

UNCLASSIFIED

COMBINED FEDERATED BATTLE LABORATORY NETWORK (CFBLNET)



2006 ANNUAL REPORT

UNCLASSIFIED

Executive Summary

The 2006 annual report provides background of the Combined Federated Battle Laboratory Network (CFBLNet) and its governance (including the flag-level CFBLNet Senior Steering Group (C-SSG), the CFBLNet Executive Group (C-EG) and the four permanent working groups), and it provides a summary of the significant events and accomplishments.

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, Trials and Assessments.

The CFBLNet supported several key warfighting Initiatives in 2006, including: multi-national connectivity for air picture; messaging services; collaboration; multi-level security Initiatives; homeland defense and crisis response tools; ship-to-ship command and control; unmanned aerial vehicle imagery; and situational awareness via enhanced tactical data link interoperability. Imagery and video systems proven on CFBLNet are currently supporting operations in Afghanistan and Iraq. The network also supported key second-tier warfighting objectives including on-line distributed war gaming and multinational training exercises. Some specific success stories include the following:

- Intelligence, Reconnaissance and Surveillance (ISR) lessons learned in live and unmanned aircraft and satellite surveillance in Empire Challenge 06 were applied immediately in support of International Security Assistance Force (ISAF) – Afghanistan.
- In Project Churchill, the US-UK bilateral trials led to enhanced communications capabilities for Unmanned Combat Air Systems.
- The United Kingdom International Support Team (UK-IST III) and the US conducted experiments that established real time wargaming for C2, consultation, and future consequence mitigation.

Additionally, several technical tests were conducted to enhance network service capabilities and interoperability. Finally, CFBLNet continued to provide a venue to explore, promote and confirm coalition capability development between the 28 charter nations plus NATO and other coalition partners.

The C-EG held two CFBLNet Management Meetings (CMMs) in 2006. During 2006, fifteen nations/organizations connected nationally to CFBLNet with six other nations acting as observers to support various Initiatives. C-EG accomplishments during 2006 included:

- Published the Strategic Plan with supporting Goals and Enabling Objectives
- Completed a significant revision of Publication 1 and associated Annexes
- Adopted Groove as the Collaborative Planning Tool of choice

- Refined the process to facilitate the participation of non-chartered nations/organizations in CFBLNet Initiatives
- Over one hundred fifteen (115) CFBLNet sites were operational in 2006

In 2006, 24 CFBLNet Initiatives were introduced, 21 Initiatives were completed. Within those Initiatives, numerous individual trials and assessments were conducted, e.g. CWID06 included 34 coalition trials and assessments, as well as many national trials held by participating nations (e.g. UK conducted 40 national trials during CWID06). Status of these Initiatives range from the “pre-nomination” stage through completed execution.

The CFBLNet Strategic Plan specifies the CFBLNet Goals and Objectives. It further specifies the enablers required to achieve these Goals. Enablers achieved during 2006 include:

- Providing end-to-end IPv4 routing on the Black backbone (Enb.1.4)
- Establishing multi-nationally agreed accreditation processes to enable secure interconnection of nationally accredited communications and information systems (CIS) (Enb.1.5)
- Improving the scheduling of Initiatives to achieve bandwidth efficiencies and resolve Initiative scheduling conflicts (Enb.3.1)
- Initiating reviews of CFBLNet performance based on Initiative outbrief reports and implementing necessary improvements (Enb.3.4)
- Assessing maturity and routing of Initiatives (Enb.3.5)

During 2007, CFBLNet will focus on:

- Capturing warfighter impact (Goal 1)
 - Warfighter impact statements in Initiative final reports
 - Increased CLR communication with warfighters
 - Capturing awards and Letters of appreciation
- Enterprise Network Management Capabilities (Enb.2.2)
 - Bandwidth monitoring, quality of service (QoS) monitoring, and Intrusion Detection Systems (IDS)
- Information Management Plan (Enb.3.7)
 - A dedicated section on information management will be included in Annex E of Publication 1 in version 5.0
- Creation of three new documents (Goal 2)
 - CFBLNet Information Pamphlet
 - Basic Guide to CFBLNet Initiatives Process
 - Basic Guide to CFBLNet Security Accreditation
- Standardized Border Protection Schemes (Enb.2.1)

UNCLASSIFIED

This page intentionally blank

The Chairman, on behalf of the Combined Federated Battle Laboratory Network (CFBLNet) Executive Group (C-EG), hereby approves the CFBLNet 2006 Annual Report.



9 MAY 07

Colonel 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

Major Noel Rings
CCEB Executive Group
CCEB C-EG Representative

Table of Contents

FOREWORD.....7

BACKGROUND.....7

2006 EVENTS.....7

PARTICIPANTS.....8

CFBLNET EXECUTIVE GROUP REVIEW9

SECURITY WORKING GROUP SUMMARY13

INITIATIVES WORKING GROUP SUMMARY.....14

DOCUMENTATION WORKING GROUP SUMMARY21

NETWORK WORKING GROUP SUMMARY.....22

CONCLUSION25

Annex A: Acronyms

Foreword

100. This report reflects the progress and accomplishments of the Combined Federated Battle Laboratory Network (CFBLNet) during the calendar year 2006.

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 Laboratory (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 for 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 infrastructure of choice for international Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) research, development, trials, and assessments (RDT&A) to explore, promote, and confirm Coalition/Combined capabilities and interoperability for the members.

2006 Events

104. Two CFBLNet Management Meetings (CMMs) were hosted in 2006.

- CMM06-1
 - Charter Nation/Organization (CN/O) Host: Australia (CCEB)
 - Location: Waldorf Apartment Hotel, Canberra, Australia
 - Dates: 6 – 10 February 2006

- CMM06-2
 - Charter Nation/Organization (CN/O) Host: United Kingdom (CCEB)
 - Location: Bailbrook House, Bath, United Kingdom
 - Dates: 2 – 6 October 2006

Participants

105. Nations and Organizations connected to CFBLNet in 2006 are listed below:

Australia (AUS)



Canada (CAN)



France (FRA)



Germany (DEU)



United Kingdom (GBR)



United States (USA)



New Zealand (NZL)



Norway (NOR)



Poland (POL)

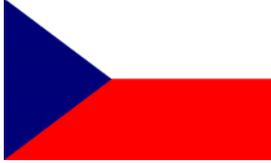


NATO

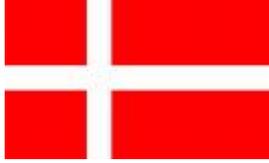


106. In addition, these nations have participated in or observed CFBLNet Initiatives at existing CFBLNet sites:

Czech Republic (CZE)



Denmark (DNK)



Hungary (HUN)



Finland (FIN)



Russia (RUS)



Sweden (SWE)



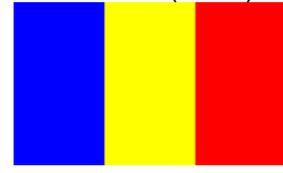
Turkey (TUR)



Portugal (PRT)



Romania (ROM)



Spain (ESP)



Netherlands (NLD)



Italy (ITA)



CFBLNet Executive Group Review

Key results in 2006

107. The Executive Group focused on institutionalizing CFBLNet processes and procedures during 2006. The C-EG met in conjunction with the working groups at CMMs in February and October 2006. Key achievements during the CMMs included expanding guidance in CFBLNet Publication 1, implementation of Groove as the collaborative planning tool for core CFBLNet business, and capturing key mission goals and objectives in the CFBLNet Strategic Plan. Changes to CFBLNet Publication 1 included: establishing a formal Initiative request process and tool (CFBLNet Initiative Information Pack--CIIP); documenting security accreditation and approval procedures; providing basic document management instructions; and refining network management controls. The Strategic Plan for the first time provided 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.

108. During 2006, the C-EG approved the development and implementation of a CFBLNet Strategic Plan, which the C-SSG approved in June 2006. The CFBLNet Strategic Plan established the following goals:

- 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.

109. The Executive Group identified 14 objectives and 23 specific tasks (Enablers) to guide progress towards these goals. Enablers included: making significant changes to the network infrastructure to increase flexibility for our customers; adding network management and monitoring capabilities; establishing multi-nationally agreed accreditation processes; installing new network technologies; implementing computer network defense capabilities; improving scheduling and control of Initiatives; capturing customer feedback to support continuous improvement; and documenting return on investment. In 2006, CFBLNet completed five Enablers and established four new Enablers to further improve customer support and increase management efficiency/effectiveness. The status of the CFBLNet Enablers is illustrated below.

CFBLNet Strategic Plan Enablers Status

Goals	Objectives	Enablers	Status
Goal. 1. Provide the most effective and well managed Coalition network environment for the conduct of concurrent Coalition C4ISR RDT&A Initiatives	Obj.1.1. Provide a dynamic, flexible and progressive environment that will enhance the ability to support concurrent experimentation Obj.1.2. Enable and support multiple concurrent enclaves for the conduct of Initiatives for different communities of interest. Obj.1.3. Provide and manage the permanent backbone network infrastructure for the conduct of Initiatives between CN/O and SN/O participants. Obj.1.4. Provide CFBLNet operations support and security. Obj.1.5. Provide relevant, accurate and timely information related to CFBLNet Initiatives and Services.	Enb.1.1 Provide and manage the CFBLNet backbone network infrastructure	ONGOING
		Enb.1.2 Provide and manage enclaves for the conduct of classified Initiatives between the Charter Nations/Organizations (CN/O)	ONGOING
		Enb.1.3 Provide and manage the CFBLNet Unclassified Enclave (CUE) for the conduct of multiple Initiatives for CN/O and SN/O participants.	ONGOING
		Enb.1.4 Implement multi-nationally agreed accreditation processes to enable secure interconnection of nationally accredited communications and information systems (CIS)	DONE
		Enb.1.5 Establish end to end IPv4 routing on the Black-backbone	DONE
		Enb.1.6 Maintain a Public Website populated with relevant and accurate information	ONGOING
		Enb.1.7 Provide a Customer Friendly Network and RDT&A capability	ONGOING
		Enb.1.8 Develop and maintain an interactive, online process for users to populate CIIPs.	PENDING
		Goal. 2. Evolve the CFBLNet to reflect emerging technologies potentially impacting operational networks	Obj.2.1. Support the Trials and Assessments of emerging technologies including IPv6, PKI and MLS Obj.2.2. Evolve the CFBLNet infrastructure and services so that it is the preferred test bed for trials and assessments of IPv6 based Initiatives, applications and services. Obj.2.3. Exploit multi-national multi-level security (MLS) solutions Obj.2.4. Support Modelling & Simulation (M&S) activities Obj.2.5. Promote the use of CFBLNet for training when not in use for Initiatives
Enb.2.2 Establish Bandwidth Management (constraint and monitoring)	ONGOING		
Enb.2.3 Exploit multi-national multi level security for cross domain solutions	PENDING		
Enb.2.4 Evolve CFBLNet infrastructure and services to be IPv6 compliant.	ONGOING		
Enb.2.5 Provide infrastructure and services able to support IPv6 Initiatives.	ONGOING		
Enb.2.6 Provide capabilities able to support MLS Initiatives.	PENDING		
Enb.2.7 Provide capabilities able to support M&S trials (real time and low latency).	ONGOING		
Enb.2.8 Examine the requirement for computer network defence (CND) capabilities and procedures for CFBLNet.	ONGOING		
Goal. 3. Provide the most effective management processes for the conduct of Coalition C4ISR RDT&A Initiatives	Obj.3.1. Develop and implement effective management processes for the conduct of CFBLNet business (e.g. improved information sharing and management procedures and more efficient business processes for the conduct of CFBLNet Management Meetings -CMM) Obj.3.2. Improve the Initiative screening process to be more flexible, efficient and customer friendly. Obj.3.3. Improve CFBLNet infrastructure, services, support and management based on analysis of Performance Reports submitted by participants following the conduct of Initiatives. Obj.3.4. Improve CFBLNet documentation processes and procedures.		
		Enb.3.2 Improve Initiative screening processes to include participation by an SN/O	ONGOING
		Enb.3.3 Evaluate methods (e.g. Groove) to improve information management and sharing within and between CFBLNet WGs	ONGOING
		Enb.3.4 Review performance of CFBLNet based on Initiative outbreak reports and implement necessary improvements.	DONE
		Enb.3.5 Maturity assessment and routing of Initiatives.	DONE
		Enb.3.6 Establish advanced Initiative scheduling capabilities (e.g. latency, bandwidth, usage, and engineering statistics) to allow more complex utilization of the network.	PENDING
		Enb.3.7 Develop a comprehensive information management plan addressing creation, coordination, storage, configuration management, and control of information.	ONGOING

110. During 2006 the C-EG approved a training based Initiative (GUST) to assess the potential benefits and costs of authorizing the CFBLNet to be used for a range of non-RDT&A-related activities. The Initiative proved training (i.e. multinational wargaming), can be effectively conducted on the CFBLNet. Further development of training based Initiatives utilizing CFBLNet will be explored during 2007.

Publication 1

111. CFBLNet Pub 1 Version 4 was approved by the C-EG in November 2006. The publication now more accurately reflects the current roles and responsibilities of the CFBLNet organization. The dynamic nature of CFBLNet business will necessitate annual review and updates of this publication, in particular the network and security annexes.

Collaborative Planning Tool

112. Following its successful CFBLNet evaluation, the C-EG endorsed the adoption of "Groove" as the collaborative planning tool for CFBLNet business. Groove improves real time information sharing, and provides a repository for information and issues being addressed by the CFBLNet community. The development of CFBLNet Information Management (IM) strategies and processes will further maximize the use of Groove in the future. It is recognized that its use imposes a number of national implementation issues for the organization, including:

- training and familiarization of the Groove capability;
- acquisition of licenses and provision of (wireless) connectivity;
- availability to users (national policies and Groove enablement); and
- information management

Key topics for 2007

113. As the CFBLNet Strategic Plan describes our long term Goals and Objectives, the C-EG will continue to monitor progress towards achieving the associated enablers and to task the WGs accordingly. In 2007, particular focus will be put on a subset of the remaining items.

114. The CFBLNet public web site, as well as our internal information management procedures, is one area that urgently needs improvement. The C-EG will therefore give priority to activities that improve these areas. This includes the introduction of several short documents aimed at explaining some of the complex procedures in very simple terms to those new to the CFBLNet.

115. With the new authorization to introduce Training oriented Initiatives onto the CFBLNet as well as overall increased volume of Initiatives, our bandwidth management capability must be strengthened to ensure our constraints management and monitoring is as effective as possible and that the network is being upgraded where necessary.

116. To address the feedback from many Initiatives on the difficulty of achieving accreditation of cross domain Initiative proposals, making progress on establishing standardized boundary protection service for CFBLNet enclaves will require significant progress and management attention.

117. Finally, more emphasis will be put on capturing potential operational warfighter benefits from Initiatives and to use these in our public information. This will ensure that the CFBLNet maintains a warfighter focus and highlights the return on investment opportunities for key stakeholders.

Security Working Group Summary

118. In 2006, the security efforts for CFBLNet focused on the documentation of a multi-nationally agreed accreditation process supporting the interconnection of nationally accredited CIS (Enabler 1.1). The Security Working Group (SWG) also started the review of the requirements for Computer Network Defence (CND) capabilities and associated procedures for the CFBLNet (Enabler 2.1).

Regarding Enabler 1.1, the SWG:

- Defined the content of the security tab of the CFBLNet Initiative Information Pack (CIIP) and emphasized the requirements for the identification of cross domain connections and the identification of data sharing agreement between the participants of the Initiative;
- Streamlined and documented the relationship between the CFBL Community and the Multi-National Security Accreditation Board (MSAB);
- Contributed to the clarification of a certain number of issues related to the MSAB (e.g. control, distribution and maximum duration of the various types of National Accreditation Endorsement Certificates (NAECs)).

Regarding Enabler 2.1, the SWG:

- Streamlined the security requirements contained in Annex C of CFBLNet Publication 1;
- Started reviewing the national policies for the exchange and exploitation of coalition Intrusion Detection System (IDS) information;
- Started a discussion with the Network Working Group (NWG) on the implementation of a global CFBLNet IDS capability.

119. The plan for 2007 is to progress the definition and implementation of CND capabilities (Enabler 2.1) while promoting the use of the CFBLNet for multi-national, multi level security cross domain solutions (Enabler 2.3).

Initiatives Working Group Summary

120. For the reporting period of 2006 the CFBLNet accommodated a growing number of C4ISR Initiatives. Twenty Initiatives were conducted over the CFBLNet during 2006 and we expect increasing amounts for 2007. The Initiatives varied in size and complexity. Some Initiatives such as CWID06 and MNE4 had embedded high numbers of multinational trials and national demonstrations.

121. To address the increasing number of Initiatives, a new Initiative management process was devised and activated in March 2006 to permit 'out of session' approvals for the growing customer base.

2006 Initiatives

122. The following table lists the 2006 Initiatives, their operational benefits and associated details.

Initiatives 2006	Operational Benefits	Participants	Completion
TDLITS1 (Feb 06)	VoIP engineering test to provide input to future warfighting deployments	FRA, NATO, GBR	Feb 06
MAJIIC SIMEX 06	MAJIIC is maturing the interoperability standards (metadata and STANAG), data sharing architecture and CONOPs for distributed theater multi-international intelligence, surveillance and reconnaissance (ISR). SIMEX 2006 is the first of a series of simulated and live exercises to develop the program products for transition into fielded NATO and national systems.	FRA, DEU, ITA, ESP, NATO, NLD, GBR, USA	Mar 06
MGT	Secure e-mail to be fielded between National Headquarters in 2007 (MIC WAN)	USA, FRA, DEU, CAN	Mar 06
MNE-4	Research into Operational processes to advise improving Multinational capabilities in the future	AUS, CAN, FRA, DEU, GBR, NATO, SWE, FIN, US	Apr 06
TDLITS2 (Apr/May 06)	Developing integration of multinational operational C2 assets	DEU, ESP, FRA, ITA, NATO, GBR	May 06
TTCP – AG4	This initiative is part a series of experiments that seek to develop an information management capability for unstructured communications like chat.	GBR, USA, AUS	Jun 06
CWID 06	<ul style="list-style-type: none"> • Test, document and develop solutions to C4 interoperability • Operational focus: develop network management procedures for coalition networks (collaboration; MNIS) • Investigate military/civil C4 challenges • Focus on common standards development 	AUS, CAN, GBR, FRA, DEU, ITA, NLD, NZL, NOR, POL, PRT, ROM, ESP, TUR, USA, NATO	Jun 06

UNCLASSIFIED

Initiatives 2006	Operational Benefits	Participants	Completion
UK-IST II	Precursor to UK-IST III activity	GBR, USA	Jul 06
Empire Challenge 06	Multinational imagery products and exploitation interoperability fielded in Afghanistan	CAN, AUS, GBR, USA	Sep 06
VBE-E	Provide improved network infrastructure service to CN/O maritime platforms	AUS, GBR, NZL, CAN	Oct 06
QoS Trial 06-01	Supporting future operational architectures	FRA, DEU, NOR, POL, CAN, NATO	Oct 06
TDLITS 06-02	Developing integration of multinational operational C2 assets	DEU, ESP, FRA, NATO, USA, GBR	Oct 06
IEG Case B	Validate mechanisms that address critical near-term operational requirements for MCCIS, NIRIS, and ICC and assess its impact on the IEG and the Functional Services and put in the context of long-term solutions.	NATO, DEU	Nov 06
DAOC/CAOC-X	This trial was the foundation for interoperability of USA/GBR air pictures. This Initiative received 4-Star praise from the UK.	USA, GBR	Dec 06
GUST	Proved interoperability of UK and German naval shore training systems.	DEU, GBR	Dec 06
UK-IST III	Established war game connectivity between USA and UK.	GBR, USA	Dec 07
CDIFT	Component development and some interoperability testing will be established on an unclassified LAN, but experimentation and demonstration of interoperability of coalition information fusion technologies in realistic scenarios will be conducted periodically on the CFBLNet. This environment will also allow additional national information fusion capabilities to be introduced that can not be hosted on an unclassified LAN.	GBR, USA, AUS, CAN	Ongoing into 07
ACP 145 Messaging	Perform organizational messaging.	GBR, USA	Ongoing into 07
CWSD Project Churchill	Collaborative program to determine the military benefit of Unmanned Combat Air Systems within future coalition operations.	GBR, USA	Ongoing into 07
CCEB PKI Interop	Establish bilateral cross-certification procedures; determine the operating characteristics and capabilities of common PKI enabled applications (S/MIME email, TLS/SSL, Ipsec)	GBR, USA	Ongoing into 07

Proposed Initiatives for 2007

123. The following table provides details of the Initiatives that plan to use CFBLNet in 2007. Further Initiatives are anticipated during the year.

Initiatives 2007	Objectives	Participants	Proposed Dates
HF Equipment Trial	To prove interoperability of UK and French HF Systems deployed on Naval Platforms	FRA, GBR	Jan 07
MAJIIC 2007	To support the MAJIIC ACTD in the upcoming exercise MAJEX sharing ISR data between the JITC at Ft Huachuca AZ, Langley AFB and the MAJIIC coalition partners at NC3A The Hague.	NATO, USA	Mar 07
DSTX VPN (UMC)	The DSTX will provide shared weapon models and simulation architectures, an integrated launch to lethality high fidelity modelling environment, visualisation and analysis tools, revision control software, data, standards and processes, as well as the ability to execute international collaborative projects between DSTO and Dstl.	GBR, AUS	Mar 07 to Dec 08
GPDN	To develop the CCEB Web Service, DNS Service, Chat Service and the technical refresh of the UK Interoperability Service using a Type 1 High Grade encrypted enclave.	AUS, CAN, USA, NZL, GBR	Apr 07 to Mar 09
IEG Case B FS Trials	Develop and validate a short- to near-term solution to exchange ADatP-3 Baseline 11 messages cross-domain while considering compliance with the emerging NATO IEG architecture and evolving architectures for deployable CIS by evolving the 2005/2006 IEG FS Security Labeler / Sanitizer.	NATO, DEU	Mar 07 to Nov 07
Performance Benchmark	Conduct various CENTRIXS (GCTF) testing scenarios in accordance with PB Test Plan. Validate that centralized services can provide better or equal performance compared to existing COCOMS and Multi-National Participants. Establish performance goals for centralized capabilities. Culturalize COCOM and Multi-National Partners use of Defense Enterprise Computing Centers (DECC) for coalition networking.	AUS, GBR, USA	Mar 07 to May 07
NTDLIOT 07-01 (ARTEL)	To conduct a NTDLIOT with various National / NATO assets	FRA, DEU, NATO, NOR, ESP, USA, GBR	Mar 07 to Apr 07
CDEP 07-01	To conduct tactical data link interoperability SIAP tests with CDEP participant PA nations assets.	AUS, DEU, ITA, NLD, ESP, USA, GBR	Mar 07 to Oct 07

UNCLASSIFIED

Initiatives 2007	Objectives	Participants	Proposed Dates
CWID 07	Evaluate technologies for utility, interoperability with existing and new systems, and security that can be moved into operational use within 6-12 months following the execution period.	USA, AUS, CAN, CZE, DNK, DEU, GBR, ESP, FRA, ITA, NATO, NLD, NOR, NZL, POL, ROU, TUR (SN/Os: AUT, FIN, SWE)	Jun 07
Empire Challenge 07	The objective is to assess near-term capability to execute Network Enabled Operations, work to resolve DCGS DIB Coalition Interoperability, evaluate emerging capabilities such as JIOC-I and DCGS Integration Backbone (DIB) in context with other C2 systems, and resolve outstanding Collection Management requirements. This demonstration will be executed at the western test ranges in China Lake, CA. EC07 includes full participation by Great Britain, Australia, and Canada.	USA, AUS, CAN, GBR, NATO	Jul 07
NUW	Based on Canadian developed Sub-Net Relay (SNR) technologies this project sets out to create an ad-hoc IP over UHF network in order to share Common Operating Picture (COP) information between collaboration platforms. By conducted a number of trials the hypothesis that the creation of the "Virtual Command Team" will enhance acquisition, tracking and ultimate prosecution will be validated.	CAN	Mar 07
MNE5	MNE 5 will explore the comprehensive strategy of the interagency community, and military support to that community. Experiment designers may include a focus on both logistics and medical issues. The focus areas that will be studied are: Comprehensive Approach - Interagency focused, Multinational Interagency Strategic Planning, Effects Based Approach to Multinational Operations, Coalition Information Strategy/Information Operations, Information Exchange Architecture, Interagency/Non-Governmental Organization Information Processes, Knowledge Development, and Effects Based Assessment.	USA, NATO, GBR, DEU, FRA, AUS, CAN (SNOs : FIN, SWE, and others to be determined)	Dec 09

Initiatives 2007	Objectives	Participants	Proposed Dates
CDEP (EL16CN)	<ul style="list-style-type: none"> • Measure the effectiveness and impact of Time Slot Reallocation (TSR) on host system performance. • De-risk future integration events involving TSR-enabled Tactical Systems. • Verify TSR functionality in JTIDS/MIDS terminals in a JDEP architecture. • Demonstrate the ability to perform testing with coalition participants using land based test sites in a DEP/JDEP architecture. • Measure and assess the ability to act as a force in a Joint/Coalition environment. • Verify joint/coalition system performance. Demonstrate JDEP/DEP via CFBLNet can be used for coalition training activities in an operationally realistic environment.	AUS, USA	Apr 07

Initiative Approval Process

124. At CMM05-3 - due to limitations in the old Initiative approval process it was decided to re-work and create a new framework for approval at CMM06-1. 'Out of session' work was conducted by the IWG to prepare a re-shaped Pub 1 Annex B and accompanying CIIP. This process, tool, and Pub 1 Annex B V3.0 outlining the routine were agreed by the C-EG in March 06 and subsequently launched. At CMM06-2 the process was reviewed and updated with minor changes to Pub 1 Annex B V4.0 and the CIIP V1.2. Views from the community were sought and it was generally agreed that the CIIP process is a great improvement in terms of tracking, cohesion, acquiring information and providing a valuable mechanism for 'out of session' approval of Initiatives.

Final Reporting and Performance Review

125. The CIIP, at Tab 11, contains the feed-back questionnaire from customers. A high percentage of these revealed that the CFBLNet as a whole performed effectively and efficiently. It must be said that when these are further distributed for internal review in accordance with step 16 of the CFBLNet Initiative Staffing Process (see Annex B Appendix 2), in many cases they attract no comments; also the customer feed-back is sometimes minimal. At CMM06-2, the C-EG tasked the Secretariat to capture any proposed improvements to the CFBLNet in the form of taskings to be endorsed by the C-EG, these being drawn from the Initiative close-out briefs.

Successes and Challenges

126. The revised Initiative approval process and CIIP introduced in March 06 was received favourably by the community and represents an effective way to conduct CFBLNet business, especially 'out of CMM session'.

127. Feed-back from all Initiatives using the CFBLNet showed high scorings and users were pleased with the CFBLNet performance in terms of achieving Initiative objectives.

128. The CFBLNet received commendation from the United Kingdom Royal Air Force for the DAOC/CAOC-X 4 Star Initiative – this gave visibility of the CFBLNet to the most senior military officer in MOD (UK). The Initiative processing and implementation of the infrastructure was rapidly developed and commissioned attracting praise at the highest level. This is considered an accolade for the Initiative approval process.

129. The drawback of long lead times on elements, such as security accreditation and cryptographic device procurement/performance that are beyond CFBLNet control, continues to frustrate the users.

Strategic Plan Enabler Achievements

130. Provide a Customer Friendly Network and RDT&A capability (Enabler 1.7).

- The outcome of all Initiative Final Reports attracts high scorings and repeat business for the CFBLNet community as a whole for their flexibility and support towards successful completion of Initiatives. To improve quality of service the community decided to generate a set of documents to allow easier use of the CFBLNet.

131. Better manage the scheduling of Initiatives to achieve bandwidth efficiencies and resolve Initiative scheduling conflicts (Enabler 3.1).

- The Initiative management process gives full visibility of timetables for events to maximize utilization of network capabilities and accommodate user schedules. A specific example would be the GUST Initiative which hosted a training event on a non-interfering basis with other ongoing Initiatives.

132. Improve Initiative screening processes to include participation by an SN/O (Enabler 3.2).

- During the IWG CMM06-2 meetings, discussions were held on the processes to encompass SN/Os into Initiatives. From experience, the USA provided the procedures and definitions which reside in Annex B, Appendix 3. It was agreed that these would be further reviewed in 2007.

133. Review performance of CFBLNet based on Initiative outbrief reports and implement necessary improvements (Enabler 3.4).

- At CMM06-2 a mechanism was devised to capture outputs from final reports that recommended improvements to the CFBLNet. These are in the form of taskings endorsed by the C-EG and delegated to the appropriate working group for investigation and implementation.

134. Maturity assessment and routing of Initiatives (Enabler 3.5).

- Step 3 of the Initiative approval process is broadcast to all CLRs (and specifically CLRs directly involved in the Initiative), to seek their approval for the CIIP to proceed for further WG review. It is at this stage that maturity is agreed and forwarded for further approval.

135. Should there be any changes (significant or minor); the lead CLR is responsible for dialogue with participants and resubmitting the CIIP as appropriate. A significant change (i.e. cross boundary devices, site changes) requires that the CIIP be recycled through the approval process. A minor change such as a change in timings is distributed to the community for visibility and action where required.

2007 Focus

136. The current Initiative approval process tool (CIIP) will be used and strengthened to provide a sound framework for Initiative management. The process will stay streamlined and not become clouded by red-tape; (it portrays the high level routines to follow and should not become over-complicated). It therefore relies on the services of the community to be flexible and pragmatic to expedite a good quality of service to customers. Increased activity to focus on any improvements with respect to CFBLNet performance could benefit the service, the vehicle here being taskings from the close-down reports.

Documentation Working Group Summary

137. The first complete version of the CFBLNet Publication 1 was completed in 2003. This document 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.

<p>Technical Arrangement (Charter) <i>Updated: DEC04</i></p>	<p>Signed & Approved by C-SSG: December 2004</p>
<p>Publication 1: Organization and Responsibilities <i>Version 4.0</i></p>	<p>Signed & Approved by C-EG: November 2006</p>
<p>CFBLNet Publication 1 – Annex A: Glossary <i>Version 4.0</i></p>	<p>Approved by C-EG: November 2006</p>
<p>CFBLNet Publication 1 – Annex B: Initiative Processing <i>Version 4.0</i></p>	<p>Approved by C-EG: November 2006</p>
<p>CFBLNet Publication 1 – Annex C: CFBLNet Security and Information Assurance Strategy <i>Version 4.0</i></p>	<p>Approved by C-EG: November 2006</p>
<p>CFBLNet Publication 1 – Annex D: Network Operations (Network/System Aspects of the CFBLNet) <i>Version 4.0</i></p>	<p>Approved by C-EG: November 2006</p>
<p>CFBLNet Publication 1 – Annex E: CFBLNet Document Management <i>Version 4.0</i></p>	<p>Approved by C-EG: November 2006</p>

138. In 2006, 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, annexes were separated and one appendix has been labelled as Unclassified Not Internet Releasable (UNIR) and is available via more secure means of transmission. A new Annex E on CFBLNet Document Management was added to describe the lifecycle and format of CFBLNet documents.

139. In 2007 the following documents will be added to reach out to potential users of the CFBLNet:

- CFBLNet Information Pamphlet
- Basic Guide to CFBLNet Initiatives Process
- Basic Guide to CFBLNet Security and Accreditation

140. Version 5 of Pub 1 will include the Information Management Plan, consolidated terms of reference, and changes to reflect progress in CFBLNet technology. An overlapping document revision cycle will be introduced for the version 6 revision cycle to allow each revision to be frozen for consistency checking prior to signature, with new changes being carried forward to the next cycle.

Network Working Group Summary

For 2006, network engineering efforts and corresponding enablers are discussed below.

141. Backbone Transport, Enabler 1.1:

- All nations continued to utilize the CFBLNet Backbone (IPv4) transport in support of unclassified and classified Initiatives. Some of the technologies tested and evaluated in enclaves off of the Backbone include Public Key Infrastructure (PKI), Joint Unmanned Combat Air System (JUCAS), Intelligence Surveillance and Reconnaissance (ISR) and Simulated War Gaming events.
- Provided CFBLNet scalability for large Initiatives such as MNE, CWID and Empire Challenge.
- A standardized Black-Backbone IP address schema was developed.
- A Network Statistics Server is now available for all nations to view Backbone network statistics.
- Bandwidth management is being conducted using “rate limiting” and Quality of Service (QoS).

142. AUSCANZUKUS + NATO (BLUE) Enclave, Enabler 1.2:

- All nations kept the BLUE Enclave up either full or part time.
- Core Services included DNS, MAIL, VoIP, Network Time Protocol (NTP) and Web Server.
- Allied Communications Publication (ACP) 145 Defense Message System (DMS) testing and evaluation was conducted on the BLUE Enclave.

143. CFBLNet Unclassified Enclave (CUE), Enabler 1.3:
- IPv6 testing was conducted in the CUE tunneling IPv6 over IPv4 using Boundary Protection Service (BPS) devices configured with 128 bit Advanced Encryption Standard (AES) encryption.
 - CUE is capable of internet access through BPS device.
 - Further developed and improved the CFBLNet IPv6 test plan that includes IPv6 testing in dual stack, tunneling and translation configurations.
 - QoS testing was completed in the CUE.
 - DNS is the only CUE Core Service required. VoIP is available as needed.
144. Four Eyes Enclave (FEE), Enabler 1.2:
- Completed physical move of the FEE from behind the BLUE Enclave to off of the Backbone.
 - Reduced double encryption and free equipment resources.
 - Eliminated single point of failure.
 - Provided Email, DNS, VoIP and Network Management Services.
145. NATO Enclave (RED), Enabler 1.2:
- Established initial instance of permanent enclave for classified Initiatives conducted among NATO members.

2007 Focus

146. In 2007 there will be an emphasis in the following network engineering efforts and areas of concern:
- Ensure compliance with the CFBLNet Strategic Plan Objectives and Enablers.
 - Adhere to CFBLNet Network Enhancement Plan.
 - Reduce number of crypto breaks wherever possible.
 - Transition from a hub and spoke configuration to a fully meshed topology.
 - Strive to maintain multinational encryption device interoperability.
 - Further implementation of the Multiprotocol Label Switching (MPLS) on the Backbone to enhance bandwidth management and QoS.
 - Conduct additional IPv6 testing and strive to be IPv6 compliant by 2008.

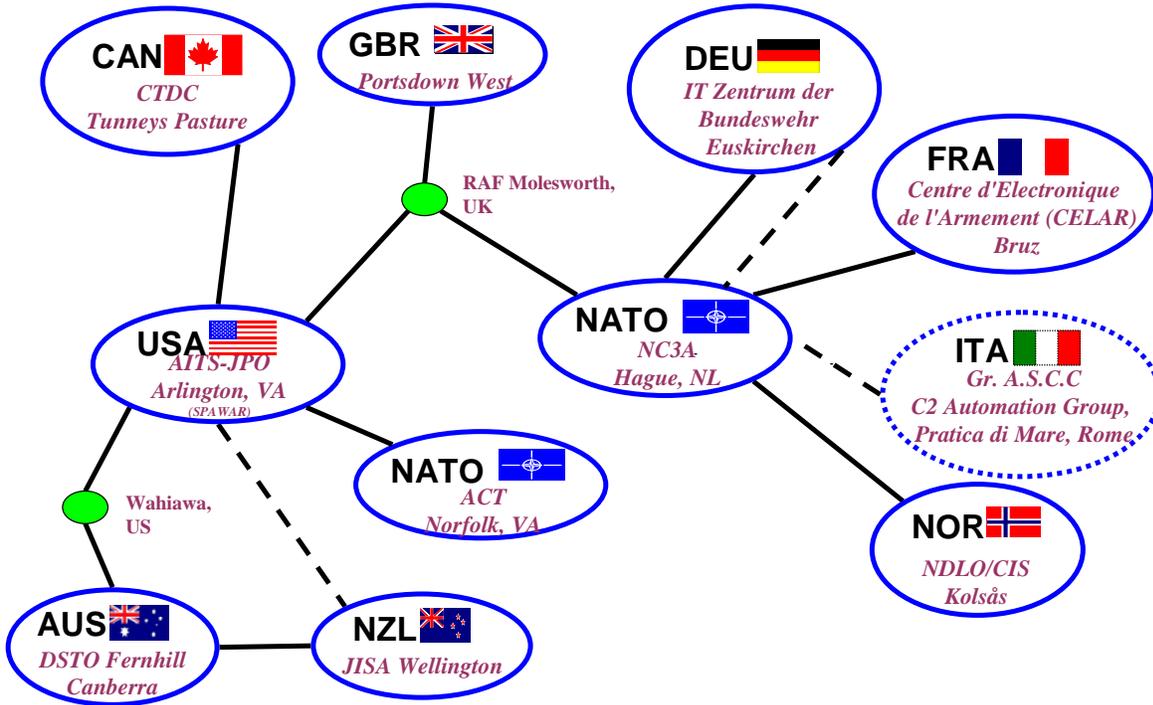
CFBLNet Sites

147. 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 in 1999, the CFBLNet was composed of 17 sites. The below table indicates the number of nominated, approved, accredited and/or operational sites that existed in 2006.

Nation/Organization	# of Sites
Australia (AUS)	13
Canada (CAN)	12
France (FRA)	6
Germany (DEU)	13
Italy (ITA)	5
NATO	9
New Zealand (NZL)	5
Norway (NOR)	6
Poland (POL)	1
Spain (ESP)	2
United Kingdom (GBR)	21
United States (USA)	23
TOTAL	116

CFBLNet 2006 Sites

148. The illustration below indicates CFBLNet Level 0 (zero) topology with national points of presence (POPs) for 2006.



CFBLNet 2006 Level 0 Topology

Annual Report Conclusion

149. In 2006, CFBLNet made significant advances in institutionalizing processes and procedures, ensuring effective, warfighter focused operations for the future. The new Initiative submission process and tool (CIIP) provides an efficient means to capture required mission, engineering, and security information and guarantees successful research, testing, and development. The CFBLNets enhanced security procedure provides clarity to an often complex and demanding process. New network tactics, techniques, and procedures focus CFBLNet engineering efforts, and facilitate successful network setup and delivery.

150. To improve customer service, the new CFBLNet Publication 1 (Version 4.0) establishes a formal feedback process to capture customer concerns and track resolution of issues. During the first three months of implementing this new process, several improvements were made to enhance future Initiatives.

151. CFBLNet Management emphasized renewed focus on warfighter impact for 2006 and 2007. To ensure the network achieves a return on investment for all contributing countries, CFBLNet processes now capture direct mission improvements based on successful Initiatives.

152. CFBLNet continues to provide the Coalition network environment supporting technical and multinational information sharing trials. There was increasing support for the CFBLNet Unclassified Environment (CUE). The procedure for the inclusion of non-charter nations and organizations in CFBLNet Initiatives and activities is now captured as part of the formal CFBLNet processes. These factors have allowed the CFBLNet to continue in its growth and evolution as the Coalition RDT&A infrastructure of choice.

153. In the upcoming year, we intend to continue focus on warfighter impact and improving our customer support. New user guides for security and Initiative submissions promise to add clarity and increase customer understanding. A new CFBLNet pamphlet will promote better understanding of the CFBLNet mission, its organizational principles, and the impact to warfighter operations for this critical multinational testing infrastructure.

Annex A: Acronyms

AFB	Air Force Base
ACP	Allied Communications Publication
ACTD	Advanced Concepts Technology Demonstration
AES	Advanced Encryption Standard
AUS	Australia
AUT	Austria
AZ	Arizona
BPS	Boundary Protection Service
C2	Command and Control
C3	Consultation, Command & Control
C4ISR	Command Control Communications Computers Intelligence Surveillance & Reconnaissance
CA	California
CAN	Canada
CCEB	Combined Communications Electronics Board
CDEP	Coalition Distributed Engineering Plant
CDIFT	Coalition Distributed Information Test Bed
CEC	Co-operative Engagement Capability
C-EG	CFBLNet Executive Group
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFBL	Combined Federated Battle Laboratory
CFBLNet	Combined Federated Battle Laboratory Network
CIIP	CFBLNet Initiative Information Pack
CIS	Communications and Information Systems
CLR	CN/O Lead Representative
CMM	CFBLNet Management Meeting
CND	Computer Network Defense
CN/O	Charter Nation/Organization
COCOM	Combatant Command
CONOPs	Concept of Operations
COP	Common Operating Picture
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
CZE	Czech Republic
DAOC/CAOC-X	Developmental Air Operations Centre/Combined Air Operations Center Exercise
DECC	Defense Enterprise Computing Centers
DEN	Denmark
DEP	Distributed Engineering Plant
DEU	Germany
DCGS	Defense Common Ground Surface Systems

DIB	DCGS Integration Backbone
DMS	Defense Message System
DNK	Denmark
DNS	Domain Name Server
DstI (DSTL)	Defence Science Technologies Laboratories
DSTO	Defence Science Technologies Office
DSTX	DSTO/DSTL
ESP	Spain
FEE	Four Eyes Enclave
FIN	Finland
FRA	France
FS	Functional Service
GBR	United Kingdom/Great Britain
GCTF	Global Counter-Terrorism Force
GPDN	Griffin Prototyping and Development Network
GUST	DEU/GBR Synthetic Training Trial
HF	High Frequency
HUN	Hungary
IDS	Intrusion Detection System
IEG	Information Exchange Gateway
IM	Information Management
IP	Internet Protocol
Ipssec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol version 6
ISAF	International Security Assistance Force
ISR	Intelligence, Reconnaissance, & Surveillance
ITA	Italy
IWG	Initiatives Working Group
JDEP	Joint Distributed Engineering Plant
JIOC-I	Joint Intelligence Operations Center-Iraq
JUCAS	Joint Unmanned Combat Air System
JWID	Joint Warrior Interoperability Demonstration
LAN	Local Area Network
M&E	Modelling & Simulation
MAJIIC	Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition
MCTS	Maritime Composite Training System
MGT	MIC Griffin Testing
MIC WAN	Multinational Interoperability Council Wide Area Network
MLS	Multi-Level Security
MNE	Multi-National Experiment
MOD	Ministry of Defence
MPLS	Multi-protocol Label Switching
MSAB	Multi-National Security Accreditation Board
MSI	Multi Sensor Integration
NAEC	National Accreditation Endorsement Certificate

UNCLASSIFIED

NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation Command & Control Agency
NLD	Netherlands
NITB	National Information Test Bed
NOR	Norway
NTP	Network Time Protocol
NUW	Networked Underwater Warfare
NZL	New Zealand
PA	Project Arrangement
PB	Performance Benchmark
PfP	Partnerships for Peace (NATO term)
PKI	Public Key Infrastructure
POC	Point of Contact
POL	Poland
PoP	Point of Presence
QoS	Quality Of Service
RDT&A	Research, Development, Trials & Assessment
RAF	Royal Air Force
RAP	Recognized Air Picture
RGP	Recognized Ground Picture
ROU	Romania
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAIP	Security Architecture Implementation Plan
SIMEX	Simulation Exercise
SN/O	Sponsored Nation/Organization
SNR	Sub-Net Relay
SWE	Sweden
STANAG	STANdardization AGreement
SWG	Security Working Group
TDLITS	Tactical Data Link, Interoperability Testing
TLS/SSL	Transport Layer Security/Secure Socket Layer
TSR	Time Slot Reallocation
TTCP – AG4	The Technical Coordination Program
TUR	Turkey
UK	United Kingdom
UK-IST	United Kingdom – International Support Team
UMC	Unified Modelling Capability
UNIR	Unclassified Not Internet Releasable
US	United States
USA	United States of America
VBE	Virtual Battle Experiment
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network