

UNCLASSIFIED

COMBINED FEDERATED BATTLE LABORATORIES NETWORK (CFBLNET)



2007 ANNUAL REPORT

UNCLASSIFIED

Executive Summary

The 2007 annual report provides background of the Combined Federated Battle Laboratories 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 continued to support several key warfighting Initiatives during 2007. Initiatives included: file transfer assurance techniques, Maritime C2 related to Sub Net Relay (SNR) supporting net centric environments, and enhancements to tactical data link (TDL) deployment. The network also supported national and coalition capability development programmes, trials and exercises throughout the year. Some specific success stories include the following:

- CFBLNet successfully demonstrated its ability to meet the demands of increasingly complex and diverse Initiatives. This success was recognized by the GBR Chief of Defence Materiel (4 star) as he visited CWID 07, and acknowledged with a Letter of Commendation the benefit of such an exercise, for rapid “fieldability” of warfighting capability and for de-risking acquisition programmes. GBR received thanks from operational staff at RAF Digby, JARIC RAF Brampton and JFCOM USA for Empire Challenge 07 and BCME respectively.
- CWID07 Initiatives conducted via the CFBLNet during 2007 have directly resulted in a number of operational capabilities being fielded or progressed through the acquisition pipeline (e.g. Assured File Transfer (AFT) by CENTCOM and DISA, Maritime C2 Information System for Italy, Tactical Emergency Asset Management deployed by US Department of Homeland Security, MobiKey Pilot program for USN Reserves).

Additionally, several technical tests were conducted to enhance network service capabilities and interoperability in the areas of data throughput (network accelerators) and Information Management. During 2007 the 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 2007. During 2007, 13 nations/organizations connected nationally to CFBLNet with 12 other nations acting as observers or participants to support various Initiatives. C-EG accomplishments during 2007 included:

- Completed a significant revision of Publication 1 and associated Annexes

- Refined the process to facilitate the participation of non-chartered nations/organizations in CFBLNet Initiatives
- Over one hundred thirty-five (135) CFBLNet sites were operational in 2007

In 2007, 21 CFBLNet Initiatives were introduced, 19 Initiatives were completed. Within those Initiatives, numerous individual trials and assessments were conducted, e.g. CWID07 included 47 coalition trials and assessments, as well as many national trials held by participating nations (e.g. NATO conducted more than 140 nationally sponsored interoperability trials during CWID07). 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 2007 include:

- Information Management Guidance (Enabler.3.7)
 - A dedicated section on information management was included in Annex E *CFBLNet Document Management* of Publication 1 in version 5.0
- Creation of three new documents (Enabler.1.7)
 - CFBLNet Information Brochure
 - Basic Guide to the Initiatives Process
 - Basic Guide to Security Accreditation
- Standardized Border Protection Schemes (Enabler.2.1)
 - A dedicated section on BPS was included in Annex C *CFBLNet Security and Information Assurance Strategy* of Publication 1 in version 5.0

During 2008, CFBLNet will focus on:

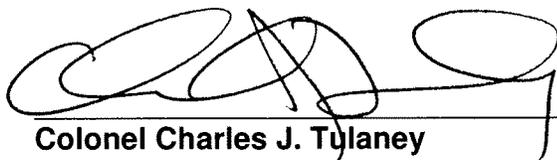
- Enterprise Network Management Capabilities (Enabler.2.2)
 - Bandwidth monitoring, quality of service (QoS) monitoring, and Intrusion Detection Systems (IDS)
- Improve Initiative screening processes to include participation by Sponsored Nations/Organisations (SN/O) (Enabler.3.2)
 - Refine processes, in particular those related to SN/O sites
- Improve CFBLNet infrastructure, services, support and management (Objective.3.3)
 - Continuation of network infrastructure and process management development to support the ever increasing demands of the RDT&A community

UNCLASSIFIED

This page intentionally blank

UNCLASSIFIED

The Chairman, on behalf of the Combined Federated Battle Laboratories Network (CFBLNet) Executive Group (C-EG), hereby approves the CFBLNet 2007 Annual Report.



5 May 08
(date)

Colonel Charles J. Tulaney
Joint Staff, J6X
C-EG Chairman/U.S. Representative

With endorsement from:

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

Lieutenant Colonel Noel Rings
CCEB Executive Group
CCEB C-EG Representative

Table of Contents

FOREWORD..... 7

BACKGROUND..... 7

2007 EVENTS..... 7

PARTICIPANTS..... 8

CFBLNET EXECUTIVE GROUP REVIEW 10

SECURITY WORKING GROUP SUMMARY 12

INITIATIVES WORKING GROUP SUMMARY..... 13

DOCUMENTS WORKING GROUP SUMMARY 22

NETWORK WORKING GROUP SUMMARY..... 24

CONCLUSION 29

ANNEX A: ACRONYMS..... 30

Foreword

100. This report reflects the progress and accomplishments of the Combined Federated Battle Laboratories Network (CFBLNet) during the calendar year 2007.

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 Laboratories (CFBLNet). Organizers from the US, NATO and Combined Communications-Electronics Board (CCEB) developed a concept for the CFBLNet 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 CFBLNet 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.

2007 Events

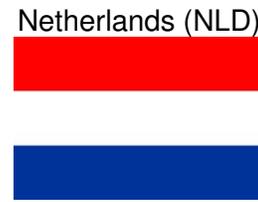
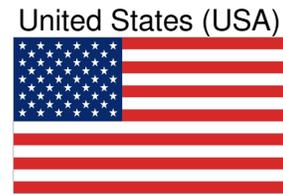
104. Two CFBLNet Management Meetings (CMMs) were hosted in 2007.

- CMM07-1
 - Charter Nation/Organization (CN/O) Host: USA
 - Location: Oracle Technology Centre, Reston, Virginia, USA
 - Dates: 19 – 23 March 2007

- CMM07-2
 - Charter Nation/Organization (CN/O) Host: Germany (NATO)
 - Location: Bundeswehr Zentrum, Dresden, Germany
 - Dates: 8 – 12 October 2007

Participants

105. Nations and Organizations connected to CFBLNet in 2007 are listed below:

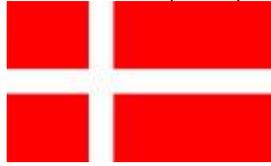


106. In addition, these nations have participated in or observed CFBLNet Initiatives at existing CFBLNet sites:

Czech Republic (CZE)



Denmark (DNK)



Hungary (HUN)



Finland (FIN)



Estonia (EST)



Sweden (SWE)



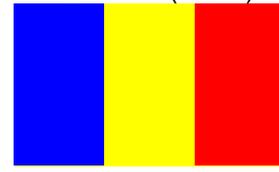
Turkey (TUR)



Portugal (PRT)



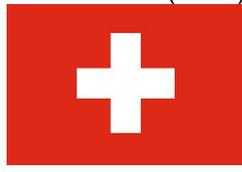
Romania (ROM)



Greece (GRC)



Switzerland (CHE)



Austria (AUT)



CFBLNet Executive Group Review

107. The C-EG focused on institutionalizing CFBLNet processes and procedures during 2007. The C-EG met in conjunction with the working groups at CMMs in March and October 2007. Key achievements during the CMMs included approving the new version 5.0 of CFBLNet Publication 1. Changes to CFBLNet Publication 1 included expanded guidance on the sponsorship process for non-charter nations, the addition of Information Management Guidance, improved consistency and clarity for the terms of reference, a major restructure to improve accessibility and clarity of Annex C *Security and Information Assurance Strategy*. The production of three short informative documents on CFBLNet (*Introduction to the CFBLNet*, *CFBLNet Initiative Process*, and *Basic CFBLNet Security Accreditation Guide*) has improved the accessibility of CFBLNet to new participants and range of Initiatives. The Strategic Plan served to guide the actions and priority of effort of the C-EG as well as the functional Working Groups, providing 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 2007, the C-EG continued to implement the CFBLNet Strategic Plan. 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 C-EG maintained the Strategic Plans 14 objectives and 23 specific tasks (Enablers) to guide progress towards the stated 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 2007, CFBLNet completed two Enablers. The end of year status for 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 (2006)
		Enb.1.2 Provide and manage enclaves for the conduct of classified Initiatives between the Charter Nations/Organizations (CN/O)	ONGOING (2006)
		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 (2006)
		Enb.1.4 Implement multi-nationally agreed accreditation processes to enable secure interconnection of nationally accredited CIS systems.	DONE (2006)
		Enb.1.5 Establish end to end IPv4 routing on the Black-backbone	DONE (2006)
		Enb.1.6 Maintain a Public Website populated with relevant and accurate information	ONGOING (2006)
		Enb.1.7 Provide a Customer Friendly Network and RDT&A capability	ONGOING (2006)
		Enb.1.8 Develop and maintain an interactive, online process for users to populate CIIPs.	PENDING (2006)
		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 Modeling & Simulation (M&S) activities Obj.2.5. Promote the use of the CFBLNet network for training when not in use for Initiatives
Enb.2.2 Establish Bandwidth Management (constraint and monitoring)	ONGOING (2006)		
Enb.2.3 Exploit multi-national multi level security for cross domain solutions	PENDING (2006)		
Enb.2.4 Evolve CFBLNet infrastructure and services to be IPv6 compliant.	ONGOING (2006)		
Enb.2.5 Provide infrastructure and services able to support IPv6 Initiatives.	ONGOING (2006)		
Enb.2.6 Provide capabilities able to support MLS Initiatives.	PENDING (2006)		
Enb.2.7 Provide capabilities able to support M&S trials (real time and low latency).	ONGOING (2006)		
Enb.2.8 Examine the requirement for computer network defence (CND) capabilities and procedures for CFBLNet.	ONGOING (2006)		
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 (2006)
		Enb.3.3 Evaluate methods (eg Groove) to improve information management and sharing within and between CFBLNet WGs	ONGOING (2006)
		Enb.3.4 Review performance of CFBLNet based on Initiative outbrief reports and implement necessary improvements.	DONE (2006)
		Enb.3.5 Maturity assessment and routing of Initiatives.	DONE (2006)
		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 (2006)
		Enb.3.7 Develop a comprehensive information management plan addressing creation, coordination, storage, configuration management, and control of information.	DONE (2007)

110. CFBLNet Pub 1 Version 5 was approved by the C-EG in December 2007. The publication has been restructured to make it more useful to users of CFBLNet based on the experience to date, and to provide a clearer description of the organization and especially the terms of reference and information management aspects. The dynamic nature of CFBLNet business will necessitate periodic review of this publication, but the expectation is that the document has now achieved sufficient stability that the update cycle can now be moved from annual to every second year.

111. The CFBLNet Strategic Plan describes the long term Goals and Objectives, against which the C-EG continues to monitor progress towards achieving the associated enablers and tasking the CFBLNet working groups accordingly. In 2008, particular focus is being placed on enablers relating to core network services and supporting new participants to the network. Upgrades to the network are being conducted as necessary.

Security Working Group Summary

112. In 2007, the security efforts for CFBLNet focused on the standardization of border protection schemes for CFBLNet enclaves (Enabler 2.1). The SWG also made significant progress on the requirements and drafting of the implementation strategy for a CFBLNet-wide Computer Network Defence (CND) capability (Enabler 2.8).

Regarding Enabler 2.1, the SWG:

- Streamlined in *Annex C: CFBLNet Security and Information Assurance Strategy* the encryption and Boundary Protection Service (BPS) requirements for cross domain connections and, in particular, highlighted the security requirements applicable to the following interconnection scenarios:
 - Unclassified Domains/Enclaves to the Internet;
 - Backbone to the Internet;
 - Sponsored Nations to the Backbone.

Regarding Enabler 2.8, the SWG:

- Defined the CND related information items that could be shared within the CFBLNet Community to improve the common security posture and submitted the list of items to the consideration of the CN/Os;
- Investigated the possibility of correlating information coming from Intrusion Detection System (IDS) deployed by the CN/Os at their interface with the Backbone;
- Investigated the security incident handling process that would accompany the CN/Os technical infrastructure.

113. The SWG also produced a *Basic Guide to CFBLNet Accreditation Procedures* with the purpose to provide an overview of the CFBLNet accreditation requirements and procedures as well as the roles and responsibilities of the authorities involved in the accreditation.

114. The plan for 2008 is to progress the definition and implementation of CFBLNet-wide computer network defence (CND) capabilities (Enabler 2.8) while investigating the pre-requisites to support MLS Initiatives (Enabler 2.6), and promoting the use of the CFBLNet for multi-national, cross domain solutions (Enabler 2.3).

Initiatives Working Group Summary

115. For the reporting period of 2007 the CFBLNet hosted twenty seven C4ISR Initiatives, this demonstrated an upward trend by six from those listed in 2006. The Initiatives varied in size and complexity, the first Initiative on the theme of Logistics was conducted over the CFBLNet in Oct 07; aiming to improve Coalition Logistics Operations for Command Chains in Afghanistan. Initiatives such as CWID07 had embedded high numbers of multi-national trials and national demonstrations from some seventeen NATO and coalition partners.

116. The following table lists the 2007 Initiatives, some operational benefits and associated details.

Initiatives 2007	Operational Benefits	Participants	Dates
HF Equipment Trial	To develop and introduce IP services over HF bearers on FRA and GBR Naval Platforms, for legacy and future builds.	FRA, GBR	Jan 07
CWSD Project Churchill	Collaborative program to determine the military benefit of Unmanned Combat Air Systems within future coalition operations.	GBR, USA	Oct 05 to Mar 07
QLF LAWG R2 Test	To improve operational logistical methodologies in Afghanistan, to give high level command chains accurate and timely visibility of the logistics status and trends. Ability to trial passage of classified information in secure environment (AUS). <ul style="list-style-type: none"> • Guaranteed connectivity to evaluate operational procedures. • Ability to analyse experimental (operational based) information and procedures post activity. • Outcomes are shaping operational procedures which will be passed to QLF Chain of Command in Early/ Mid 2008. 	AUS, CAN, GBR, USA	Sep 07 to Oct 07
ACP 145 Messaging	To perform and develop formal messaging prior to deployment on operational command and control systems.	GBR, USA	Aug 05 to Sep 07

Initiatives 2007	Operational Benefits	Participants	Dates
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	Feb 07 to Mar 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. Culturalise COCOM and Multi-National Partners use of Defence Enterprise Computing Centres (DECC) for coalition networking.	AUS, GBR, USA	Mar 07 to May 07
CWID 07	<p>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.</p> <p>CIS testing has direct impact on the interoperability of coalition CIS which will have to co-operate in future NRF operations (DEU).</p> <p>C2 software development used in Afghanistan under an Urgent Operational Requirement to enhance its operability and following CWID 07 it was returned to operational use (GBR).</p> <p>Resulted as invaluable support for testing and integration of C2 systems within wide and stimulation environments. CWID is apparently the only useful way for implementing new interoperability capabilities in our C2 systems. C4I Defence has been literally improved and empowered by joining the CWID community. Ten Italian C4ISR systems have taken part in CWID 2007 in June. C4I Defense system has been positively assessed in terms of interoperability under NRF11-12 (ITA).</p>	AUS, CAN, CZE, DEU, DNK, ESP, FRA, GBR, ITA, NATO, NLD, NOR, NZL, POL, ROU, TUR, USA (SN/Os: AUT, FIN, SWE)	Jun 07
NTDLIOT 07-01 (ARTEL)	To conduct a NTDLIOT with various National and NATO assets to improve tactical C2 interoperability.	FRA, DEU, NATO, NOR, ESP, USA, GBR	Mar 07 to Apr 07
BCME	BCME is a USA Initiative for the conduct of experiments disseminating Consequence Mitigation information to Friends and Allies. BCME includes collaboration with GBR as a pathfinder in developing the first instantiation of BCME capability for Consequence Mitigation information dissemination and display.	GBR, USA	Aug 07 to Nov 07
QoS IPV6 2007	Demonstration of end to end network quality of service amongst multi-national distributed sites over an IPV6/IPV4 WAN.	DEU, FRA, NATO	Oct 07 to Nov 07

Initiatives 2007	Operational Benefits	Participants	Dates
NUW	<p>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.</p> <p>The March 07 Final Trial designed to test the hypothesis that Net-centric warfare has a distinct advantage over organic only operations. A preliminary assessment of trial success lies in an analysis of the original trial objectives as stated in the published Cruise Plan. All of the objectives were achieved with only a few exceptions. As such, this trial was an unqualified success and bodes well for the future of SNR as a vehicle for Net-centric warfare (CAN).</p>	CAN	Mar 07
Empire Challenge 07	<p>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, USA.</p>	AUS, CAN, GBR, NATO, USA	Jul 07
WW07	<p>Historically, the CAN Forces tactical aviation community trained and evaluated their candidates on the Advanced Tactical Aviation Course (ATAC) using live exercises. In recent years, the ability to support the ATAC in this manner has been severely constrained. In 2006, Commander 1 Wing decided to conduct the culminating exercise, Winged Warrior (WW) 2006, in a synthetic environment. While WW06 was considered sufficiently successful to evaluate student performance, a number of deficiencies were identified that, if corrected, would improve the realism of the exercise and provide a more effective training and evaluation tool.</p> <p>Synthetic training successful, advancing our capability stagnant (CAN).</p>	CAN	Aug 07 to Oct 07
NRF11-IETV Test	<p>The FRA Rapid Reaction Corps (FR-RRC) will be providing the LCC for NRF rotation 11. Other units from FRA shall provide additional functionality and C2 elements for NRF rotations 11 and 12. The main purpose of test plan is to implement a sound process to assess the ability of the FRA-provided CIS to fully interoperate with NATO DCIS during those NRF rotation</p>	FRA, NATO	Oct 07 to Nov 07

Initiatives 2007	Operational Benefits	Participants	Dates
NTDLIOT 07-02 (Shebloski)	<p>To develop and improve C2 tactical assets interoperability (in particular warships), this Initiative also incorporated PfP nations.</p> <p>2 Star Brief- NATO TDL Interoperability Tests have facilitated identification and correction of faults in E-3D mission system software, leading to improved E3-D situational awareness in Coalition operations (GBR).</p> <p>Resulted in effective data link testing for preparing the warfighter for using their typical operational platforms and assets (ITA).</p>	DEU, ESP, FRA GBR, ITA, NATO, NOR, USA. (SN/Os: SWE, AUT, CHE)	Oct 07
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	Nov 07
IEG Case B FS Trials	<p>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 Labeller / Sanitiser.</p> <p>Results will lead to enhance the operational baseline and are being implemented in the DEU Navy and the NATO IEG Light Project (DEU).</p>	DEU, NATO	Mar 07 to Nov 07
ICECAP	<p>The purpose of the ICECAP Initiative(s) is to provide an environment in which ISAF will exploit and planned C2IS to command and control operations. It will focus primarily on operations and intelligence Functional Area Systems (FAS) and desktop collaborative tools. ICECAP Initiative will be a vehicle capable of being used for tests, experimentation, and validation to derive more effective ways of providing information to the warfighter and to ensure that plans for new or improve capabilities will provide ISAF with the expected efficiency gain.</p>	NATO, USA	Jul 07 to Dec 07

Initiatives 2007	Operational Benefits	Participants	Dates
CDEP 07-01	<p>To conduct tactical data link interoperability SIAP tests with CDEP participant PA nations assets.</p> <p>The C-DEP Multilateral Event is assessed as an invaluable venue to test interoperability amongst Tactical Command and Control Systems sharing a synthetic environment. The simulated exercise has shown the peculiarity to enhance Hi-Fidelity to real world through Ground Truth Data. At the moment, analysis and evaluation of recorded data are underway and will continue (ITA).</p> <p>Increase interoperability in joint and combined operations and influence the way our forces train and fight in the future (DEU).</p> <p>It is highly likely that operational platforms of participating nations will have to interoperate in future operations. As such, this Initiative was a valuable first step in de-risking this activity (GBR).</p>	AUS, DEU, ESP GBR, ITA, NLD, USA	Ongoing into May 08
CDIFT	<p>Coalition information fusion to input to acquisition programmes to enhance MN interoperability and support collaboration between countries in the development of new information fusion capabilities. A TTCP C3I Initiative.</p> <p>This Initiative is a TTCP C3I Information Fusion Technical Panel (TP1) activity to establish a distributed, heterogeneous coalition environment to support development and evaluation of information fusion technologies and applications. This will enable coalition interoperability, and support collaboration between coalition countries in the development of new information fusion capabilities (AUS).</p> <ul style="list-style-type: none"> • The CDIFT is an R&D activity, which has not been deployed in operational environments, but it has demonstrated technologies to support rapid integration of heterogeneous coalition systems with a loosely coupled, distributed information grid. • The information fusion capabilities under development will support the collection, association, correlation, assessment and summarisation of disparate information elements from a wide range of information sources to enhance the war-fighter's situation awareness in varied domains, including: Air Operations and Air Defence, Maritime Domain Awareness, Urban Operations, and Cyber/Information Operations. • The technologies demonstrated in the CDIFT are currently being examined by DSTO with the outlook to develop systems to augment situation awareness for air operations in the ADF. 	AUS, CAN, GBR, USA	Ongoing into Jul 08

Initiatives 2007	Operational Benefits	Participants	Dates
VBE E Net Test	Examine effectiveness of uninhabited air vehicles and third party targeting on coalition operations.	AUS, CAN	Ongoing into Feb 08
GUST 07	Training Initiative to link DEU and GBR Naval simulators in order to provide high fidelity training for warfighters. Increase interoperability in joint and combined operations and influence the way our forces train and fight in the future (DEU).	DEU, GBR	Ongoing into Feb 08
ACP 145 Interoperability Testing	Extending and supporting ACP145 capabilities for the GBR/USA ACP 145 operational Environment (i.e. validate gateway software fixes).	GBR, USA	Ongoing into Nov 08
CCEB PKI Interoperability	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 Jul 09
GOSHAWK	The Synthetic Environment Research Facility (SERF) secure LAN, is located at DRDC Toronto. The SERF is a participant on the War In A Box (WIB) enclave. Currently when not connected to WIB the SERF LAN participates in a series of simulations called Coalition Mission Training Research (CMTR). The purpose of CMTR is to study the role of distributed simulation technologies in training aircrew and key staff personnel for coalition air operations. Northern Goshawk is specifically focused on the study of Forward Air Controllers. This Ex will continue in multiple iterations until 2010.	CAN	Ongoing into Nov 10
NATO AITB	Primary support of risk reduction in the areas of national and NATO systems interoperability and integration in the ALT DAMB Target Architectures	DEU, ESP, FRA, GRC, ITA, NLD, POL, USA	Ongoing into Dec 13

117. The following table provides details of the Initiatives that plan to use CFBLNet in 2008, with eight Initiatives from the list above continuing activity in 2008 from 2007. Further Initiatives are anticipated during the year. It can be seen that Initiatives such as NATO AITB extend to 2013.

Initiatives 2008	Objectives	Participants	Proposed Dates
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 AUS and GBR.	GBR, AUS	May 08 to Dec 08

UNCLASSIFIED

Initiatives 2008	Objectives	Participants	Proposed Dates
PTDLIOTS 08-01 (Schueller)	Tactical Data Links Interoperability Test Syndicate (TDLITS) to incorporate Partner Nations.	DEU, ESP, FRA, ITA, NATO, NOR, USA (SN/O: SWE)	Apr 08
CDIT	Correlation/De-correlation Interoperability trials between USA and GBR airborne assets	GBR, USA	Aug 08
CWID 08	A venue for multi-faceted objective assessment of technologies encouraging cooperation among coalition partners while reducing risk in acquisition. Evaluation of technology for utility and inter-operability with existing and new systems and security products to be moved into operations within 12 to 18 months.	USA, NZL, AUS, GBR, CAN, NATO, DEU, NOR, ITA, ESP, CZE, DNK, FRA, POL, ROU, TUR (SN/O: SWE, FIN)	Jun 08
SIGMD&S PA 1	Design, build, execute and analyze MTMD SIGDM&S Missile Defence scenario. Establish and verify processes and CFBLNet infrastructure is suitable for future MTMD M&S PA initiatives.	USA, AUS, CAN, DEU, NLD	Sep 08
TDLIOT 08-02 (Major Bob)	Await CIIP submission	DEU, FRA, ESP, FRA, GBR, ITA, NATO, USA	Oct 08
GPDN	To develop the CCEB Web Service, DNS Service, Chat Service and the technical refresh of the MN Interoperability Service using a Type 1 High Grade encrypted enclave. Technology will be deployed in Coalition command and control systems.	AUS, CAN, GBR, NZL, USA	May 08 to Mar 09
VCDOAS	Await new CIIP submission - (See 2007 event above)	AUS, CAN, GBR, USA	TBA
COSMOS	COSMOS is a USA Advanced Concept Technology Demonstration (ACTD). In addition to the USA the ACTD involves AUS, CAN, GBR and more recently Singapore. The participants are developing a way to allow the unambiguous sharing of information between coalition partners and to collapse the number of operational networks required, while maintaining need-to-know levels of separation. COSMOS will employ the MIP C2IEDM data model to address the unambiguous sharing aspects and use VPN technology augmented with configuration and control tools to achieve the need-to-know separation requirements. The USA NSA is overseeing the design of the security components. Each participant nation will validate this approach against a national C2 system. In Australia's case the national system is BCSS. BCSS is being extended to support a C2IEDM interface.	AUS, CAN, GBR, USA,	TBA

Initiatives 2008	Objectives	Participants	Proposed Dates
MCTS	Inter-operability of tactical maritime assets	GBR, USA	TBA
Empire Challenge 08	Extended Awareness (EA), under the Joint Operational Test Bed System (JOTBS) integrates operations, information and technical capabilities around unmanned systems as part of the Joint Functional Concept for Battlespace Awareness. EA II and EA III further the work of previous Forward Look experiments.	USA, AUS, CAN, GBR, NATO	Jul 08

118. At CMM07-1 and 2, fine tuning was made to the Initiative management and approval process in order to improve the 'quality of service' to the customer base. These revisions are reflected in the latest *CFBLNet Publication1 V5.0 Annex B: Initiative Processing* and accompanying CFBLNet Initiative Information Package (CIIP) V1.4. The Initiative approval process continues to be an improvement in terms of tracking, cohesion, acquiring information and providing a valuable mechanism for 'out of session' approval of Initiatives. The Secretariat has set up a space on Groove to provide all Initiative details, to include CIIP history; this has proved invaluable for the instant tracking of Initiative status.

119. CIIP changes over 2007 were in the main to enrich its substance in terms of the Initiative responsibilities for security regulations, legal agreements and key material distribution. Development work is in progress by the Secretariat to construct an online CIIP for users to populate as assisted by Lead Charter Nation / Organisation (CN/O) Lead Representatives (CLR).

120. The CIIP contains a feed-back questionnaire from customers. A high percentage of these revealed that the CFBLNet continues to perform effectively and efficiently in this complex environment and customers will use the CFBLNet again. The common issues identified are:

- Sponsorship of non-chartered nations;
- Security accreditation of sites and Initiatives;
- Key material distribution; and
- Service outages (crypto issues).

121. Any lessons learnt from Initiatives that experience delivery of service difficulties are captured, reviewed and if possible improvements are implemented.

122. Feed-back from all Initiatives using the CFBLNet rated highly and users were pleased with the CFBLNet performance in terms of achieving Initiative objectives.

123 To highlight an example, the Information Exchange Gateway (IEG) Case B Initiative results will lead to an enhancement of the operational baseline and are being

implemented in the German Navy and the NATO IEG Light Project. Other examples include:

- GBR developed under an Urgent Operational Requirement (UOR) the C2 software used in Afghanistan to enhance its operability and following CWID07 it was returned to operational use.
- GBR 2 Star Brief - NATO TDL Interoperability Tests have facilitated identification and correction of faults in E-3D mission system software, leading to improved E3-D situational awareness in Coalition operations.
- GUST 07 represented a training Initiative conducted over the CFBLNet linking together GBR and DEU Fleet Warship Operator Simulators and QLF the first coalition logistics Initiative, demonstrating the developing nature of CFBLNet.

124. The CFBLNet has successfully demonstrated its ability to meet the demands of increasingly complex and diverse Initiatives. This success was recognized by the GBR Chief of Defence Materiel (4 star) as he visited CWID 07, and acknowledged with a Letter of Commendation the benefit of such an exercise, for rapid “fieldability” of warfighting capability and for de-risking acquisition programmes. GBR received thanks from operational staff at RAF Digby, JARIC RAF Brampton and JFCOM USA for Empire Challenge 07 and BCME respectively.

125. As examples of improved administrative effectiveness:

- The revised Initiative approval process and the CIIP updates implemented in 2007 continue to be received favourably by the community, and they are proving to be an effective way to conduct CFBLNet business, especially ‘out of CMM session’.
- The production of Basic Guide Documentation to assist CFBLNet users in terms of the Initiative and Security Approval Processes has proved extremely useful; in particular to brief potential user about CFBLNet.

126. The expanding list of mission partners dictates flexible and responsive procedures for the incorporation of non-chartered nations and organizations. A significant challenge for CFBLNet management is to establish effective processes for integrating new users into the CFBLNet Community. Key challenges are the development of legal and security documentation among nations and organizations, e.g., nation-to-nation Information Sharing Arrangements – much of which is outside the scope of CFBLNet.

127. It is intended during 2008 to address where the CFBLNet can rationalise its approach on these challenges, albeit some dependencies are outside the CFBLNet jurisdiction, but the CFBLNet management intends to forge a way ahead for expanding partnerships.

128. The following Strategic Plan Enablers have progressed:

- Most Initiatives within the programme are enclave based using NATO, USA or National type 1 cryptographic devices. (Enabler 1.2)
- The outcome of most Initiative Final Reports continue to attract high scorings and repeat business for the CFBLNet community as a whole for their flexibility and support towards successful completion of Initiatives. (Enabler 1.7).
- The Initiative management process gives full visibility of timetables for events to maximise utilisation of network capabilities and accommodate user schedules. Weekly teleconferences take place between the Secretariat and Initiative Chair to monitor the dynamic situation and report changes to the community for implementation. (Enabler 3.1). (A specific example would be the GUST 07 Initiative which hosted a training event on a non-interfering basis with other ongoing Initiatives and CDEP that required extended use of the CFBLNet.)
- During CMM07 - 1 and 2, discussions were held on the processes to efficiently encompass SN/Os into Initiatives, the outcome is recorded in CFBLNet Publication Annex C *CFBLNet Security and Information Assurance Strategy* largely based on the experiences of the USA sponsoring SWE. Further experiences during the months of Oct 07 to Feb 08 for PTDLIOTS 08-01 (SCHUELLER) a NATO partnering Initiative that wished to involve SWE on home soil. Lesson learnt from this will be examined and the process simplified as an ongoing upgrade practice. (Enabler 3.2).
- A mechanism is running 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. (Enabler 3.4).
- 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 working group review. It is at this stage that maturity is agreed and forwarded for further approval. (Enabler 3.5).

129. During 2008, given the maturity of CFBLNet documentation, the organization will now focus on enhancing the CFBLNet 'quality of service' in support of the RDT&A community. A particular focus will be the solicitation of values added or benefits of using CFBLNet to support operational capability development and Defence acquisition cycles. Therefore increased momentum will be added in an attempt to capture 'golden nugget' type information.

Documents Working Group Summary

130. 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 align="center">Technical Arrangement (Charter) <i>Updated: DEC04</i></p>	<p align="center">Signed & Approved by C-SSG: December 2004</p>
<p align="center">Publication 1: Organization and Responsibilities <i>Version 5.0</i></p>	<p align="center">Signed & Approved by C-EG: December 2007</p>
<p align="center">CFBLNet Publication 1 – Annex A: Terms of Reference <i>Version 5.0</i></p>	<p align="center">Approved by C-EG: December 2007</p>
<p align="center">CFBLNet Publication 1 – Annex B: Initiative Processing <i>Version 5.0</i></p>	<p align="center">Approved by C-EG: December 2007</p>
<p align="center">CFBLNet Publication 1 – Annex C: CFBLNet Security and Information Assurance Strategy <i>Version 5.0</i></p>	<p align="center">Approved by C-EG: December 2007</p>
<p align="center">CFBLNet Publication 1 – Annex D: Network Operations (Network/System Aspects of the CFBLNet) <i>Version 5.0</i></p>	<p align="center">Approved by C-EG: December 2007</p>
<p align="center">CFBLNet Publication 1 – Annex E: CFBLNet Document Management <i>Version 5.0</i></p>	<p align="center">Approved by C-EG: December 2007</p>
<p align="center">CFBLNet Publication 1 – Annex F: CFBLNet Information Management Guidance <i>Version 5.0</i></p>	<p align="center">Approved by C-EG: December 2007</p>
<p align="center">CFBLNet Publication 1 – Annex G: Glossary of Terms <i>Version 5.0</i></p>	<p align="center">Approved by C-EG: December 2007</p>

131. In 2007, revisions to Publication 1 included improving the internal consistency of the document in content and use of terms, ensuring that information was cross-referenced. The terms of reference were updated, reflecting progress in CFBLNet technology. A new Annex (F) *CFBLNet Information Management Guidance* on

CFBLNet Information Management Guidance was added to describe the basic principles of information management to be applied by the CFBLNet community.

132. The following documents were published and distributed for use in 2007 to promote awareness among potential CFBLNet users:

- CFBLNet Information Brochure
- Basic Guide to the Initiatives Process
- Basic Guide to CFBLNet Accreditation Procedure

133. Version 6 of Pub 1 is planned for issue in 2009. It is not currently planned to include any major additional sections, but to include procedural updates and changes to reflect progress in CFBLNet technology.

Network Working Group Summary

134. The following Strategic Plan Enablers involving the Network Working Group have progressed:

- Provide and manage the CFBLNet Backbone Network Infrastructure (Enabler 1.1):
 - Nations continued to utilize the CFBLNet Backbone (IPv4) transport in support of unclassified and classified Initiatives, In addition some nations and organisations implemented IPv6 in their Backbone segment in parallel to IPv4. Some of the technologies tested and evaluated in enclaves off of the Backbone include:
 - Distributed Simulation of DIS / HLA and hardware in the loop systems.
 - Provided CFBLNet scalability for large Initiatives such as CWID, NATO-AITB and Empire Challenge.
 - A standardized IPPhone numbering template schema was developed which initiatives can use as starting point. Temporary Initiatives in their own enclave can apply a modified IPPhone scheme if required.
 - A Network Statistics Server is been used to view Backbone network statistics.
 - A Network Baseline test tool suit is been evaluated for standard Bandwidth testing.
 - Bandwidth management is being conducted using “rate limiting” and Quality of Service (QoS).
- Provide and manage enclaves for the conduct of classified Initiatives between the CN/Os (Enabler 1.2)
 - AUSCANZUKUS + NATO (BLUE) Enclave:
 - 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.

- AUS-CAN-GBR-USA Enclave (Four Eyes Enclave – FEE):
 - All nations kept the FEE up either full or part time.
 - Core Services included DNS, MAIL, VoIP, Network Time Protocol (NTP) and Web Server.
 - A broad number of initiatives, e.g., Empire Challenge 07 and Virtual Capability Development & Operational Analysis Symposium (VCDOAS)/QLF were conducted on the FEE Enclave in 2007.
 - Advanced technology tests performed on FEE in 2007 included performance testing of:
 - ❖ ‘Raw uIP’ (intended to make it possible to communicate using the TCP/IP protocol suite even on small 8-bit micro-controllers) and TCP traffic.
 - ❖ QoS on VCDOAS/QLF which was successful and is now permanent on FEE for VOIP.
 - ❖ Crypto impact on network performance resulting in enhanced understanding.
 - ❖ WAN acceleration devices Q4 2007.
 - NATO Enclave (RED):
 - Established initial instance of permanent enclave for classified Initiatives conducted among NATO members.
 - Provide and manage the CFBLNet Unclassified Enclave (CUE) for the conduct of multiple Initiatives for CN/O and SN/O participants. (Enabler 1.3)
 - Charter nations agreed to support a minimal configuration for CUE
 - DNS is the only CUE Core Service required. VoIP is available as needed
 - Advanced technology tests performed on CUE in 2007 included testing of:
 - IPv6 by tunneling IPv6 over IPv4 using Boundary Protection Service (BPS) devices configured with 128 bit Advanced Encryption Standard (AES) encryption. (Result: CUE is capable of internet access through BPS device.)
 - ❖ Further developed and improved the overall CFBLNet IPv6 test plan that includes IPv6, testing in dual stack, tunneling and translation configurations.
 - ❖ In relation to this development several nations and organisation have tested and End to end native IPv6 initiative, including IPv6 configured in the Backbone in support of this initiative.
 - QoS with results pending completion of tests which are ongoing
135. In 2007 the network engineers focused on:
- Completed initial build of the NATO Red Enclave on the Backbone.
 - NATO Red Enclave NOC established.
 - Provided DNS, email, VoIP, Web, Dir, NTP and Network Management Services. VTC services are planned for 2008.
 - Used by NATO Information Exchange Gateway trials and support the NATO

major multiyear NATO-AITB events.

136. In 2008 there will be an emphasis in the following network engineering efforts and areas of concern:

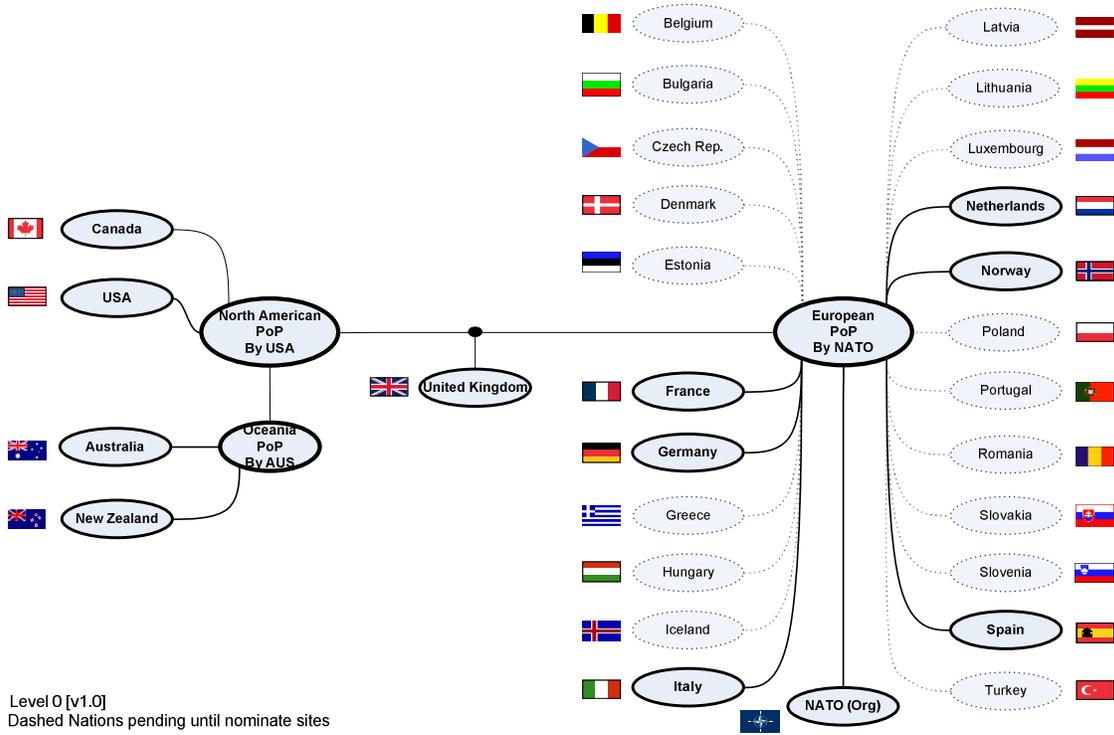
- Ensure compliance with the CFBLNet Strategic Plan Objectives and Enablers (continued).
- Adhere to CFBLNet Network Enhancement Plan.
- Reduce number of crypto breaks wherever possible, phase out non-IP encryptors where possible.
- Transition from a hub and spoke configuration to a more meshed topology.
- Strive to maintain multinational encryption device interoperability.
(note/observation: all Charter nations and organisation have access to one common IP encryptor, though usage is depending on National policy and procedures.)
- Continued implementation of the Multiprotocol Label Switching (MPLS) on the Backbone to enhance bandwidth management and QoS.
- Continue additional IPv6 testing and strive to be IPv6 compliant by end of Q4 2008.

137. CFBLNet sites are the physical locations accredited through national/ organizational assurance agencies in accordance with the National/Organisational and CFBLNet security processes 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 2007.

Nation/Organization	# of Sites
Australia (AUS)	12
Canada (CAN)	23
France (FRA)	6
Germany (DEU)	16
Italy (ITA)	5
NATO	9
New Zealand (NZL)	6
Norway (NOR)	6
Poland (POL)	1
Spain (ESP)	2
The Netherlands (NLD)	5
United Kingdom (GBR)	26
United States (USA)	22
TOTAL	139

CFBLNet 2007 Sites

138. The illustration below indicates CFBLNet Level 0 (zero) topology with national points of presence (POPs) for 2007.



CFBLNet 2007 Level 0 Topology

Conclusion

139. In 2007, CFBLNet made significant advances in improving processes, procedures, and educating users in utilizing the CFBLNet in support of delivering capabilities to the warfighter. The new Initiative submission process and tool (CIIP) continues to evolve as an efficient means to capture required mission, engineering, and security information and guarantees successful research, testing, and development. The expanding interest in products offered by the CFBLNet have forced ever greater demands on the efficient management of resources and attendance to the timely delivery of network enhances, to include the extension of services to new partners and sites. New network tactics, techniques, and procedures (TTPs) will require continued focus on CFBLNet engineering efforts, planning and set-up.

140. The Publication 1 (V5.0) establishes a more formal and transparent feedback process to capture customer concerns and track resolution of issues, as will providing greater detail for addressing emerging partnerships. The first iteration for introducing a new sponsored nation site will occur during 2008.

141. CFBLNet management processes now capture direct feedback on mission improvements from hosted Initiatives. CFBLNet Management continues to focus on the warfighter, measuring our success on our contribution to the delivery of capabilities and technologies.

142. CFBLNet continues to provide the Coalition network environment supporting technical and multinational information sharing trials. During 2007 significant progress was achieved toward all participants being connected to the CFBLNet Unclassified Environment (CUE), allowing the CFBLNets continuing growth and evolution as the Coalition RDT&A infrastructure of choice.

143. During 2008 we will remain an essential enabler to the validation and enhancement of interoperability of current and future operational systems. The CFBLNet will support an increasing customer base in identifying and assessing new technologies for coalition information sharing whilst exploring opportunities for new partnerships.

Annex A: Acronyms

ACP	Allied Communications Publication
ACTD	Advanced Concepts Technology Demonstration
AES	Advanced Encryption Standard
ADatP-3	Allied Data Publication No 3
ADF	Australian Defence Force
AITB	Alt Integrated Test Bed
Alt	Active Layered
ATAC	Advanced Tactical Aviation Course
AUS	Australia
AUT	Austria
BPS	Boundary Protection Service
C2	Command and Control
C2IS	C2 Information Systems
C2IEDM	Command & Control Information Exchange Data Model
C3	Consultation, Command & Control
C3I	Command, Control, Communications & Intelligence
C4I	Command, Control, Communications, Computers, & Intelligence
C4ISR	Command Control Communications Computers Intelligence Surveillance & Reconnaissance
CAN	Canada
CCEB	Combined Communications Electronics Board
CDEP	Coalition Distributed Engineering Plant
CDIFT	Coalition Distributed Information Test Bed
C-EG	CFBLNet Executive Group
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFBLNet	Combined Federated Battle Laboratories Network
CIIP	CFBLNet Initiative Information Pack
CIS	Communications and Information Systems
CLR	CN/O Lead Representative
CMM	CFBLNet Management Meeting
CMTR	Coalition Mission Training Research
CND	Computer Network Defense
CN/O	Charter Nation/Organization
COCOM	Combatant Command
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
DCGS	Defense Common Ground Surface Systems
DECC	Defense Enterprise Computing Centers
DEN	Denmark

DEP	Distributed Engineering Plant
DEU	Germany
DIB	DCGS Integration Backbone
DMS	Defense Message System
DNK	Denmark
DNS	Domain Name Server
DRDC	Defence Research and Development Canada
Dstl (DSTL)	Defence Science Technologies Laboratories
DSTO	Defence Science Technologies Office
DSTX	DSTO/DSTL
ESP	Spain
EST	Estonia
FAS	Functional Service Area
FEE	Four Eyes Enclave
FIN	Finland
FR-RRC	French Rapid Reaction Corps
FRA	France
FS	Functional Service
GBR	United Kingdom/Great Britain
GCTF	Global Counter-Terrorism Force
GPDN	Griffin Prototyping and Development Network
GRC	Greece
GUST	DEU/GBR Synthetic Training Trial
HF	High Frequency
HUN	Hungary
ICECAP	ISAF C4I Experimental Capability
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
JARIC	Joint Air Reconnaissance Intelligence Centre
JDEP	Joint Distributed Engineering Plant
JFCOM	Joint Forces Command
JIOC-I	Joint Intelligence Operations Center-Iraq
JTIC	Joint Interoperability Test Command
JTIDS/MIDS	Joint Tactical Information Distribution System/Management Information & Data System
JWID	Joint Warrior Interoperability Demonstration
LAN	Local Area Network

LAWG	Log Architecture WG
M&S	Modelling & Simulation
MAJIIC	Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition
MCTS	Maritime Composite Training System
MLS	Multi-Level Security
MOD	Ministry of Defence
MPLS	Multi-protocol Label Switching
MSAB	Multi-National Security Accreditation Board
MSI	Multi Sensor Integration
NAEC	National Accreditation Endorsement Certificate
NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation Command & Control Agency
NLD	Netherlands
NITB	National Information Test Bed
NOR	Norway
NSA	National Security Agency
NTDLIOT	NATO Tactical Data Link Interoperability Test
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
PTDLIOT	Partner National Tactical Data Link Interoperability Test
QLF	Quadrilateral Logistic Forum
QoS	Quality Of Service
R&D	Research & Development
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
SERF	Synthetic Environment Research Facility
SIMEX	Simulation Exercise
SN/O	Sponsored Nation/Organization
SNR	Sub-Net Relay
SWE	Sweden
STANAG	STANdardization AGreement
SWG	Security Working Group
TDL	Tactical Data Link

TDLITS	Tactical Data Link Interoperability Testing
TLS/SSL	Transport Layer Security/Secure Socket Layer
TP1	Technical Panel
TSR	Time Slot Reallocation
TTCP – AG4	The Technical Coordination Program
TUR	Turkey
UK	United Kingdom
UMC	Unified Modelling Capability
UNIR	Unclassified Not Internet Releasable
US	United States
USA	United States of America
VBE	Virtual Battle Experiment
VCDOAS	Virtual Capability Development & Operations Analysis Symposium
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WIB	War In a Box
WG	Working Group(s)
WW	Winged Warrior