COMBINED FEDERATED BATTLE LABORATORIES NETWORK (CFBLNET)

2010 ANNUAL REPORT

Executive Summary

The 2010 Annual Report provides a summary of the significant events, accomplishments and management process improvements of the Combined Federated Battle Laboratories Network (CFBLNet).

The CFBLNet was created and is maintained to provide the infrastructure of choice for international Coalition Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C5ISR) Research, Development, Trials, Demonstrations, Training and Assessments (RDT&A). The 2010 Annual Report demonstrates that CFBLNet continues to be extremely effective and agile in achieving this goal, and ultimately enhancing coalition warfighter capability and national of the United States, Combined Communications Electronics Board (CCEB) and NATO nations.

Building upon the growth and significant successes of CFBLNet since its inception in 1999, the CFBLNet organization turned its focus firmly upon improving process efficiency, enhancing the operational representation of CFBLNet capabilities, and providing both operational relevance and a return on resource investments to CFBLNet's customers in a continuing austere financial climate.

CFBLNet continues to be heavily utilized by the Mission Partners and in 2010, 23 C5ISR RDT&A Initiatives were successfully conducted, varying in size and complexity. Most importantly, continued investments in CFBLNet's 155 Mbps backbone has allowed a significant increase in capability to support modelling and simulation training initiatives as well as extending the enclave that directly supports the warfighters in Afghanistan through the coalition interoperability assurance and validation.

The network supported national and international C5ISR capability development efforts throughout the year with specific success stories including:

- CTE2: A globally distributed and secure Coalition Test & Evaluation Environment (CTE2) was established to assure and validate pre-deployment interoperability of ISAF mission partner C4ISR capabilities proposed for use on the Afghanistan Mission Network (AMN) to exchange critical information for coalition operations based on 8 coalition mission threads (CMT). In 2010, this global network connected Battle Lab facilities within NATO (NC3A and NCSA), USA, GBR, CAN, ITA, and FRA, with NOR, SWE and DEU scheduled to join in 2011. CFBLNet provided the persistent multi-nationally accredited secure network infrastructure needed to support comprehensive Coalition Interoperability and Assessment Validation (CIAV) data flows between applications/systems that support the CMTs. This resulted in numerous interoperability improvements to ISAF Battlespace Awareness capabilities and Common Operational Picture CONOPs, while demonstrating a persistent test and integration capability for efficiently establishing and maintaining an operationally relevant C5ISR baseline.

- CWID 2010 objectives focused on demonstrating capabilities to address multinational, joint, and interagency information sharing gaps. These themes and capability gaps are derived from Joint Urgent Operational Need Statements, Service equivalents, COCOM Integrated Priority Lists (IPL), COCOM Science and Technology Integrated Priority Lists, USJFCOM C2 Capability Portfolio Management (C2 CPM) identified capability gaps, and other coalition, Service and Joint Staff source documentation.

  Coalition, Combatant Command, Service and Agencies (C/C/S/A) capability gaps, and technologies that provide

  - The first ever transfer of live Link-22 maritime track data to a Coalition CWID technology trial connected to the CWID Secret network. This information was shared with Coalition forces operating in Lillehammer, Norway.
  - Successfully disseminated cross-coalition link picture using NATO recognized formats; enabled a shared common operating picture for all air, land and maritime tracks.
  - Demonstrated a potential cross-domain solution to e-mail services, Extensible Messaging and Presence Protocol (XMPP) chat services, web services, and document sharing all of which were governed by a common security policy based on open standards to meet the requirements for providing a network enabled capability.
  - Provided U.S. military, Department of Homeland Security, and local responders a capability to rapidly form a community of interest and exchange critical information in response to a terrorist attack.
  - Demonstrated a technology application that allowed operators to view “live” 3-D models of operational units from different coalition forces within the Google Earth environment.
  - Successfully integrated U.S. Army’s Publish and Subscribe System (PASS) and Command Post of the Future (CPOF) with the United Kingdom and NATO that required the command and control system feed to conduct scenario events.
  - The Joint Automated Deep Operations Coordination System (JADOCS) received NATO Air Tasking Orders (ATO) from NATO and NATO nation systems to confirm JADOCS processing of NATO ATO message format. The system used the NATO ATO to demonstrate JADOCS weapon target pairing capability.

- The NATO Tactical Data Link Interoperability Test Syndicate (NTDLIOTS) conducted its 7th event using CFBLNet between 14 TDL platforms in NATO and 7 nations, clearing 55 previously identified interoperability issues and discovering 131 provisional interoperability issues that were adjudicated to ensure that the Warfigher knows and understand the interoperability risks with each North Atlantic Treaty Organisation (NATO) nation’s TDL operational platforms.

- The NATO Active Layered Theatre Ballistic Missile Defense (ALTBMD) ALT DAMB Integration Test Bed (AITB) program conducted no less than 12 interoperability

events on CFBLNet during 2010, including the very successful Joint Project Optic Windmill. Characterising CFBLNet as a stable very high speed HLA/DIS network with solid security, operational benefits have been very high and significant program savings have already been realised.

The C-EG held two CFBLNet Management Meetings (CMMs) in 2010. These enabled further accomplishments which include:

- C-EG: Formally approved Sweden and Finland as a Guest CFBLNet Mission Partners (GMPs).

- C-EG: Decided to decommission the original CFBLNet Blue (Secret releasable to NATO/AUS/NZL) enclave, as the minor use of it no longer justified the cost of maintaining it.

- C-EG: Defined yearly calendar of deliverables and CMM recurring agenda items for each CMM, on a 2 year cycle, to ensure an understanding of expectations and synchronization of working group efforts.

- C-EG: Reduced the length of CMMs from two 4.5 days meetings a year to one CMM of 3.5 days, and a CFBLNet Engineering & Security Meeting (CESM) of much reduced attendance meeting on as a required basis. Further efficiencies will be sought once the new cycle has matured and it is likely that some may be found; for example, the CESM may be able to be held following a major Initiative meeting thus reducing travel costs further.

- C-EG: Developed annual letter outlining CMM responsibilities and participation requirements to ensure National support to CFBLNet management.

- C-EG: Selected the All Partners Access Network (APAN) as the primary collaborative environment for CFBLNet Management Meeting coordination, but continues to support use of Groove by the working groups as appropriate. All Web, Wiki and WG electronic material consolidated within the CFBLNet Group Space of APAN.

- SWG: Provided guidance on how to conduct CFBLNet Initiatives at the Top Secret classification level.

- DWG: Improved information flow to existing and potential CFBLNet users, including expanded use of APAN and submission of articles to military magazines.

- Secretariat: Invited Guest Mission Partners (GMPs) to future CMMs.

- Secretariat: In conjunction with NATO Information Assurance (IA) professionals, performed a vulnerability assessment of the CFBLNet Productivity Tool (CPT) and approved its use for CFBLNet management.

This page intentionally blank

The Chairman, on behalf of the Combined Federated Battle Laboratories Network (CFBLNet) Executive Group (C-EG), hereby approves the CFBLNet 2010 Annual Report.

8 July 2011

Mr. Steve E. Pitcher, GS-15 (date)
Joint Staff, J6
C-EG Chairman/U.S. Representative

With endorsement from:

Mr. Einar C. Thorsen, A5
NATO C3 Agency
NATO C-EG Representative

Wg Cdr Richard Elder
CCEB Executive Group
CCEB C-EG Representative

Table of Contents

FOREWORD 8

BACKGROUND 8

2010 EVENTS 8

PARTICIPANTS 9

CFBLNET STRATEGIC PLAN ENABLERS STATUS 10

SECURITY WORKING GROUP SUMMARY 12

INITIATIVES WORKING GROUP SUMMARY 13

DOCUMENTS WORKING GROUP SUMMARY 15

NETWORK WORKING GROUP SUMMARY 17

ANNEX A: 2010 INITIATIVES (CLOSED) 22

ANNEX B: CONTINUING AND PROJECTED INITIATIVES FOR 2011 30

ANNEX C: GLOSSARY 39

Foreword

This report reflects the progress and accomplishments of the Combined Federated Battle Laboratories Network (CFBLNet) during the calendar year 2010. The report provides an outline of activities from the CFBLNet Executive Group (C-EG) and the four permanent working groups.

The sustaining vision of the CFBLNet is to provide the infrastructure of choice for international Coalition Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance (C5ISR) research, development, trials, and assessments (RDT&A) to explore, promote, and confirm Coalition/Combined capabilities and interoperability for the members.

Background

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 USA, 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 Warrior Interoperability Demonstration (JWID).

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.

As of April 2011, there were 215 CFBLNet sites connected through a 155 Mbps backbone between 13 CFBLNet Mission Partners (nations and organizations) which was cross certified and accredited for coalition interoperability use at the secret releasable level.

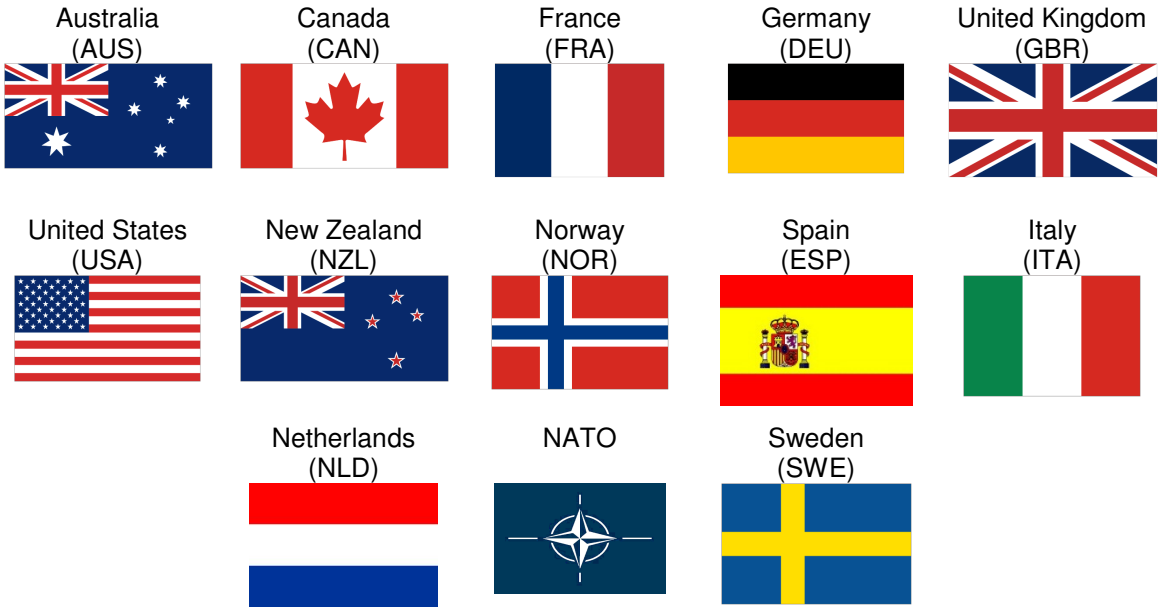
2010 Events

Two CFBLNet Management Meetings (CMMs) were hosted in 2010.

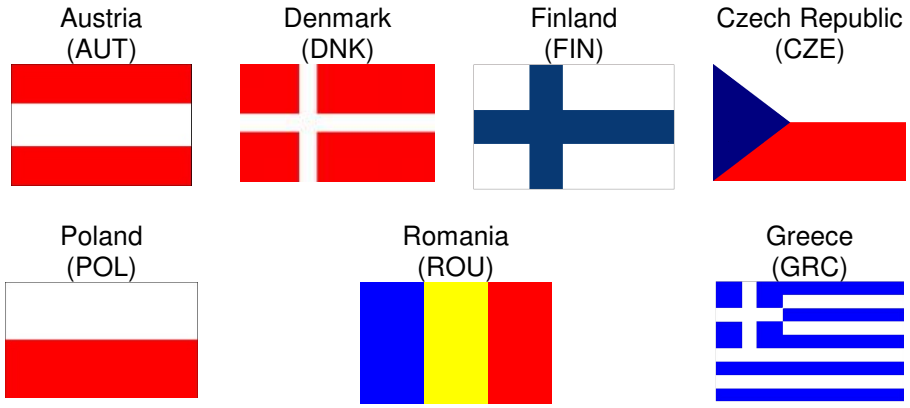
- CMM10-1
  - Host: *United States*
  - Location: *Mitre Corporation, Suffolk, Virginia*
  - Dates: *19 – 23 April 2010*
- CMM10-2
  - Host: *NATO/Italy*
  - Location: *C4I Systems and Transformation Department, Rome, Italy*
  - Dates: *18 – 22 October 2010*

Participants

The nations and organizations connected to CFBLNet in 2010 are listed below:



In addition, the following nations have participated in or observed CFBLNet Initiatives at existing CFBLNet sites:



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	ENDURING
		Enb.1.2 Provide and manage enclaves for the conduct of classified Initiatives between the Charter Nations/Organizations (CN/O)	ENDURING
		Enb.1.3 Provide and manage the CFBLNet Unclassified Enclave (CUE) for the conduct of multiple Initiatives for CN/O and SN/O participants.	ENDURING
		Enb.1.4 Implement multi-nationally agreed accreditation processes to enable secure interconnection of nationally accredited CIS systems.	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	ENDURING
		Enb.1.7 Provide a Customer Friendly Network and RDT&A capability	ENDURING
		Enb.1.8 Develop and maintain an interactive, online process for users to populate CIIPs.	ONGOING
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.2.1** Establish a standardized border protection scheme for CFBLNet enclaves.	DONE
		Enb.2.2 Establish Bandwidth Management (constraint and monitoring)	DONE
		Enb.2.3 Exploit multi-national multi level security for cross domain solutions	DONE
		Enb.2.4 Evolve CFBLNet infrastructure and services to be IPv6 compliant.	DONE
		Enb.2.5 Provide infrastructure and services able to support IPv6 Initiatives.	DONE
		Enb.2.6 Provide capabilities able to support MLS Initiatives.	ONGOING
		Enb.2.7 Provide capabilities able to support M&S trials (real time and low latency).	DONE
		Enb.2.8 Examine the requirement for computer network defence (CND) capabilities and procedures for CFBLNet.	DONE
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.3.1** Better manage the scheduling of Initiatives to achieve bandwidth efficiencies and resolve Initiative scheduling conflicts.	DONE
		Enb.3.2 Improve Initiative screening processes to include participation by an SN/O	DONE
		Enb.3.3 Evaluate methods (eg Groove) to improve information management and sharing within and between CFBLNet WGs	DONE
		Enb.3.4 Review performance of CFBLNet based on Initiative outbrief reports and implement necessary improvements.	ENDURING
		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.	STOPPED
		Enb.3.7 Develop a comprehensive information management plan addressing creation, coordination, storage, configuration management, and control of information.	DONE

Notes on the Strategic Plan implementation

Significant progress has been made on achieving the Strategic Enablers, and thereby the strategic goals and objectives, since the last Annual Report. This achievement is primarily due to the persistent efforts of the Working Groups and the C-EG is proud to say that CFBLNet is very close to performing at the ambition level of our current vision.

Enablers marked as DONE are those where an enabler has been achieved and the results have been published, mostly in the form of an update to Pub 1.

Enablers marked as ENDURING are those where an enabler has been achieved, the results have been published, and processes are being followed to sustain the benefit of the enabler.

Enablers marked as ONGING are those were work have started, but the results are not yet mature enough for publication. The following enablers fall into this category:

- 1.8 Develop and maintain an interactive, online process for users to populate CIIPs. Good progress was seen during 2010, and a functionally complete prototype is ready for demonstration and assessment. It is anticipated that release of the tool will be authorized shortly after CMM11-1.
- 2.6 Provide capabilities able to support MLS Initiatives. The Security WG is defining what such capabilities would be and what subset would be possible to supply as part of the CFBLNet offerings. A proposal to provide a trusted data labelling tool will be assessed for suitability in this context.

Enablers marked as STOPPED are those where C-EG has realized that (further) work on this enabler will not deliver the perceived benefits.

Security Working Group Summary

The following section highlights issues related to CFBLNet management's security support to initiatives executed during 2010, specifically addressing customer understanding of security guidance and requirements, and timeliness of accreditation and certification support. Additionally, this section describes how the Security WG accomplished their tasks related to evolving CFBLNet capabilities, in accordance with the strategic plan's goals and objectives supporting future initiative requirements.

In order to support greater understanding within the Security Working Group (SWG) and between the SWG and our CFBLNet customers the Terms of Reference was updated and republished.

The SWG agreed on a process to enable them to carry on business between CFBLNet Management Meetings with increased effectiveness via email correspondence and a monthly teleconference.

The SWG recommended alterations to the Security Tab of the CFLBNet Initiative Information Pack (CIIP) that would facilitate the endorsement in a timely manner. An additional query field was recommended for the Initiative Final Report Tab in order to gain more insight into the customer requirements so as to improve our processes.

The SWG discussed how to conduct Top Secret Initiatives and concluded that it would be covered by each Nation's encryption and physical security policies. It was further confirmed that Memorandums of Understanding (MOUs) or Information Security Agreements (ISAs) will be required for any activity at any Classification run over the CFBLNet. These updates will be documented in the next version release of the CFBLNet Publication 1.

Initiatives Working Group Summary

The following section highlights issues related to how the current CFBLNet processes supported Initiative requirements executed during 2010. It specifically addresses customer understanding and their ability to follow the current CFBLNet guidance for conducting Initiatives using CFBLNet. Furthermore, this section highlights feedback from the customers on the use of the CFBLNet productivity tool, as well as the effectiveness and timeliness of current CFBLNet procedures and technical support. Specific emphasis it placed on identifying and implementing recommendations on streamlining CFBLNet processes. Additionally, the section describes how the WG accomplished their tasks related to evolving CFBLNet in accordance with the strategic plan's goals and objectives in support to future initiative requirements.

During the 2010 reporting period the CFBLNet hosted and planned into 2011 a total of 23 C5ISR and RDT&A Initiatives. Initiatives varied in size and complexity from small scale bi-lateral events to multi-lateral events such as the TDLIOTS series involving many NATO Nations. Initiative characteristics have continued to change, with recent and greater emphasis towards support to pre-deployment training, interoperability, and validation.

Annexes A and B provides a list of all of the Initiatives completed or started in 2010, highlights of the intended operational benefits, and the list of participating Nations and Organisations for each Initiative. Annex A provides a list of Initiatives where were closed in 2010. Annex B provides a list of Initiatives which either started in 2010 and are continuing into 2011 or are projected to occur in 2011.

The CFBLNet Charter now embraces Guest Nations and Organizations as Mission Partners. This change is now reflected throughout the Initiative approval framework. Core and Guest Mission Partners now follow similar procedures for gaining access CFBLNet infrastructure and gaining approval to participate in and sponsor Initiatives across the CFBLNet. Emphasis was also given to adding and streamlining documentation to instruct Core members how to achieve Guest sponsorship, Site nominations and Initiative approvals. In 2010, guest nations have participated in the following events;

Initiative	*Guest Nation*	*Type of Participation*
EC10	SWE, FIN, JPN, ROK	Observers Only
CWID10	SWE,FIN, AUT	Full Participation
DNBL JISR-1	SWE	Full Participation

The Secretariat has developed a prototype Web-based CFBLNet Productivity Tool (CPT) which will enable multi-national visibility and approval for an Initiative. The CPT will further provide an Initiative Calendar, reporting features and give visibility of where CIIPs are within the approval process. Full operating capability of the CPT is expected in 2011 with an operational demo planned for CMM11-1.

User feedback continues to be very appreciative of the services that the CFBLNet organisation and infrastructure offers in providing cost effective secure solutions and networks to enable a spectrum of collaborative Initiatives to take place. CFBLNet Customers have come to expect the following services:

- The 'one stop shop' package to provide a secure network environment for multi-national collaboration, engendering security and established trust framework;

- Provide Subject Matter Experts (SME) expertise for 'leading edge' secure networking, distribution of crypotgrarphic key and security accreditation to easily enable collaborative events;

- Meets bandwidth demands and Quality of Service (QoS) for training and simulation type traffics;

- National and multi-national network distribution to key sites and assets;

- Expertise in hosting and enabling complex events such as CWID and Empire Challenge.

Initiatives conducted since the inception of CFBLNet reveal the following emerging trends:

- Pre-deployment training over long time periods, 24 x 7 coverage, over multiple time zones, sometimes on short notice and with high network availability;

- Infrastructure extension to include Guest Mission Partners, operations, industry and Other Government Departments (OGDs);

- In order to meet International Data Sharing Agreements for Initiatives there has been a marked increase in the number of required temporary and permanent security enclaves. These requirements bring greater demands for engineering manpower and equipment, and in particular Type 1 Encryption Devices which cause issues for participant nations and organisations to support within their budgets;

- Many customers are now looking at linking operational simulators over CFBLNet to reduce the stresses on operational assets and minimise cost.

Documents Working Group Summary

The following section highlight issues related to how the current CFBLNet documentation set supported initiative planning and execution during 2010, specifically addressing information campaigns aimed at increasing general awareness of CFBLNet capabilities, success stories, and potential for further warfighter benefits. Additionally, the section describes how the WG accomplished their tasks related to evolving CFBLNet in accordance with the strategic plan's goals and objectives in support to future initiative requirements.

The original version of the CFBLNet Publication 1 was completed in 2003. The latest version (Version 6.0) was released in December 2009. With continued improvement cycles the document has evolved with new requirements and direction and provides up-to-date information. The next version of this document is expected in 2011, though draft versions are continuously updated to reflect the last changes. A summary of the status of the Technical Arrangement (Charter); Strategic Plan; all Publication 1 and its Annexes; and the CFBLNet User Documents are contained below. The Documents Working Group (DWG) is working towards a refreshing way to bring the consolidated information in clear information modules to our current and potential CFBLNet Mission Partners, possibly through the use of WIKI technology.

In 2010, the focus was on improving the public information flow to our user base, through projects like refreshing/modernising the CFBLNet public portal, creating integrated information packages and considering the modular information approach. In addition, efforts were undertaking to publish CFBLNet articles in various military publications.

DOCUMENT	STATUS
Technical Arrangement (Charter) *Updated: MAY2009*	Signed & Approved by C-SSG: May 2009
Strategic Plan *Updated: FEB06* *Version 1.0*	Signed & Approved by C-SSG: February 2006
Publication 1: Organisation and Responsibilities *Version 6.0*	Signed & Approved by C-EG: November 2009
CFBLNet Publication 1 – Annex A: Terms of Reference *Version 6.0*	Approved by C-EG: November 2009

DOCUMENT	STATUS
CFBLNet Publication 1 – Annex B: Initiative Processing *Version 6.0*	Approved by C-EG: November 2009
CFBLNet Publication 1 – Annex C: CFBLNet Security and Information Assurance Strategy *Version 6.0*	Approved by C-EG: November 2009
CFBLNet Publication 1 – Annex D: Network Operations (Network/System Aspects of the CFBLNet) *Version 6.0*	Approved by C-EG: November 2009
CFBLNet Publication 1 – Annex E: Site Processing *Version 6.0*	Approved by C-EG: November 2009
CFBLNet Publication 1 – Annex F: GMP Sponsorship Processing *Version 6.0*	Approved by C-EG: November 2009
CFBLNet Publication 1 – Annex G: CFBLNet Document Management *Version 6.0*	Approved by C-EG: November 2009
CFBLNet Publication 1 – Annex H: CFBLNet Information Management Guidance *Version 6.0*	Approved by C-EG: November 2009
CFBLNet Publication 1 – Annex I: Glossary of Terms *Version 6.0*	Approved by C-EG: November 2009
CFBLNet Information Brochure Tri-Fold	Latest Release: September 2010
Basic Guide to CFBLNet Initiatives Process *Version 2.0*	Latest Release: November 2009
Basic Guide to CFBLNet Accreditation Procedures *Version 2.0*	Latest Release: November 2009
Guidelines for Guest CFBLNet Mission Partners *Version 1.0*	Latest Release: November 2009

Network Working Group Summary

The following section highlight issues related to how the current CFBLNet infrastructure supported initiative planning and execution during 2010, specifically addressing advice to initiatives on selection or establishment of appropriate enclaves, network topology, network technologies, infrastructure services, and infrastructure management and support. Additionally, the section describes how the Network Working Group (NWG) accomplished their tasks related to evolving CFBLNet in accordance with the strategic plan's goals and objectives in support to future initiative requirements.

For 2010, the highlights of the network engineering efforts were as follows:

Coalition Test and Evaluation Environment (CTE2): CFBLNet continued installation and activation of second phase of the ISAF Test Bed on the CFBLNet to support Afghanistan Mission Network (AMN) interoperability testing. Installation of CFBLNet sites for CTE2 Phases One and Two and future phases are summarized as follows:

- Conceptual phase (December 2009)
    - Joint Interoperability Test Command – Indian Head (JITC-MD), Indian Head, MD
    - DISA MNIS-PMO North Fairfax (NFX), Arlington, Virginia (USA)
    - DSTL, Portsdown West, Hampshire (GBR)

- Phase One (March-June 2010)
    - U.S. Defense Information Systems Agency, Joint Interoperability Test Command (JITC), Indian Head, Maryland (USA)
    - Command & Control Battle Lab (C2BL), Defense Command College (DCC), Schrivenham, Oxfordshire (GBR)
    - NATO Consultation, Command and Control Agency (NC3A), The Hague, (NLD)

- Phase Two (August-October 2010)
    - Command & Control Battle Lab (C2BL), Defense Command College (DCC), Schrivenham, Oxfordshire (GBR)
    - U.S. Defense Information Systems Agency, Joint Interoperability Test Command (JITC) Indian Head, Maryland and Fort Huachuca, Arizona, (USA)
    - U.S. Army Central Technical Support Facility (CTSF), Fort Hood, Texas (USA)
    - U.S. Joint Forces Command (USJFCOM), Joint Systems Integration Center (JSIC), Suffolk, Virginia (USA)
    - NATO Consultation, Command and Control Agency (NC3A), The Hague, (NLD)
    - Canadian Forces Experimental Network, Louis St-Laurent building (CFX-LSL), Ottawa (CAN)

- Future sites and phases to continue in 2011 include:
    - SPAWAR Systems Center – San Diego (SSC-SD), Point Loma, San Diego, California (USA)
    - NATO CIS Services Agency (NCSA), Mons, (BEL)
    - Marine Corps Tactical Systems Support Activity (MCTSSA), Camp Pendleton, California (USA)
    - Electronic Systems Command (ESC) – Communications Electronics Interface Facility (CEIF), Hanscom Air Force Base (AFB), Massachusetts (USA)
    - Délégation Générale de l'Armement Maitrise de l'Information (DGA MI) Référentiel d'Interoperabilité Technique (RIT), Bruz (FRA)
    - Italian Army Battle Lab - Comando Trasmissioni e Informazioni Esercito (Co.T.I.E.), Anzio, Rome (ITA)
    - Others to be determined

Empire Challenge 2010 (EC10): EC10 encompassed major changes to the host venue location and security domains supported. The main venue location was changed from Naval Air Warfare Center – Weapons Division (NAWC-WD), China Lake, California to the U.S. Army Military installation Ft. Huachuca, Arizona. This effort involved the installation of four permanent and ten temporary CFBLNet nodes on Ft. Huachuca, Arizona. The main participating security domain was changed to an International Security Assistance Forces (ISAF) equivalent 43-Eyes domain. It also included three additional domains (4-Eyes, an Unclassified Community of Interest (COI), and an Internet Café) to support the Empire Challenge 2010 (EC10) Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) whose primary focus is to support C4ISR deployment and problem resolution for the IRAQ and Afghanistan missions. The EC10 supported successful testing of several guard cross-domain objectives to process the transfer of high-speed imagery signals.

The following sites/nodes were installed and activated in support of EC11:

- Temporary Sites installed and activated:
    - Intelligence Electronic Warfare Test Directorate (IEWTD) – Intelligence Systems Integration Laboratory ((ISIL) (IEWTD-ISIL), Trailer D/E, Ft Huachuca, Arizona (USA)
    - IEWTD-ISIL Tree Line, Ft Huachuca, Arizona (USA)
    - Network Enterprise Technology Command (NETCOM) Director Of Information Management (DOIM) (NETCOM/DOIM), Node E, Ft Huachuca, Arizona (USA) (IP Hub Radio Site #2)
    - U.S. FOB, East Range, Ft Huachuca, Arizona (USA)
    - U.K. FOB 1, East Range, Ft Huachuca, Arizona (USA)
    - U.K. FOB 2, East Range, Ft Huachuca, Arizona (USA)
    - Canada FOB, East Range, Ft Huachuca, Arizona (USA)
    - Hubbard Airfield, East Range, Ft Huachuca, Arizona (USA)
    - Site Uniform, South Range, Ft Huachuca, Arizona (USA)
    - Site Boston, South Range, Ft Huachuca, Arizona (USA)

- Permanent sites:
  - U.S. Joint Forces Command (USJFCOM) - Joint Systems Integration Command (JSIC) JFCOM-JSIC), Suffolk, Virginia (USA)
  - USJFCOM - Joint Interoperability Lab (JIL) (JFCOM-JIL), Suffolk, Virginia (USA)
  - NETCOM/DOIM Dial Central Office (DCO), Ft Huachuca, Arizona (USA)
  - NETCON/DOIM Node A, Ft Huachuca, AZ (IP Hub Radio Site # 1)
  - Joint Integration Test Command (JITC), Ft Huachuca, Arizona (USA)
  - IEWTD-ISIL, Ft Huachuca, Arizona (USA)
  - GCIC, Langley AFB, Virginia (USA)
  - Command & Control Lab (C2L), Naval Surface Warfare Center – Dahlgren Division (NSWC-DD), Dahlgren, Virginia (USA)
  - DISA MNIS-PMO NFX, Arlington, Virginia (USA)
  - Louis Saint Laurent, Ottawa (CAN)
  - Canadian Forces Warfare Center (CFWC), Shirley's Bay, Ottawa, (CAN)
  - Defense Science & Technology Office (DSTO), Fern Hill Park, Canberra, Australian Captial Territory (ACT) (AUS)
  - Defence Imagery and Geospacial Organization (DIGO), Russell Offices, Canberra, ACT (AUS)
  - Defence Science Technology Office (DSTO), RAAF Edinburgh, Adelaide, South (AUS)
  - North Atlantic Treaty Organization (NATO) – NATO Consultation, Command, & Control Agency (NC3A), The Hague , Netherlands
  - NATO Allied Command Transformation (ACT), Norfolk, Virgina
  - Defense Science Technology Laboratory (DSTL), Portsdown West, Hampshire (GBR)
  - DSTL, Porton Down, Wiltshire (GBR)
  - Air Warfare Center (AWC), RAF Waddington, Lincolnshire (GBR)
  - Command & Control Battle Lab (C2BL), DCC, Schrivenham, Oxfordshire(GBR)

- Canadian equipment located at the Multi-National Information Sharing Portfolio Management Office (MNIS PMO) North Fairfax (NFX), Arlington, Virginia will be life cycled (upgraded and replaced) to enhance network capabilities in support of multiple initiatives which occur concurrently.

- Established the Iceland simulated site within the NC3A, The Hague, NL facility to support testing of high latency, low bandwidth links on the NATO Red Network which has now been made available to other enclaves.

- Established a new NATO node in Supreme Headquarters Allied Powers Europe (SHAPE), Mons, Belgium. This enabled NATO organizations to connect over the NATO General Purpose Communication Service (NGCS) Network.

- Created a transmission gateway node in Amsterdam, NLD. The establishment of this transmission gateway node provides less expensive and more convenient access for NATO nations to connect to the CFBLNet.

- Established a new 100 Mbps link from the NATO reach-out node of Amsterdam, NLD to the USA node of Mechanicsburg, PA.

- Established a new OC-3 155 Mbps link into CTFS, Ft. Hood, Texas to support the CTE2 test environment on the CFBLNet.

- Upgraded CFBLNet service into CDSA, Damneck, Virginia from 3 Mbps to an OC-3 155 Mbps.

- Installed a U.S. CFBLNet PoP with OC-3 155 Mbps throughput at NATO Allied Command Transformation (ACT), Norfolk, VA which replaced the T-1 1.544 Mbps leased line from NATO ACT, Norfolk, VA to NFX, Arlington, Virginia.

- Installed a U.S. CFBLNet PoP with DS-3 45 Mbps throughput at the Defense Information Systems Agency (DISA) Eagle / Sky 7 facilities in support of the ICI Initiative.

- The AUS to USA connection was upgraded by the USA by replacing the AUS provided 5 Mbps interface with a U.S. provided 45 Mbps interface and equipment installed in the AUS Defence Communication System (DCS) Canberra facilities at His Majesty's Australian Ship (HMAS) Harman, Canberra, Australian Capital Territory (ACT), Australia. This facilitated Australia's migration from ATM to MPLS and the USA being able to extend the BGP gateway to AUS vice the USA Point of Presence (at NFX). As a future action, NZL is planning to create a similar gateway with the USA at HMAS Harman. In addition, the USA is planning to expand the bandwidth connection from 45 Mbps to an OC-3 155.52 Mbps.

- Completed the Southern loop of the OC-3 ring within the U.S. by adding the OC-3 connections from JFCOM, Suffolk, Virgina and SSC-SD Point Loma, California to Ft. Huachuca, Arizona. This provides for a complete self-healing OC-3 ring within the USA.

- Finalized the schedule for changes to the Autonomous System Number (ASN) assignments for the CFBLNet Blackbone [05JAN11].

- Discussed and established an implementation plan for Multicast strategies within the CFBLNet secured enclaves.

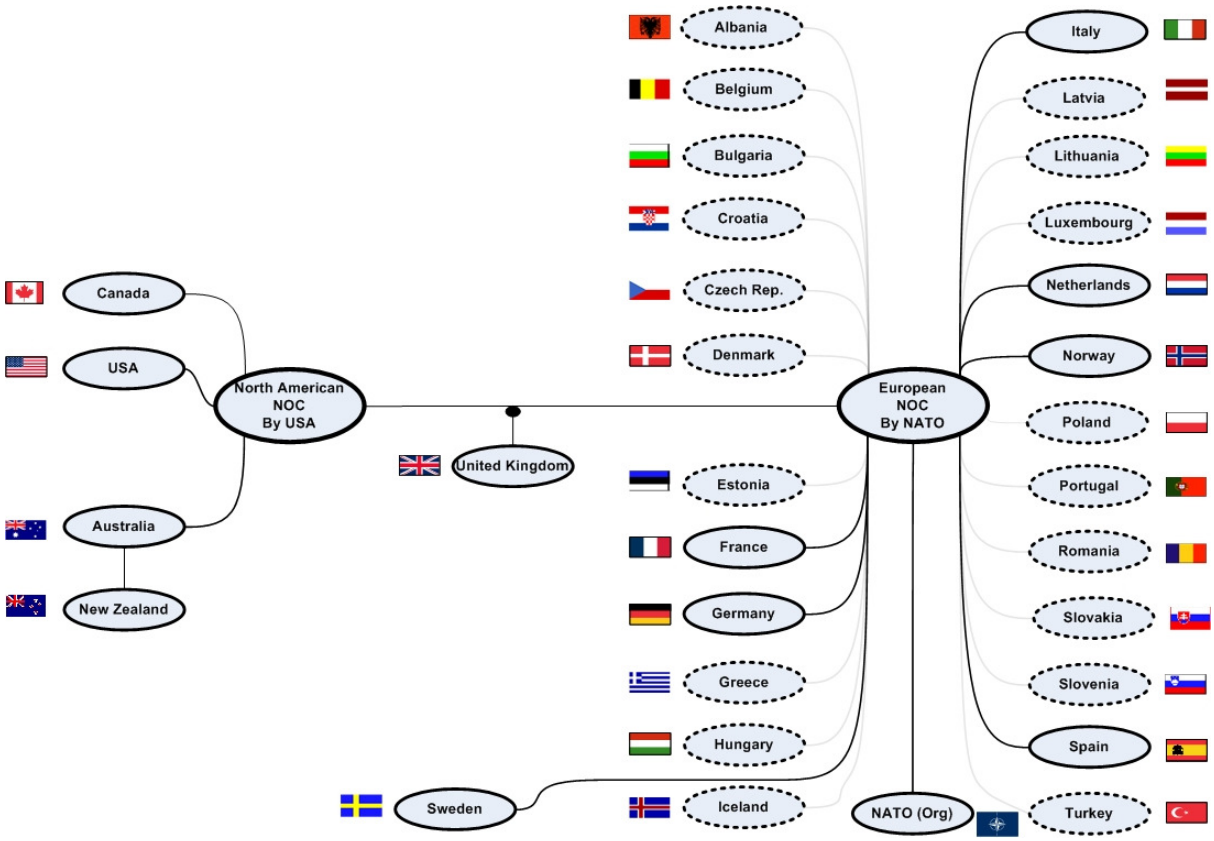
- Discussed and agreed within the joint NWG/SWG session the implementation of a centralized Network Monitoring capability with read only access.

- Canada Command is pursuing a connection to the U.S. Joint Forces Command (JFCOM) – Joint Training Experimentation Network (JTEN) via CFBLNet.

- Equipment at the Crow's Nest Canadian presence located at the British Army Training Unit (BATU), Suffield, Alberta, has been upgraded.

Nation/Organization	# of Sites	Nation/Organization	# of Sites
Australia (AUS)	14	New Zealand (NZL)	6
Canada (CAN)	32	Norway (NOR)	7
France (FRA)	4	Poland (POL)	1
Germany (DEU)	16	Sweden (SWE)	3
Italy (ITA)	8	Spain (ESP)	5
NATO	13	United Kingdom (GBR)	37
The Netherlands (NLD)	12	United States (USA)	42
Total CFBLNet Sites: 200			

CFBLNet 2010 Sites



2010 CFBLNet Topology

Annex A: 2010 Initiatives (Closed)

The following articulates the feedback, successes and recommendations of those Initiatives that used CFBLNet and submitted close down reports at one of the 2 CFBLNet Management Meetings (CMMs) in 2010.

Griffin Prototype Development Network
GPDN – GBR-020-06

Objective: To develop the CCEB Web Service, DNS Service, Chat Service and the technical refresh of the multi-national Interoperability Service using a Type 1 High Grade encrypted enclave. Technology will be deployed in Coalition Command and Control systems.

Operational Benefits: Initial trialling has resulted in USA/GBR operational interoperability for GRIFFIN, to be further enhanced for other nations.

Customer Feedback: CFBLNet possess the background and experience to form secure coalition connections. During the first phases of GPDN the CFBLNet performed well and GPDN was grateful for the support and expertise of CFBLNet Network Engineers. GPDN will look towards CFBLNet to provide guidance on MN HAIPE compliant cryptos as GPDN trialling enters a second phase in 2010 to 2011 time frame.

Development over CFBLNet will enhance GRIFFIN operational capabilities. 1st phase functionality migrated to operational GRIFFIN.

Participants: AUS, CAN, GBR, NZL, USA
Dates: December 2006 – November 2009

Crypto Modernization Initiative
CMI – USA-011-08

Objective: To test the KG 250 capability to encrypt IP data.

Customer Feedback: CFBLNet provided adequate Management and Technical Support to the Initiative. CFBLNet QoS met the requirements of CMI and there were no apparent network outages. CFBLNet provided a fine R&D platform for CMI which we would use again. CMI has already enhanced operational capability as it has been deployed operationally on CENTRIX. One success of CMI is that it has established operational TTP for the KG250.

Participants: USA
Dates: 28 October 2008 – 1 November 2009

Coalition Distribution Fusion Testbed
CDIFT – AUS-008-06

Objective: Coalition information fusion to input to acquisition programmes to enhance multi-national interoperability and support collaboration between countries in the development of new information fusion capabilities.

This Initiative is a TTCP C3I Information Fusion Technical Panel 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.

Operational Benefits: To develop a Science & Technology capability to explore Coalition technologies for information fusing.

Customer Feedback: AUS lead found the AUS and GBR technical and administrative support for CFBL excellent and very helpful in providing guidance, and very responsive to Initiative requirements.

The US had issues in re-accreditation of the AFRL node, which prevented AFRL participation in the CFBLNet CDIFT initiative beyond the very early stages. CAN (DRDC-Valcartier) also had issues getting access to the TACLANES in the timeframes required by the CDIFT. This resulted in CFBL being very inflexible in scheduling experimental activities with CDIFT. This resulted in the forced cancellation of some CDIFT planned activities.

Quality of service was met from an AUS and GBR perspective. US (AFRL) only participated in the early stages, in which time the service was adequate. Long lead times for the CAN node.

There were outages on a number of occasions but AUS/GBR/CAN staffs were able to quickly work through problems. These outages were network and crypto related.

CFBLNet is not responsive enough and is too costly for CDIFT requirements. CFBLNet appears to be geared for single events, rather than maintaining an ongoing environment for collaboration, joint development and experimentation, which is what CDIFT was trying to achieve.

Long lead times and inflexibility with scheduling with international partners made it unsuitable for CDIFT requirements. CDIFT do not plan to use CFBLNet in future, and are investigating alternative collaboration mechanisms that are more flexible and affordable.

Operational benefits could not be realised at this time - in part because of the unsuitability of CFBLNet as a mechanism for international collaboration in the development (rather than demonstration) phase.

The goal of CDIFT was to develop an S&T capability to explore coalition technologies for information fusion.

Development over CFBLNet would enhance GRIFFIN operational capabilities.

Several demonstrations of the capability were given in GBR to industry stakeholders. The CDIFT capability developed on the CFBLNet was also demonstrated at a prestigious international conference (Fusion 09).

Participants: AUS, CAN, GBR, USA
Dates: 14 April – 23 December 2009

Defence Science Technologies Exchange Virtual Private Network
DSTX VPN – AUS-014-06

Objective: A three year collaborative Science and Technology project that aims to develop a Unified Modelling Capability.

Operational Benefits: 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.

Participants: AUS, GBR
Dates: 01 December 2008 – 01 December 2009

Combined Interoperability Test
CIT 10 – AUS-016-09

Objective: Conduct tactical Data Link Interoperability trials between AUS and USA tactical assets based at Fyshwick and Fort Huachuca. The Joint Interoperability Test Command (JITC) located in Fort Hucahuca, AZ (USA) and the Australian Defence Force Tactical Data Link Authority (ADFTA) located in Fyshwick, Australia conducted future Interoperability Tactical Data Link (TDL) testing. The participants established a circuit path leveraging both parties existing CFBLNet nodal stacks of equipment. The first phase conducted a connectivity check using an ICMP packet (PING) to verify the circuit path was clean and the encryption devices were synchronized. The second phase was to implement both participants Local Area Networks (LAN) in order to validate data and certify specific systems under test (SUT). The third phase confirmed Test tools (hardware & software) suites were compatible between JITC and Australian designated test facilities. The fourth phase facilitated a full interoperability test event between Australian defense forces and the United States.

Operational Benefits: Network Link connectivity preparation between the USA and AUS participants for future Combine Interoperability Test phases to certify specific systems under test.

Customer Feedback: The flawless availability of the CFBLNet enabled JITC and Australia to successfully conduct an extensive combined interoperability test event. The end result of this initiative will provide the Pacific Combatant enhanced operational capability to interoperate Link 16 and Link 11 with Australia.

Participants: AUS, USA
Dates: 02 January – 30 September 2010

Coalition Warrior Interoperability Demonstration
CWID 2010 – USA-009-10

Objective: Enables USA Combatant Commanders and their Allies to investigate new technologies. CWID is the annual event that enables U.S Combatant Commanders and the international community to investigate new and emerging technologies. The demonstration builds a temporary global network over which cutting edge communications technologies interact. CWID 10 Evaluated technologies for utility, interoperability and IA that can be implemented for operational use within a 6-24 month period following the execution period. Support CENTRIX/ISAF efforts to Improve Coalition Command, Control and Coordination for both Conventional and Irregular Warfare Operations, Improved Leader Centric, Net Enabled Operations, Enhance Coalition Battle Space Situational Awareness, Enhance Coalition Logistics Planning and Coordination, Enhance Coalition, Military, Government Agency, International Organization and Non-government Organization Partnership Building Capabilities, Improved Secure Information Sharing Between Disparate Security Domains and Communities of Interest in an Operational Environment and Improved Centralized Command, Decentralized Control for Irregular/Hybrid Warfare Units.

Operational Benefits: Evaluates new technologies that can be moved into the operational environment within 6 – 24 months.

Customer Feedback: One of our larger Initiatives on CFBLNet, CWID focuses on C2 and leader-centric/net-enabled solutions that the traditional US DoD acquisition process is not currently addressing. CWID 2010 participation included 19 nations plus NATO.

CFBLNet services were successfully federated and satisfied all known requirements. This was one of the few years that no network outages were experienced. CFBLNet is the only logical network able to support an extensive Coalition Initiative like CWID. Explore synergies with CTE2, AMN Test Bed, and Empire Challenge. The CWID Trial Transition and Information Working Group (T2IWG) will identify technologies that transition to operational capability. Note for transition of Google Earth server for use in EC as well as CWID: Suggest separating drives with separate builds to avoid the need to sanitize between events. Following a successful CWID, some of the most promising technologies are moving into the latter stages of the Technology Readiness Levels so that they can be introduced into operations.

Recommendations: Chat services should be selected early to ensure requirements can be met rather than use workarounds. Early and more frequent reminders of accreditation status and modifications are required to satisfy accreditation standards and timelines.

Participants: USA, GBR, CAN, NZL, NATO, DEU, NOR, ITA, DNK, FRA, POL, ROU, ESP, TUR, NLD, EST, AUS
Dates: 01 April – 30 June 2010

Empire Challenge 10
EC10 – USA-011-10

Objective: Empire Challenge 2010 was an Under Secretary of Defense for Intelligence (USD(I)) sponsored U.S. Joint Forces Command (USJFCOM) executed joint/combined Intelligence,

Surveillance and Reconnaissance (ISR) interoperability demonstration. EC10 focused on improving the ability of the International Security Assistance Force (ISAF) Afghanistan to effectively and efficiently manage, access and use ISR to improve command and control (C2), and enhancing information sharing and situational understanding to improve the effectiveness of operations while minimizing collateral damage in a complex environment.

- DCGS Enterprise Interoperability
- C2 - ISR Data Integration to Support Operations in a Complex Environment
- C2 & ISR Management to Achieve Persistent Surveillance Over Key Terrain
- ISR Support to JCAS/Strike to Achieve Combat Effectiveness & Minimize Civilian Casualties & Fratricide
- Information Sharing to Support Multinational / Whole of Government Interoperability

During execution of this Initiative two Technical Delivery issues were raised. An outage of the ATM switch in Arlington caused interruption to service and there was a requirement to upgrade some crypto, switches and routers. CFBL will address these issues by creating an Inventory of USJFCOM owned equipment stored in DISA Labs that will allow for easy identification of spares holdings. CFBL plan to upgrade Crypto and switches to their routers at Fort Huachuca.

Operational Benefits: Extended awareness for integrating operations, information and technical capabilities around unmanned systems.

Participants: AUS, CAN, GBR, NATO, FRA, DEU, NLD, ESP, NOR, NZL, DNK, SWE, FIN
Dates: 26 July – 13 August 2010

NATO Tactical Data Link Interoperability Test 09-02
NTDLOITS 09-02/ARNETH – GBR-006-09

Objective: To provide a vehicle for NATO Tactical Data Links interoperability Test Syndicate. Initiative conducted a NTDLIOT with various National / NATO assets through the period of execution. This is the 7th NTDLIOT to be conducted over the CFBLNet since the first tests were conducted on 16 Oct 06.

Operational Benefits: Interoperability trials with NATO operational assets.

Customer Feedback: CFBLNet met requirements, ideal platform for TDLIOTS activity. No recorded network outages. NTDLIOTS community plan to use CFBLNet for future NATO interoperability testing. No tasking is on CFBLNet to improve its service is necessary.
The CFBLNet is utilized to provide a forum in which all participating NATO and Authorised Partner nations are able to test IO capabilities and limitations with other participating nations over a secure distributed network.

The test results are documented and forwarded to the C3 IWG for review and publication within the TDL War fighter community.

The TDLITS successfully tested 14 TDL platforms and cleared 55 identified interoperability issues and discovered 131 provisional interoperability issues.

All identified IOIs are adjudicated to ensure that the Warfigher knows and understand the

interoperability risks with each NATO nation's TDL operational platforms.

Participants: DEU, ESP, FRA, GRB, ITA, NATO, NLD, NOR, USA
Dates: 03 – 27 November 2009

NATO Tactical Data Link Interoperability Test 10-01
NTDLIOTS 10-01/HODGES – GBR-001-10

Objective: To provide a vehicle for NATO Tactical Data Links interoperability Test Syndicate. Initiative conducted a NTDLIOT with various National / NATO assets through the period of execution. This is the 7th NTDLIOT to be conducted over the CFBLNet since the first tests were conducted on 16 Oct 06.

Operational Benefits: Interoperability trials with NATO operational assets.

Customer Feedback: CFBLNet met requirements, ideal platform for TDLIOTS activity. No recorded network outages. NTDLIOTS community plan to use CFBLNet for future NATO interoperability testing. No tasking is on CFBLNet to improve its service is necessary.
The CFBLNet is utilized to provide a forum in which all participating NATO and Authorised Partner nations are able to test IO capabilities and limitations with other participating nations over a secure distributed network.

The test results are documented and forwarded to the C3 IWG for review and publication within the TDL War fighter community.

The TDLITS successfully tested 14 TDL platforms and cleared 55 identified interoperability issues and discovered 131 provisional interoperability issues.

All identified IOIs are adjudicated to ensure that the Warfigher knows and understand the interoperability risks with each NATO nation's TDL operational platforms.

Participants: DEU, ESP, FRA, GBR, ITA, NATO, NOR, USA
Dates: 05 – 30 April 2010

Australian – United States Distributed Engineering Plant
AUSDEP – USA-001-09

Objective: Tactical Data Link and C4ISR interoperability testing.

Operational Benefits: This initiative verified some operational capabilities and limitations between AUS and USA navies.

Customer Feedback: Initiative was an experiment and will require additional experiments to come to a final conclusion or result. Testing was able to verify some operational capabilities and limitations between the Australian Navy and U.S. Navy. Testing was considered a success in most areas. AUSDEP was an experiment; therefore the parts that could not get a true success were still a positive due to it being the first time this was attempted. CFBLNet personnel were very professional and prompt when working with the AUSDEP program. They were able to answer all questions or direct us to the appropriate personnel to answer the

questions needed. Technical support was outstanding and readily available to help with our needs.

CFBLNet met all deadlines required by the program and in some cases CFBLNet personnel helped expedite parts of the CIIP process allowing the initiative stay on track

There were no recorded network outages due to a casualty on the CFBLNet side of the house. Some network outages were experienced on the RED side of the network and these were due to configuration issues or keymat changeover.

AUSDEP were able to successfully prove some portions of their experiment as reported above in terms of how they communicate with the Australian Navy. Data is still being analyzed and will be reported out to the Australian Navy and U.S. Navy DEP program offices at a later date.

Recommendations: CFBLNet should provide a more in depth description/requirements for the completion of the CIIP package. There was one issue regarding the level of detail required for the CIIP package that led to some possible security issues. This issue was rectified and testing was resumed but will need clarification for future events.

Participants: AUS, USA
Dates: 27 April – 10 September 2009

Image Product Library v6.5.1 Technical Assessment
IPL Tech Assess – USA-013-09

Operational Benefits: Enhancements of PRISM Interoperability Coalition Partners.

Customer Feedback: CFBLNet provided very efficient technical delivery with no recorded outages. However, CFBLNet needs to provide an emulation or enclave that equates to ISAF Secret. This would make this Initiative a more frequent customer of CFBLNet as it concentrates on Afghanistan Mission requirements. The operational benefits that were achieved are enhanced PRISM interoperability with Coalition partners.

Participants: USA
Dates: 20 July – 18 September 2009

Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition
MAJIIC 09 – USA-011-09

Objective: The Multi-Sensor Aerospace/Ground Joint ISR Interoperability Coalition (MAJIIC) program is an agreement amongst nine nations to implement standards and capabilities that enable sharing of Intelligence, Surveillance and Reconnaissance products. The program agreements include the conduct of experiments and exercises to test the developed capabilities and capture lessons learned that will lead to further improvements and enhancements.

Operational Benefits: A subset of MAJIIC known as CENTAUR will deploy to the field next year.

Customer Feedback: The CFBLNet technical delivery team always exceeds the requirements

making MAJIIC 09 a highly successful event with no recorded outages. All objectives for this exercise were met. Further testing of MAJIIC will continue for the near future, but, a subset of MAJIIC known as CENTAUR will deploy to the field next year.
Participants: USA, NATO, CAN **Dates:** 20 October – 30 November 2009

Annex B: Continuing and Projected Initiatives for 2011

Highlighted here are Initiatives which were started in 2010 or sooner but have not yet completed their execution as well as Initiatives planned for 2011

Virtual Capability Development & Operations Analysis Symposium 2009 - VCDOAS

Objective: Facilitate knowledge sharing between Capability Development and Operational Analysis Organisations in AUS, CAN, GBR and USA.

Operational Benefits: The perceived benefit is for the symposiums to extend communications channels to enable information sharing of key events that could be addressed.

Participants: AUS, CAN GBR, USA
Dates: Ongoing pending coalition decisions

JSF OMS Collaborative Network - JOC- A

Objective: This event is to integrate the Coalition Warfare Development Facility in China Lake USA to the Maritime Integration and Support Centre at Portsdown West GBR. This connection will represent and Coalition Network to facilitate collaborative planning and the exchange of information to exercise Joint Strike Fighter (JSF) Mission Planning and other applications.

Operational Benefits: The first step in determining a way of working which will permit the development of equipment CONOPS/CONUSE within JSF USA and GBR baseline for both DOB and Carrier Operation conducted in the Coalition environment.

Participants: GBR,USA
Dates: Ongoing

Maritime Missile Defence Single Encryption Enclave - MTMD-SEE

Objective: The Maritime Missile Defence contains three elements BMC4I, CDEP and M&S. BMC4I is required to support exchange of classified technical information amongst the MMD Coalition. These themes will lead to a 1*/2* 'at sea demonstration' anticipated for 2015 to de-risk the intended improvements to Coalition Maritime Integrated Air and Missile Defence capability.

Operational Benefits: BMC4I is required to support exchange of classified technical information (email, FTP and occasional teleconference). BMC4I is one Working Group of the Coalition MMD Forum (others include CDEP and Modelling & Simulation) operating under a Coalition Memorandum of Understanding MMD Forum Principals.

Participants: AUS, CAN, DEU, ESP, FRA, GBR, ITA, NLD, USA
Dates: Ongoing

NATO Live Virtual Constructive - NLVC

Objective: The NATO Live Virtual and Constructive (NLVC) will create a NATO mission training and rehearsal asset. NLVC will provide a Joint Capability and will link NATO and national simulation systems. In the current phase NC3A are carrying out a series of tests running an

HLA (and or DIS) federation with national and NATO simulations and C2 systems such as the NATO Airborne Warning and Control System (NAEW) Mission Trainer simulators. NLVC is funded by Allied Command Transformation (ACT) as part of the Snow Leopard program.

Operational Benefits: Preparing for E3A involvement in a virtual CAS training and for Weapons Controller training.

Participants: NATO
Dates: Ongoing

CENTRIXS-ISAF (CX-I) Test and Evaluation Environment - CTE 2

Objective: The Goal of CENTRIXIS-ISAF (CX-I) Test and Evaluation Environment is to establish a distributed test environment to support CENTRIXIS-ISAF interoperability testing between USA and NATO applications, data interchanges. From a USA perspective, current plans are to establish a CENTRIXIS-ISAF "DECC Node" at JITC Indian Head (JITC_IH) which will also serve for the time being as an "operational" CENTRIXIS-ISAF node. By connecting with GBR node with the OVERTASK representation of the ISAF Mission S~~~~~ configuration (applications and equipment string) and NFX for support of this small Test Evaluation Environment for CENTRIXIS-ISAF and those nodes would provide the core for USA participation. From There, JITC-IH will initiate priority interoperability testing with the tempo and priorities dictated by CENTCOM. This initiative will be able to test interoperability between USA CENTRIXIS-ISAF and NATO ISAF Secret environment. Based on the information Exchange Requirement priorities, all applications which are to be placed on network will be tested to ensure no interoperability issues are present.

Operational Benefits: This Initiative allows all applications to be tested on CTE2 before going onto Theatre. All the interoperability issues and patches will be applied before it is introduced into the warfighter environment thus ensuring minimal impact to the operator. In addition and equally important to applications testing, the test environment has to simulate the actual operational environment which consists of many nodes with multiple application configurations. At a fairly fast rate we will foster the incremental addition to appropriate service and condition labs as enclaves nodes to simulate the operations environment , the first of which, if possible, will be PM Battle Command at Fort Monmouth as they have the majority of the C2 systems Coalition nodes ready to join right now in addition to the GBR include NCSA (NATO Communication and Information Systems Services Agency) in Mons, BE, and node in CAN to help the enclave achieve a realism and flexibility.

Participants: CAN, NATO, GBR, USA
Dates: Ongoing

NATO Tactical Data Link Interoperability Test Syndicate
NTDLIOTS 10-02 MAYNARD

Objective: Information to be supplied.

Operational Benefits: Information to be supplied.

Participants: tbd

Dates: Ongoing

Improved Connectivity Initiative - ICI

Objective: This is AUS/USA Integration Trial between AUS DSM user web and CFE application access through the REL DMZ to SIPRNet

Operational Benefits: It will enable deployment of improved connectivity initiative and allow for all user access to Web and CFE applications from their national desktops.

Participants: AUS, USA
Dates: Ongoing

CENTRIXS Cross Enclave Request Identity Management Testing - CCER Idm

Objective: The MNIS Programme was established to alleviate the challenges of sharing vital information with coalition partners in today's fast-pace dynamic warfighting environment. CENTRIXS Cross Enclave request Identity management testing provides the community of interest services and applications for the future global information grid. This supports the planning and execution of military operations as well as humanitarian assistance and disaster relief operations.

Operational Benefits: Allows a new converged network for information sharing across common operating environments.

Participants: USA
Dates: Ongoing

CENTRIXS Cross Enclave Requirement Collaboration Tool Test - CCER Collab

Objective: The MNIS Programme was established to alleviate the challenges of sharing vital information with coalition partners in today's fast-pace dynamic warfighting environment. CENTRIXS Cross Enclave request Identity management testing provides the community of interest services and applications for the future global information grid. This supports the planning and execution of military operations as well as humanitarian assistance and disaster relief operations.

Operational Benefits: Solutions are being evaluated to determine if they address issues that have been experienced during CFBL Net Initiatives (e.g. Empire Challenge and CWID).

Participants: USA
Dates: Ongoing

Defence Science Technologies Exchange - DSTX

Objective: An Anglo Australian MOU for Science and Technology covering a bi-lateral agreement that aims to develop a unified modeling capability.

Operational Benefits: It will provide shared weapon models and simulation architectures, and integrated launch to lethality high fidelity modeling environment, visualization and analysis tools, standards and processes as well as the ability to execute project collaboration between DSTL

and DSTO.

Participants: AUS, GBR
Dates: Ongoing

Voice and Video over Internet Protocols - VVOIP

Objective: The first of three phases to develop a CAN and USA interoperability for voice and video traffic over IP assured services.

Operational Benefits: Voice and video interoperability for these nations over IP encryption prior to deployment.

Participants: CAN, USA
Dates: Ongoing

Griffin Prototyping and Development Network - GPDN 10

Objective: A prototyping and development network for linking of CCEB nations to investigate and implement interoperability services and technical refreshes.

Operational Benefits: To develop the CCEB Web Service, DNS Service, CDCIE Chat Service and any possible de-risking of the migration to ICI.

Participants: AUS, CAN, GBR, NZL, USA
Dates: Ongoing

ABCA - Allied Auroras - ABCA AA

Objective: Test and evaluation for a proof of concept ABCA distributed synthetic environment.

Operational Benefits: Define, create and test a simultaneous distributed SE Capability.

Participants: AUS, CAN, GBR, NZL, USA
Dates: Ongoing

Coalition Virtual Flag

Objective: To conduct a coalition distributed SE training event. This event will encompass operators participating from their home stations as well as from coalition manned C2 facilities (focused on air operations).

Participants: AUS, CAN, USA
Dates: Ongoing

NATO Education and Training Network (MSG-68)

Objective: NATO Education and Training Network Initiative facilitates the support of NATO, NATO nations and mission partners in the area of exercises, training and education. The

objective of NETN is to assess the distributed simulation and learning capabilities that NATO, Partner and Contact Nations, Schools, and Agencies have that could contribute to the NETN capability.

Operational Benefits: This initiative demonstrates a way forward for interoperability, technical standards and architectures to link these training and education canters to provide a persistent capability. The NETN Initiative will also identify and recommend roles and responsibilities of the NATO, Partner and Contact Nation organizations responsible for distributing and maintaining M&S capabilities within the scope of NETN.

Participants: NATO and NATO Nations, AUS, CAN, GBR, NZL, USA
Participating GMP's: AUT, CHE, FIN, SWE
Dates: Ongoing

Distributed Network Battlelabs (DNBL) – JISR Step 1

Objective: The NATO Distributed Networked Battle Lab initiative was to compress the NATO capability development cycle and to improve mission effectiveness and interoperability of capabilities when they are delivered to operational forces. Distributed Networked Battle Lab has the potential to support the capability development cycle, from concept development through to fielding. JISR Step 1 Testing was planned to complete full motion video (FMV) capabilities pre-deployment interoperability verification for ISAF.

Operational Benefits: The use of Battle Laboratories in a distributed environment will enable the early and standardize collaborative testing and experimentation, which should lead to the improvement of operational efficiency and coherence for military capabilities.

Interim Customer Feedback: Total of 4 NATO-JISR Step 1 experiments were completed with FRA, ITA, DEU, GBR, between April and October 2010, 2 of them making use of CFBLNet infrastructure (FRA, ITA). CFBLNet demonstrated outstanding support in all areas of the national and organisational teams for NATO-JISR with just one issue of reduced bandwidth available for ITA Testing in July. Further NATO-JISR events planned for 2011 are to include GBR, FRA, ITA, DEU, SWE and others, and are expected to be multi-year until 2015.

The Operational Benefits were very high for the JSIR Community. Major achievements were accomplished between the various systems from the participants. Several savings were already accomplished and reduced risk prior to deployment.

Successes include solid security and reduced effort and risk in connecting national systems with NATO systems in theatre of operations.

Participants: DEU, FRA, GBR, ITA, NATO
Dates: May-November 2010

Afghan Mission Network Training (AMN Training) - AMN Training

Objective: The AMN Training Initiative facilitates the support of AMN Mission partners in the area of exercises, training and education.

Operational Benefits: The AMN Training Initiative will enable all HQs, NATO and AMN Nations to;

i) Train in a coalition environment that replicates the theatre environment
ii) Validate and configure systems prior to arriving in theatre.
iii) Facilitate pre-deployment coordination and situational awareness with coalition Partners.
iv) Identify capability gaps and develop solutions prior to deployment.

Participants: IOC NATO and US. Other AMN nations expected to follow.
Participating GMP's: FIN, SWE expected to participate at later time.
Dates: Ongonig

Crow's Nest

Objective: To link together GBR Land Forces based in Germany, Canada and the United Kingdom for the purpose of conducting pre-deployments training.

Operational Benefits: This initiative will improve connectivity to BATUS synthetic wrap to enable concurrent training exercises to take place between Synthetic training establishments. This will improve training and pre-deployment training for British troops and coalition partners.

Participants: GBR
Dates: Ongoing

CAN Forces – Joint Training Experimentation Network - CF-JTEN

Objective: It will be used to connect CAN to coalition partners for the purpose of a seamless training environment that supports a broad spectrum of Joint and Service training requirements.

Operational Benefits: J10 delivers a distributed individual and collective Joint Training capability to the warfighter minimizing the requirement for 'face to face training' - "train as we fight".

Participants: AUS, CAN, GBR, USA
Dates: Ongoing

NATO ALTDAMB Integration Test Bed (AITB) - NATO AITB

Objective: Primary support of risk reduction in the areas of national and NATO systems interoperability and integration of Target Architectures.

Operational Benefit: The NATO ALTDAMB Integration Test Bed (AITB) has been a high profile interoperability and requirements validation capability for the Programme and for NATO. The effectiveness of the ITB has been further enhanced by the turn key solutions and capability offered by the CFBLNet and its network management team. The existence of a test network with connections already in place to the majority of ALTDAMB National Labs and system sites facilitated the ITB connection to hardware-in-the-loop testing some 9 months earlier than originally planned. The CFBLNet is, and will continue to be, a major enabler of our test programme.

Interim Customer Feedback: A Total of 12 NATO-AITB events for 2010 were planned, 3 events were planned between end Oct up to end December.
CFBLNet demonstrated outstanding support in all areas of the national and organisational teams for NATO-AITB.
A further 8 NATO-AITB events planned for 2011 including a large scale Ensemble Test (2) in Dec 2011. Multiple events are planned yearly until 2013.

The Operational Benefits were very high for the AITB Community. Major achievements were accomplished between the various systems from the participants. Several savings have already been achieved.

Successes include stable very high speed HLA/DIS network in support of NATO-AITB with solid security. Successfully used during Joint Project Optic Windmill.

Participants: DEU, ESP, FRA, GRC, ITA, NATO, NLD, POL, USA
Dates: Ongoing

WiSARD 2.0 – Web Service for All-source Releasability and Dissemination

Objective: (WiSARD) is an initiative in the DCGS Coalition Focus Team series sponsored by USD (I) for Coalition interoperability.

Operational Benefits: The Web Service for All-source Releasability and Dissemination (WiSARD) is an Initiative in the DCGS Coalition Focus Team series sponsored by USD (I) for Coalition Interoperability. This initiative will provide a web service to allow Foreign Disclosure Officers (FDOs) to perform their mission more effectively via a Web service for net-centric, Service Oriented Architecture (SOA) based operations. This capability will permit the rapid response to new operational release requirements as conditions warrant. With the advent of ad hoc coalitions that can change on a moments notice, WiSARD can greatly facilitate the foreign disclosure officer's ability to respond. A service such as WiSARD is essential for efficient cross-domain federated operations with coalition partners. The effective use of WiSARD throughout both Department of Defense (DoD) and the Intelligence Community (IC) would significantly enhance the ability to operate in a coalition environment. This demonstration will be performed at the WarCap Demonstration Canter - Pentagon.

Customer Feedback: CFBLNet met our requirements in terms of appropriate management and technical support, flexibility and effectiveness. There was a drop out of service at the WARCAP demo but CFBLNet quality of service met the Imitative requirements. This Initiative is in the process of transitioning to the Warfighter to improve operational benefits. CFBLNet facilitated a very successful demonstration.

Participants: USA
Dates: Ongoing

NTDLIOT 10-02 (MAYNARD) - NATO TACTICAL DATA LINK INTEROPERABILITY TEST 10-02

Objective: NATO Tactical Data Links Interoperability Test Syndicate (TDLITS) TDL IO Test (NTDLIOT).

Operational Benefits: To conduct a NTDLIOT with various National Warfighter Benefits (Include expected / NATO assets

Participants: FRA, DEU, GBR, ITA, NATO, NLD, NOR, ESP, USA
Dates: Ongoing

AAMOST Topic 156

Objective: This initiative is an AAMOST activity to facilitate in-depth knowledge sharing and collaboration between panel members in AUS, and GBR, that is not possible using only unclassified channels. Specific objectives include a demonstration and comparison of cultural analysis tools and techniques in order to develop best practice and promote interoperability.

Operational Benefits: Development of methodologies and tools for the analysis of socio-technical systems.

Participants: AUS, GBR
Dates: Ongoing

CESMO - Cooperative Electronic Support Measure Operation

Objective: The purpose of the new link is to collaboratively develop and test a software interface between a Dstl led electronic surveillance capability CESMO, a similar US System (Network Centric Collaborative Targeting (NCCT); developed by L-3 Communications) and a CESMO Client developed by Norway (FFI). The XML data that would be sent across the link would (at times) be from an operational platform, hence the requirement for a Secret connection. The exchange of data will be covered under an amendment to a project agreement in the NATO Air Force Armaments Group (NAFAG) MOU.

Operational Benefits: The link will allow for collaborative development and testing of a software toolset to improve co-operative collection and fusion of Electronic Surveillance data to support allied operations. The system to which the UK will be connected to in the US is likely to be fitted to multiple UK platforms in the future. Having a link to this capability will allow Dstl to conduct research and testing on potential future MoD systems and ensure that de-risking activities are completed prior to the Procurement stage.

Participants: GBR, USA, NOR
Dates: Ongoing

ANNRN - Anglo-Netherlands-Norwegian Research Network

Objective: The Anglo-Netherlands-Norwegian Research Network (ANNRN) initiative is setup to exchange information and to discuses research information on a secret level between personnel of the participating research facilities. Norway may participate later on.

Operational Benefits: The ANNRN Initiative will provide easier, safer and faster exchange of information between research facilities in the countries mentioned below.

Participants: NLD, GBR

Dates: Ongoing

WiSARD 2.0 – Web Service for All-source Releasability and Dissemination

Objective: (WiSARD) is an initiative in the DCGS Coalition Focus Team series sponsored by USD (I) for Coalition interoperability.

Operational Benefits: The Web Service for All-source Releasability and Dissemination (WiSARD) is an initiative in the DCGS Coalition Focus Team series sponsored by USD (I) for Coalition Interoperability. This initiative will provide a web service to allow Foreign Disclosure Officers (FDOs) to perform their mission more effectively via a Web service for net-centric, Service Oriented Architecture (SOA) based operations. This capability will permit the rapid response to new operational release requirements as conditions warrant. With the advent of ad hoc coalitions that can change on a moments notice, WiSARD can greatly facilitate the foreign disclosure officer's ability to respond. A service such as WiSARD is essential for efficient cross-domain federated operations with coalition partners. The effective use of WiSARD throughout both Department of Defense (DoD) and the Intelligence Community (IC) would significantly enhance the ability to operate in a coalition environment. This demonstration will be performed at the WarCap Demonstration Center - Pentagon.

Participants: USA
Dates: Ongoing

CVF 11-4 - Coalition Virtual Flag 11-4

Objective: CVF 11-4 is a Coalition distributed Synthetic Environment (SE) training event. This event, will have operators participating from their home station as well as from a Coalition manned C2 facility. Event will focus on Air Operations in a simulated Theatre.

Operational Benefits: CVF 11-4 will define, create, test, and utilise a Coalition distributed SE environment. C-EG member Y/N Date Method Comments Evaluate the potential of Coalition training within a SE environment. CCEB Identify simulation interoperability gaps and potential solutions NATO. Inform on national simulation development.

Participants: AUS, CAN, GBR, USA
Dates: Ongoing

PTDLIOT 11-01 (ARMEDE) - PARTNER NATIONS TACTICAL DATA LINK INTEROPERABILITY TEST 11-01

Objective: Partner Nations Tactical Data Links Interoperability Test Syndicate (TDLITS) TDL IO Test (PTDLIOT).

Operational Benefits: To conduct a PTDLIOT with various National, NATO and Partner Nation assets.

Participants: AUS, FRA, CAN, DEU, GBR, ITA, NATO, NLD, USA
Dates: Ongoing

Annex C: Glossary of Acronyms

A

AMN	Afghanistan Mission Network
APAN	All Partners Access Network
ATO	Air Tasking Orders
AUS	Australia
AUT	Austria

C

C/C/S/A	Coalition, Combatant Command, Service and Agencies
C2	Command and Control
C2BL	C2 Battle Lab
C4ISR	Command Control Communications Computers Intelligence Surveillance & Reconnaissance
C5ISR	Coalition Command Control Communications Computers Intelligence Surveillance & Reconnaissance
CAIV	Coalition Interoperability and Assessment Validation
CAN	Canada
CCEB	Combined Communications-Electronics Board
CDEP	Coalition Distributed Engineering Plant
CDIFT	Coalition Distributed Information Test Bed
C-EG	CFBLNet Executive Group
CFBLNet	Combined Federated Battle Laboratories Network
CHE	Switzerland
CIIP	CFBLNet Initiative Information Pack
CLR	CMP Lead Representative
CMM	CFBLNet Management Meeting
CMP	CFBLNet Core Mission Partner
CMT	Coalition Mission Threads
CN/O	Charter Nation/Organization
CND	Computer Network Defense
COCOM	Combatant Command
CONOPS	Concept of Operations
CPM	Capability Portfolio Management
CPOF	Command Post of the Future
CPT	CFBLNet Productivity Tool
C-SSG	CFBLNet Senior Steering Group
CTE2	Coalition Test and Evaluation Environment
CUE	CFBLNet Unclassified Enclave
CWID	Coalition Warrior Interoperability Demonstration
CZE	Czech Republic

D

DCC	Defense Command College
DEN	Denmark
DEU	Germany
DNK	Denmark
DWG	Documents Working Group

E

EC	Empire Challenge

ESP	Spain
EST	Estonia

F

FIN	Finland
FRA	France

G

GBR	United Kingdom/Great Britain
GMP	Guest CFBLNet Mission Partner
GPDN	Griffin Prototyping and Development Network
GRC	Greece

H

HLA/DIS	High Level Architecture/Distributed Interactive Simulator
HUN	Hungary

I

IA	Information Awareness
IPL	Integrated Priority List
Ipv4	Internet Protocol version 4
Ipv6	Internet Protocol version 6
ISAF	International Security Assistance Force
ITA	Italy
IWG	Initiatives Working Group

J

JADOCS	Joint Automated Deep Operations Coordination System
JITC-AZ	Joint Interoperability Test Command (Ft Huachuca, Arizona)
JITC-MD	Joint Interoperability Test Command (Indian Head, Maryland)
JWID	Joint Warrior Interoperability Demonstration

L

LAN	Local Area Network

M

M&S	Modelling & Simulation
MAJIIC	Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition
MLS	Multi-Level Security
MNIS PMO	Multinational Information Sharing Portfolio Management Office
MPLS	Multi-protocol Label Switching
MSAB	Multi-National Security Accreditation Board
MTMD	Maritime Theater Missile Defense

N

NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation Command & Control Agency
NFX	North Fairfax
NLD	Netherlands
NOR	Norway
NTDLIOTS	NATO Tactical Data Link Interoperability Test Syndicate
NZL	New Zealand

O

OGD	Other Government Agencies

P

PASS	Publish and Subscribe System
POC	Point of Contact
POL	Poland
PTDLIOT	Partner National Tactical Data Link Interoperability Test

Q

QoS	Quality Of Service

R

RDT&A	Research, Development, Trials & Assessment
ROU	Romania

S

SME	Subject Matter Expert
SN/O	Sponsored Nation/Organization
SWE	Sweden
SWG	Security Working Group

T

TDL	Tactical Data Link
TDLITS	Tactical Data Link Interoperability Testing
TUR	Turkey

U

UK	United Kingdom
USA	United States of America
USJFCOM	United States Joint Forces Command

V

VCDOAS	Virtual Capability Development & Operations Analysis Symposium
VPN	Virtual Private Network
WAN	Wide Area Network

W

WG	Working Group

X

XMPP	Extensible Messaging and Presence Protocol

For more information, please visit us on the Internet at:
www.CFBLNet.info
or contact our Secretariat at:
CFBLNetgroup@disa.mil.