



ALLIED COMMAND TRANSFORMATION

**NATO NETWORK ENABLED CAPABILITY (NNEC)
Conference 05 -07 April 2011**



Conference Report

Table of Contents

Executive Summary	3
Conference Aims	5
Conference Agenda.....	6
Conclusions.....	7
Annex A: Conference Facts	10
Annex B: Conference Highlights.....	13
Annex C: Conference Feedback	43
Annex D: Conference Agenda	44

This page intentionally left blank

Executive Summary

The 8th annual NNEC conference took place from 05 - 07 April 2011 in Helsinki, Finland, the first time in a PfP country. The theme for this year's conference was "Comprehensive Approach – NNEC as an enabler." Due to the raising interest the conference was held in several plenary sessions as well as in four break-out sessions concentrating on, Technology to improve information sharing, Human Factors & Processes supporting NNEC, Cyber Security and NNEC Practical applications.

The conference was attended by 441 personnel representing 27 of the 28 NATO nations, 10 non-NATO Nations, European Defence Agency (EDA), European Union (EU) and, representatives from the SHAPE, NC3B, NACMA, NAMSA, NC3A, NCSA as well as representatives from Research Organisations and a large participation of Industry. Also for the first time a representative from the International Committee of the Red Cross (ICRC) attended the conference.

The intent of Day 1 was to set the scene and demonstrate the connection between the Comprehensive approach and NNEC. After the conference was officially opened by the Finish Chief of Defense, General Ari Puheloinen, and DSACT General Mięcyslaw Bieniek, the attendees were introduced in the topic by keynotes from the Director NATO HQ C3 Staff MGen Hines and the deputy chief executive of the EDA, Dr. Adam Sowa. Mr. Pekka Haavisto, Member of the Finish Parliament noted that information sharing and the comprehensive approach can be beneficial to the military as well as to the civilian side of operations. Information sharing is not just an academic exercise but makes a difference in the everyday life and work for the soldiers in current missions as well as in future missions. Following the numerous suggestions from the previous NNEC conference, the organization committee of the NNEC conference arranged for a young "digital native," Mr Teemu Arina to address the challenges for NNEC in the near future. His brief was remarkably impressive and extremely well received by the attendees. The presentations of NEC related efforts of EU and USJFCOM completed the mission oriented picture.

During the morning of Day 2, a further view on the necessity and the specific challenges of introducing the Comprehensive Approach into Theatre was presented and discussed with the attendees. The afternoon sessions were separated into four tracks examining Technology to improve information sharing (Breakout Session 1); Human factors and processes supporting NNEC (Breakout Session 2); Cyber Security (Breakout Session 3); and NNEC Practical Applications (Breakout Session 4).

On Day 3 different approaches to NNEC and the comprehensive approach were presented to the audience. The EDA perspective presented by Mr. Marcel Staicu, followed by Mr. Yrjo Benson, State IT Director and Chief Information Officer FIN with a presentation of Service integration and networking in future society in Finland. Colonel Geerlof Kanis, Director of the Command and control Center of Excellence laid down the challenges of Command and Control – human aspects. Captain (N) Anders Olovsson gave the audience an overview on the Swedish Armed Forces experience concerning NNEC and the comprehensive approach from his time at the anti-piracy operation ATALANTA. Finally, Mr. David Waxman, Chief Technical Officer, IBM described "Cross government integration

through technical innovation.” The conference concluded with a summary brief by ACOS C4ISR & NNEC, MGEN Willemse as well as the closing remarks by BGen Salmi.

Annex B contains a synopsis of each presentation.

Key points of the conference include:

- Today’s problems cannot be solved in traditional ways
- Greater cooperation and information sharing - including with non-NATO entities - is vital
- NNEC and Comprehensive Approach can benefit war-fighters, disaster responders, peace-keepers
- Trust is essential for Comprehensive Approach
- Social Networking is major element of recent events
- As Mr Arina said: “Social media is an extension of the person”
- We are now in hyper-connected world, linking information, location, people and context
- NATO needs to work out how to address this issue
- Needs to prepare and be ready for political decisions

The Conference continues to provide a key forum to the NNEC Community-of-Interest for the sharing of ideas as well as networking. The location for the 2012 conference is still to be determined.

Conference Aims

As espoused by many of the NNEC leadership, NNEC is about people first, then policy and doctrine, processes and then technology. The presentations and keynotes made it evident that the technology is an enabler to share more relevant information for better decision-making as well as being able to communicate intent and instructions. The importance of Information sharing in an NNEC environment to enable the comprehensive approach has been made evident and underlined with many practical examples.

This conference attempted to point out the necessity to share information as well as to manage it and to clearly convey the operator’s requirements to NATO bodies, NATO and non-NATO Nations, international organisations, governmental and non governmental organisations as well as to industry to enable a truly comprehensive approach. Additionally, it informed the broader NNEC Community of Interest on continuing developmental efforts and implementation progress on NNEC including how to assess the degree of net-centricity.

Finally both the comprehensive approach and NNEC, even though supported by technology are a matter of communicating with people. Thus, the conference is designed as a forum for dialogue between different people of different nations, between different cultures, between scientists, operators, war-fighters and technicians, with the aim to foster understanding and trust, to demonstrate NATO, national and civilian developments in the field of NNEC and thus encourage and support the information sharing process.

Conference Agenda

The 2011 Conference agenda was designed to underline the importance of NNEC in enabling the comprehensive approach and to demonstrate the links between the theory and the reality in a mission environment. This set the stage for the rest of the conference. Day 2 had a dual purpose of laying down some practical examples for information sharing as well as the ACT activities towards NNEC and examining potential concepts, human factors, technology enablers and addressing Information Assurance as a vital part of NNEC. Day 3 concentrated on different perspectives on the comprehensive approach and NNEC as an enabler as well.

The complete Agenda will be provided in Annex D.

Conclusions

1. Key messages:

a. Today's problems cannot be solved in traditional ways

Beginning with the opening keynote speech from General Puheloinen, he was the first one to point out that today's problems cannot be solved in traditional ways. This was repeated by several speakers in different presentations throughout the conference together with an emphasis on the need for greater cooperation and information sharing.

The potential benefits to all parties: war-fighters, disaster responders, peace-keepers; NGOs and even local civilians, are clear.

As highlighted by General Hines, greater sharing also requires greater trust and an acceptance of the greater risks involved. Risk management will therefore be vital but we need to be aware that the fallout from wikileaks does not create a climate of risk aversion.

b. Social networks have been key to recent world events

This topic was taken forward by Mr Arina in his excellent depiction of the hyper-connected world in which we, and especially the next generation, are now living.

This challenging new world is here now, and NATO clearly needs to work out how to address the issue. We need to prepare and be ready for political decisions which may not be too far away.

c. NNEC and the comprehensive approach

NATO's Comprehensive approach and NNEC share some important factors like mutual trust, the understanding of cultural differences and the will to share information in order to reach mission success more efficiently. NNEC as NATO's effort to facilitate such information sharing is vital to the comprehensive approach.

d. Increase the urgency of addressing

- federation of Networks and FAS
- Information management issues
- Information assurance including cyber defence

2. Attendance

a. Budget considerations

The tight budgets obviously restricted the travel for attendees from NATO

organisations considerably and led to a decline of participants from 132 in 2009 to 60 in 2010, a decrease by 55%. In 2011 this number raised to 72 again, a significant 20 % increase.

Due to the limitations of the conference facility, registration had to be stopped in order to not exceed 450 attendees.

b. Topic

The increasing number of participants from industry, NATO and Partner Nations demonstrate a clear interest in NATO's effort to promote NNEC in general and in the field of information management in particular. With the increasing flow of information from different sources, it does become more and more apparent, that the way information is treated and managed will be of utmost importance in the future to provide planners and war fighters with the right and relevant information, at the right time.

As many attendees coming from a technical career, the significance of NATO's effort to establish policy, direction and guidance to prepare it and the nations for information age capabilities seems to be generally underestimated. Promoting the importance of the human factor, as well as the importance not only for technical solutions, but also for the policies allowing these solutions should be further pursued. In this context, Cyber Security plays a major role for any future NNEC System.

c. Location

Adding to the general budgetary challenges is obviously the location of the conference venue. The unusual high participation from various representatives of Industry and Nations clearly demonstrates; that a location in Europe is more attractive to the mostly European participants, thus increasing the participation of these groups considerably and helping NATO to spread the "Share to Win" message.

d. Number of attendees :

- 441 attendees
- 44 speakers
- 27 of 28 NATO nations represented
- 9 PfP partner nations represented
- 158 Industry representatives participated
- Representatives from the EDA, EU and ICRC

3. Summary

The NNEC awareness campaign and in particular some actual projects like the Afghan mission network are raising NNEC more and more towards national and industrial centre of attention. While it is still a challenge to get the operational community on board, there is certainly an increasing awareness between the nations and international organisations to find a harmonized approach to NNEC.

The 6 year comparison chart provided in Annex A clearly supports the increased awareness of all COIs, but also shows that participation of NATO organisations is still relatively low.

The NNEC conference is greatly appreciated by all attendees as the only NATO venue to foster communication between different communities of interest, exchange information, gather ideas and be briefed about the developments and implementation progress of NEC and NNEC as well as the significance and advantages in real world operations.

In particular this year's participation of the industry should be pointed out. The increase to 158 attendees is a quite remarkable demonstration on the side of the industry to support NATO in its efforts to reach NNEC.

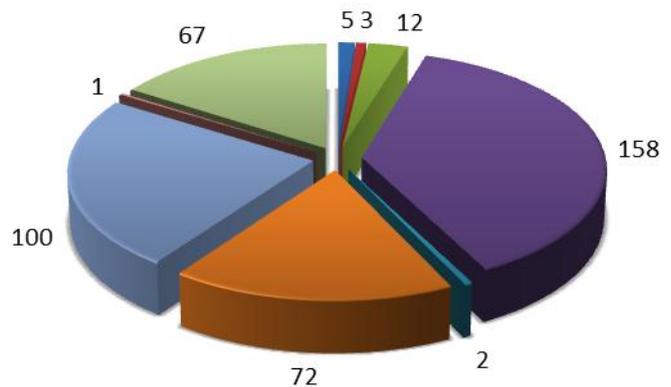
Annex A: Conference Facts

The 8th NNEC Conference was hosted by Allied Command Transformation (ACT) and co-hosted by the Finnish Defence Command. The Conference hosted 441 attendees from NATO, Nations, industry and international organizations, as detailed below. Please note in particular the increase of participation from representatives of the industry. The theme of the conference was “Comprehensive Approach – NNEC as an enabler.”

Attendee information on the 2011 Conference is listed below and depicted in figures 1 - 5.

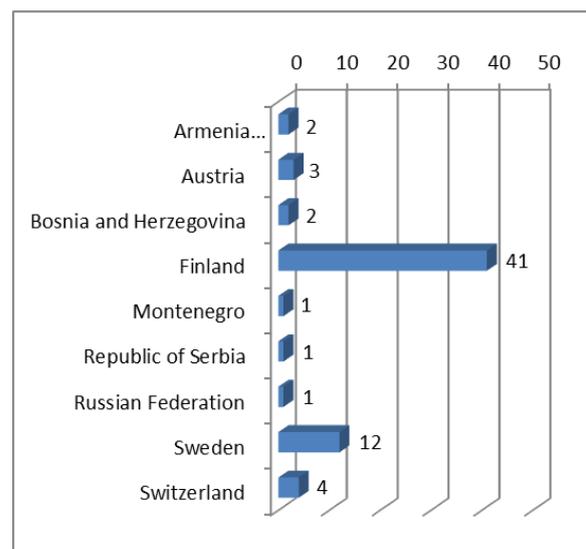
Total Attendees: 441

Academia	3
COE (Centers of Excellence)	5
EU / EDA	3
Government Organization	12
Industry	158
Med Dialogue	2
NATO & NATO Agencies	72
Representatives from NATO Nation	100
Navy Reserve Support	4
Non-NATO Nation	1
Other	13
PfP (Partnership for Peace) Nation	67
(blank)	1



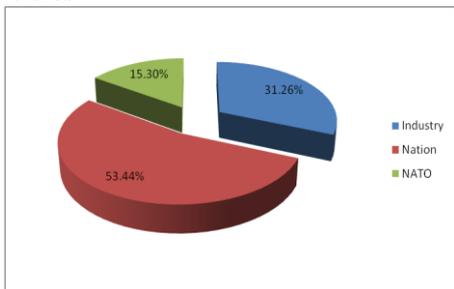
Attendees from Partner Nations: 67

Armenia	2
Austria	3
Bosnia and Herzegovina	2
Finland	41
Montenegro	1
Republic of Serbia	1
Russian Federation	1
Sweden	12
Switzerland	4



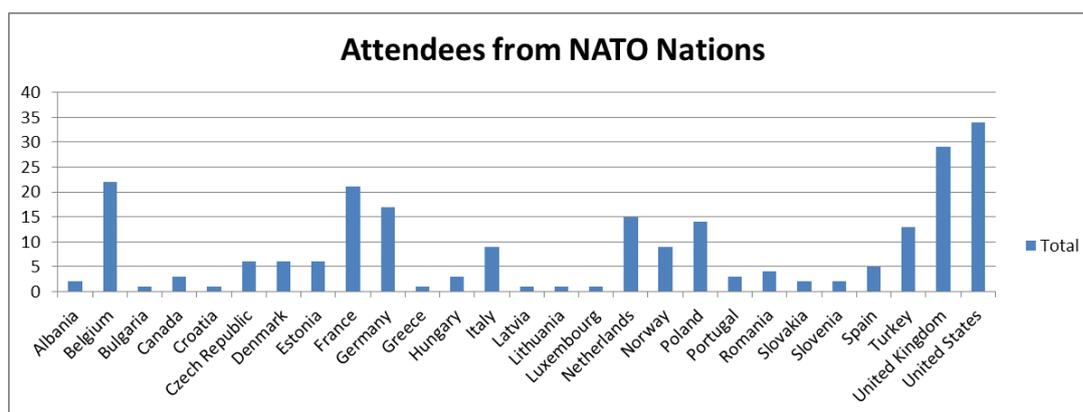
Attendees by Industry, Nations, NATO Entities

Industry 31.26%
 Nation 53.44%
 NATO 15.30%



Attendees from NATO Nations : 231 (includes NATO bodies, industry, national representatives, ...)

Albania	2	Lithuania	1
Belgium	22	Luxembourg	1
Bulgaria	1	Netherlands	15
Canada	3	Norway	9
Croatia	1	Poland	14
Czech Republic	6	Portugal	3
Denmark	6	Romania	4
Estonia	6	Slovakia	2
France	21	Slovenia	2
Germany	17	Spain	5
Greece	1	Turkey	13
Hungary	3	United Kingdom	29
Italy	9	United States	34
Latvia	1	Iceland	0

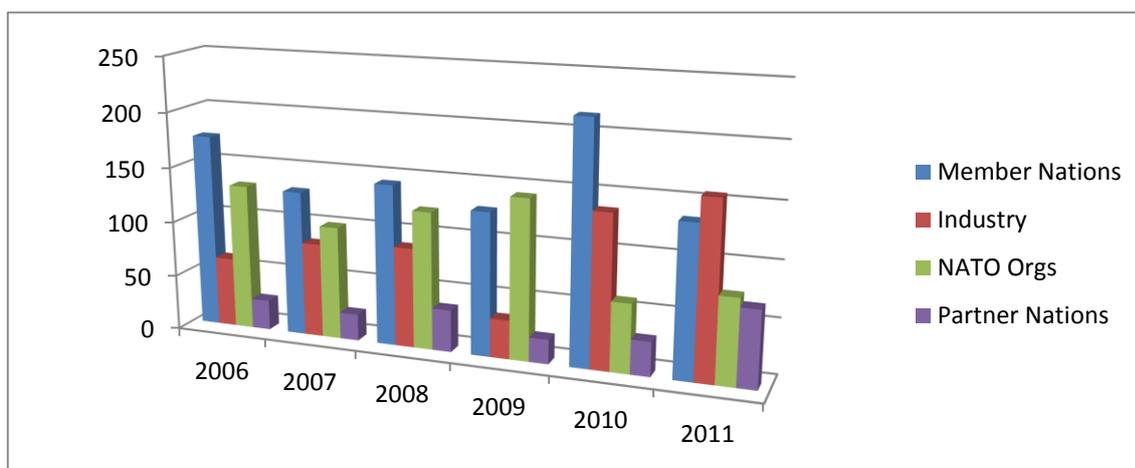


6 Year Comparison:

An increase in interest by NATO and non-NATO Nations is clearly visible, as well as the remarkable increase of participation of representatives of industry.

The increase of the participation of Partner Nations and the decrease of the participation of Member Nations is partly due to the co-hosting of the conference in a PfP country.

	2006	2007	2008	2009	2010	2011
Member Nations	175	131	145	129	216	144
Industry	63	85	90	35	138	158
NATO Orgs	132	102	124	144	62	72
Partner Nations	27	24	38	22	31	67
Total	397	342	397	330	447	441



The graph above depicts a steady increase of Industry participation as well as a steady increase of participation of Partner nations, while the level of participation of member nations is (except for 2010 in Italy) rather constant.

NATO organisations obviously suffering from budget cuts and the ongoing agency reform still managed to increase their presence at the 2011 NNEC conference compared to the year before, a further indication that NNEC is still a major topic of interest.

The attendance of the ICRC at the 2011 conference marks the first participation of a NGO. With NATO's comprehensive approach, further efforts should be made to invite more NGOs and international organisations to attend the conference.

Annex B: Conference Highlights

Tuesday, 05 April 2011 – Day 1

Moderated by MGEN Jaap Willemse, ACOS C4ISR & NNEC, HQ SACT

08:30 Keynote
General Ari Puheloinen Chief of Defence, Finland
<ul style="list-style-type: none">• Cooperation between nations is vital especially to small countries like Finland• Strategy of total defence in Finland recently revised• Defence Forces frequently called to assist other forces• Social networks have been key elements in recent world events• Today's problems cannot be solved by traditional military means

08:55 Keynote 2
General Mieczyslaw Bieniek, Deputy Supreme Allied Commander Transformation
<ul style="list-style-type: none">• Many partner nations and industry partners here• Particular welcome to Red Cross, EDA, NCOIC, EU• Sharing not an end but a means to achieve a goal• Enables more economy, efficiency, effectiveness• Need to prepare for and stay ahead of political decisions• Need to work out how to adapt / respond to social networking?• NNEC Comprehensive approach benefits both soldiers in field and disaster responders.

09:20 Keynote 3

Major General Glynne Hines
Director, NATO HQ C3 Staff

- Self-interest may override need for cooperation
- Technology is just a tool and mutual trust is vital
- Some way to go in order to achieve levels of trust needed to achieve comprehensive approach
- Need to forge links before the urgent need arises
- Comprehensive approach will fail without effective information sharing but sharing brings risks
- Risk management is vital but beware fallout from wikileaks derailing a comprehensive approach

09:45 Keynote 4

Dr. Adam Sowa
Deputy Chief Executive, European Defence Agency

- Global threats not all military
- EU well suited to comprehensive approach using NEC as an enabler
- Afghanistan shows advantages of greater cooperation
- EDA is at centre of EU development of NEC Roadmap tracking tool
- Good relationship exists between ACT and EDA

10:35 Needs and requirements for network enabled capabilities in multi-agent crisis management operations

Mr. Pekka Haavisto
Member of Parliament, Finland

- Full cooperation between civil and military brings benefits to both sides
- Many questions for civil intervention: Do you start with civil society or armed groups? What is role of neighbours? Does West have an agenda? Do we have a common agenda? Peace or justice first? Negotiations can be destroyed by trying to bring criminals to court when negotiations in progress.
- Military problems may have social elements – Somalian teenagers want to be pirates. Identities of pirates are known but there is a lack of incentives to stop piracy e.g.: buying rifles and paying for education as alternative.
- Comprehensive approach needs to address physical and social issues.
- Parallel activities needed. Negotiations, Military activity, civil coordination.

11:10 Comprehensive Approach: NNEC
Vice Admiral Carol Pottenger Deputy Chief of Staff Capability Development, HQ SACT
<ul style="list-style-type: none"> • NNEC is the bridge between political guidance and how to achieve the required results • NNEC is not a singular capability - should be capabilities • Tech solutions are the easy part – the others need to be addressed • Some concerns about AMN
Question (by)
<p>Industry Representative: There are also political problems to consider NNEC. What can NATO do to connect political and technical policy makers?</p> <p><i>A: NNEC is still a black box to many people who do not understand what it is. We need to socialize it more.</i></p>
<p>NC3A – More and more nations involved. What is ACT doing?</p> <p><i>A: Speaker is leading a Task Force to address Innovative and Multinational approaches. This is taking a pragmatic approach and NC3A is involved. These requirements will need to have NNEC included and ACT needs to lead.</i></p>

11:45 An ICRC Perspective on the Comprehensive Approach
Monsieur Francois Bellon International Committee of the Red Cross (ICRC)
<ul style="list-style-type: none"> • There is not a single concept of Comprehensive Approach or humanitarian action. Diversity is the rule in both cases. • Humanitarian intervention is not a substitute for political / military action • The actors in a crisis do not share common objectives. Peace-making and peace-building are not primary objectives of humanitarian intervention • Risk that CA may blur humanitarian aid and political and military aims to defeat an enemy; such distorted perception could risk both humanitarian agents and beneficiaries. • Impartiality, Neutrality, Independence are key values for Red Cross which cannot be abandoned and reinstated at will. • Humanitarian agencies must accept CA but actors should not claim same goals. • Humanitarian actors must show more consistency and debate consequences of own choices. • Red Cross was born on the battlefield and understands the military view

13:30 Implementing Network Enabled IT Services for NATO's Coalition Operations

Lieutenant General Kurt Herrmann
Director of NCSA

NNEC lessons learned

- Presentation of NCSA
- Current operations already network enabled
- Interoperability is a prerequisite for NNEC
- Creation of a centralization and data center to share the data in implementing virtualization.
- CIS for COIN Operations : Information sharing is key
- NATO 's information technology roadmap
- AMN

Core network for time sharing, and minimizing other networks

AMN is the overall catalyst

- Service management framework

Established in AMN in 2010

- Active threats

Cyber attacks

- Cyber Defense in NATO will increase in importance
- Information Assurance
- Future NATO CIS Support

14:15 Net generation's approach to networking and information overload

Mr. Teemu Arina
CEO, Dicole OY FIN

- Cloud computing will be a very important perspective in this decade and the continuation of the current Web which is a social media.
- Information is instant on the Internet.
- Internet is an extension of your mind.
- Information overload is actually dealing with uncertainty. The problem is an inability to adapt. Information overload is a filter failure. It is not a problem if we have good tools.
- We are now in hyper-connected world, linking information, location, people and context.
- 4 domains :
 - Known domain
 - Knowable domain is about research. Information is not something you collect, it is a flow
 - Complex domain (networked and Emergent practice). Environment is

<p>changing rapidly. The problem is to analyse the information to display it, the social network is an extension of you.</p> <ul style="list-style-type: none"> ○ Turbulent domain (unknown – novel practice)
<p>Question (by)</p>
<p>Netherlands Army: What are your views on security?</p> <p>A: <i>Security limits use of information. With my model, there is a different approach, no need of security but of transparency. The culture is not ready for that yet, but a younger person is a sharing person. It is easier now for people to connect and to find information. In 20 years it will be considered strange not to be on Facebook or similar.</i></p>
<p>Your model had 4 quadrants. How do you bring them together?</p> <p>A: <i>Those quadrants are always connected. The old system had point to point connections; the new model has no point to point. They are in balance</i></p>
<p>SACEUR – What is your view on the movement of power from state to non-state through social media</p> <p>A: <i>I am not an expert on this topic. Today the public is well informed. Information is good and there is a need for transparency.</i></p>
<p>When are you going off-line?</p> <p>A: <i>Effectively never. Reality is on-line and people are the sensors</i></p>
<p>Does new technology help to link people?</p> <p>A: <i>Yes to a degree. When you connect you tend to join to people of similar views – no challenge</i></p>
<p>What is the future?</p> <p>A: <i>Futures cannot be predicted. Futures can be created now.</i></p>

<p>15:15 Comprehensive C4ISR Approach</p>
<p>Major General (Ret) Georges D'Hollander General Manager NATO C3 Agency</p>
<ul style="list-style-type: none"> ● Doing more of the same will not be good enough. ● Embracing a comprehensive approach needs a change of approach. ● Experience of AMN shows that interoperability cannot be added later – must be planned. ● Keeping pace with technology is a challenge. ● Future NATO Mission Infrastructure will be needed.

Question (by)
Italy – Aeromechnica: If we have 64,000 NATO troops we have 64,000 smart phones – are we thinking of using this network? <i>A: We should explore possibilities, although there is a question of security.</i>
Frans Picavet IBM: Some years ago there was mention of standardised building blocks. Now introduced ESB in AMN without any competition, or reference to NIAG report? <i>A: Not enough time to use standardise. Had to use the best available. The requirements were there, and there was nothing in the market.</i>
Industry: Is there any discussion with industry concerning Revised acquisition procedures? <i>A: There was a study concerning the acquisition process although outcome not clear. It is now linked to the Agency Review.</i>

16:25 Applying NNEC Concepts to Air Command Control System (ACCS)
Dr. Gerhard van der Giet, General Manager NATO Air Command and Control System Management Agency (NACMA)
<ul style="list-style-type: none"> • ACCS is an example of NNEC. • ACCS was conceived as an integrated system of systems and incorporates many NNEC tenets which pre-existed NNEC. • NACMA has aligned ACCS for NNEC. • ACCS is a major player in NNEC environment; driven by similar concerns; undertaking various NNEC experiments to see what further convergence can be achieved.
Question (by)
Frans Picavet IBM: How flexible in light of new command structure? <i>A: The system may need to be resized to cope with 2 instead of 3 CAOCs. The software is unchanged.</i>

Wednesday, 06 April 2011 – Day 2

Moderated by MGEN Jaap Willemsse, ACOS C4ISR & NNEC, HQ SACT

08:30 Network Enabled Defence in Finland
Lieutenant General Markku Koli Chief of Defence Command, Finland
<ul style="list-style-type: none">• NEC most important element in defence.• Cooperation is key.• Finland started in 1997 at tactical level, through operational to strategic and back in cycle lasting to 2010.• Now implementing strategy written 8 years.• Now implementing Interoperability. Cooperation - especially with NATO – has been key.• Social media technologies will show the way ahead.• Cyber warfare is the biggest challenge.
Question (by)
How to organize outsourcing? A: <i>It is difficult and takes time. It must be done in stages</i>
How to engage the public opinion? How to connect with EU and NATO? A: <i>It's a political question and I have only technical answers. But they can and should be linked in the future.</i>

09:05 ATOS Origin Presentation
Lieutenant General (Ret) Jo Godderij, Former Director General International Military Staff (DGIMS)
<ul style="list-style-type: none">• Comprehensive Approach to our Collective Security in a networked Environment.• Collective security in a different way from the beginning.• Comprehensive Approach started to be talked in Afghanistan.• NATO cooperation now. Nowadays NATO talks with everybody. Now we have a NATO network enable environment – planning information.• Combine Network Environment and Comprehensive Approach we will have the ideal situation: coherence and interdependence.• At the London Olympic Games, it will have Information Technology systems – management system. They have a technology Operations Centre. Everything is tested.

- The secret of OG success: Testing / Experience / Risk Management / Discipline / Partnership
- Challenges that require excellent delivery: on-time / on-budget / new environment (every two years) / security risk / Large Scale and Complex / sustainability
- Important is the environment: community / collaboration / different network but one mission / SHARE TO WIN
- Everybody evolved in a common goal – comprehensive approach – Olympic Games are a comprehensive approach in a NEC environment and also here it is nothing less than.

09:40 Information Superiority based on NATO-National Interoperability services

Mr. Valery Rousset

C4I capability development, Thales Defence & Security

- The goal – run from interconnected systems to interoperability services
- Challenges to interoperability: Proliferation of battlespace objects brings legacy C4I standards to the limit
- Supporting NNEC rationale, from federation to integration: Evolutive competency levels: deconfliction, coordination, collaboration, coherence
- Thales - A decade in support of National interoperability towards NATO - Coalition support & key framework nation enablers
- NATO Interoperability Services : operational benefits of information exchange data models
- Recent implementation were on full-NATO capability package on bi-SC AIS
- From top to bottom, application on AMN – The principles of AMN: a federation of networks (Network is transparent to the Information System)
- Conclusions: A long-standing track record of supporting NATO transformation & interoperability; a proven capability to rapidly industrialise & deploy FASs; A reactive and innovative service-based support to CURs

Question (by)

To enable exchange of information to civilian partners – should we focus on use of civilian standards?

A: *Future is now. Challenge is making a security interact between civil and military community. We need to have the military standards but also the internet (civil standard).*

10:40 NNEC Demonstrator / Security Model for NNEC

Dr. Alberto Domingo, Deputy Branch Head, C4ISR & NNEC Branch, HQ SACT

Dr. Hermann Wietgreffe, Principal Scientist, NATO C3 Agency

Mr. Geir Hallingstad, Principal Scientist, NATO C3 Agency

- NNEC, where are we? NNEC is transitioning from concept to reality, most notably in the area of Information Sharing / There is sufficient knowledge and there are sufficient tools / A growing number of capabilities address NNEC as a user requirement / There are still some issues that prevent full NNEC compliancy
- What are the issues – most of them related with processes
- NNEC + - We can share information with non operational actors in the field
- Summary of facts – NATO and Nations are moving towards milestone #1 (information sharing) / NNEC+ addresses those issues, while embracing the Comprehensive Approach and the outcome of the Lisbon Summit / ACT efforts aimed to support on-going implementation activities and increase their scope, demonstrate the feasibility of the NNEC+ approach, and trigger a review of the current information assurance model
- NNEC+ User Requirements:
 - Plug-in anywhere, have access to everything needed, based on role/function and not limited to military actors, type of connectivity/location and type of terminal
 - Instant availability of new information
 - Maximum reuse of information, services and processes
 - Users can generate new services, can authorize new users/information sources and can access all services after one authorization
 - Keep appropriate Information Assurance (IA)
- Demonstrator Implementation Outline:
 - A single network, moving security from the network domain to the information domain
 - Attribute based access control (ABAC)
 - Service Oriented Architecture (SOA)
 - Single sign-on
 - Dynamic Service registration and discovery
 - Re-use of existing services (mediation)
- NNEC+ Demonstrator benefits – Enforces a holistic approach to NNEC and related Information Assurance aspects / Visual part promotes understanding of NNEC principles and benefits / Physical implementation constitutes a validation platform for NNEC builders to gain pivotal know-how
- Challenges – Mediation for existing services / Multi-Level Security environment / Access anywhere / Flexible authorization / Users as both consumers and providers of services
- Conclusions and way ahead – Worthwhile to build the demonstrator /

- Demonstrator feasibility analysis nearing completion
- NNEC Demonstrator / Security Model for NNEC Principles of the Security model – Prevent and react (balance preventive and reactive measures on cyber space) and Content labeling (the equipment has those requirements – abandon classical security labels; use content labels and separated / policy maintenance)
 - Conclusion and Way Forward – Our mode of operation needs to change / Balanced preventive and reactive measures / Feasibility
 - General conclusions:
 - NNEC implementation is satisfactorily evolving towards achieving milestone #1 (Generalized Information Sharing).
 - Most issues are now related to federation of processes (NNEC milestone #2) and supporting technology and tools (NNEC milestone #3).
 - NNEC+ targets the objectives of milestone #2, while embracing the Comprehensive Approach and the outcomes of the Lisbon Summit.
 - NNEC has focused so far on the art of the doable, while NNEC+ will imply significant changes to the way we handle and disseminate information. Overall, costs might remain as they are.
 - The NNEC demonstrator is a quick and inexpensive tool to capture real requirements, to develop solutions, to identify areas of concern, to develop information assurance requirements and to increase awareness of NNEC operational advantages.
 - There is a need for a careful revision of current information assurance model, to balance user requirements, policy and mechanisms and achieve sufficient information protection.
 - The study on a new information assurance model identifies the NNEC+ approach as feasible, and provides a number of solutions for a steadfast implementation.
 - This opens the door to many efforts. Stakeholders in general, and Nations and Industry in particular, are invited to participate.

Question (by)

What are the impacts and challenges of requiring individuals to label all information?
A: *It's no different to what is done today. We have to label the information; we have to put the right label on. Today this requires knowledge of policies which should not be necessary in future.*

Request to expand on security communication.
A: *We are not implementing changes in information flow.*

11:50 Afghan Mission Network – A practical application of NNEC

CAPT John Nankervis & CAPT Mike Horsefield, Branch Head Crisis Response Operations / CPP CAM, HQ SACT and SHAPE

- NATO already has an Alliance Mission Network – it is the NATO secret LAN.
- Need is for a Future Mission alliance network.
- COM ISAF achieved AMN by accepting risk and dictating solution. Share to win became more important than need to know. A federation of the willing where users could look into one apparent domain with no restrictions on human interaction. It moved communication from maturity level 1 to 3.
- It covered Chat, VOIP, Email with attachments, GAL, Web, VTC, FFT exchange
- Must not judge AMN on a harsh list of NNEC tenets. Information sharing is the key. Key element is trust with participant nations believing that individual national networks will not be compromised.
- AMN guidance mirrors NNEC principles. Nations choose to join because risk of not joining is greater than risk of joining.
- NNEC Tenets = AMN Op Order. Nations take on AMN as part of their own systems. One mission, one team, one fight ensures unity of effort.
- “AMN” may mean different things to different nations. To an Afghan all ISAF soldiers are the same. Different teams need to access previous reports to enable correct action. All IED reports are available to all so that trends etc can be identified. Still only a tool.
- Part of the challenge is training people before they go into theatre. People need to know what to ask for.
- Training could be carried out in stovepipes but users in United Endeavour 110-2 elected to emulate AMN in a training network. Some technical glitches had to be fixed just as they will be in theatre.
- NNEC and AMN provide a foundation. Easy to add new mission partner. Enables NGOs to communicate. Raises questions of tagging.
- Better tools needed for decision makers needed.
- AMN has 75000 users – not perfect but a long way down road. Eliminated barriers – sidelined some policy issues.
- Training is still a potential problem. System administrators need to understand different user situation.

Question (by)

Bram ACT- You touched on possibility of Allied Mission Networks. Should we set the standards or design our own network and let nations come “if they want”?

A: *Answers: If we have common standards we should use them. If nations follow national NNEC standards and NATO publicises them we will have at least some of*

what we need.

Industry. What are the challenges and real use of VTC in AMN?

A: *VTC currently works mainly within the NATO domain.*

Industry: Context is all and the challenge is resources. There is a limit on bandwidth which may limit benefits. Thoughts?

A: *Bandwidth will come in time. Bigger challenge is lack of common terms and lexicon. You need to look at where we were and we cannot ignore policy.*

Wednesday, 06 April 2011 – Day 2 – Breakout Session 1

Technology to improve information sharing

Moderated by Colonel Frederic Sakhochian, NNEC Branch, HQ SACT

13:40 Priorities for aligning with future information technology
Mr. Rick Parkington General Dynamics Information Technology
<ul style="list-style-type: none">• Achieving Responsibilities: Fulfilling mission support requirements, Reducing cost, Standardizing processes, Reducing the time to implement technology, etc.• Data Centers needs an Innovative Evolution for the future.• Virtualization is very important to reduce equipments, costs, etc.• Cloud Computing should be adopted in the future.• Cyber Security is critical and is an increasing demand.• Diversify Human Machine Interface.
Question (by)
Views of maturity of this concept A: <i>In the area of technology, the concept is fairly mature (software, virtual machine, etc); In the area of implementation is not enough mature.</i>

14:15 Cloud Computing as an enabler
LCDR Patrick Ratier C4ISR & NNEC, HQ SACT
<ul style="list-style-type: none">• How NATO understands this new technology.• Cloud computing is the evolution and convergence of many independent computing trends.• Not good for all NATO business areas, Step-by-step approach is needed.• Information sharing barriers - Security is critical.• Cloud computing opportunities – Data more accessible, on demand, more tools available on line.• Concerns –Again the Security is the main concern (Cyber defense, data lost, etc..)• Realistic outputs - Cloud Computing would certainly enable more info sharing if processes have been optimized in first hand. This kind of journey needs a global strategy to be efficient and effective.• Comprehensive Approach Use case - MSA Cloud is a good example for working in the cloud - <i>MSA Cloud would provide a Comprehensive approach tool to consolidate a white Unclass picture.</i>

Question (by)
How NATO will get “Data Security” in the cloud. <i>A: NATO will try first use a private cloud to assure the security, moving later to other compliant models.</i>
NATO reforms to adopt this new technology <i>A: We need first fix our own organization. NCSA is taking care of this and it is an on-going work.</i>

15:15 Real time information sharing and multi-criteria decision analysis enabled by LTE technology
Mr. Frederic Sutter Alcatel-Lucent
<ul style="list-style-type: none"> • Short overview of long-term (LTE) technology – The most important capability is a very high speed wireless access with high performance on the field. • What is next? The Alcatel-Lucent LightRadio. • LTE offers multiple advantages for military usage. • LTE provides higher throughput and can share videos in real time. • LTE can be implemented in Land, Air and Maritime. • LTE is the only future radio technology <ul style="list-style-type: none"> ○ That can change the way missions will be performed by using COTS technology ○ Able to spare money, time, personnel to save lives
Question (by)
IPAD 2 is compatible with this technology? <i>A: All the new devices like IPAD2, Nokia, Samsung, etc. are compatibles with this new technology.</i>
Distance of the signal? <i>A: Depending on the antenna and other factors, in general terms is about 5 or 10 Km</i>

15:50 Tools to support information sharing & knowledge management.
Mr. John Redmayne NATO Joint Analysis & Lesson Learned Centre (JALLC)
<ul style="list-style-type: none"> • Introduction to JALLC: Mission, Structure, Organization. • JALLC Main Activities: Support to ISAF, NATO LL Portal, NATO LL Database and NATO LL Handbook.

- JALLC Approach: Collect and Connect Formal and Informal information's.
- Report about Social Network Analysis Exercise (STEADFAST JUNO 2010): E-Mails, Social Network, etc.

Question (by)

How does JALLC use the Social Network Tool?

A: The tool is used with the support of NCSA, to obtain the title of the messages, address, etc to be included in an Excel spreadsheet; The data is then analyzed to obtain the results. It's a very simple tool.

16:25 The Comprehensive Approach applied to situational awareness: A Paradigm shift from data sharing to intelligent data fusion

Mr. Christoph de Preter
Luciad

- Information about LUCIAD Company: Mainly working for rapid development of Geospatial Situational Awareness applications (Date visible) and future technologies. The company has many customers like NATO, NC3A, SAIC, etc.
- Three different Trends: CIMIC (Japan), Asymmetric Threat (Somalia, ISAF, Libya, etc) and NEC/ Coalition of the willing.
- The company is looking for centralize data management, control data overload and to make the data available quicker for the user.
- The use of flexible solutions like open standards and re-use of existing infrastructure are essential for the future.
- Benefits using services are: High data volume processing, high data volume storage and central data management.

Wednesday, 06 April 2011 – Day 2 – Breakout Session 2
Human Factors and Processes supporting NNEC

Moderated by Dr. Nancy Houston, HQ SACT

14:15 The Comprehensive Approach – Will it accelerate or hinder NNEC?
Dr. Peter Essens Netherlands Organisation for Applied Scientific Research
<ul style="list-style-type: none">• Presentation focused on the CA - NNEC relationship and how well CA assumptions and principles match NNEC.• Human interaction is important and people have varying core issues. They may be independent or interdependent, with diverse objectives, interests, ways of working and planning horizons.• There may be a mismatch of technology bases with no one common level of interaction/collaboration and no clear concept of what information to share.• Diversity has to be respected and any aspiration for uniformity or integration is doomed to fail.• CA is essentially a human-centric challenge; there is a need to work with multi-level dependencies, to accept that interaction and dialogue are prime objectives and to understand that low technology levels can satisfy the need.• NNEC underlying thinking is based upon classical systems concept. The NEC Maturity thinking is misleading and misplaced in a CA context, since it underestimates the complexity of information and of coalitions.• CA underlying thinking is that Unity of Purpose and Unity of Effort can be brought up to the level of Unity of Command through integration / coherence - without saying so.• In answer to the question posed, CA can hinder NNEC development if NNEC perspective remains as is, and does little to support CA development due to mismatch in technology focus. Also if CA is taken seriously in its essential requirements, then NNEC underlying concepts and maturity levels thinking need to be adjusted• Alternatively, CA can accelerate NNEC development if the opportunity is taken for NNEC to become what it should be i.e. about people first, then processes, and then technology!• NNEC needs to exploit the essence of CA to find a correct supporting position.

15:15 How Cognitive differences impact information understanding
Mr. Andrew Leggatt BAE Systems (Operations) Ltd

- Need to understand what prevents relationships being more united than they are in order to address issues that affect collaboration.
- UK is leader in field with the establishment of the Stabilisation Unit (originally the Post-Conflict Reconstruction Unit).
- Experiments have shown that message accuracy is mainly based on perceived source. Users are naturally cautious (distrusting) and apply simple heuristics which ignore less-familiar or prestigious sources. This could hinder collaboration and effective use of networked information.
- One possible solution would be to educate users about information sources and trust in order to train them to make optimum judgements.
- The Comprehensive Approach, supported by NEC, is about people and making relationships.
- Concepts such as NEC and the Comprehensive Approach are only theories until they are used in practice by human beings.

15:50 Introducing the HFI-DTC Consortium and Human Views for MODAF
Mr. Richard McMaster University of Birmingham, UK
<ul style="list-style-type: none"> • Questions: Can this person/these people, in this job, with this training, perform these tasks, using this equipment, to these standards, under these conditions? HFI addresses these issues. • Human Views provide a language through which Systems Engineers and Human Factors Engineers can work together. • System capabilities are affected by human performance, creating risks and opportunities. • Use of Human Views provides multiple perspectives on the human component of a system which complement architecture frameworks to produce a more comprehensive view of the interoperability issues. • As part of this process, Military Stabilisation and Support Group have been using the information to revise their training programme.

16:25 The challenge of creating an ordered information domain
Mr. Peter Pharaoh NATO HQ C3 Staff
<ul style="list-style-type: none"> • Presentation based upon NIMA. • NATO Strategic Concept and the Comprehensive Approach are potential ‘game-changers’ for the Alliance. • Establishing mutual trust with an expanded population of Non-NATO Entities

is a 'stretch target.'

- Information sharing requires willingness to share; an ability to share and a sharing rule.
- Sharing works best in ordered Information Domain as is being facilitated by NIMA.
- A cultural shift is required to make information sharing work.
- This will place great emphasis on human factors especially the need to build trust.

Wednesday, 06 April 2011 – Day 2 – Breakout Session 3
Cyber Security

Moderated by Mr. Ryan Vacanti, HQ SACT

13:40 Cyber Security in NEC
Lt Col Nestor Ganuza Cooperative Cyber Defence Centre of Excellence (CCDCOE)
<ul style="list-style-type: none">• No notes

14: 15 Federating Enterprise Security Management
Ms Sandi Roddy Defense Information Systems Agency (DISA), US NSA
<ul style="list-style-type: none">• Roles of COMSEC custodians and IT Administrators are blurring.• Need to ensure that defence of network does not adversely affect operations and that security does not prevent information exchange.• Discussion on identity management, attribute management, policy management and key management.• Composition of a security // key management infrastructure, cryptographic end components and the threat picture all drive the answer of what is good enough.• Recommendations:<ul style="list-style-type: none">○ Expand dialogue on federating Security Management○ Integrate technology roadmap to align with security management needs○ Converge on robust infrastructures that perform across the breadth of the cyber environment○ Collaborate to deliver consistent message to vendors: “Comply with Standards, Compete on Implementation”

15:15 Cyber Defense for Mission Assurance through Mission Oriented Cloud Architecture
Mr. Wesley Rhodes IBM Software Group, Strategy & Technology
<ul style="list-style-type: none">• Discussion on MOCA = Mission Oriented Cloud Architecture which uses several technologies:<ul style="list-style-type: none">○ Deep Packet Inspection – To analyze data flows within the cloud to

detect anomalous behaviour in real-time

- Advanced Analytics – To detect and react to abnormal patterns of network traffic, user presence and behaviour in order to protect the cloud infrastructure
- Context Accumulation – To reduce the time needed to achieve actionable insight
- Resilience - To be able to reconfigure cloud networks and resources to ensure military relevance of the core applications
- Virtual server protection – to be able to use a highly virtualized environment with situational awareness of vulnerabilities and attacks
- Autonomic Defence – to defend at machine speed

15:50 Information exchange in multi-level security/cross domain environment

Mr. Bernard Roussely
Bertin Technologies

- Information Assurance not first priority for users. IA must not get in way, to decrease performance; reduce functionality; or prevent “business as usual”. Must also be cheap.
- Challenge is to grant authorized users access to all information they require in a transparent and secure manner in accordance with the existing security policies.
- Main risks due to interconnections:
 - Information leakage to the “low side” through direct leak (accidental or deliberate) or by use of covert channel
 - Attacks from the “low side” to the “high side” include denial of service, loss of integrity and data loss.
 - Vulnerability sources: people, procedures, software (bugs, malware, etc.) and hardware bugs.
- Several technical solutions to address cross domain information sharing requirements, e.g.:
 - “air gap” = resource intensive, cumbersome, with media transport open to loss or diversion
 - Physical diode
 - Firewall / Guard
 - Information Exchange Gateways (IEGs)
 - Workstation: MLS, MILS, KVM, Multiple boot WS...
 - Each solution has pros and cons and no “one size fits all” solution
- A combination of solutions (e.g., MILS WS + Guard) may satisfy most user requirements.
- Company offering Client / guard demos at CWIX 2011

16:25 Multi-level security “Threatscape Update”

Mr. Don Smith

Dell Inc (Substitute speaker)

- Dell has acquired security company “SecureWorks”
- Covered wide range of recent attacks with particular mention of recent attack on Epsilon used by numerous companies.
- Over 4600 domains targeted in Q4 2010
- Targets:
 - Online banking, payment services, store cards targeted around Thanksgiving / Black Friday
 - Online betting companies
 - Credential theft against “mainstream services” such as Google, Yahoo, Live/Hotmail, Monster
 - Web injects against mainstream services inviting users to enter Credit Card numbers to continue.
- Noted a change in mode of operation moving from simple credential theft to fraudulent transactions via web injects. Attackers understand and capitalise on human behaviour.
- Ongoing automated processing of Trojan configurations allows company to Watch for client URLs being targeted (amongst other things!)
- Summary: We’ve got to get better against new Platforms, new actors, new forms of distribution and increasing complexity albeit using old techniques...

Wednesday, 06 April 2011 – Day 2 – Breakout Session 4
NNEC Practical Applications

Moderated by Mr. David Burton, CTO, NC3A

13:40 NC3A CTO and its role in NNEC Delivery
Dr. Paul Howland Chief C4ISR, NC3A
<ul style="list-style-type: none">• Advantages of NNEC well known but transitioning to service orientated approach poses unique challenges.• NC3A delivering NNEC today (e.g. Air Command and Control (C2) Information Services (IS), Afghanistan Mission Network (AMN) and MAJIIC) and the NC3A CTO is well-placed to identify shortfalls in NATO process:<ul style="list-style-type: none">○ NATO acquisition processes lack agility especially for urgent operational requirements○ Project focus leads to stovepipes and a lack of responsibility for big-picture coherency○ Focus is on systems rather than capabilities○ No single overarching vision or roadmap○ Poor alignment between nations and NATO○ Ineffective governance○ Inadequate operationally representative testing○ Use of theatre as a test bed• NC3A working to improve effectiveness, cost efficiencies and greater coherence but problem is bigger than NC3A alone.• NC3A is engaging with internal projects and portfolios; with national CTO/CIOs and industry bodies; and with other NATO bodies to help develop a NATO C4ISR Vision to define where we are going, and NATO C4ISR Strategy to define how to get there.• Practical NNEC requires:<ul style="list-style-type: none">○ A clear vision and strategy to align NATO and nations○ Architectural and standards approach○ A focus on programmes rather than projects, and capabilities rather than systems;○ Effective governance;• CTO is trying to address this within NC3A but a coordinated approach across NATO and nations is required.• A Chief Technology Office operating across NATO could deliver better programmatic coherence, effective implementation and fiscal savings.

14:15 MAJIIC2 – Processes and Technology

Lt Col Arle Brustad

Chairman of the MAJIIC National Project Officers, Norwegian Army

- Mission is to improve the Operational Commander’s decision-making by enhancing Situational Awareness.
- Business model is to develop agreed standards and Concepts of Operation as guiding requirements for national and NATO acquisitions.
- IT focus is on integrating JISR processes and Information Systems to optimize operational efficiency and effectiveness to enhance integrity and agility of military decision making.
- Action being taken to enhance existing capabilities through additional intelligence products (multi-INT), Cross Community of Interest (COI) interoperability, operational process effectiveness and efficiency enhancements.
- The evolution of NATO NEC / SOA Core Services will be taken forward through delivery of MAJIIC as a scalable cross COI NNEC capability within the NATO Service Framework.
- The End State of MAJIIC 2 will provide scalable, flexible and interoperable JISR focused capabilities to support Joint/Coalition operations.
- This will lead to:
 - Increased Ops resource efficiency – doing more with less
 - Improved mission effectiveness – timely & accurate information exchange
 - Lower investment cost – burden sharing during development
 - More Operationally effective utilization of technology
 - Risk reduction to future NNEC acquisition

15:50 Presentation CFC / CMO

Lt Col Michael Hendrigan

Civil Military Fusion Centre

- Presentation described the Civil-Military Fusion Centre (CFC)/CMO “CimicWeb” Capability
- Official NATO policy and practical experience in complex natural and man-made crisis situations make clear the need for better interaction and cooperation with Non-NATO actors to facilitate a Comprehensive Approach.
- CFC operating under two operations requirements: one from HQ ISAF to provide support in Afghanistan and another from Joint Command Lisbon to monitor events in North East Africa, where NATO is providing the African Union with logistical support.
- Thousands of organizations may be working in a crisis area with different and

- possibly competing agendas.
- Many of whom will not wish to work with NATO, but even these must be known to NATO in order to de-conflict activities.
 - For others, cooperation and coherence may enable all participants to achieve individual goals more effectively.
 - There are many barriers to information sharing between military and civil actors that must be brought down for NATO to achieve a truly comprehensive approach:
 - Military culture is very different than those of many IOs and NGOs which may cause friction. Use of cultural stereotypes does not help.
 - “Need to Know” mentality and Classification Policy versus a “Need to Share”. The military has an “information protection” mentality and will not share with a person/organization not deemed to have the “need to know”.
 - Most military personnel not involved in CIMIC/Civil Affairs do not understand and have not been trained in interacting with civil actors. Training should become an essential part of military training.
 - Non-classified communication passed on classified infrastructure makes it difficult to share.
 - Trust between parties may not exist and needs to be built at all levels.
 - The scale of military presence may overwhelm other actors.
 - The research and low-level analysis conducted by the CFC is primarily used by Knowledge Managers to communicate with representatives of the CIV-MIL community working at the Operational and Strategic level.
 - A Civil Military Fusion Centre and CimicWeb experiment which commenced in January 2008, ended on 30 June 2010. The final experiment report is about to be released.
 - Chiefs of Staff from Allied Command Operations and ACT will be discussing the transition of the CFC from ACT to ACO command and control on 1 July 2011.

16:25 Underwater Networking
Mr. Alessandro Berni NATO Undersea Research Centre (NURC)
<ul style="list-style-type: none"> • The presentation described NURC work. • NURC’s mission is to deliver innovative and field-tested maritime science and technology solutions to implement NATO’s Strategic Concept. • Maritime environment is important since 2/3 of Earth’s surface is covered by oceans. • There is a need to deliver persistent surveillance of the sea, from a military and civilian perspective for Maritime Security and Environmental Monitoring

- Network-Enabled Cooperative Surveillance provides:
 - Cross platform interoperability of NATO UW systems
 - Link underwater and above water
 - Gateways to existing operational NATO C2 systems
- JANUS is a robust signalling method for underwater.
- Communications
- NURC has demonstrated that Delay/Disruption Tolerant Networking (DTN) DTN can be used to transparently and reliably interconnect “traditional” IP-based network with underwater acoustic networks.
- The software framework developed is suited for use in maritime hybrid networks in which data has to be delivered reliably across highly heterogeneous links.
- Future work is required on the integration with above water networks and application-layer data formats and messaging standards.

Thursday, 07 April 2011 – Day 3

Moderated by MGEN Jaap Willemse, ACOS C4ISR & NNEC, HQ SACT

08:30 European Defence Agency and EU NEC
Mr. Marcel Staicu European Defence Agency (EDA)
<ul style="list-style-type: none">• Core drivers for EDA are:<ol style="list-style-type: none">1. Comprehensive Approach2. NEC3. Radio Spectrum Management4. Space5. Single European Sky• EDA must follow EU's Comprehensive Approach development in which the Civil Dimension is very important.• Finalised in Dec 2010, the EDA NEC Implementation Study (NEC IS) proposes the NEC Vision (the "what?") and the NEC Roadmap (the "how?")• Further actions within EDA are: NEC monitoring of related initiatives, preparing an NEC framework and NEC experimentation.• Mechanisms of coordination with NATO are:<ol style="list-style-type: none">1. EU – NATO Capability Group (formal place to discuss)2. Common Member States (21 countries shared)3. Staff to Staff contacts with ACT, IMS, NHQC3S, NC3A, C2CoE• NEC also amongst the coordination topics for EDA and ACT:• EDA also continues to coordinate with industry and NCOIC.
Question (by)
BGen Booman – Dir CIS SHAPE. Is there a mission network? A: <i>The framework Op HQ and Force HQ was developed by nations and brought with them in accordance with the Framework Nation principle. There is nothing similar to the AMN.</i>
Mechanica Group Rep. Please expand on air transportation next steps. A: <i>The aim is to pool and share air for crisis response. Currently not coordinated. Need for distributed tool which could be used for planning and operation of these air assets. Requirement and costs being developed. Depending on costs there will be a demonstrator of the fully fledged tool.</i>

09:05 Service integration & networking in future society, case Finland
Mr. Yrjo Benson State IT Director, CIO
<ul style="list-style-type: none">• Aim to achieve technical interoperability, semantic interoperability, organisational interoperability, legal interoperability with a Political Context.• Description of the Enterprise Architecture• One slide describing Common ICT Architecture – very clear and

<p>understandable!</p> <ul style="list-style-type: none"> • Several successes but some ICT challenges remain: <ul style="list-style-type: none"> ○ Finland not strong on top-down governance in the Central Government and very weak among Local Governments. ○ Central and Local Governments' ICT are not effectively linked. ○ No centralized patient and treatment data base and several Health IT development projects not well enough integrated. ○ Overlapping data collection with name, address etc. is frequently asked, even though they are available in well-managed central online data base. ○ Too often ICT is implemented without improving the underpinning processes and practices. • Tools and processes description pointing out that keeping old ways of working and new tools is the worst, since it costs without producing benefits. • Since he had no definition of "Comprehensive Approach" he produced and described his own.
Question (by)
<p>Italian MOD Gen Bologna – Presented a wide programme – 5M investment. Italy spent much more. How was the programme prioritised?</p> <p>A: <i>(E-services, common IT services, Harmonised IT services, Information security and contingency planning.) Interoperability is No 1. ICT spending in Finland is rising because it is seen as good value</i></p>
<p>IBM. Shared service solution – Please explain.</p> <p>A: <i>Two years ago Finland founded an organisation that channels ICT. These ICT service centres buy and disseminate ICT throughout Finnish organisation.</i></p>

09:40 The Challenges of Command and Control - Human Aspects
Colonel Geerlof Kanis, Director, Command and Control Centre of Excellence (C2CoE)
<ul style="list-style-type: none"> • C2 is developing strongly with technical enablers now available as standard services such as AMN and Link 16. • Main issue is how to exploit to improve Command and control and business process. Understanding human aspects is key. • Human operators are an essential part of these systems and understanding how they perceive and react to information provided is vital. • Need to address four elements: <ol style="list-style-type: none"> 1. Individual characteristics 2. Team roles 3. National profiles

4. Philosophy

- For C2 these can be further grouped under three main aspects:
 1. Situational Awareness
 2. Human Communication
 3. Human Awareness
- There are serious issues associated with communication, understanding and cross-cultural trust.
- Need to beware of pitfalls of using technology:
 - Structural
 - Caused by human perception
- Need to understand the human domain:
 - Humans are defined by their individual characteristics
 - Humans act according their preferred role
 - Humans behave according to their culture, profile and philosophy and it may take decades to change behaviours learned from parents
- Human communication is essential and it is necessary to exploit human communication and understanding.

Question (by)

It takes decades to change mother's programme. Do you think the way we present information will change?

A: There are many options for man/machine interfaces. People do not see the same things. No single solution.

10:45 Swedish experiences from the EU anti-piracy operation ATALANTA

Captain(N) Anders Olovsson

Commander of the 4th Naval Warfare Flotilla, Swedish Armed Forces

- On-going since December 2008 with the following tasks:
 1. Protect World Food Program (WFP)
 2. Protect vulnerable shipping
 3. By presence act preventive against piracy
- EUNAVFOR –MANDATE TO ACT:
 1. Conducted within ESDP (European Security and Defence Policy)
 2. Supported by UN Security Council Resolutions 1814 / 1816 / 1846 / 1851:
- Swedish contribution 2010 (HSwMS Carskrona, support in Djibouti)
- Both NATO and Sweden have systems for war fighting needs such as SSM targeting but other factors are important for operations like ATALANTA:
 1. Systems open for other users, not just NATO or Partner Nations
 2. Effective Recognised maritime Picture (RMP)
 3. Command of units over a vast Area of Operations
 4. Wide and reliable MIL and/or CIV satellite bandwidth: Large amounts

<p>of CONFIDENTIAL data, not least IMINT</p> <ul style="list-style-type: none"> • “The standard NATO way” has many dialects (Link 11, NS WAN etc.). • For a country like Sweden, new solutions every time (both exercises and operations). • SATCOM coverage and costs are big issues. • MERCURY is the only common system, but it is only Unclassified. • If NATO wants non-member support a long term solution must be found for harmonising requirements.
Question (by)
<p>MG Willemse: How many systems are mission specific? A: <i>Not many – most are generic</i></p>

11:20 Cross government integration through technical innovation
<p>Mr. David Waxman IBM Software Group</p>
<ul style="list-style-type: none"> • Australian Defence ICT challenge: <ul style="list-style-type: none"> ○ Too many independent systems ○ Complex and unmanageable ○ Interoperability too hard to deliver – time, cost, and technical issues ○ Costs twice as much, takes twice as long to deliver ICT ○ No control over Defence Information Environment capability ○ Too many stove-piped lines and user interfaces for basic business processes • New Australian CIO said he could not afford to keep operating that way. • New vision was to buy IT like a car, i.e., “the Platform” not as a collection of bits paid for as you go. • Task is now for a glorified plumber. Partners concentrate on the parts on top which interface with the users. • Widespread adoption of the Platform. • Improvements are rolled into the Platform then reviewed by customers. • More and more non-defence organisations are interested in the Platform. Cyber remediation requires minimal changes. A better option would be to roll the changes into the revised Platform. A very similar concept is used for applications. • Australians have 7 instances of this Platform. Allowed 30 days to complete but now takes 3 days for complete SOA Platform.
Question (by)

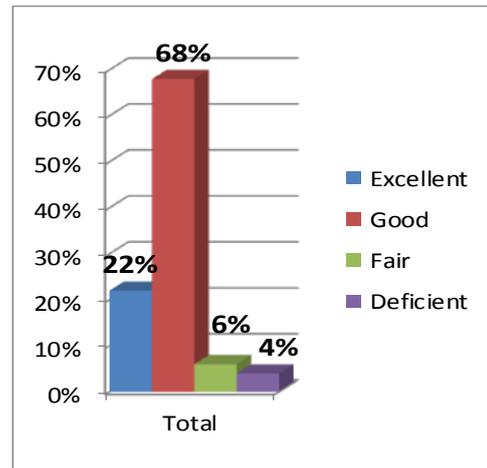
Gen Bologna – Italy. NC3A should follow. Could the agency take this approach to provide a catalogue of full products?

A: Yes, but it needs to be taken up by all players working together

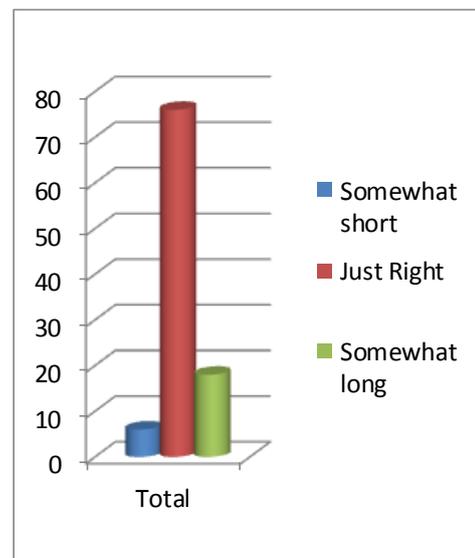
Annex C: Conference Feedback

Conference attendees are annually provided an opportunity to comment on how well the Conference achieved its aims and how well it met the personal expectations of the attendee. This year, 300 attendees (67%) provided responses to the survey, with highlights provided below:

- Attendees expressed a high degree of satisfaction for the conference as measured by the number of responses
Excellent 22%
Good 68 %
Fair 6 %
Deficient 4 %



- The duration of the conference was rated as “just right” by 76 % of the attendees.



- Most of the participants appreciated the operational focus and the reminder that NNEC’s reason for being is to support those in the field. With that said, Technical participants requested more technical discussions and Operational participants requested more operational discussions.
- Many participants requested more practical examples of concepts, prototypes and actual implementations as well as associated lessons learned
- In some cases, sound quality together with personal speaking styles hindered the ability of non-anglophone attendees to fully comprehend the presentations

Annex D: Conference Agenda

Tuesday 5 April – Day One

Moderated by Major General Jaap Willemse, ACOS C4ISR & NNEC, HQ SACT

07:30–17:00	Registration in Conference Lobby
08:15	Administrative Brief and Opening Remarks <i>Major General Jaap Willemse and Lieutenant Colonel Michael Buttler, HQ SACT</i>
08:30	Keynote <i>General Ari Puheloinen, Chief of Defence, Finland</i>
08:55	Keynote <i>General Mieczyslaw Bieniek, Deputy Supreme Allied Commander Transformation</i>
09:20	Keynote <i>Major General Glynne Hines, Director, NATO HQ C3 Staff</i>
09:45	Keynote <i>Dr. Adam Sowa, Deputy Chief Executive, European Defence Agency</i>
10:10	Networking and Coffee Break
10:35	Needs and requirements for network enabled capabilities in multi-agent crisis management operations <i>Mr. Pekka Haavisto, Member of Parliament, Finland</i>
11:10	<i>Comprehensive Approach: NNEC</i> <i>Vice Admiral Carol Pottenger, Deputy Chief of Staff Capability Development, HQ SACT</i>
11:45	An ICRC Perspective on the Comprehensive Approach <i>Monsieur Francois Bellon, International Committee of the Red Cross (ICRC)</i>
12:20	Lunch Break
13:40	Implementing Network Enabled IT Services for NATO's Coalition Operations <i>Lieutenant General Kurt Herrmann, Director, NATO CIS Services Agency (NCSA)</i>
14:15	Net generation's approach to networking and information overload <i>Mr. Teemu Arina, CEO, Dicole OY FIN</i>
14:45	Networking and Coffee Break
15:15	Comprehensive C4ISR Approach <i>Major General (Ret) Georges D'Hollander, General Manager NC3A</i>
16:25	Applying NNEC Concepts to Air Command Control System (ACCS) <i>Dr. Gerhard van der Giet, General Manager, NATO Air Command and Control System Management Agency (NACMA)</i>
20:00–22:30	NNEC Conference Dinner, Congress Center, Fennia Ballroom, 2nd Floor (business/lounge suite)

Wednesday Morning 6 April – Day Two

Moderated by MGEN Jaap Willemse, ACOS C4ISR & NNEC, HQ SACT

08:15	Administrative Brief Lieutenant Colonel Michael Buttler, HQ SACT
08:30	Network Enabled Defence in Finland Lieutenant General Markku Koli, Chief of Defence Command, Finland
09:05	ATOS Origin Presentation Lieutenant General (Ret) Jo Godderij, Former Director General, International Military Staff (DGIMS)
09:40	Information Superiority based on NATO-National Interoperability services Mr. Valery Rousset, C4I capability development, Thales Defence & Security
10:15	Networking and Coffee Break
10:40	NNEC Demonstrator Dr. Alberto Domingo, Deputy Branch Head, C4ISR & NNEC Branch, HQ SACT and Dr. Hermann Wietgreffe, Principal Scientist, NATO C3 Agency
11:15	NNEC Demonstrator / Security Model for NNEC Mr. Geir Hallingstad, Principal Scientist, NATO C3 Agency
11:50	Afghan Mission Network – A practical application of NNEC CAPT John Nankervis & CAPT Mike Horsefield, Branch Head Crisis Response Operations / CPP CAM, HQ SACT and SHAPE
12:20	Lunch Break

BREAKOUT SESSIONS

Wednesday Afternoon 6 April – Day Two

Breakout Session 1: Technology to improve information sharing

Moderated by Colonel Frederic Sakhochian, NNEC Branch, HQ SACT

13:40	Priorities for aligning with future information technology Mr. Rick Parkington, VP & Chief Technology Officer for the Intelligence Solutions Division, General Dynamics Information Technology
14:15	Cloud Computing as an enabler LCDR Patrick Ratier, C4ISR & NNEC, HQ SACT
14:50	Networking and Coffee Break
15:15	Real time information sharing and multi-criteria decision analysis enabled by LTE technology Mr. Frederic Sutter, VP in Charge of Defence markets, Alcatel-Lucent
15:50	Tools to support information sharing & knowledge management Mr. John Redmayne, Principal Operational Research Analyst, NATO Joint Analysis & Lessons Learned Centre (JALLC)
16:25	The Comprehensive Approach applied to situational awareness: A Paradigm shift from data sharing to intelligent data fusion Mr. Lode Missiaen, PhD, CEO and Founder of Luciad

Breakout Session 2: Human Factors and Processes supporting NNEC

Moderated by Dr. Nancy Houston, HQ SACT

13:40	Human Challenges in NNEC Dr. Nancy Houston, C4ISR & NNEC Branch, HQ SACT
14:15	The Comprehensive Approach – Will it accelerate or hinder NNEC? Dr. Peter Essens, Netherlands Organisation for Applied Scientific Research
14:50	Networking and Coffee Break
15:15	How Cognitive differences impact information understanding Mr. Andrew Leggatt, Human Factors Senior Principal Scientist and Group Leader at the Advanced Technology Centre, Filton, BAE Systems (Operations) Ltd
15:50	Introducing the HFI-DTC Consortium and Human Views for MODAF Mr. Richard McMaster, Research Associate, University of Birmingham, UK
16:25	The challenge of creating an ordered information domain Mr. Peter Pharoah, NATO HQ C3 Staff

Breakout Session 3: Cyber Security

Moderated by Mr. Ryan Vacanti, HQ SACT

13:40	Cyber Security in NEC Lieutenant Colonel Nestor Ganuza, Manager of Cyber Security in NEC, Cooperative Cyber Defence Centre of Excellence (CCDCOE)
14:15	Federating Enterprise Security Management Ms Sandi Roddy, Chair of NATO SMI AdHoc WG, Defense Information Systems Agency (DISA), US NSA
14:50	Networking and Coffee Break
15:15	Cyber Defense for Mission Assurance through Mission Oriented Cloud Architecture Mr. Wesley Rhodes, Deputy CTO, IBM Software Group, Strategy & Technology
15:50	Information exchange in multi-level security/cross domain environment Mr. Bernard Roussely, Bertin
16:25	Multi-level security Mr. Don Smith, Dell Inc.

Breakout Session 4: NNEC Practical Applications

Moderated by Mr. David Burton, CTO, NC3A

13:40	NC3A CTO and its role in NNEC Delivery Dr. Paul Howland, Chief Technical Officer – Chief C4ISR, NC3A
14:15	MAJIIC2 – Processes and Technology Lieutenant Colonel Arle Brustad, Chairman of the MAJIIC National Project Officers, Norwegian Army
14:50	Networking and Coffee Break
15:15	NATO Joint Intelligence Surveillance & Reconnaissance (JISR) Step 2 – the Mechanism to Achieve Practical NNEC in ISAF Mr. Casper Wienberg, JISR IPT Lead, HQ SACT
15:50	Presentation CFC / CMO Lieutenant Colonel Michael Hendrigan, Director, Civil Military Fusion Centre
16:25	Underwater Networking Mr. Alessandro Berni, NATO Undersea Research Centre (NURC)

Thursday 7 April – Day Three

Moderated by MGEN Jaap Willemse, ACOS C4ISR & NNEC, HQ SACT

08:15	Administrative Brief Lieutenant Colonel Michael Buttler, HQ SACT
08:30	European Defence Agency and EU NEC Mr. Marcel Staicu, Project Officer, European Defence Agency (EDA)
09:05	Service integration & networking in future society, case Finland Mr. Yrjo Benson, State IT Director, CIO
09:40	The Challenges of Command and Control - Human Aspects Colonel Geerlof Kanis, Director, Command and Control Centre of Excellence (C2CoE)
10:15	Networking and Coffee Break
10:45	Swedish experiences from the EU anti-piracy operation ATALANTA Captain(N) Anders Olovsson, Commander of the 4th Naval Warfare Flotilla, Swedish Armed Forces
11:20	Cross government integration through technical innovation Mr. David Waxman, Chief Technical Officer, IBM
11:55	Summary and Closing Remarks MGEN Jaap Willemse
12:30	End of Programme