: Initiative Processing <i>Version 3.0/DEC05</i> <i>Note: This document is represented by a place holder. A major rewrite was initiated at CMM05-3. CLRs are the Point of Contact for the information normally contained in this Annex. Version 3.01 is expected in February 2006.</i>	Approved by C-EG: December 2005
CFBLNet Publication 1 – Annex C: CFBLNet Security and Accreditation Strategy <i>Version 3.0/DEC05</i> <i>Note: Appendices to this document are maintained separately due to their classification.</i>	Approved by C-EG: December 2005
CFBLNet Publication 1 – Annex D: Network Operations (Network/System Aspects of the CFBLNet) <i>Version 3.0/DEC05</i> <i>Note: Most of the appendices to this document are maintained separately due to their classification level.</i>	Approved by C-EG: December 2005

127. In 2005, revisions to Publication 1 included an effort to make the majority of the document available at the 'Unclassified' security label to allow for widest distribution. In this effort, several annexes were separated and have been labeled as Unclassified Not Internet Releasable Internet (UNIR) and are available via more secure means of transmission.

Networks, Systems and Services Summary

128. In 2005, network engineering efforts included the following:

1. Further developed the CFBLNet Black Backbone (IPv4). Backbone services are IP routing, network monitoring, and DNS. All CFBLNet nations are currently on the Backbone.
2. Further developed and gained support for the CFBLNet Unclassified Non-Internet releasable Enclave (CUE). The primary purpose of the CUE is to support non-Secret cleared personnel and/or non-CFBLNet nations and unclassified initiatives. The secondary purpose is to support the development of Multi-Level Security (MLS) and IPv6 solutions.
3. Created a CFBLNet CUE IPv6 Road Map, which provides an IPv6 Address Schema. In addition, developed an IPv6 test plan that includes IPv6 testing in dual stack, tunneling and translation configurations.
4. Proposed CFBLNet Scalability for future CWID Initiatives and others which require a permanent capability for temporary access of nations who are not charter CFBL members.
5. Developed a CFBLNet Crypto Topology Diagram, which clearly identifies where CFBLNet infrastructure crypto breaks exist and enhances CFBLNet initiative engineering support.
6. Developed a CFBLNet Future Implementation Plan, which discusses end-to-end IPv4 on the Backbone, CUE, and internet access from the CUE.

CFBLNet Sites

129. CFBLNet sites are the physical locations accredited through national/ organizational assurance agencies in accordance with the CFBL security process and approved by the C-EG. CFBLNet sites, whether permanent or temporary, must be nominated by the national/organizational lead to the Secretariat. At its inception, the CFBLNet was composed of 17 sites. Table 1 indicates the number of sites that were Operational at some point throughout 2005.

Nation/Organization	Operational
Australia (AUS)	5
Canada (CAN)	11
France (FRA)	4
Germany (DEU)	5
Italy (ITA)	3
NATO	5
New Zealand (NZL)	1
Norway (NOR)	4
Spain (ESP)	1
United Kingdom (GBR)	6
United States (USA)	15
TOTAL	60

Table 2: CFBLNet 2005 Operational Sites

130. Illustration 2 indicates CFBLNet Level 0 (zero) topology with national points of presence (POPs) for 2005.

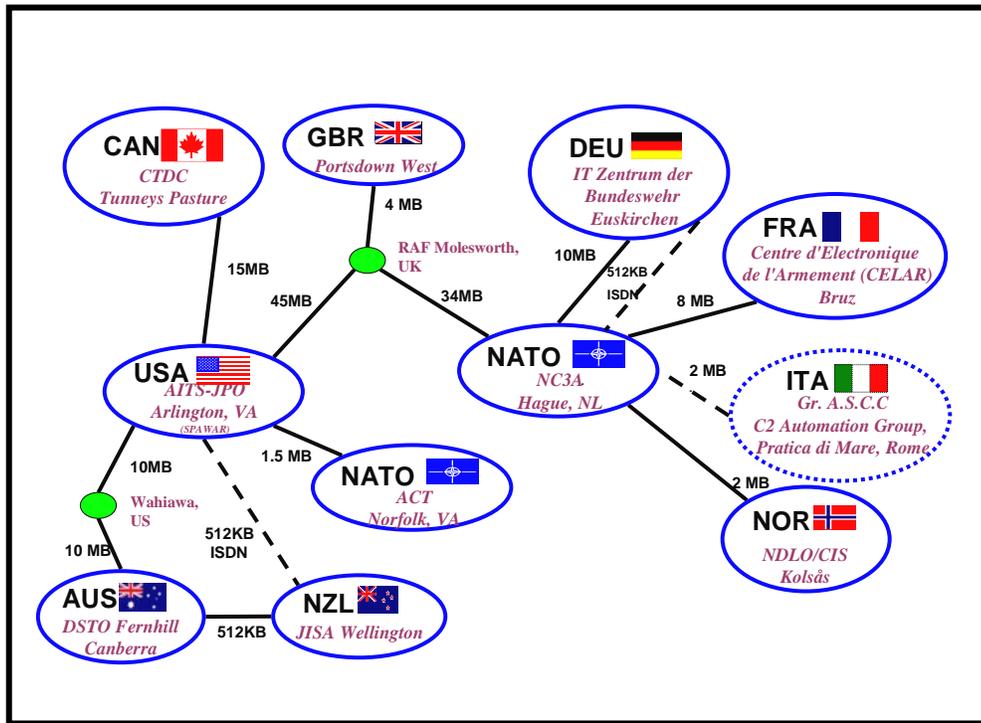


Illustration 2: CFBLNet 2005 Level 0 Topology

New Site Interests in 2005

131. The following CFBLNet sites were introduced to the CFBLNet in 2005.

Sponsor	Name/Location
CAN	CFEC, Ottawa Ontario
CAN	SBML, Ottawa, Ontario
CAN	MARPAC, Esquimault, British Columbia
CAN	JIFC, Ottawa, Ontario
DEU	Bonn, Germany
DEU	Bundeswehr Technical Center for Information Technology and Electronics: Gerding
DEU	Naval Office/Naval C2S Command: Wilhelmshaven
DEU	Training Area: WeissKeissel
DEU	IABG: Ottobrun
ESP	Maudo Artilleria Antiaerea (MAA), Madrid
FRA	Arcueil, France
FRA	Creil, France
GBR	QinetiQ: Bedford
GBR	BMEC Brennan House BAE Systems: Farnborough
GBR	MWS
ITA	COI, Roma
ITA	GrASCC: Practica di Mare, Rome
ITA	COTIE Army: Anzio, Rome
ITA	MARITELE: Rome, S. Rosa
ITA	COMITMATFOR: S. Vito, Taranto
NATO	E3A Component: Geilenkirchen, Germany
NATO	Ataturk WSCC, Istanbul, Turkey
NATO	SHAPE: Mons, Belgium
NATO	Glons, Belgium
NATO	JWC Ulsnes, Norway
NZL	Linton Army Camp
USA	Defence Threat Reduction Agency, Second Site (DTRA2), Arlington, Virginia
USA	Combat Direction Systems Agency (CDSA), Dam Neck, Virginia
USA	Langley AFB, Virginia
USA	Wright Patterson AFB, Ohio
USA	Fort Detrick, Maryland

Table 3: New Site Interests for CFBLNet 2005

CFBLNet Services

132. Core services are robust, reliable and stable network services, which have been developed and deployed on the network to facilitate initiatives. They are managed and supported directly by the nation/organization. Core services are further sub-divided into critical and supporting (Value Added) infrastructure, to distinguish between those services that are essential and desirable for operating and supporting the CFBLNet.

Core Services
IP Addressing
NSAP Addressing
Domain Name Service (DNS)
Routing Protocols (e.g. OSPF, BGP4, IGP, EIGP)
Messaging (SMTP)
Web (HTTP)
Network Time Protocol (NTP) Source
News (NNTP)
Network Management (SNMP)
IP Telephony Call Manager
IP Telephony (Network Management phone)@each site

Table 4: CFBLNet 2005 Core Services

Conclusion

133. Although CFBLNet continues to be an invaluable asset for multinational C4ISR capability and interoperability testing, the CFBLNet must continue to change to meet evolving customer requirements.

134. CFBLNet continues to provide the Coalition network environment supporting technical and multinational information sharing trials. Additionally, the development and increasing support for the CFBLNet Unclassified Environment (CUE) and breaking ground for the inclusion of non-charter nations and organizations in CFBLNet Initiatives and activities has allowed the CFBLNet to continue in its growth and evolution as the Coalition RDT&A infrastructure of choice.

135. In the upcoming year, to foster continued growth and further enable meeting customer requirements the CFBLNet organization will; continue to develop the Enabling Objectives and Required Actions of the Strategic Plan, improve the governance and processes supporting the conduct of Initiatives on the CFBLNet, and further develop an agreed upon position on the adoption of a collaborative planning and support tool for the conduct of CFBLNet business.

Acronyms

AUS	Australia
AWG	Active Working Group
BGP4	Border Gateway Protocol Version 4
C3	Consultation, Command & Control
C ⁴ ISR	Command Control Communications Computers Intelligence Surveillance & Reconnaissance
CAESAR	Coalition Aerial Surveillance and Reconnaissance
CAN	Canada
CCEB	Combined Communications Electronics Board
CDEP	Coalition Distributed Engineering Plant
CEC	Co-operative Engagement Capability
C-EG	CFBLNet Executive Group
CFBL	Combined Federated Battle Laboratory
CFBLNet	Combined Federated Battle Laboratory Network
CHROMEIQ	Coalition Hostage Rescue Operation with Mobile Environment and QoS
CLR	CN/O Lead Representative
CMM	CFBLNet Management Meeting
CNF	Coalition Naval Fires
CN/O	Charter Nation/Organization
COSMOS	Coalition Secure Management and Operations Systems
C-SSG	CFBLNet Senior Steering Group
CUE	CFBLNet Unclassified Enclave
CWID	Coalition Warrior Interoperability Demonstration
CWSD	Coalition Warfare System Demonstration
DCTS	Defense Collaborative Tool Suite
DEU	Germany
DNK	Denmark
DNS	Domain Name Server
DTRA	Defence Threat Reduction Agency
EIGP	Extended Interior Gateway Protocol
ESP	Spain
FIN	Finland
FRA	France
FST	Fleet Synthetic Training
GBAD	Ground Base Air Defence
GBR	United Kingdom/Great Britain
HTTP	Hyper Text Transfer Protocol
HUN	Hungary
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol version 6

ITA	Italy
JWID	Joint Warrior Interoperability Demonstration
KOR	Republic of Korea
MAJIIC	Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition
MCTS	Maritime Composite Training System
MGD	MIC Griffin Domain
MLS	Multi-Level Security
MNE	Multi-National Experiment
MSAB	Multi-National Security Accreditation Board
NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation Command & Control Agency
NLD	Netherlands
NNTP	Network News Transfer Protocol
NOR	Norway
NSAP	Network Service Access Protocol
NTP	Network Time Protocol
NZL	New Zealand
OSPF	Open Shortest Path First
PACRIM	Pacific Rim
PfP	Partnerships for Peace (NATO term)
POC	Point of Contact
POL	Poland
PRIT	Ptarmigan-Rita Interoperability Test
QMM	Quarterly Management Meeting
QoS	Quality Of Service
RadMerc	Radiant Mercury
RDT&A	Research, Development, Trials & Assessment
ROU	Romania
ROK	Republic of Korea
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SWE	Sweden
TDLITS	Tactical Data Link, Interoperability Testing
TUR	Turkey
UK-IST	United Kingdom – International Support Team
UNIR	Unclassified Not Internet Releasable
USA	United States of America
VBE	Virtual Battle Experiment