



**GLOBAL CONNECTIONS**

# Coalition Partner Sites

**C**WID 2006 is the premier event to investigate coalition interoperability issues, and coalition partners work with U.S. organizations and agencies to define solutions that can be applied to the operational community. CWID assesses technological, security, software or procedural capabilities that address unique requirements in each country and provide information exchange solutions. Cooperation among Allied participants is essential to moving coalition interoperability to the next level.

**PARTICIPANTS**

-  **AUSTRALIA**
-  **CANADA**
-  **FRANCE**
-  **GERMANY**
-  **ITALY**
-  **THE NETHERLANDS**
-  **NEW ZEALAND**
-  **NORWAY**
-  **POLAND**
-  **PORTUGAL**
-  **ROMANIA**
-  **SPAIN**
-  **TURKEY**
-  **UNITED KINGDOM**
-  **UNITED STATES**
-  **NATO**

This Chairman of the Joint Chiefs of Staff annual event conducts interoperability trials to test and evaluate technologies and capabilities which enable the exchange of information among agencies, Services, combatant commands and multinational participants.

U.S. European Command is the host combatant commander for 2006 and 2007. This is the first time the event has been hosted outside of the U.S. Hosting CWID at the only forward-deployed combatant commander focuses the event on the forward-deployed warfighter and on our Coalition environment.



*Hosting CWID at the only forward-deployed U.S. combatant commander focuses the event on the forward-deployed warfighter and on the Coalition environment.*



**U.S. SCHEDULE OF EVENTS**

- May 30-June 23: Execution
- May 30-June 4: National Integration/Final Testing and Trial Set-Up
- June 5-11: Coalition Integration, Scenario Training and Rehearsal
- June 12-22: Execution and Assessment
- June 19-22: Visitor Week
- June 23: Hot Wash

This year's participants include Australia, Canada, New Zealand, United Kingdom and NATO. The event examines a range of technologies to enhance the collaborative information environment that the U.S. Joint Chiefs of Staff, combatant commanders and other Defense agencies are developing. The end result should be enhanced information sharing, increased situational awareness, improvements in database fusion and dissemination, and information security. CWID leadership is also emphasizing the accompanying concept of operations and tactics, techniques and procedures that will facilitate a more responsive fielding solution.

CWID 2006 will also assess capabilities and technologies that allow information sharing between Homeland Security and Homeland Defense partners in both the United States and Canada.

One of CWID's primary challenges is enhanced coalition interoperability. CWID focuses on defining solutions to interoperability issues, ensuring those solutions can be applied to the operational community and enabling a standard solution for information sharing between coalition partners. The demonstration also features information exchange across multiple domains.

Clearly, CWID has a global presence, addressing coalition interoperability, homeland security, and homeland defense issues at every opportunity.

**NATO OBSERVERS**

-  **CZECH REPUBLIC**
-  **DENMARK**
-  **HUNGARY**

**PARTNERSHIP FOR PEACE OBSERVERS**

-  **FINLAND**
-  **RUSSIA**
-  **SWEDEN**



## COMBINED COMMUNICATIONS ELECTRONICS BOARD

# Australian Defence Organisation

*The Australian Defence Organisation is participating in the U.S. Coalition Warrior Interoperability Demonstration 2006. The aim is to pursue developments in Combined and Joint C4ISR capabilities and to improve combined and joint interoperability between multi national systems.*



### AUSTRALIA'S PARTICIPATION

Australia's participation involves the standing up of an integrated Australian/New Zealand/Canadian Joint Division to which Australia contributes land and air forces. Australian participation operates from the Command and Control Systems Battle Laboratory at Fern Hill Park, a Defence Science and Technology Organisation (DSTO) facility in Canberra. Small geo-spatial and securi-

### AUSTRALIAN SPONSOR

RADM M.J. Tripovich, AM, CSC  
Head Capability Systems  
Capability Development Group

ty elements are also supporting the activity.

Australian liaison officers are augmenting the staff at Combined Forces Air Component Commander (CFACC), Hanscom Air Force Base; the Combined Communications Control Centre – Rear (CCCC-Rear), Defense Information Systems Agency (DISA), Arlington; Linton Army Base, New Zealand; and the Defence Research and Development Centre, Valcatier, Canada.



**OPPORTUNITIES PRESENTED BY CWID 2006**

- CWID provides an opportunity for Defence and industry to explore and demonstrate new and evolving C4ISR concepts and capabilities in a simulated operational environment.
- CWID assists the Defence operational community to more clearly articulate capability user requirements, through increased awareness and understanding of emerging concepts and technologies.
- CWID allows Australia to engage with participating nations in combined and coalition interoperability initiatives and to influence the development of the evolving Combined Information Environment.
- CWID enables Australia to develop knowledge and expertise in networking and C4ISR systems engineering in a combined and coalition environment.

**OPERATIONAL FOCUS AREAS**

- Multi Level/Multi Domain Security - Provide solutions to enable the secure electronic exchange of information across combined, coalition, joint and interagency information domains.
- Situational Awareness - Provide solutions to enable a common understanding of the battlespace in the combined, coalition, joint and interagency information domains.
- Information Management - Provide solutions to store, retrieve, fuse, disseminate and present appropriate information within com-

combined, coalition, joint and inter agency information domains.

■ Collaborative Tools - Provide solutions to enable real and near real time collaboration in combined, coalition, joint and interagency information domains.

■ CIS Technologies - Provide solutions that are scalable and that enable combined, coalition, joint and interagencies to exchange electronic information across the various information domains, which might be bandwidth constrained, deployed or mobile.



**GENERAL CONTACTS**

**Australian CWID 2006 Director**  
 LTCOL Meg Dugdale  
 Tel: +61 2 61 274 949  
 meg.dugdale@defence.gov.au

**Scenario Assessment and Training Manager**  
 MAJ Arthur Dugdale  
 Tel: +61 2 61 274 950  
 arthur.dugdale@defence.gov.au

**System Engineering and Security Coordination CFBL/CWID**  
 Mr Ian Hogg  
 Tel: +61 2 62 651 262  
 ian.hogg@defence.gov.au

**Systems Manager CFBL/CWID**  
 Mr Stan Cutler  
 Tel: +61 2 62651342  
 stan.cutler@defence.gov.au

**Networks CFBL/CWID**  
 Mr Phil Douglass  
 Tel: + 61 2 62657841  
 phil.douglass@defence.gov.au

**KEY DATES CWID 2006**

[Australian Perspective]

- 30 May to 4 June  
Trial system setup commences
- 5 June to 11 June  
Trial set to work and Warfighter training
- 12 June to 18 June  
CWID trials week 1
- 19 June to 23 June  
CWID trials week 2
- 20-22 June  
Visitors period
- 23 June  
CWID hotwash
- September  
Assessment report



**VIPS AND VISITORS**

Visitors from the Defence Force, other Government agencies and industry are invited to observe the activity at DSTO Fern Hill Park during the period 20 to 22 June 2006. Visitors should contact the Australian CWID Director to coordinate the visit. International visitors should send security clearances through their respective diplomatic posts.

*Australia is sponsoring and supporting the following interoperability trials:*

**AUSTRALIAN SPONSORED INTEROPERABILITY TRIAL**

**IT05.13** Microsoft Australia: Coalition Command Collaboration Services

**AUSTRALIAN SUPPORTED INTEROPERABILITY TRIALS**

**IT01.20** Integrated Information Management System

**IT01.28** Mission Management Suite (MMS)

**IT01.50** Multinational Interoperability Toolkit (MIT)

**IT02.21** Multinational Coalition Security System (MNCSS)

**IT02.45** Command Center Portal Framework (CCPF)

**IT03.16** Intelligent Road/Rail Information Server (IRRIS)

**IT05.17** WMD Collaborative Advisory Response System (WMDCARS)

**IT05.51** FORCEnet Distributed Channel Services (FnDCS)

**IT05.66** Coalition Shared Information Network Environment (COSINE)



**COMBINED COMMUNICATIONS ELECTRONICS BOARD**

# Developing Solutions for Canada

*The Coalition Warrior Interoperability Demonstration provides Canada with a dynamic opportunity to evaluate new and emerging C4I technologies for use in the Canadian Forces and other government departments, and to develop solutions to interoperability challenges nationally, and with Canada's principal allies.*

Within Canada, CWID has primarily been a program of the Department of National Defence (DND) in conjunction with other Allied militaries. The Department of Public Safety and Emergency Preparedness Canada (PSEPC) was invited as a participant beginning in 2004. This mirrored CWID participation of Homeland Security / Defence organizations by the United States. Although CWID remains a DND initiative, PSEPC has once again partnered with DND in 2006. In addition to PSEPC, CWID 2006 is marked by an increased awareness and support by other government departments and

their attendant agencies. This has allowed CWID to evolve into a venue that explores solutions for purely military purposes as well as those of common interest to domestic security and public safety organizations within Canada.

CWID tests the interoperability of cutting edge technologies that address either current or future operational needs at the multinational, joint or inter-agency level. CWID brings together 23 separate nations, including different military services and government agencies, on one global experimentation network. The Demonstration allows first hand experience with issues of new capabilities and the chance to measure the effectiveness of the latest technologies. If successful, selected technologies can then be rapidly transitioned into service. Technologies are tested at CWID through Interoperability Trials and examined against specific objectives.

**AIM**

The aim of Canada's participation in CWID 2006 is to enhance interoperability within a military coalition and domestic security environment.



**SUPPORTING TRANSFORMATION**

As detailed in the Defence Policy Statement 2005, the Canadian Forces (CF) is currently undergoing its single largest transformation since Unification in the late 1960s. This transformation will require the CF to adopt a fully integrated and unified approach to operations and future force development.

**CWID SUPPORTS TRANSFORMATION BY:**

- Aiding improved coordination with other government departments and interoperability with allied forces through the investigation of emerging technology
- Providing a venue to explore new solutions for command, control, communications, computers, intelligence, surveillance and reconnaissance capabilities (C4ISR)
- Allowing greater emphasis on the experimentation of technologies that can support developing doctrine, concepts and capabilities

**SCENARIO BASED EVALUATION**

An exercise scenario provides context for the Demonstration and a realistic evaluation of Interoperability Trials. This allows military and government personnel to use technologies in a manner that closely matches their potential use in the real world. While the technologies are being used, Operational Research Scientists measure their performance and effectiveness. The results of this research are shared with all government participants as a group and each technology vendor on an individual basis.

**DUAL SCENARIOS**

For CWID 2006, two scenarios were created. One scenario involves a traditional military expeditionary coalition in a

**CANADIAN OBJECTIVES**

The objectives for Canadian participation in CWID 2006 are:

1. Coalition Command and Control (C2)
2. Coalition Information Sharing
3. Continuity of Operations
4. Net Enabled Services
5. Integrated Logistics

**SENIOR NATIONAL REPRESENTATIVE**

Captain (Navy) Kevin Laing  
Commandant CFEC

fictional region overseas. The second scenario addresses the requirements of domestic security within North America. For the military coalition scenario, Canada's focus is on a unified national command and an integrated force involving all three Environmental Elements operating seamlessly with coalition partners. The domestic security scenario is led by PSEPC with close participation from DND, the RCMP, Health Canada and other Government Agencies. The primary international partner for the domestic security scenario is the United States with its various Homeland Security / Defence Agencies.

**EXPERIMENT DIRECTOR**

Major Pat Bailey, CFEC  
613.991.6154  
FAX: 613.991.5819  
bailey.pa@forces.gc.ca

**DEPUTY EXPERIMENT DIRECTOR**

Major George Sherwood, CFEC  
613.990.7506  
sherwood.g2@forces.gc.ca

**PUBLIC AFFAIRS OFFICER**

Jessica Lawson, CFEC  
613.990.7542  
lawson.ja@forces.gc.ca



**NATIONAL CWID 2005 SITES**

Canadian participation will involve activities within Canada, NATO, US, UK, AS, and NZ.

- The Canadian Forces Experimentation Centre (CFEC), located at Shirley's Bay, Ottawa Ontario coordinates all experimentation and Interoperability Trials for Canada within the CWID program and will be the main site for CWID 2006.
- Other Canadian sites include Valcartier Quebec, Winnipeg, Manitoba, and two technical sites in the Ottawa area.

**PARTICIPATION AT COALITION SITES**

Canada will deploy staff to the main NATO CWID site in Lillehammer Norway, the Coalition Air Component site at Hanscom AFB Massachusetts, and Coalition Maritime Component site in San Diego California. Canada will host war fighters from Australia and the United Kingdom.

**CWID ACCREDITATION AND SECURITY ISSUES**

Mr. Paul Sabourin  
Network Security Accreditation  
D IM Secur, 613.991.6034

**ALL VIPS AND VISITORS TO CF CWID SITES CONTACT**

Major George Sherwood  
613.990.7506  
sherwood.g2@forces.gc.ca

**CANADIAN TRIAL PARTICIPATION**

**CANADIAN LED**

<b>IT01.28</b>	Mission Management Suite - MMS
<b>IT01.34</b>	Mobile/Static Real-Time Radiological Surveillance Network – MobRadNet
<b>IT02.21</b>	The Multi National Coalition Security System - MNCSS
<b>IT02.24</b>	M3Data Information Sharing System – M3Data ISS
<b>IT02.25</b>	Distributed Common Ground System - DCGS
<b>IT02.45</b>	Command Centre Portal Framework System – CCPF
<b>IT04.33</b>	Logik v3.0 for Rapid Intelligence Analysis and Exploitation
<b>IT05.41</b>	Knowledge Management Framework – KMF
<b>IT05.52</b>	Rapid Triage Medical Workbench - RTMW

**CANADIAN PARTICIPATION**

<b>IT03.09</b>	Document Access Servlet – DAS
<b>IT05.13</b>	Coalition Command Collaboration Services – CCCS
<b>IT05.37</b>	Joint Effects Based Command and Control – JEBC2

**NOTE:** Technical details all of Trials listed are contained at the back of this Guidebook

**CANADIAN FORCES**

**DIRECTORATE AIR REQUIREMENTS (DAR):** through the Air Force Command and Control Information Systems Project (AF-



CCIS), DAR is leading one Interoperability Trial (IT 1.28 Mission Management Suite/MMS) and participating in five (IT 2.21 Multi National Coalition Security System/MNCSS, IT 2.24 M3 Data

Information Sharing System/M3Data ISS, IT 5.13 Coalition Command Collaboration Services/CCCS, and IT 4.27 Commercial Joint Mapping Toolkit/CJMTK, and IT 5.37 Joint Effects based Command and Control/JEBC2)

**DEFENCE RESEARCH AND DEVELOPMENT CANADA (VALCARTIER):** technical support to Interoperability Trials sponsored by DAR



**DIRECTORATE MARITIME REQUIREMENTS SEA:** leading one Interoperability Trial (IT 2.21 Multi National Coalition Security System/MNCSS) and providing role players to act as the Canadian Naval Task Group during execution



**DIRECTOR LAND COMMAND INFORMATION:** participating in one Interoperability Trial (IT 2.25 Distributed Common Ground System/DCGS) and providing role players to act as the Canadian Mission Specific Task Force during execution



**DIRECTOR JOINT FORCE CAPABILITY:** leading one Interoperability Trial (IT 2.25 Distributed Common Ground System/DCGS), Canadian point of contact and participating in one US led trial (IT 5.13 Coalition Command Collaboration Services/CCCS), and participating in four (IT 2.24 M3 Data Information Sharing System/M3Data ISS, IT 1.28 Mission Management Suite/MMS, 2.21 Multi National Coalition Security System/MNCSS, and IT 2.45 Command Centre Portal Framework System/CCPF)



**CANADIAN FORCES COMMAND SYSTEM PROJECT:** analysis of various Trials for possible inclusion into Canadian service

**WEBSITE**

For more information on CWID, visit the following sites:

[www.cwid.js.mil](http://www.cwid.js.mil)  
<http://www.ops.forces.gc.ca/cfec>

**NETWORK TECHNICAL AUTHORITY**

Maj Rock Wiegand, CFEC  
 613.990.7610  
[wiegand.hg@forces.gc.ca](mailto:wiegand.hg@forces.gc.ca)

**SCENARIO COORDINATOR**

Mr. Paul McCumber, Contractor  
 613.990.7602  
[mccumber.pr@forces.gc.ca](mailto:mccumber.pr@forces.gc.ca)

**OPERATIONAL RESEARCH**

Ms. Melanie Bernier, CFEC  
 613.991.6151  
[bernier.my@forces.gc.ca](mailto:bernier.my@forces.gc.ca)

**TRIAL COORDINATOR**

Mr. Andreas Psarras, CFEC  
 613.990.7647  
[psarras.ap@forces.gc.ca](mailto:psarras.ap@forces.gc.ca)

**NETWORK ENGINEER**

Mr. Walter Baziuk, CFEC  
 613.990.7602  
[baziuk.wg@forces.gc.ca](mailto:baziuk.wg@forces.gc.ca)

**AIR FORCE AND NATO AIR FORCE POINTS OF CONTACT**

Maj Walter Norquay, Sponsor  
 613.990.2539  
[norquay.wsf@forces.gc.ca](mailto:norquay.wsf@forces.gc.ca)

Capt Paul Bolduc  
 Air Force & National NATO Lead  
 613.944.5708  
[bolduc.jvp@forces.gc.ca](mailto:bolduc.jvp@forces.gc.ca)

Maj Bernard Deschenes  
 Technical Advisor  
 418.844.4000 ext 4555  
[deschenes.jb@forces.gc.ca](mailto:deschenes.jb@forces.gc.ca)

Mrs Marie Ladouceur  
 Air Force Coordinator  
 613.992.0373  
[ladouceur.me@forces.gc.ca](mailto:ladouceur.me@forces.gc.ca)

**NAVY POINT OF CONTACT**

LCdr Ken Dufour  
 819.997.6124  
[dufour.ka@forces.gc.ca](mailto:dufour.ka@forces.gc.ca)

**CFCS POINT OF CONTACT**

Cdr Tim Addison  
 613.945.5020  
[addison.th@forces.gc.ca](mailto:addison.th@forces.gc.ca)

**DJFC POINT OF CONTACT**

Maj Luc Boucher  
 613.945.5039  
[boucher.lr@forces.gc.ca](mailto:boucher.lr@forces.gc.ca)

**DIRECTORATE INTELLIGENCE INFORMATION MANAGEMENT**

Mr. Paul Morin  
 613.992.7666  
[morin.pj@forces.gc.ca](mailto:morin.pj@forces.gc.ca)

**DNBCD POINT OF CONTACT**

Lt(N) Donald Munro

**DIRECTOR NUCLEAR BIOLOGICAL CHEMICAL DEFENCE:** leading one Interoperability Trial (IT 1.34 Mobile/Static Real-Time Radiological Surveillance Network/MobRadNet)

**DIRECTORATE INTELLIGENCE INFORMATION MANAGEMENT:** leading one Interoperability Trial (IT 2.45 Command Centre Portal Framework System/CCPF)

**JOINT INFORMATION AND INTELLIGENCE FUSION CAPABILITY PROJECT:** participating in five Interoperability Trials (IT 2.24 M3 Data Information Sharing System/M3Data ISS, IT 2.25 Distributed Common Ground System/DCGS, IT 2.45 Command Centre Portal Framework System/CCPF, IT 4.33 Logik v3.0 for Rapid Intelligence Analysis and Exploitation, and IT 5.41 Knowledge Management Framework)



**MAPPING AND CHARTING ESTABLISHMENT:** Canadian point of contact and participating in one US led trial (IT 4.27 Commercial Joint Mapping Toolkit/CJMTK)



**CANADIAN FORCES JOINT IMAGERY CENTRE:** participating in one US led trial (IT 4.27 Commercial Joint Mapping Toolkit/CJMTK)

**DIRECTORATE INFORMATION MANAGEMENT SECURITY:** network security and accreditation

**NATO CWID**

**DIRECTORATE AIR REQUIREMENTS (DAR) –** Through the Air Force Command and Control Information Systems Project (AFCCIS) leading one Interoperability Trial



**OTHER GOVERNMENT DEPARTMENTS**

**DEPARTMENT OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS CANADA:** full partner in CWID 06 and leading the Homeland Security scenario, sponsoring three trials (IT 2.24 M3 Data Information Sharing System/M3Data ISS, IT 4.33 Logik v3.0 for Rapid Intelligence Analysis and Exploitation)

tation, and IT 5.41 Knowledge Management Framework) and providing role players to simulate the Government of Canada Operations Centre to participate in two further trials (IT 2.45 Command Centre Portal Framework System/CCPF, and IT 5.37 Joint Effects Based Command and Control/JEBC2)

**HEALTH CANADA:** Through its Nuclear Protection Bureau, Health Canada is participating in one Interoperability Trial (IT 1.34 Mobile/Static Real-Time Radiological Surveillance Network/MobRadNet)



**ROYAL CANADIAN MOUNTED POLICE:** as a first-time participant, the RCMP is evaluating CWID for possible use in validating technology solutions



**DEPARTMENT OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS CANADA**

Public Safety and Emergency Preparedness Canada (PSEPC) fulfills the fundamental role of government to safeguard the public's safety and security. PSEPC provides policy leadership and delivers programs and services in the areas of:

- National security and emergency management
- Policing, law enforcement and borders
- Corrections and crime prevention.

The department also ensures cohesion among the six agencies that report to the Minister of Public Safety and Emergency Preparedness. These include:

- Royal Canadian Mounted Police (RCMP)
- Canadian Security Intelligence Agency (CSIS)
- Canada Border Services Agency (CBSA)
- Canada Firearms Centre (CAFC)
- Correctional Service of Canada (CSC)
- National Parole Board (NPB)

**PSEPC CWID 2006 OBJECTIVES:**

- To improve Situational Awareness for the Government Operations Centre
- To test and evaluate Net Centric Enterprise Services
- Evaluate solutions that facilitate information exchange between domains of differing security classifications

**PSEPC CWID 2006 ROLE:**

- Provide staff to the main Canadian Forces Site at Shirley's Bay
- Increase awareness of emerging technologies in order to further develop the Department's capabilities
- Evaluate situational awareness and collaborative information environment products for the department and the Government Operations Centre



613.944.5157  
munro.dc2@forces.gc.ca

**JIFC POINT OF CONTACT**

Maj Peter Lipohar  
613.944.7962  
lipohar.p@forces.gc.ca

**MCE POINT OF CONTACT**

Maj Yannik Michaud  
613.996.8763  
michaud.y@forces.gc.ca

**CFJIC POINT OF CONTACT**

LCol Robert Williams  
613.943.6044  
williams.rs@forces.gc.ca

**PSEPC POINT OF CONTACT**

Mr. Shane Livingstone  
613.991.5028  
shane.livingstone@psepc-sp-pcc.gc.ca

**RCMP POINT OF CONTACT**

Mr. Marc Morin  
613.998.7548  
marc.morin@rcmp-grc.gc.ca

**HEALTH CANADA POINT OF CONTACT**

Mr. Denis Carrière  
613-948-2581  
denis\_carriere@hc-sc.gc.ca



Inside the demonstration, CWID 2005



**CANADIAN FORCES EXPERIMENTATION CENTRE (CFEC)**

CFEC provides the venue and leadership required for successful CWID execution. Primarily CFEC is responsible to:

- Provide military personnel and Defence Scientists at the Canadian Main Site to augment Joint and Tactical Operational Assessment Teams
- Coordinate the National Experimentation Campaign for CWID
- Form and coordinate the Coalition Data Assessment Team
- Coordinate all Interoperability Trial equipment, personnel, assessment, and reports
- Coordinate CFX Net connectivity for Canadian Sites, including Trial Engineer Support, Cryptography, and Network Security Accreditation
- Collect and compile all data to produce a CWID 2006 Final After Action Report
- Produce and distribute the CWID 2006 Executive Summary outlining all National and Coalition achievements and "Lessons Learned" during CWID Execution
- Coordinate VIP visits, Media Day, and Coalition Staff in/out of Canada





**COMBINED COMMUNICATIONS ELECTRONICS BOARD**

# New Zealand Defence Force

*CWID Warrior Interoperability Demonstration (CWID) provides the New Zealand Defence Force the best means currently available to participate in the collective development, demonstration and assessment for suitability of C4I capability and technology solutions to meet near term interoperability challenges in a joint, coalition and civil authority environment.*

**AIM**

The aim of the New Zealand Defence Force (NZDF) participation in CWID is to assist in the determination of current and future NZDF Joint and Single Service C4I capability requirements for effective coalition interoperability.

**THE NEW ZEALAND DEFENCE FORCE OBJECTIVES FOR PARTICIPATION**

- Investigate and practice command and control of NZDF force elements within a (simulated) coalition environment.
- Enhance the NZDF profile by demonstrating commitment to coalition interoperability, whilst assisting CWID allies to achieve their participation objectives.
- Enhance the NZDF C4I knowledge and experience base.
- Identify the utility and applicability to the NZDF of current and emerging C4I systems and applications; and
- Support the Joint Command and Control System (JCCS) acquisition and development process



**CWID SPONSOR**

Assistant Chief Strategic Commitments and Intelligence (AC SCI) on behalf of the Chief of Defence Force.

**CWID LEAD PLANNER**

LT COL Paul Dragicevich, RN-ZSigs, J6  
 PH: +64 4 529-6600  
 FX: +64 4 529-6609  
 paul.dragicevich@nzdf.mil.nz

**CWID MANAGEMENT**

A CWID Management Team (CMT), co-chaired by the Lead Planner and a representative from the Directorate of Joint Command, Control, Communications and Information Systems (JCIS), and comprising representatives from HQ NZDF, HQ Joint Forces New Zealand (JFNZ), Joint Information Systems Agency (JISA) and single Services provides oversight and policy development for NZDF JWID activities.

**FOCUS FOR THE NZ ARMY DURING CWID 2006: NETWORK ENABLEMENT**

Enabling headquarters at Brigade and below with information technology is the primary objective for the NZ Army during CWID 2006. CWID 2006 is helping the NZ Army to determine:

- The means by which information is communicated.
- The means by which the information is collected, stored and displayed.
- The interaction with Joint and Coalition forces.
- The structure and procedures required by a networked enabled command post.



**DEMONSTRATION OBJECTIVES**

**DA 1 COMMAND POST OPERATIONS:**  
The integration of technology with the people and procedures required for successful command and control - Organisation and Task Focus

**DA 2 INFORMATION MANAGEMENT:**  
The distribution, management, storage and display of information - Information Focus.

**DA 3 NETWORK INFRASTRUCTURE:**  
The necessary hardware, networks, services and applications required by the networked enabled command post - Technology Focus.

**NEW ZEALAND ARMY**

The NZ Army is establishing a Brigade and deployed Battalion Headquarters within the Army Simulation Centre at 2 LFG in Linton, Palmerston North. The Army's participation is helping to determine the level of digitisation required for C2 and situational awareness at the tactical level.

The Army site will demonstrate network enabling of the Army's new Light Operational Vehicle Command and Control variant, tactical range extension utilising Satellite Command and Control on the Pause, and EPLRS radios.

**POINT OF CONTACT**

**ARMY LEAD PLANNER AND SITE MANAGER:**  
Maj James Dryburgh  
PH: +64 4 496-0482  
FAX: +64 4 496-0493  
james.dryburgh@nzdf.mil.nz

**SITE ENGINEERS:**  
Capt Chris Mortiboy  
PH: +64 6 351-9305  
christopher.mortiboy@nzdf.mil.nz

**WOI Brian Chalmers**  
PH +64 4 5275-056  
brian.chalmers@nzdf.mil.nz

**ROYAL NEW ZEALAND AIR FORCE**



The RNZAF CWID Site will be hosted at the Whenuapai Air Force Base, Whenuapai, Auckland.

Whenuapai Air Force Base is located near the upper reaches of the Waitemata Harbour (20 minutes drive north west of Auckland city) and comprises the RNZAF's transport and maritime patrol squadrons as well as the Royal New Zealand Navy's Squadron of Seasprite Helicopters and all the supporting units to these flying squadrons.

**RNZF AIM**

To expose as wide range of RNZAF personnel as possible to current and emerging C4I technologies and the implications these have for RNZAF involvement in Joint and Combined operations.



**RNZAF PRIORITIES/OBJECTIVES**

- Trials that support the introduction to service of the P-3K2
- Trials that support collaborative planning and conduct of Joint Operations

**POINTS OF CONTACT**

**RNZAF LEAD PLANNER:**  
SQNLDR Peter Amyes  
PH: +64 3 4651098  
FX: +64 3 4651098  
peter.amyes@nzdf.mil.nz

**RNZAF LEAD PLANNER:**  
SQNLDR Rob Stockley  
PH: +64 4 496 0533  
FX: +64 4 496 0538  
rob.stockley@nzdf.mil.nz

**SITE MANAGER:**  
SQNLDR Nigel Cooper  
PH: + 64 9 417 7000 Ext 7763  
FX: + 64 9 417 7738  
nigel.cooper@nzdf.mil.nz

**RNZAF SITE ENGINEER:**  
FGOFF Mike Martin  
PH: + 64 9 4177000 Ext 7540  
FX: + 64 9 4177808  
michael.martin@nzdf.mil.nz

**RNZAF INTEROPERABILITY TRIALS**

- IT01.28** Mission Management Suite (MMS)
- IT02.21** The Multi National Coalition Security System (MNCSS)
- IT02.45** Command Centre Portal Framework (CCPF)
- IT03.09** Document Access Serverlet (DAS)
- IT05.13** Coalition Command Collaboration Services (CCCS)
- IT05.51** FORCENet Distributed Channel Services (FnDCS)



**NEW ZEALAND CWID 2006 SITES**

The NZDF topology provides sufficient functionality to allow the NZDF to participate within CWID at a national strategic, and deployed tactical Force Element level within real world network constructs and constraints. CWID 2006 CTF security domain will be hosted within New Zealand.

- **LINTON:** Headquarters 2 Land Forces Group (HQ 2LFG) will host the NZDF Prin-



**POINTS OF CONTACT**

For more information about NZDF CWID 2006 activities, contact the following:

**ENGINEERING LEAD**

LT Graham Gunter, RNZN  
 PH: +64 4 529-6630  
 FX: +64 4 529-6609  
 graham.gunter@nzdf.mil.nz

**ASSESSMENT LEAD**

Capt Marc Wright, RNZALR  
 PH: +64 4 529-6802  
 FX: +64 4 529-6609  
 marc.wright@nzdf.mil.nz

**SECURITY LEAD**

Mr Paul Hortop  
 PH: +64 4 496 0165  
 FX: +64 4 496 0159  
 paul.hortop@nzdf.mil.nz

**CCEB LEAD**

LTCDR Danny Kaye, RNZN  
 PH: +202 328-4808  
 FX: +202 265-9238  
 selwyn.kaye@nzdf.mil.nz

**NZ INDUSTRY IT CONTACTS**

Microsoft / IT 5.13:  
 Mr Bryan Gallagher  
 PH: +64 21 655 123  
 bryang@microsoft.com

**WEB SITES**

<http://nzdf.mil.nz/cwid> (Past, current and future CWID planning information)  
<http://www.cwid.js.mil> (go to New Zealand under Allied Sites)

cipal CWID Effort consisting of a Divisional, Brigade and Battalion Headquarters demonstrating Operational and Tactical level information exchange between all three Headquarters. The Headquarters will be supported by deployed elements of the Network Information Assurance Team providing CND support to battlefield commanders.

- **PORIRUA:** The Joint Information Systems Agency (JISA) permanently hosts the Combined Federated Battle Laboratory Network (CFBLNet) Point of Presence (PoP)

- **AUCKLAND:** The Royal New Zealand Air Force will establish an Air Operations Centre (RNZAF AOC) at RNZAF Base Auckland. The RNZAF AOC will concentrate on trials that assist the management of data collected by aircraft for distribution to users and on trials that assist command and control of air operations.

**OTHER CWID SITES**

The NZDF will deploy Liaison Officers to the following sites for execution period:

- CTF (Stuttgart)
- CFLCC (Dahlgren, VA)
- CFMCC (San Diego, CA)
- CFACC (Hanscomb MA)
- UK CWID Site (Portsmouth West)
- NATO HQ (Lillehammer, Norway)

**THE NZDF WILL FULLY PARTICIPATE IN AND HOST THE FOLLOWING ITS WITHIN NZ**

<b>IT01.62</b>	Mobile Forces Solution (MOFS/MCCIS)
<b>IT02.21</b>	The Multi National Coalition Security System (MNCSS)
<b>IT03.09</b>	Document Access Servlet (DAS)
<b>IT04.03</b>	Wide Area Interoperability System (WAIS) and ACU-1000
<b>IT05.13</b>	Coalition Command Collaboration Services (CCCS)

**THE NZDF WILL PARTICIPATE IN THE FOLLOWING ITS VIA NETWORK ACCESS**

<b>IT05.06</b>	Visualization for Information Assurance (VIA)
----------------	---

**THE NZDF WILL ACTIVELY OBSERVE THE FOLLOWING ITS AT NLO SITES**

<b>IT01.01</b>	Northern European Command - C2 Information System (NEC CCIS)
<b>IT01.14</b>	U.S. Chemical Biological Radiological and Nuclear Modelling (USCBRNM)
<b>IT01.53</b>	Coalition and Civil Agency Capable Wireless Information Transfer System (C3WITS)
<b>IT04.36</b>	Global Broadcast Service (GBS)





## COMBINED COMMUNICATIONS ELECTRONICS BOARD

# United Kingdom Links C2 Levels

*The United Kingdom's (UK's) aim for the Coalition Warrior Interoperability Demonstration (CWID) is to enhance interoperability and UK forces' capability through the use of networked CIS in order to provide information superiority.*

### OVERVIEW

This year is the largest CWID so far for the UK with 40 UK trials, 11 Coalition trials and 6 NATO trials, with over 250 technical and military players operating within the UK alone. We will link rear based strategic assets direct to tactical platforms, incorporating all strategic, operational and tactical levels of command, as well as connect all domains from above secret to unclassified, all on one network using the current and future Global Communications Network systems. Trials will include 7 in-service and future distributed but integrated mission planning systems, 4 CND systems, 2 joint targeting, engagement and battlespace management tools and a fully functioning Joint Operational Picture portal complete with COP, JIP, JEP and JLP layers. In particular, this will be the first year that we demonstrate a fully integrated and dynamic ISTAR dissemination system incorporating in-service ground stations, image libraries and exploitation tools with web enabled imagery databases, query tools and novel information exploitation tools.

### TRIAL INTEROPERABILITY

The UK is committed to meaningful participation in CWID as part of our programme to improve interoperability in a coalition context: a very high priority task. Our trials rely on data derived from the coalition WAN. In addition, the UK is an active participant in both US and NATO CWID either by providing trials/demonstrations in the US or at Lillehammer, or by contributing to data on the coalition WAN. Each trial will exchange live data at either the national or coalition level through the period of the demonstration. It is important for the UK that the network used is fully security accredited, as it carries real data.

### UK NATIONAL LEAD

Wg Cdr Stephen Borthwick RAF  
SO1 Capability Strategy Systems  
DEC CCII  
Ministry of Defence  
+44 207 807 8526  
stephen.borthwick538@mod.uk

### UK NATIONAL COORD & SCENARIO LEAD

Maj Gavin Saunders PWRR  
SO2 CWID  
DEC CCII  
Ministry of Defence  
+44 2392 217657  
gavin.saunders217@mod.uk

### UK TRIALS COORD

WO1 Neil Mellor RA  
SO3 CWID  
DEC CCII  
Ministry of Defence  
+44 2392 217715  
nmellor@dstl.gov.uk

### TECHNICAL LEAD

Viv Danks  
Team Leader  
Deployed Network Solutions  
QinetiQ  
+44 1684 896891  
vgdanks@qinetiq.com

### SECURITY LEAD

Peter Smulovic  
CWID Project Manager  
DSTL  
+44 2392 217458  
psmulovic@dstl.gov.uk

### ASSESSMENT LEAD

Nick Dingle  
Land Systems Assessment  
DSTL  
+44 2392 912274  
njdingle@dstl.gov.uk

### FACILITY MANAGER

Anita Hay  
Mercury Building Manager  
DSTL  
+44 2392 917506  
ahay@dstl.gov.uk

### AREAS TO BE ADDRESSED AT CWID 06

- Resilient Information Infrastructure
- Information Accessibility
- Collaborative Working
- Shared Situational Awareness

The Ministry of Defence is again also engaging in significant risk-reduction activity for the Defence Information Infrastructure (DII) programme, using CWID trials to provide inputs to the DII network to prove secure coalition interoperability.

### LOCATION

The principal UK CWID site is located at Portsmouth West, the Defence Science and Technology Laboratory's site near Portsmouth in the South of England. As well as hosting the CWID trials, at the same time the UK is hosting its participation in TRIDENT WARRIOR 06 at Portsmouth West.

### OWNERSHIP

UK involvement in CWID is sponsored by the Capability Manager (Information Superiority), Air Vice-Marshal Stuart Butler, and responsibility for delivering the programme lies with the Director Equipment Capability (Command Control and Information Infrastructure), Brigadier Simon Shadbolt. As we continue to develop the crucial Network Enabled Capability (NEC) required by our armed forces in the years ahead, CWID has the potential to assume ever greater importance, not only in resolving interoperability issues but also in reducing the degree of risk inherent in all such programmes.

**KEY ROLES FOR CWID IN THE UK**

- It helps to identify the potential of new, evolving and low-risk technologies that might help to meet our C4I/ISTAR capability requirements
- It offers potential solutions to interoperability issues
- It brings together industry, the research community and the military users in a forum in which they can explore innovative approaches to filling capability gaps
- In an effort to build on the success achieved in previous years, CWID will again be used for risk reduction

All of these strands are vital if we are to deliver enhanced capabilities and real benefits to those involved in current and future operations, in an efficient, cost effective and timely manner.

**RELATED WEBSITES**

The UK CWID website at [www.dtai.mod.uk/cwid](http://www.dtai.mod.uk/cwid) contains further information about UK CWID 06 including descriptions of trials.

**VISITORS**

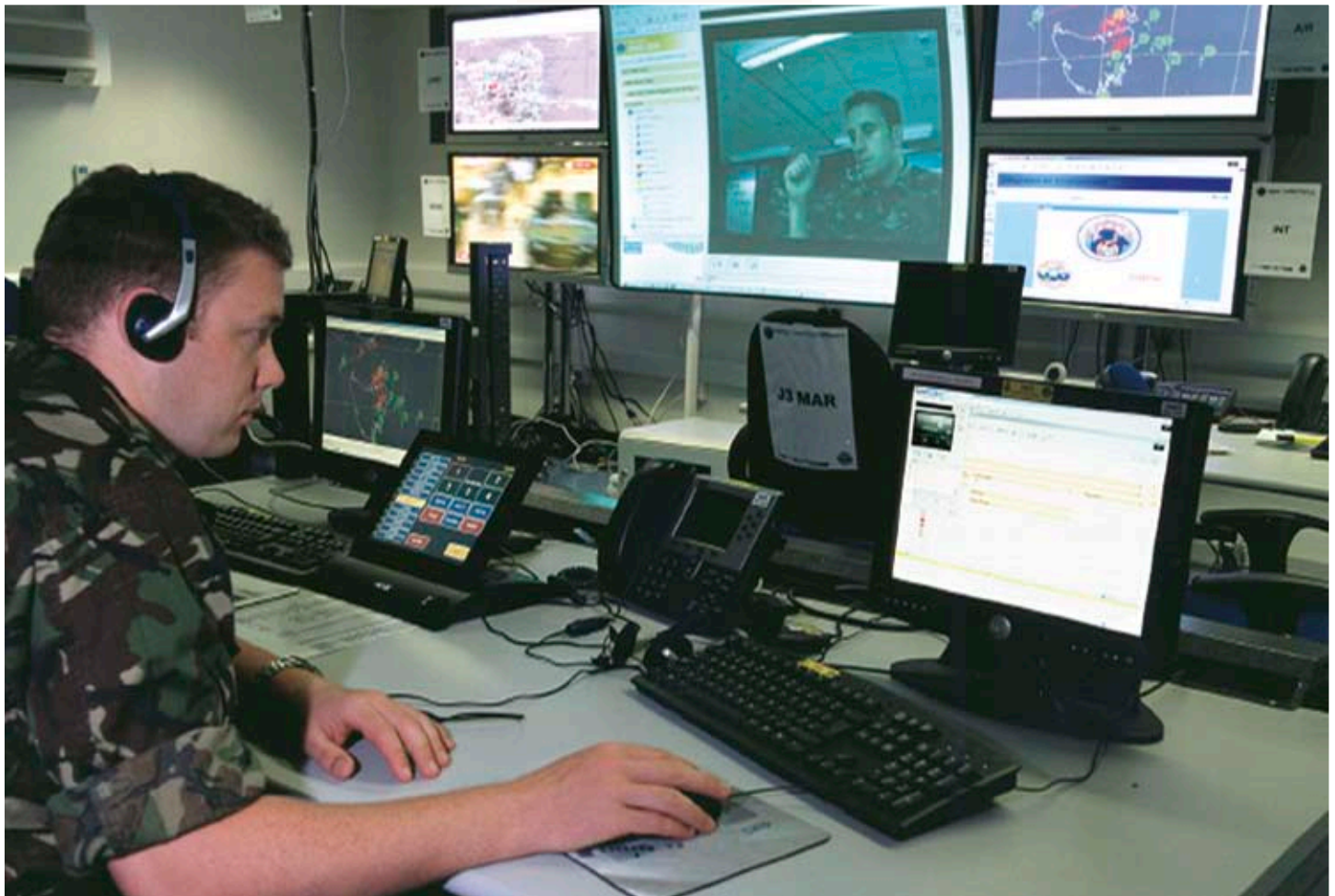
Vistors' Week for CWID in the UK will take place at Portsmouth West over the period 19-22 June 2006. Anyone wishing to visit should apply via the UK CWID website.



**INDUSTRY PARTNERS**

The UK acknowledges the active participation of a large number of industrial partners, many of whom have trials at US, UK and/or NATO CWID sites. The Defence Science and Technology Laboratory, Dstl, is contracted to host the UK CWID site and provide facilities, security and assessment of UK and Coalition trials. QinetiQ is contracted to provide the UK CWID network and manage its connections to the coalition network. In addition, UK CWID receives valuable contributions from industry partners, who, whilst not exhibiting trials in the US, provide a significant input to the US planning conferences, helping to ensure the success of CWID.

QinetiQ has been instrumental since 2000 in designing and delivering the UK Secure Network for JWID/CWID. This has been de-



QinetiQ WADI helping to enable NEC

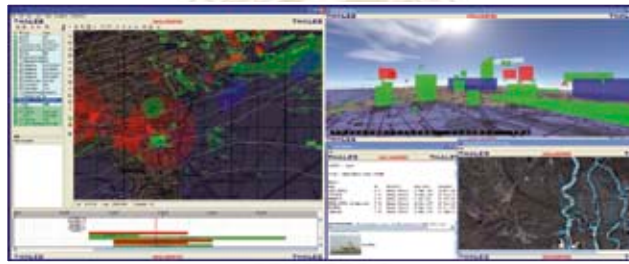


**DEFENCE SCIENCE AND TECHNOLOGY LABORATORY [Dstl]** is a UK Ministry of Defence (MoD) facility. Apart from the site and infrastructure, Dstl also provides: links to CFBLNet; associated cryptographic devices; equipment and personnel to support the QinetiQ CWID technical team. Dstl also provides administration, catering and security to support both CWID and the associated visitors' programme. Contact Details: [psmulovic@dstl.gov.uk](mailto:psmulovic@dstl.gov.uk)

livered using the Wide Area Distributed Infrastructure (WADI) Solution.

Thales Air Operations celebrates its fifth year of participation in the JWID/CWID programme. In addition, the company has supported the UK CWID team throughout all UK and US planning conferences since 2002, contributing to scenario and Air Tasking Order/Airspace Control Order (ATO/ACO) production.

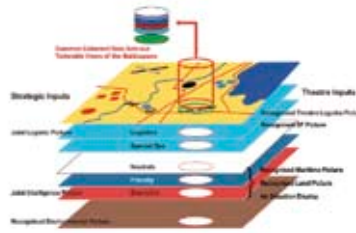
BAE Systems INSYTE will perform the role of System Integration for the ISTAR trials and demonstrations for



Thales Air Operations



BAE Systems



Fujitsu

CWID 2006 in the UK. The demonstration shows the interoperation of D3 products in separate security domains.

Fujitsu is participating in US CWID with its Logistics Information eXchange (LogIX) and Coalition openJOP (Co-JOP) that are registered in NATO CWID. These trials, which have UK national equivalents, interface with coalition partners and are information providers to the UK openJOP, providing shared situational awareness.

## United Kingdom Trials Matrix

TRIAL ID	TITLE	COMPANY/ ORGANISATION	POINT OF CONTACT	POINT OF CONTACT E-MAIL ADDRESS
<b>UKIT 02</b>	Web Based Secure Situational Awareness	Thales Air Operations	Martin Boughen	Martin.boughen@uk.thalesgroup.com
	Provision of a Multi Level Secure protected shared Situational Awareness capability offering static and dynamic intelligence data to provide additional features to an enhanced Common Operational Picture.			
<b>UKIT 03</b>	Provision of Geospatial Information (Joint Environment)	HQ DGI	Maj Phil Maye	Dgia-hq-sys1-so2@dgia.mod.uk
	Provision of geospatial information and imagery intelligence through: Web Geoserver; product publishing and dissemination capabilities; collaboration and sharing of geo/ IMINT products and services with coalition partners.			
<b>UKIT 05</b>	White Shipping Demonstrator	DSTL	Stephen Ablett	sjalett@dstl.gov.uk
	The provision of an all source commercial shipping picture.			
<b>UKIT 06</b>	Collaborative Mission Support and planning	Westland Helicopters Limited	M T Smith	smithmt@whl.co.uk
	A development in support of the UK MOD's policy of convergence and commonality in the area of Mission Support Systems and their potential for providing coherent network ready solutions in collaborative planning allowing reduction in planning times, more responsive planning and faster achievement of mission aims.			
<b>UKIT 07</b>	Juniper Enterprise Communications Environment	Juniper Networks (UK)	Tim Hearn	thearn@juniper.net
	Support to the QinetiQ CWID core engineering team in the areas of: IP Routing , Netscreen Firewalls, Application Acceleration, WAN Acceleration.			
<b>UKIT 08</b>	Tactical High Grade Messaging over HF	NEXOR	Steve Penny	Steve.penny@nexor.com
	Provision of tactical messaging gateways, formal messaging solutions, web based military client capability and Active Directory ACP133 capabilities.			
<b>UKIT 09</b>	Role Based Identity Management and Information Accessibility	Thales UK Security Division	Leigh Richardson	Leigh.richardson@thales-esecurity.com
	An identity management system that provides physical identity, electronic identity, controlled access to web based applications and Cryptographically protected audit logs.			
<b>UKIT 11</b>	Enriched COP	Northrop Grumman Mission Systems	Colin Fieldgate	cfieldgate@ngms.eu.com
	The bringing together of a wide range of disparate information sources into the Common Operating Picture (COP) in order to create an Enriched COP. Thus allowing the user can access a greater depth of information through the means of the COP.			
<b>UKIT 15a</b>	IPv4-IPv6 Interoperability	CISCO Systems		
	The connection of IPv4 and IPv6 networks and the demonstration of subsequent interoperability without loss of functionality.			
<b>UKIT 15b</b>	Computer Network Defence Capability	CISCO Systems	Paul King	pking@cisco.com
	Provision of a capability to protect networks and network services from attack. This includes attack detection and proactive mitigation techniques.			

<b>UKIT 16</b>	Chemical and Biological Warning and Reporting	DSTL	Andrew Howe	aghowe@dstl.gov.uk
	The development of the interoperability of future UK and US Chemical, Biological, Radiological and Nuclear warning, reporting and modelling capabilities.			
<b>UKIT 25</b>	Portable Multipurpose Communication Capability	NSSL Ltd	Ray Adams	Ray.adams@satcom-solutions.com
	A demonstration of the capability of the new IMARSAT B-GAN service to support a number of activities simultaneously.			
<b>UKIT 27</b>	Bowman/ CIP Interoperability	General Dynamics UK Ltd	Jeremy Creasey	Jeremy.creasey@generaldynamics.uk.com
	The demonstration of the sharing of accurate C2 and ISTAR information between the Tactical Land environment, Joint Headquarters and Coalition Partners through the latest Bowman/ CIP infrastructure.			
<b>UKIT 35</b>	Integrated Logistic Management	Fujitsu Services	Tina Quenault	Tina.quenault@uk.fujitsu.com
	The provision of a Integrated Logistics Management Capability providing information into the Joint Logistics Picture and integration into specific layers of the Joint Operational Picture.			
<b>UKIT 36</b>	Joint Operational Picture Portal	Fujitsu Services	Tina Quenault	Tina.quenault@uk.fujitsu.com
	A demonstration of a system-independent delivery of the Joint Operational Picture (JOP).			
<b>UKIT 37</b>	Deployed Common Ground Station	Raytheon Systems Ltd	Graham Pearson	Graham.pearson@Raytheon.co.uk
	To demonstrate a state of the art multi-int capability underpinning a Joint Intelligence Picture, including comprehensive analytical toolsets to discover, develop and present knowledge for decision makers.			
<b>UKIT 38</b>	Joint Effects Based Tactical Targeting System	Raytheon Systems Ltd	Graham Pearson	Graham.pearson@Raytheon.co.uk
	To demonstrate state of the art joint collaborative targeting using the Joint Effects Tactical Targeting System (JETTS) within national and coalition domains drawing on shared situational awareness.			
<b>UKIT 40</b>	Defence Information Infrastructure (Future Deployed)	MOD DII Integrated Project Team	Andy Evason	Andy.evason344@mod.uk
	Risk reduction activity for the deployed element of the UK Ministry of Defence's forthcoming implementation of a single information infrastructure for the UK defence community.			
<b>UKIT 41</b>	JMPS Interoperability with UK Infrastructure and UK MPS	Joint Combat Aircraft Integrated Project Team	Sqn Ldr Bob Arber	Jca-t6@x400.r.mil.uk
	Establishment of the extent of JMPS interoperability with UK C4I and UK MPS in order to de-risk Joint Combat Aircraft Off Board Mission Support development			
<b>UKIT 43</b>	FALCON	BAE Systems	John Loader	John.loader@baesystems.com
	Provision of a realistic comms infrastructure, by employing the Falcon tactical communications 'backbone' that will, in the future, replace the Ptarmigan and Euromux mobile communications systems in service with both the Army and RAF.			
<b>UKIT 46</b>	Air Mission Planning System	EDS	Nick Hill	Nick.hill@eds.com
	Interoperation of the in-service AMPA system with abroad range of other Mission Planning systems and assets in a dynamic and testing scenario.			
<b>UKIT 47</b>	JADOCS	Fujitsu Services	Kevin Parry	Kevin.parry@ukfujitsu.com
	Integration of JADOCS into the existing UK information infrastructure.			
<b>UKIT 48</b>	MOD Computer Network Defence	JSCC	Dave Freeman	
	To conduct an exercise of UK Computer Network Defence organisations, policy and infrastructure implementation for both fixed and deployed defence networks.			
<b>UKIT 52</b>	Above Secret Operations	BAE Systems	John Loader	John.loader@baesystems.com
	Investigation into the inter-security domain passage of information.			
<b>UKIT 53</b>	Imagery and Information Management System (D3)	BAE Systems	John Loader	John.loader@baesystems.com
	The bringing together of multiple imagery sources into an imagery management library for the exploitation by imagery analysts and subsequent storage and dissemination of imagery intelligence products.			
<b>UKIT 54</b>	Autonomous UAV	BAE Systems	John Loader	John.loader@baesystems.com
	A demonstration of an IRAD program for the sensor and mission management of a UAV			
<b>UKIT 60</b>	ASTOR Ground Segment in a Network-Enabled Environment	Raytheon Systems Ltd	Graham Pearson	Graham.pearson@Raytheon.co.uk
	To demonstrate the ASTOR Ground Segment within a Network Enabled environment			
<b>UKIT 55</b>	ICRI	Resilient Communications	Maj Gary Green	gary.green408@mod.uk
	Interconnection of Bowman and SINGARS radio systems via an audio socket interface.			
<b>UKIT 56</b>	Bowman Interoperability with JTRS	General Dynamics/ RCUK	Jeremy Creasey	Jeremy.creasey@generaldynamics.uk.com
	Exploration of Bowman interconnection with JTRS networks			
<b>UKIT 64</b>	JCS (Logs)	BAE Systems	Ben Swann	ben.swann@baesystems.com
	Provision of essential logistics information to deployed headquarters			



**NORTH ATLANTIC TREATY ORGANISATION**

# NATO Transformation Force

*The cornerstone of NATO’s transformational capability is the NATO Response Force (NRF). By design, these forces will be agile, joint and expeditionary and must be supported by “network-enabled capabilities based on a robust and flexible CIS foundation.”*

The shared vision of the two Strategic Commands (Allied Command Operations and Allied Command Transformation) is that NATO forces, including the NRF, achieve a state of Decision Superiority that in turn is enabled by achieving Information Superiority through networked forces. Allied Command Transformation (ACT) is therefore engaged in efforts to create forces that are capable of achieving this type of Decision Superiority.

ACT is driving the development of concepts and systems that can achieve Information Superiority, and are tested and validated using the full spectrum of available exercises, trials, and experiments – such as CWID.

**NATO CWID 2006**

Building on the successes achieved in CWID 2005, NATO will continue to use CWID as an avenue to progress Transformation within the Alliance. Allied Command Transformation has invested significant effort to align the Scientific Programme of Work (SPOW) activities with testing activities such as CWID.

As a result, capabilities which are being examined to support the rollout of NATO NEC can be explored and evaluated. As proposed by the NATO HQ C3 Staff, CWID will also be used as one of the test venues to validate the interoperability of NATO and national C2IS that have been committed to NRF 9 and 10. The operational commitments for these NRFs (shown in figure below) commence in July 2007 and as such, any interoperability issues that are identified as a result of trials conducted in CWID can be addressed and resolved prior to that time.



**POINTS OF CONTACT  
ACT/C4I**

Cmdr. Clark Price  
NATO CWID Director  
cprice@act.nato.int  
+1 757 445 3556

Mr. D.C. Taylor  
NATO CWID Senior Analyst  
dtaylor@act.nato.int  
+1 757 445 3556

**NATO CWID EXECUTION SITE**

Camp Jorstadmoen in Lillehammer, Norway, will again host the NATO 2006 CWID event. The Camp has a military history dating back to 1750 and has been in use by the Norwegian Army Signal Corps since 1945. The Camp was selected by the Norwe-

gian parliament to be the site of the Joint CIS Training Centre within Norway. The Camp has taken on this new role, which complements the Joint and Coalition nature of the testing that will be conducted in CWID 2006.

**NETWORK TOPOLOGY, NATO DOMAIN, LILLEHAMMER**

The NATO CWID 2006 network at Camp Jorstadmoen is build around a common domain referred to as the Coalition Task Force (CTF) / NATO Response Force (NRF) domain. In CWID 2005 this domain was referred to as the CWID 'purple' domain.

Several nations use Information Exchange Gateways (IEGs) to separate their national LANs from the common domain, thereby analyzing the interoperability over their cross-domain solutions.

NATO CWID network architecture has its primary site at Camp Jorstadmoen. The diagram below depicts additional national sites used in conjunction with NATO CWID tests which are conducted remotely.

**PARTICIPATING NATIONS AND AGENCIES**

There will be 19 nations and agencies actively participating from the NATO execution site in Lillehammer and an additional 3 nations who will attend as observers. NATO will participate with C2 systems from each of the operational environments: the maritime MCCIS, the air ICC and the Land LC-CIS.

**THE NATO SCENARIO AND NRF STRUCTURE**

The NATO Scenario was designed for the NATO Response Force, which is driven by the underlying principles: "first force in, first force out" and tailored for a specific mission. The NATO scenario complements the US scenario. The NRF will be capable of performing certain missions by its own, as well

**2006 NATO OBJECTIVES**

In addition to five coalition objectives, there are two specific NATO objectives:

**OBJECTIVE 1:** Conduct testing to validate the interoperability between C2I systems required in NRF rotations 9 & 10 in support of the certification process.

**OBJECTIVE 2:** Provide network tools to facilitate the management of information, enabling automatic discovery and integration technologies that promote loose coupling between C2 systems and components.

as participating with the US CTF. Deployed as a stand-alone force for Crisis Response, the NRF scenario has the following capabilities:

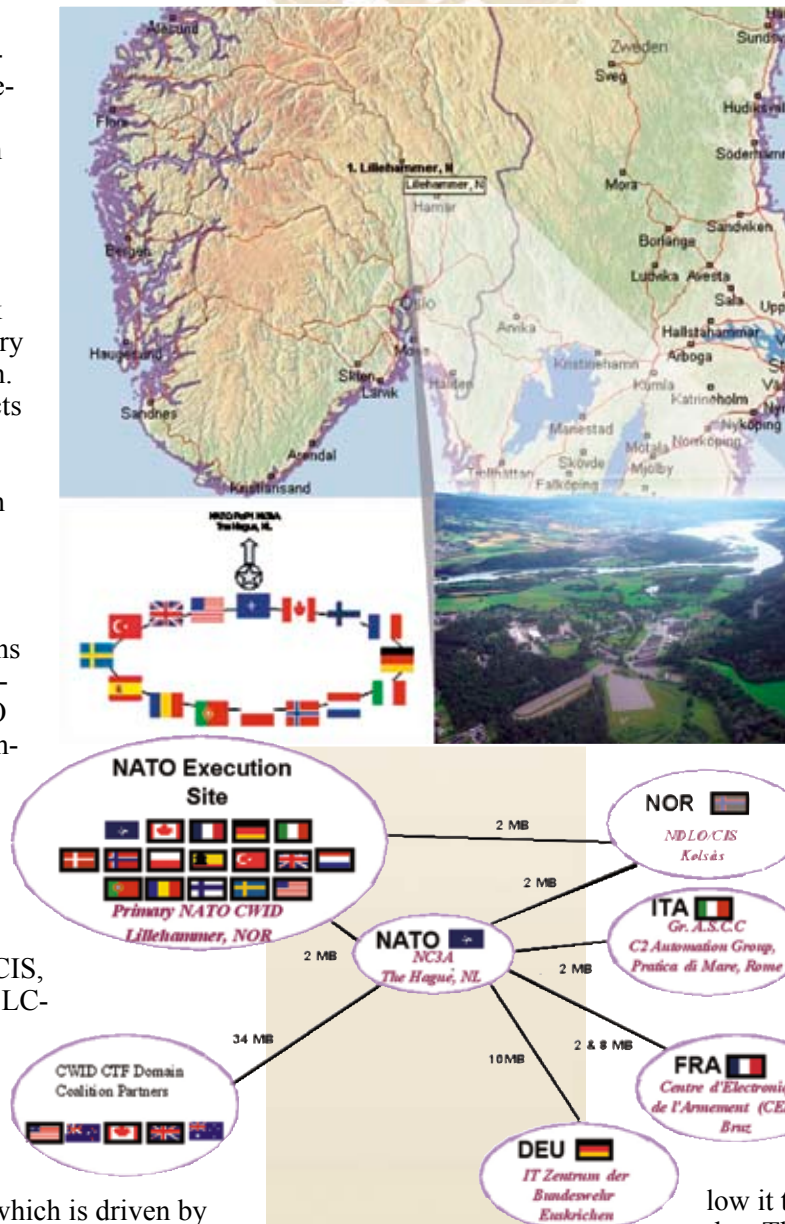
- Evacuate non combatants from crisis area
- Support consequence management (including chemical, biological, radiological and nuclear incidents)
- Support in a humanitarian crisis situation
- Manage crisis response operations, including peace-keeping
- Counter terrorism operations
- Embargo operations

The NATO CWID Scenario flexibility gives it unique character, enabling it to be tailored to test the interoperability of the various NATO and national Command and Control systems as well as individual C4ISR trials.

The scenario Command and Control structure and related NATO and national C2 systems and interactions that will be used for NATO CWID 2006 are depicted in the following diagram:

For 2006 the NRF structure is loosely based on NRF rotations 9 and 10. It will operate under the command and control of a Joint Force Headquarters that will extract a permanent Deployable Joint Task Force staff as forward command element. The NRF Air component will provide a rapidly deployable capability to conduct appropriate air tasks. The Land Components for the NRF contains a structure sufficient to allow deployment of a tailored brigade size formation composed of manoeuvre elements and the requisite support and breadth of assets to allow

it to conduct a wide range of land tasks. The NRF Maritime components will comprise a force up to a NATO task force size including a carrier battle group with associated surface and subsurface combat units, amphibious forces, naval MCM units and auxiliary support vessels.



# NATO Interoperability Trials and Demonstrations

## CANADA

CA-UNAAAT IT and ID which imports ADatP-3 Air Tasking Orders from multiple NATO C2 Information Systems and converts them into USMTF 2000 Messages format (text and XML formats).

## FRANCE

FR-BFSA ID of EADS Imp@act Blue Force Tracking System. Tracks are exchanged and displayed between BFT systems from different nations, through a specific tracks exchange interface (NFFI)

FR-MUSE-MMHS ID of formal and personal Military Message Handling System.

FR-SAIS ID of technical services through a Littoral Warfare scenario. Supports an international Services Oriented Architecture (SOA), which provides Network-Centric Capabilities.

FR-SIC21 IT of the French Maritime C2I system within the NATO scenario.

FR-SICF T-BMS FT ID of the BATS (Battlefield Awareness Tracking System) involving the two French systems SICF for decision level and T-BMS for Mission / Action level to demonstrate the capability to aggregate the RGP on different operation theaters.

FR-SICF T-BMS IT of formatted Message exchange for SA, TO/ACO in XML and MIP DEM, Block 2. T-BMS participates as a subordinate (Airborne Battalion) of the French Brigade

## GERMANY

GE-ADLER IT that demonstrates Information exchange between the GE Artillery command, control and weapons deployment system ADLER and other ASCA/AFATDS compatible systems.

GE-Army CCIS IT and ID developed out of the fielded German Battlefield-Management-System "FAUST" and covers brigade (usually divisional) to troop-level. It distinguishes itself by extensive staff-functions for supporting HQ and Command Posts. Blue Force Tracking, Situation Display and Map Processing are some of the functions used.

GE-CLICC IT and ID: Computational Linguistics in C2 Systems (CLICC - Automatic processing of human language). CLICC acts as an intelligence centre receiving and enhancing INTEL and CROP information and providing information gathering, data fusion and ISR dissemination in a collaborative environment.

GE-DIG IT and ID of Domain Specific Information Generator (DIG, product name SIENA) which composes and executes real-time crisis scenarios thus providing real-time and realistic ADatP-3 formatted Situation Report messages (OWNSITREP, ENSITREP) and Intelligence messages (INTREP).

GE-Geoinformation Services IT and ID that transfers geospatial and METOC data into a classified network. After data collection and evaluation a Recognised Environmental Picture (REP) is generated and provided as Web-Services.

GE-HEROS IT and ID of ADatP-3 (BL 12.2) based Information exchange between the GE C3I system HEROS and other MIP conform C2IS. The Information exchange between HEROS and other MIP C2IS using standard protocol TCP/IP; MIP Data Exchange Mechanism (DEM) and C2 Information Exchange Data Model, C2IEDM

GE-ICARUS IT and ID which provides information sharing across security boundaries through an Information Exchange Gateway (IEG).

GE-IEG ID and performance test to place the entire German domain behind an Information Exchange Gateway.

GE-INIOCHOS IT and ID of Battlefield Management System on the tactical and operational command level demonstrating MIP data replication over CFBLnet and low bandwidth communication.

GE-JCCIS IT and ID of GE Joint Command & Control Information System (JCCIS) which provides core system capabilities for common and specific Functional Area Services and aims to connect to a logistics system as well as share the operational picture. An Information Exchange Gateway may be used.

GE-Link 16 RASP ID using the SIMPLE (and DIS) protocol to demonstrate and test the interoperability with other CWID 2006 participants, e.g. ACCS LOC1 (RT), to create a common operational Air picture.

GE-MOFS/MCCIS IT and ID of high performance and high availability IP platform with secure broadband satellite communication between ship and land. Applications used on this platform include: RMP (MCCIS); RAP (ICC/NIRIS); ATO/ACO (ICC);LDAP Single-Sign-On (WISE); WEB-based COP (WISE); VOICE over IP; Information Exchange Gateway (IEG) Case B Architecture

GE-NETWORK GRID OF SENSORS ID of a combination of reconnaissance information from various sources (air based / link 16 and ground based / smart sensor web), correlation and fusion of this information within an IDCP (STANAG 4162) and distribution via various web servers to different users (in various nations) with different information content, based on their role

GE-SAP-DFPS IT and ID that manages combined/joint logistic units and facilities by providing reports about the logistic status; receives tracking information (MIP/ADatP-3) and providing information about logistic stocks (MIP/ADatP-3)

GE-SSDS MKIII Secure data Spreading System transfers unclassified data, e.g. SAP or Geoinformation, in a classified environment using a One-Way Gateway supporting FTP.

## ITALY

IT-BFT ID of Blue Force Tracking Tool used at tactical level to provide situational awareness of Land/Joint Units and Intelligence units which provides basic geographic information and tools to export positional data to C2 Systems

IT-C4I Defense IT and ID of C4I Defense Joint System designed to provide top-level strategic capabilities, lying above the tactical functionalities offered by the C2 systems of each Armed Force. It supports the Operational Commander in OPS planning and tasking (Orders Generation) and in Tactical Situation Analysis and Monitoring.

IT-INCWERA ID. INCWERA (Italian Network Centric Warfare Enterprise Reference Architecture) is the National NCW (Network Centric Warfare) model through which the Italian MoD is developing the national reference architecture addressed to a Network Centric Warfare / Network Enable Capability.

IT-ISR_WS	ID of ISR_WS workstation provides pre exploited GMTI and ESM data to ISR network and exploited ISR information to both ISR network and C2 systems to increase situational awareness.
IT-MCCIS	IT of system designed to provide Maritime Commanders and their Staffs a state-of-the-art, automated information management system capable of supporting Italian Navy Commanders in planning and executing military activities to meet National objectives. MCCIS-Italy is based on a server/client architecture using HP UNIX servers and a mixture of HP UNIX and WINDOWS NT/2000 clients.
IT-MCCIS-MAJIC	IT and ID of Multi-sensor Aerospace Joint ISR Interoperability Coalition (MAJIC)
IT-SIACCON 1AW+PSOT	IT of Army C2 system is used to support the Commanders in Analysis of Tactical Situation, Mission Planning, Orders and Directives Handling and operation monitoring. ID of PSOT as an Italy-France project with the interoperability of PSOT modules in an international NATO context.
IT-SIACCON 2	ID of Army C2 system designed to support the Commanders in Analysis of Tactical Situation, Mission Planning, Orders and Directives Handling and operation monitoring. SIACCON 2 is MIP Block 2 compliant thus allowing information exchange and RGP Sharing with NATO/PfP Joint & Single service C2 System.
IT-SiCCAM	ID of C2 System that provides air operations planning and tasking, RASP reception and diffusion, message handling and air-bases management.
<b>NATO</b>	
NATO-ACCS LOC 1	ACCS ID is designed and developed to support the planning, tasking, execution and reporting of combined joint air operations.
NATO-ACCS LOC 1 STVF	ID of ACCS LOC1 System Test & Validation Facility (STVF) that is supporting the integration, testing and validation of the ACCS LOC1 Core Software.
NATO-ACCS LOC1 (RT)	ID of ACCS is designed and developed to support the planning, tasking, execution, monitoring and reporting of combined joint air operations.
NATO-ADAMS/EVE/ CORSOM	IT and ID to achieve increased interoperability with NATO Land, Air and Maritime C2 systems, NATO COP and National Deployment Planning and Execution Systems like JOPES and JEMMS and Web Map Servers.
NATO-BFSA II	ID of interoperability between National and NATO Blue Force Tracking Systems (FTS).
NATO-COSINE	IT of a non real-time information (document, image) sharing mechanism that allows sharing and control of information between coalition partners.
NATO-CSSI-IVAS	CSSI and IVAS reside within the focus work area "NATO Network-Enabled Capability - Interoperability (NNIS)", which includes: Information definition, Information cohesion, and Information access.
NATO-DIODE	ID of the NC3A Information Diode to facilitate network management data transfer from a 'deployed' network into a situational awareness system located in a central network management centre.
NATO-EXCITE	IT and ID to demonstrate shared data objects information exchange capabilities.
NATO-ICC	ID of ICC (NATO-wide Integrated Command and Control Software for Air Operations) that provides powerful tools for planning, tasking, reporting and situational awareness.
NATO-IEG	ID of a NATO Information Exchange gateway providing IEG case B core services (Email, Directory Services, Formal messaging, Web services) and IEG case C capabilities (i.e. Mailguard), host additional IEG services (NATO-IEG FS, NATO-PKIGW), and provide a platform to enable the NATO-Cosine trial.
NATO-IEG FS	ID to test and demonstrate interoperability of an Information Exchange Gateway using functional services outside a lab environment
NATO-ITTI	ID to de-risk the evolutionary IPv6 transition before operational deployment by working with NATO nations within an operational scenario.
NATO-LC2IS	IT of the NATO LC2IS that will provide Joint Land C2 Services for the NATO levels of command in multi-national coalition based operations.
NATO-MFAG	The Multi Functional Access Gateway (MFAG) is developed to provide a uniform access into the NGCS.
NATO-NECCIS	Exchange of ATOs/ACOs in ADatP-3 Format with NATO ACCS, NATO ICC and US TBMCS
NATO-PKIGW	ID of the NC3A PKI Gateway to enable two way authenticated and confidential SSL/TLS web access between two interconnected coalition partners Communication and Information Systems (CIS).
NATO-TIDE Sprint	ID of TIDE Sprint brings together the extended community (NC3A, ACT and Nations) to discuss and evolve the concepts behind NNEC and spiral development.
NATO-XGUARD	ID of an accredited mail guard system to facilitate email exchange between a deployed military operation and a civil entity (Non-Government Organisation - NGO, Press, etc).
NATO-XLABEL	ID of the XML Guard component of the NC3A XML Security Labelling System.
NATO-ADDLJ	IT to provide Air de-confliction and defence integration and co-ordination to support the Land Component Commander in the Joint Environment.
NL-IEG	ID of a National to NATO Information Exchange gateway
NL-ISIS	IT and ID of ISIS (Integrated Staff Information System) – an operational high echelon C2IS system with C2IEDM compliance which is integrated in MIP.

Continued next page

**NORWAY**

NO-NORDIS-S	IT and ID of NORDIS-S: the new secure platform for Norwegian C4ISR Systems.
NO-NORTaC C2IS	IT and ID of NORTaC C2IS - Norway's primary Command and Control system for tactical land operations from Div to Bn level using MIP DEM block 2.
NO-SecSOA	ID of secure and dynamic Web Services for interoperability between coalition partners in Network Enabled Capability (NEC) operations.

**POLAND**

PL-SOA WS	ID of a secure Web Services environment.
PL-SZAFRAN	IT and ID of a Tactical Command and Control Information System that supports the planning and control of Army operations on corps, division, brigade and battalion level, and the exchange of information among national and allied command posts.

**PORTUGAL**

PT-SICCE	IT and ID of SICCE – an operational high echelon C2IS system that is C2IEDM compliant and integrated into MIP.
----------	--

**ROMANIA**

RO-SIAAB	IT and ID of a battle command system designed for command posts and units operating at the tactical level (Brigade and Battalion).
----------	--

**SWEDEN**

SE-IS SWERAP	IT and ID of a developmental system for the EU Nordic BG HQ in 2008.
--------------	--

**SPAIN**

SP-AT12	ID of an Advanced Trusted Information Interoperability demonstrator that enables secure the data exchange between Nations using the new Web Services technology in a trust common environment.
SP-BITACORA	IT and ID of network security analysis, including management and detection of system attacks.
SP-IP over HF	ID to test interoperability of Spanish Navy fielded and experimental equipment with Turkish system and other similar NATO or National systems. Encrypted and Non-Encrypted E-Mail exchange and chat room.
SP-LogICA	ID of how a security incident that affects a remote network can be tracked, investigated and resolved, showing advanced techniques in event detection, correlation and notification.
SP-SIMACET MIP B2	IT and ID of the Spanish Army C2IS MIP BI 2 Gateway using data replication exchange mechanism (DEM) and message exchange mechanism (MEM)

**TURKEY**

TU-IEG	ID of a secure information exchange among NATO nations of information using LDAP, HTTP, HTTPS, and SMTP protocol proxies.
TU-IP over HF	IT and of IP over HF, STANAG 5066 compliant equipment developed by Turkish Naval Forces and a national Institute (TÜBITAK).
TU-OMEGA	IT of a C2I system software that aims to automate the operations in TU Navy HQ Operational Centers for decision support, using GIS to display operational picture and formatted messages to gather information.
TU-TACCIS	ID of TACCIS (Tactical Area Command and Control Information System) - a situational awareness and decision making tool within NRDC-T and its subordinates.
TU-TICCS	ID of TICCS: Integrated Command and Control System of Turkish Air Force that includes Battle Mgmt, Resource Mgmt, and Documentation Mgmt Subsystems

**UNITED KINGDOM**

UK-CoJOP	ID of the CoJOP Hub will primarily provide a platform for UK interoperability with the US-NATO Air C2 Interoperability Evaluation (UNITE), NATO ACCS and ICC trials.
UK-CSAT	IT and ID that delivers network enabled C2 using internationally agreed structured information exchange standards and provides a UK coalition situation awareness terminal and acts as a UK coalition situation awareness gateway in Lillehammer.
UK-DII (FD)	ID of a prototype system for the Future Deployed element of the Defence Information Infrastructure, with its associated prototype Boundary Protection device.
UK-I64	ID of the transition mechanisms available for interworking between IPv4 and IPv6 environments.
UK-LogIX	LogIX ID provides a platform for information exchange between logistics systems.
UK-Mercury	ID of a military version of a new means of implementing a commercial mobile communications network.

**UNITED STATES**

US-AFATDS	ID of the exchange of coordination, planning and fires messages across the network with the FR and GE artillery systems.
US-GCCS-A	IT and ID of GCCS-A which provides a Common Operational Picture (COP), Relevant Ground Picture (RGP) and C2PC Situational Awareness services during the scenario trials.
US-TBMCS-UNITE	ID using Net-centric internet technologies for cross-domain information exchange between NATO and US C2 Systems.