

UNCLASSIFIED

COMBINED FEDERATED BATTLE LABORATORY NETWORK (CFBLNET)



2004 ANNUAL REPORT

UNCLASSIFIED

UNCLASSIFIED

The Chairman on behalf of the Combined Federated Battle Laboratory Network (CFBLNet) Executive Group (C-EG) hereby approves the *CFBLNet 2004 Annual Report*.

A handwritten signature in black ink, appearing to read "Lloyd E. Gilham", is written over a horizontal line. To the right of the signature, the date "11/29/04" is handwritten.

Capt. Lloyd E. Gilham, USN

(date)

Joint Staff, J6B

C-EG Chairman/U.S. Representative

With endorsement from:

Mr. Einar C. Thorsen

NATO C3 Agency

NATO C-EG Representative

Colonel Richard Gervais, CAN

CCEB C-EG Representative

Table of Contents

FOREWORD 4

BACKGROUND 4

2004 EVENTS 4

PARTICIPANTS 5

EXECUTIVE GROUP REVIEW 6

INITIATIVES SUMMARY 8

SECURITY SUMMARY 10

DOCUMENTATION SUMMARY 10

NETWORKS, SYSTEMS AND SERVICES SUMMARY 11

CONCLUSION..... 15

Additional Resources

Appendix: Acronyms

CFBLNet 2004 Annual Report Data CD

Foreword

This report reflects the progress and accomplishments of the Combined Federated Battle Laboratory Network (CFBLNet) during the calendar year 2004. In addition, a CD that consists of documents, briefings and other data accompanies this report.

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 Lab (CFBL). Organizers from the US, NATO and Combined Communications-Electronics Board (CCEB) developed a concept for the CFBL that built on the Coalition Wide Area Network that was established each year for the Joint Warfare Interoperability Demonstration (JWID).

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

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

2004 Events

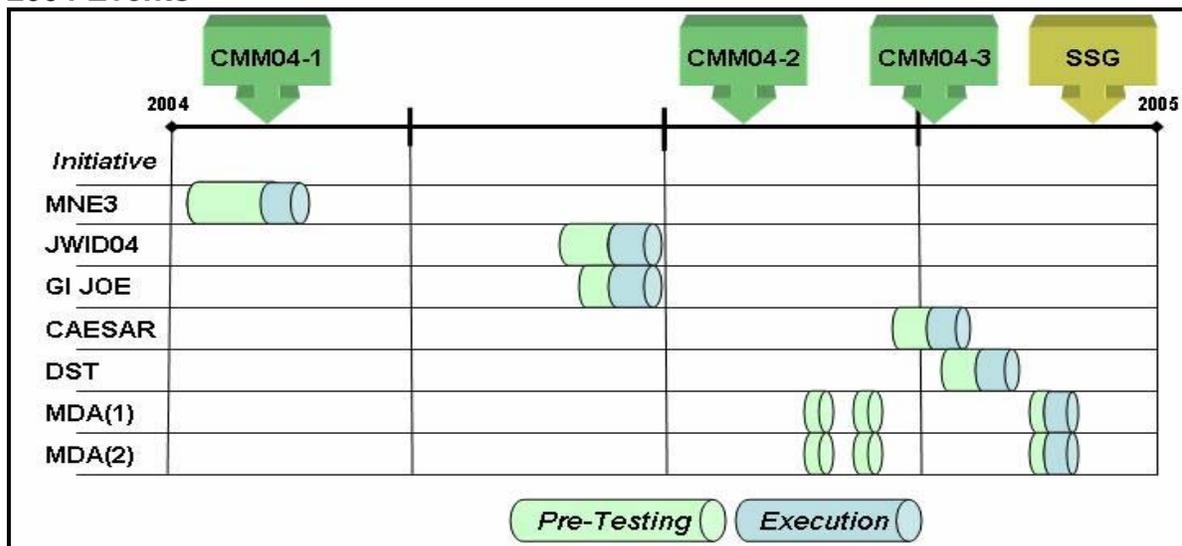
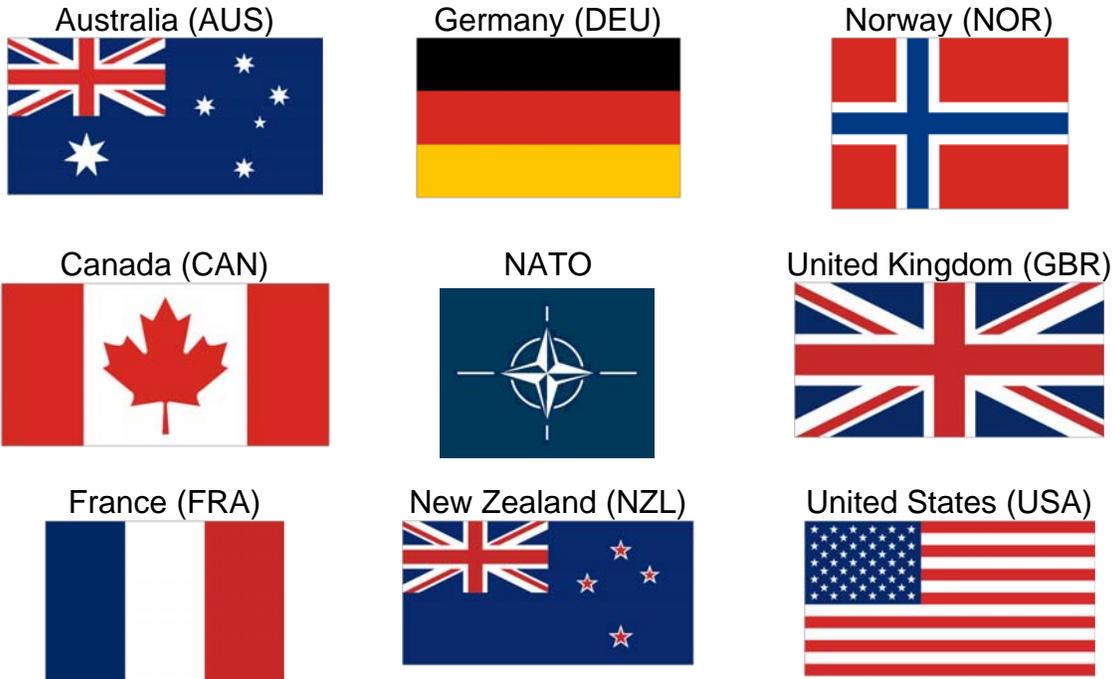


Illustration 1: CFBLNet 2004 Events Time line

Participants

Nations and Organizations permanently connected to CFBLNet in 2004 are listed below:



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



Executive Group Review

1. **C-EG Decisions** were recorded at three CFBLNet Management Meetings (CMMs) held throughout 2004:
 - a. Participation by all Nations/Organizations is encouraged at CMMs and Working Groups meetings.
 - b. Agreed in principle to employment of VPNs and/or Cryptologically separated domains.
 - c. If VPNs are used for an Initiative event, it is the National Lead's responsibility to coordinate Initiatives and cleansing of data at the close of the experiment.
 - d. VPN core services shall not degrade CFBLNet Core service capability.
 - e. Temporary CFBLNet Sites must provide projected start and end dates for connectivity to the CFBLNet.
 - f. Long term (on going) Initiatives shall provide at least an annual status update to the EG and general body.
 - g. Future Initiatives must address manpower and support requirements (to include any CCCC functions).
 - h. Concurred in principle to develop a scalable capability for temporary access.
 - i. Designated Working Groups in two categories
 - i. Active Working Groups
 - Security Working Group (SWG)
 - Network Working Group (NWG)
 - ii. Virtual Working Groups
 - Initiatives Working Group (IWG)
 - Documents Working Group (DWG)
 - j. The Cycle for Documentation review will be as follows:
 - i. At the first CMM of the year (CMM1) all charter documents will be reviewed for potential updates and changes.
 - ii. During a publicized time between CMM1 and CMM2 (typically in the month of MAY) all proposed changes must be submitted to the Secretariat/DWG Chair for incorporation into a final document for final coordination.
 - iii. By the start of CMM2 a new baseline should be submitted to the EG for final approval.
 - k. Amendments to the Charter were proposed.
 - i. The Removal of terms "Test and Evaluation (T&E) and replacing with "trials and assessment".
 - ii. Removal of terms relating to the AITS-JPO as the "Executive Agent" (in paragraph 7).
 - l. Decided not to have a CFBLNet Management Plan.
 - m. Agreed to support the CFBLNet Unclassified Enclave (CUE).
 - n. Endorsed the CWID proposal about the Purple Enclave. EG also noted that the Blue Core services are maintained.
 - o. Supported the Black backbone.

- p. Agreed with NWG recommendation to remove the term developing services. Services are either core supporting or core critical.
- q. Supported the NWG research of a collaboration tool to be utilized by the CFBL WGs and EG.
- r. Agreed that CFBLNet will be promoted as the network of choice for IPv6 development.

2. **Major tasks assigned** by the C-EG to subordinate bodies include the following:

- a. The National Lead or an appropriate sponsor must brief CFBLNet Initiatives at scheduled CMMs. Additionally, the appropriate representation must be available in WG meetings to address Security and Network matters.
- b. Each Initiative shall provide POCs for each participating nation/organization.
- c. SWG Chair must ensure MSAB representation at each CMM (Default will be host Nation's MSAB representative)
- d. The NWG will document the current Architecture, which will be used as the baseline architecture document.
- e. The NWG should add 'Validation of the Site Status Table' as a permanent agenda item for CMMs.
- f. The Secretariat and the USA Action Officer will review for additional changes to the Charter as needed (i.e. signature blocks) and prepare for final signature by the SSG and provide the rationale for changes to the EG
- g. The Secretariat to contact the US IPv6 Program Office (DISA) and coordinate and organize a presentation by CMM05-1.
- h. The Secretariat and the WG Chairs to provide a Draft CFBLNet Implementation Plan for IPv6 at CMM05-2.

3. **Implications** arising from the decisions and actions taken by the C-EG:

- a. Working Group Chair positions will be ratified by the EG based on 24 Month assignments. WG Chairs will work in close coordination with the Secretariat.
- b. Active Working Groups (AWGs) will have sessions at CMMs.
- c. Virtual Working Groups (VWGs) are expected to complete assignments electronically without actually meeting physically. Only the Chair of a VWG is required to attend CMMs.
 - i. National Leads are considered the primary POC for all actions regarding the VWGs.
 - ii. VWG Chair Positions will default to the Secretariat if there are no Volunteers
- d. The SWG Chair must be an official government or military (employed by the government) representative.

- The Rotation Cycle will be as follows: CCEB – NATO – US, however, volunteers will take precedence.
- e. The NWG Chair is a permanent position for the US and must be an official government or military (employed by the government) representative, effective as of CMM05-2.

4. There were no **irresolvable matters** that required elevation to the C-SSG.

Initiatives Summary

Seven CFBLNet Initiatives completed execution in 2004. In addition to the Initiatives listed in this section, other Initiatives conducted testing throughout the year.

MNE 3 (Multinational Experiment 3)
Participants: AUS, CAN, DEU, FRA, GBR, USA, NATO
Objective: Explore how a distributed coalition task force headquarters conducts effects based planning.
Execution: February 2004

JWID 04 (Joint Warrior Interoperability Demonstration 2004)
Participants: CCEB nations, NATO nations, Republic Of Korea (ROK), Partnership for Peace (PfP) nations
Objectives: Multi-level security; language translation; situational awareness interoperability; core network services for “operational” CWAN; network vulnerability assessment; logistics interoperability.
Execution: June 2004

GI JOE (Geospatial Intelligence Joint Operations Experiments)
Participants: USA, CAN, GBR, AUS
Objectives: Integration of NGA Imagery Libraries; Integration of Multi-International sources available; Integration of other “J” databases available (Logistics, Civil, etc.)
Execution: June 2004

Coalition Aerial Surveillance and Reconnaissance (CAESAR)
Participants: USA, NATO
Objectives: Conduct Technical Interoperability Experiment to prepare for transition to MAJIC (Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition) environment for future trials.
Execution: October 2004

Distributed Simulation Trial (DST/TTCP)
Participants: AUS, CAN, GBR, NZL, USA
Objectives: Maritime Picture Compilation and Information Exchange Experimentation; Multinational Experimentation Infrastructure Development and De-risking
Execution: October 2004

Missile Defence C2 interoperability trial (MDA (1))
Participants: USA, NATO
Objectives: Explore means and mechanisms to exchange and co-ordinate C2 activities for MD planning, Situational Awareness, and Consequence Management.
Execution: November 2004

Missile Defence C2 interoperability trial (MDA (2))
Participants: USA, GBR
Objectives: Explore means and mechanisms to exchange and co-ordinate C2 activities for MD planning, Situational Awareness, and Consequence Management.
Execution: November 2004

New Initiatives Interests in 2004

The following CFBLNet Initiatives were introduced to the CFBLNet in 2004. The status of these listed Initiatives range from 'pre-nomination' stage through completed execution.

Lead	Initiative Name	Meeting
USA	Coalition Secure Management and Operations System (COSMOS)	CMM04-1
USA	Coalition Aerial Surveillance and Reconnaissance (CAESAR)	CMM04-1
USA-GBR	Naval Fires Coalition Testing	CMM04-1
USA	Multinational Experiment 4 (MNE4)	CMM04-2
CAN	Distributed Simulation Trial (TTCP MAR TP-1)	CMM04-2
CAN	MIC Griffin Domain (MGD)	CMM04-2
DEU	Recognized Maritime Picture (RMP) Information Exchange Trial	CMM04-2
USA	Missile Defense Agency (MDA) (USA/GBR)	CMM04-2
USA	Missile Defense Agency (MDA) (USA/NATO)	CMM04-2
GBR	Ptarmigan – RITA Interoperability Trial (PRIT)	CMM04-3
CAN	Knowledge Management LOE (Segment of MNE)	CMM04-3
USA	Coalition Warrior Interoperability Demonstration 2005 (CWID05)	CMM04-3

Table 1: CFBLNet 2004 Initiative Interests

Security Summary

During 2004, the security efforts for CFBLNet included the following:

1. Defined the types of boundary protection system requirements for interconnection of Coalition security domains/enclaves.
2. Developed documentation and procedures for the Coalition to support nations/organizations policies, practices and procedures
3. Developed a list of general security requirements for Multi-Level Security (MLS).
4. Provided security procedures for guest nations/organizations to participate in CFBLNet Initiatives.

Documentation Summary

The first version of the CFBLNet Publication 1 was completed in 2003. Changes and updates to this document have continued in 2004 as the CFBLNet continues to evolve with new requirements and direction. All documents are UNCLASSIFIED and are available for regular use via request or from CFBLNet Websites.

1. Version 1 documentation published on CD in January 2004 and provided at CMM04-1 for national representatives and meeting attendees (Also, available via the CFBLNet Website)
2. Version 2 documentation changes were made based primarily on EG Guidance provided at QMM03-3 and CMM04-1. No changes were made to Annex C and Annex D.

Technical Arrangement (Charter) Original Document (Update proposed to the C-SSG in December 2004)	Signed and Approved by C-SSG: August 2002
Publication 1: Organization and Responsibilities <i>Version 2.0/DEC04</i>	Signed and Approved by C-EG: December 2004
CFBLNet Publication 1 – Annex A: Glossary <i>Version 2.0/DEC04</i>	Approved by C-EG: December 2004
CFBLNet Publication 1 – Annex B: Initiative Processing <i>Version 2.0/DEC04</i>	Approved by C-EG: December 2004
CFBLNet Publication 1 – Annex C: CFBLNet Security and Accreditation Strategy <i>Version 2.0/DEC04 (No Changes)</i>	Approved by C-EG: Version # change only
CFBLNet Publication 1 – Annex D: Network Operations (Network/System Aspects of the CFBLNet) <i>Version 2.0/DEC04 (No Changes)</i>	Approved by C-EG: Version # change only

Networks, Systems and Services Summary

In 2004, network engineering efforts included the following:

1. Developed and gained National/Organizational support of the CFBLNet Black Backbone (IPv4). Backbone services are IP routing, QoS, network monitoring, and DNS.
2. Developed and gained support for the CFBLNet Unclassified Non-Internet releasable Enclave (CUE). The primary purpose of the CUE is to support non-Secret cleared personnel and/or non-CFBLNet nations and unclassified initiatives. The secondary purpose is to support the development of Multi-Level Security (MLS) and IPv6 solutions.

3. Proposed CFBLNet Scalability for future CWID Initiatives and others which require a permanent capability for temporary access of nations who are not charter CFBL members.
4. Promoted CFBLNet as the network of choice for IPv6 development.

CFBLNet Sites

CFBLNet sites are the physical locations accredited through national/organizational assurance agencies in accordance with the CFBL security process and approved by the CFBLNet Executive Group (C-EG). CFBLNet sites, whether permanent or temporary, must be nominated by the national/organizational lead to the Secretariat. At its inception, the CFBLNet was composed of 17 sites, and in 2004 has grown to more than 80 Operational and Approved sites in 11 countries and NATO. Table 1 indicates the number of Operational, Approved and Nominated sites. Operational sites are fully connected and accredited sites on the CFBLNet. Approved and Nominated sites are sites that are in the process of becoming Operational sites.

Nation/ Organization	Operational	Approved	Nominated
Australia (AUS)	14	7	0
Canada (CAN)	10	2	0
France (FRA)	2	0	2
Germany (DEU)	4	0	1
Italy (ITA)	0	1	1
NATO	4	1	0
New Zealand (NZL)	1	6	0
Norway (NOR)	5	0	0
Spain (ESP)	0	1	1
Romania (ROU)	0	1	0
United Kingdom (GBR)	4	6	0
United States (USA)	8	9	1
TOTAL	52	34	6

Table 2: CFBLNet 2004 Operational, Approved and Nominated Sites

New Site Interests in 2004

The following CFBLNet sites were introduced to the CFBLNet in 2004. A complete listing of the sites and site status is available on the information CD that accompanies this report.

Sponsor	Name/Location	Type	Meeting
USA	DISA - Slidell, Louisiana	Permanent	CMM04-1
USA	USFK - Yongsan, Korea	Temporary	CMM04-1
CAN	Shirley's Bay Mobile Lab, Ottawa	Temporary	CMM04-1
DEU	MoD, Bonn	Permanent	CMM04-1
DEU	Bundeswehr Analyses and Study Centre, Waldbrö	Permanent	CMM04-1
DEU	Naval Office, Rostock	Temporary	CMM04-1
DEU	SEMA CCI, Meppen	Temporary	CMM04-1
DEU	Air Force Office, Köln-Wahn	Temporary	CMM04-1
ITA	Gr.A.S.C.C C2 Automation Group, Pratica Di Mare	Temporary	CMM04-1
ESP	Regimiento de Transmisiones Estrategicas 22, Madrid	Temporary	CMM04-1
ROU	Mechanical Brigade, Bistrita	Temporary	CMM04-1
AUS	CEA Lab, DSTO Pyrmont, Sydney	Permanent	CMM04-2
AUS	TADL Lab Fyshwick, Canberra	Permanent	CMM04-2
AUS	DISTAL Lab, DSTO Edinburgh, Adelaide	Permanent	CMM04-2
AUS	Focal Lab, DSTO Edinburgh, Adelaide	Permanent	CMM04-2
NZL	DTA Auckland	Temporary	CMM04-2
USA	NORTHCOM Federal Building, Colorado	Permanent	CMM04-3
USA	NORTHCOM Peterson AFB Colorado	Permanent	CMM04-3
FRA	DGA, Arcueil	Permanent	CMM04-3
FRA	Creil AFB, Creil	Permanent	CMM04-3
NATO	ACCS System Testing and Verification Facility (STVF), Glons, Belgium	Temporary	CMM04-3

Table 3: New Site Interests for CFBLNet 2004

Illustration 2 indicates CFBLNet Level 0 (zero) topology with national points of presence (POPs) for 2004.

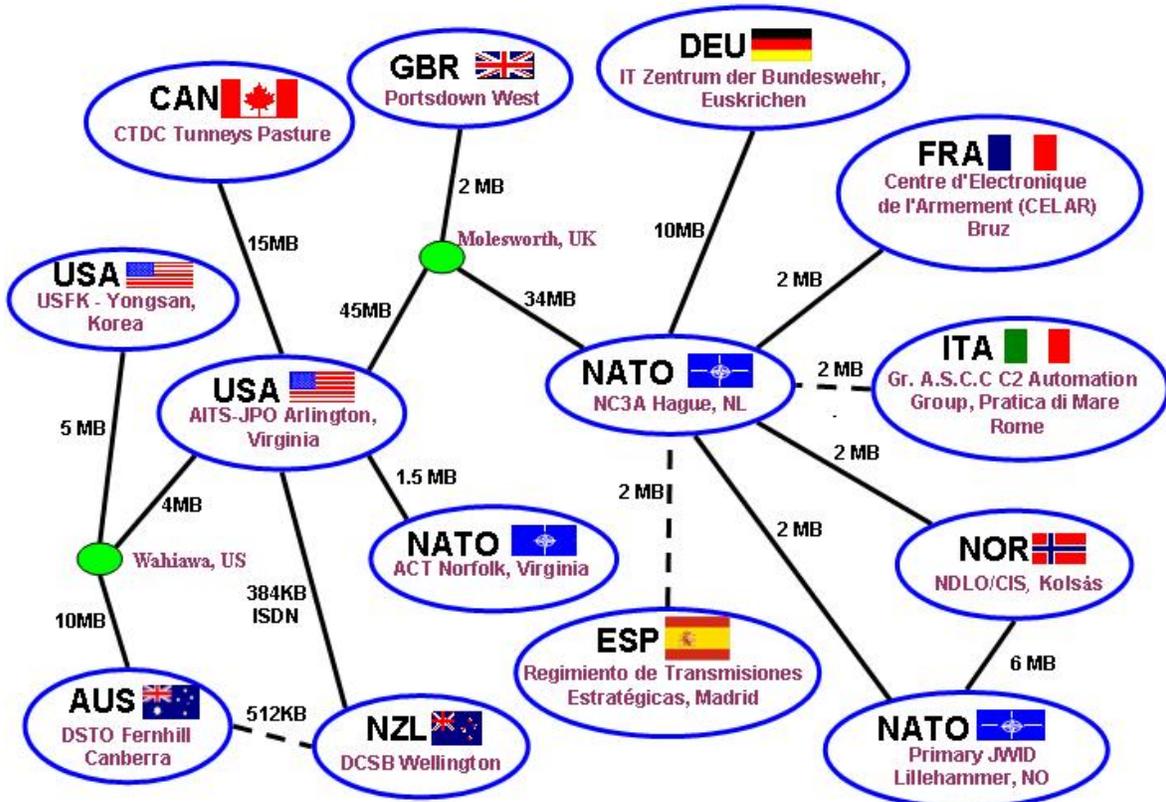


Illustration 2: CFBLNet 2004 Level 0 Topology

CFBLNet Services

The CFBLNet engineers agreed to remove the category of developing services during CMM04-3. Core services are robust, reliable and stable network services, which have been developed and deployed on the network to facilitate initiatives. They are managed and supported directly by the nation/organization. Core services are further sub-divided into critical and supporting (Value Added) infrastructure, to distinguish between those services that are essential and desirable for operating and supporting the CFBLNet.

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

Table 4: CFBLNet 2004 Core Services

Conclusion

From inception to the end of 2004, the Combined Federated Battle Laboratory has continued to experience steady growth and increased participation. The growing interest in conducting initiatives on CFBLNet has attributed to the increase in infrastructure and services provided. The number of sites have increased by over 150% overall.

The CFBLNet environment began as a single classification domain, but quickly evolved into a variety of restricted classification domains. In addition, member nations identified requirements to sponsor non-member nations as participants in proposed initiatives

The CFBLNet has been an invaluable asset for multinational C4ISR capability and interoperability testing. Even though the objective for the near future is coalition operations and interoperable capabilities that enable information sharing across multiple security domains, CFBLNet must continue to change to meet evolving customer requirements such as the implementation IPv6 and Multi-Level Security.

Acronyms

AITS-JPO	Advanced Information Technology Services-Joint Program Office
AUS	Australia
AWG	Active Working Group
BGP4	Border Gateway Protocol Version 4
C2	Command and Control
C3	Consultation, Command & Control
C ⁴ ISR	Command Control Communications Computers Intelligence Surveillance & Reconnaissance
CAESAR	Coalition Aerial Surveillance and Reconnaissance
CAN	Canada
CCCC	Combined Communications Control Center
CCEB	Combined Communications Electronics Board
C-EG	CFBLNet Executive Group
CFBL	Combined Federated Battle Laboratory
CFBLNet	Combined Federated Battle Laboratory Network
CMM	CFBLNet Management Meeting
COSMOS	Coalition Secure Management and Operations Systems
C-SSG	CFBLNet Senior Steering Group
CUE	CFBLNet Unclassified Enclave
CWAN	Coalition/Combined Wide Area Network
CWID	Coalition Warrior Interoperability Demonstration
DEU	Germany
DNS	Domain Name Server
DST	Distributed Simulation Trial
DWG	Documents Working Group
EG	Executive Group
EIGP	Extended Interior Gateway Protocol
ESP	Spain
FIN	Finland
FRA	France
GBR	United Kingdom/Great Britain
GI JOE	Geospatial Intelligence Joint Operations Experiment
HTTP	Hyper Text Transfer Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol version 6
ITA	Italy
IWG	Initiative Working Group
IWGC	Initiatives Working Group Chair
JWID	Joint Warrior Interoperability Demonstration
KOR	Republic of Korea

UNCLASSIFIED

LDAP	Lightweight Directory Access Protocol
MAJIC	Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition
MAR	Maritime Systems Group
MDA	Missile Defense Agency
MLS	Multi-Level Security
MNE	Multi-National Experiment
MSAB	Multi-National Security Accreditation Board
NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation Command & Control Agency
NGA	National Geospatial Agency
NNTP	Network News Transfer Protocol
NOR	Norway
NSAP	Network Service Access Protocol
NTP	Network Time Protocol
NWG	Network Working Group
NWGC	Network Working Group Chair
NZL	New Zealand
OSPF	Open Shortest Path First
PACRIM	Pacific Rim
PfP	Partnerships for Peace (NATO term)
POC	Point of Contact
POL	Poland
QMM	Quarterly Management Meeting
QoS	Quality Of Service
RDT&E	Research, Development, Test & Evaluation
ROU	Romania
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SWE	Sweden
SWG	Security Working Group
SWGC	Security Working Group Chair
TP-1	Technical Panel One
TTCP	The Technical Cooperation Program
USA	United States of America
VPN	Virtual Private Network
VWG	Virtual Working Group
WG	Working Group