



**NORTH ATLANTIC TREATY ORGANIZATION  
ORGANIZATION DU TRAITÉ DE L'ATLANTIQUE NORD**

HEADQUARTERS, SUPREME ALLIED COMMANDER  
TRANSFORMATION  
7857 BLANDY ROAD, SUITE 100  
NORFOLK, VIRGINIA 23551-2490



## **NATO NETWORK ENABLED CAPABILITY**

# **9<sup>th</sup> NNEC CONFERENCE**

**Vienna, Austria, 27 - 29 March 2012**

## **Conference Report**

**contact: NNEC Branch**  
is-nnec@act.nato.int  
<http://nnec.act.nato.int/>



This page intentionally left blank

## Table of Contents

Table of Contents.....	3
Executive Summary.....	4
Aims of the conference.....	5
Key outcomes.....	6
NNEC alive and well, new challenges ahead.....	6
Implementation.....	6
Technical and non-technical interoperability.....	6
Planned implementation.....	7
Interaction with Partners.....	7
Information sharing, management, information assurance and cyber defence.....	7
"Technology" breakout session wrap-up.....	7
"Human Factors" breakout session wrap-up.....	8
"Information Assurance & Cyber Defence" breakout session wrap-up.....	8
"NNEC Practical Applications" breakout session wrap-up.....	8
Conclusion.....	10
Annex A: Conference Facts.....	11
Annex B: Conference Feedback.....	14
Annex C: Memorable quotes and presentation captures.....	16
Memorable quotes.....	16
Tuesday, March 27 <sup>th</sup> , keynotes and plenary presentations captures.....	18
Wednesday, March 28 <sup>th</sup> , plenary presentations captures.....	30
Wednesday, March 28 <sup>th</sup> , breakout sessions presentations captures.....	35
Breakout 1: Technology.....	35
Breakout 2: Human factors.....	37
Breakout 3: Information assurance and cyber defence.....	39
Breakout 4: NNEC practical applications.....	42
Thursday, March 29 <sup>th</sup> , plenary presentations captures.....	46
Annex D: Conference Agenda.....	53
Agenda overview.....	53
Tuesday 27 March – Day One – Keynotes and Plenary.....	54
Wednesday 28 March – Day Two – Plenary and Breakout sessions.....	55
Thursday 29 March – Day Three - Plenary.....	57

## Executive Summary

The 9th annual NNEC Conference “Implementing NNEC: Future Mission Network” took place 27 to 29 March 2012 in Vienna, Austria. It was the second time the conference was held in a Partnership for Peace (PfP) nation after Helsinki, Finland in 2011.

Day 1 set the scene for the remainder of the Conference, demonstrating the importance of NNEC for the development of the FMN (Future Mission Network), as well as achievements and challenges ahead.

The conference was officially opened with keynotes by the Austrian Chief of Defense, General Entacher, developing all dimensions of security for a Partner country like Austria, and DSACT General Bieniek, underlining the key leverage of NNEC for Transformation. They were followed by the Director NATO HQ C3 Staff Major General Fermier on behalf of NATO Assistant Secretary General Defence Investment (ASG DI), who pictured the current global environment, stressing all NATO strains of actions on the NNEC endeavour and by the Capabilities Director of the European Defence Agency (EDA), Brigadier Jonathan Mullin, expressing similar challenges and effective synchronisation between the EU and NATO. Presentations on Cybersecurity and NEC related efforts towards FMN by the host nation, representatives from ACO and ACT, followed by briefs on secure information sharing and how NNEC challenges were met by the Director of NCSA and General Manager of NC3A completed the government and Alliance views.

Those views were complemented with industry briefs by Google, ATOS, and IBM, emphasizing the relevance of information sharing as pivotal to the military as well as to the civilian, making sense of information, and the opportunities borne by newer technologies, setting the frame for the following two days.

Day 2 started in plenary format with key presentations further investigating challenges and solutions, and continued in the afternoon in breakout sessions format, focusing on the key areas of Technology, Human Factors & Processes, Information Assurance & Cyber Defence and NNEC Practical implementations.

Day 3 was held in plenary, with final briefs of global interest, further examples of practical NNEC implementations and the wrap up of the conference, stressing the achievements as well as the challenges ahead.

The Conference continues to provide a key forum to the various communities of interest for the sharing and exchange of information and ideas and thinking the way forward, as outlined in the key outcomes of the conference. There was a general understanding that NNEC, and its next emblematic implementation FMN, can never just be a technical solution: education, training and exercises will play an essential role in enabling seamless collaboration in future missions.

This report also incorporates some follow-on actions derived from the Conference.

The 10th NNEC Conference, “coNNECTing Forces”, will take place in Portugal, in early Spring 2013. The theme has obvious reference to the Connected Forces Initiative, stressing the active actions needed to effectively connect Forces in a comprehensive approach.

## Aims of the conference

NNEC is about people first. The NNEC conference is NATO's key event to inform and exchange information and ideas on the development and way ahead of NNEC, defined as "the Alliance's cognitive and technical ability to federate the various components of the operational environment from the strategic level (including NATO HQ) down to the tactical level through a networking and information infrastructure", along the lines of NATO's political guidance and strategic concept.

The NNEC concept is widely supported and accepted as the Afghanistan Mission Network served as a proof of concept. Information sharing is becoming the rule rather than the exception, and the central message conveyed by the conference is the necessity to share information, which brings implications for all stakeholders to enable an information-sharing environment, with associated doctrine, policy and processes. The increased amount and flow of information requires new ways of providing the right and relevant information at the right time to the right people, as well as new ways of protecting it, in relation to cyber defence.

Information sharing is therefore fragile, as it builds upon trust.

NNEC is also about policy and doctrine, processes and technology; nevertheless, technology is an enabler to share more relevant information for better decision-making as well as being able to communicate intent and instructions. Industry participation is essential to show the latest approaches to information assurance, technology, processes and human factors to reach more effective and efficient communication and collaboration, as well as providing an opportunity to develop better understanding of current NATO challenges by industry.

As a summary, generic goals of NNEC Conferences are to increase the understanding of NNEC and show progress, to encourage and support information sharing and collaboration, to propagate the necessity of NNEC for mission effectiveness, to initiate and support networking, cooperation and collaboration amongst the different Communities of Interest, and finally to emphasize the non-technical aspects of NNEC.

For the 2012 Conference, a specific goal was to show progress and status on the various aspects of operationalizing and implementing NNEC, as the first emblematic practical implementation of NNEC was achieved with the Afghanistan Mission Network.

Another specific goal was to prepare the ground for the Future Mission Network, and how the Alliance may achieve the next emblematic implementation of NNEC through planned capabilities. Identifying the best trade-off between scope and time, under budget constraints, while underlining how continuous development in the field of NNEC serves as a baseline for initial and also subsequent instantiations of FMN.

The theme "Implementing NNEC: Future Mission Network" and the Conference agenda were designed accordingly. Forty-five presentations from Nations, NATO entities, academia and industry developed different aspects of or in relation to NNEC and FMN. The complete Agenda is provided in Annex D.

## Key outcomes

### NNEC alive and well, new challenges ahead

As initial expectations for NNEC may have been perceived and possibly even formulated at some point in time in the broadest and most ambitious extent, the 2012 NNEC Conference was essential in pointing out the achievements of NNEC, and having everyone realize that initial goals were met.

NNEC Tenets and Principles have permeated all aspects of capability development, the paradigm has effectively shifted from “need to know” to the “need to share - share to win” acception, pointing out the need for information sharing for mission effectiveness and efficiency in a coalition environment and comprehensive approach context.

Most importantly, the Afghanistan Mission Network served as first emblematic implementation of NNEC, as well as proof of concept.

The 2012 NNEC Conference helped spread the realization that the initial goals for NNEC have been achieved, and that these achievements are fragile. It also helped identify new challenges ahead on the path to the ultimate NNEC goal as political guidance develops. Next emblematic steps will be made with the first instances of Future Mission Network, building on the solid ground that the NNEC strategic framework has developed over time.

### Implementation

As shown in the NNEC compliance assessment of AMN, conducted using the NNEC Criteria, the implementation part was the most difficult, reflecting the fact that part of AMN was procured through CUR (Crisis Response Urgent Requirements). Implementation is a difficult topic when it comes to federating various systems, it relates to both C3 and program governance in NATO, and is probably today’s greatest challenge facing FMN. Pragmatism, aiming at simple “80%” solutions, a strong will to be even more outcome focused, will be needed when integrating the planning process of the NDPP to ensure success, e.g. using NNEC ‘federability’ criteria and as the NATO Communications and Information (NCI) Agency is established on July 1<sup>st</sup> later this year. It is anticipated that under the FMN concept, different instances Mission Networks will be needed to address different types of operations, and also benefit from specific initiatives addressing key Community of Interest challenges as JISR for example.

### Technical and non-technical interoperability

Interoperability is not just about technology; nevertheless technology is an enabler. Faster adoption of standards, whether they be specific or open, and good use of technology - making the most of existing, emerging and potentially disruptive technologies, were identified as key future challenges as civilian information technology lifecycles become somehow cogent, stressing the need for appropriate engagement with industry.

Tools already exist, such as the Framework for Collaborative Interaction (FFCI), Technology for Information, Decision and Execution Superiority (TIDE) Sprint or multi-purpose events such as Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX), or the Steadfast series of exercises.

Ultimately, interoperability is non-technical; it is about people, and their ability to effectively work together whatever tools and systems they use. The importance of Joining and Exit instructions for example was seen critical in the AMN success. It is essential to address the human factors aspects, as cognitive limits could be reached by information overflow, and taking into account the characteristics of 'Generation Y' raised with social media, and the importance of social media in today's world. Education, training and exercises – tools for proven interoperability – should become, as the operational tempo decreases, the surest way not only to retain but also develop operational interoperability and effectiveness achieved by Allies.

All actions for maintaining trust are essential as it is only upon trust that information sharing is possible.

### Planned implementation

Under the budget constraints faced by many member nations, planning coherence of national (including headquarters) and NATO capabilities becomes even more acute, and may foster re-use of NATO solutions amongst Allies and possibly partners as appropriate. Again, education, training and exercises need be reinforced to ensure achieving this coherence as the operational tempo decreases. These also contribute to maintaining awareness on the value of NNEC tenets and principles, and trust.

### Interaction with Partners

As outlined at the Lisbon summit, the involvement of Partners is a strategic part of successful operations. Appropriate interaction with Partners, as well as international, government or non-government organizations and addressing the non-military aspects of the comprehensive approach brings challenges to the constructs of NNEC capabilities that will be addressed in the FMN development.

### Information sharing, management, information assurance and cyber defence

Finally, in a context of extended information sharing of information, new challenges arise in information management as we reach cognitive limits of human beings and challenge cognitive abilities of organizations, in information assurance as newer models are needed, with an obvious extension to cyber-defence.

### "Technology" breakout session wrap-up

As dependency on information increases and budget constraints strengthen, the technology breakout session showed the added value new technologies can provide:

- making the most of existing systems (cost-efficiency) with examples on mobile radio networking
- increasing NEC systems resiliency and availability with examples on monitoring mixed satcom – infrastructure networks and complements to satellite positioning systems
- pointing out potentially disruptive emerging technologies with an example on nano-satellites.

### "Human Factors" breakout session wrap-up

The human factor is essential. Entering the information age calls for change management to address the human-related issues including policy, processes, organisation and training.

The importance of taking into account the prominence and potential of social media was outlined, all the more as now most soldiers belong to 'Generation Y', and are used to using tools characterized to some extent by a sense of community and a level of trust.

Trust in shared information, situation awareness, and more generally, a sense of community is essential.

Key points from the session:

- human issues are the most difficult to address (and perhaps why the focus keeps returning to the technology component of networks)
- information sharing is a behaviour not a technology, there should be an 80 / 20 focus on people / technology
- NATO interoperability would benefit from a holistic approach to planned information sharing. A high-level mandate is needed to address organizational, policy, procedural & training issues
- social tools (including chat) are key in supporting situation awareness and contribute to the development of human trust and networks.

### "Information Assurance & Cyber Defence" breakout session wrap-up

The information Assurance & Cyber Defence breakout session highlighted the validity of the following approaches:

- keeping bad things out and secrets in
- when possible, have plans to restrict disruption
- renew efforts to amend / modernise / refine policies
- balance risk against usability, the 100% solution does not exist, push for 70 / 30
- there is no single solution, one size does not fit all
- pursue combination solutions that together provide confidence.

### "NNEC Practical Applications" breakout session wrap-up

The NNEC practical implementation breakout session was essential in showing a broad panel of NNEC implementations, and most importantly in identifying the following success factors from the various lessons learned:

- clarity of vision: built on strong leadership and change management
- community of interest: owning the business, sharing common values and trust
- business intelligence, critical to effective governance
- coherence, covering programmatic and technical aspects
- outcome focus
- pragmatism: legacy, incremental development

- strategic risk management, addressing business value and impact
- access management (including cross domain) to critical data
- appropriate industry engagement
- consider best of breed solutions, *de facto* standards.

As a conclusion, staying agile and ready to react is key since threats morph as solutions are found. Some potential is seen in solutions where information is tagged rather than networks.

## Conclusion

The NNEC Conference remains an extremely valuable C2 community venue. It allows the sharing of NNEC progress updates, a broad exchange of views and investigation of the way ahead. The outcomes of the NNEC Conference show the importance of NNEC at the core of ACT activities, covering most areas of the ACT trident. This includes increased shared awareness of challenges ahead, influencing the way forward for all stakeholders and opening a yearly cycle with other events such as CWIX, Tide Sprint, Industry Days, the Steadfast series of exercises to name a few. All of which loop back into the following year's Conference.

The 9<sup>th</sup> NNEC Conference also provided input for some of the items discussed at the Chicago summit.

The 10<sup>th</sup> NNEC Conference will address and explore the relevant Chicago Summit guidance and decisions. The theme will be "coNNECTing Forces", in obvious reference to the Connected Forces Initiative, stressing the active actions needed to effectively connect Forces in a comprehensive approach. It will take place in Portugal, in early Spring 2013.

## Annex A: Conference Facts

The 9th NNEC Conference was co-hosted by Allied Command Transformation (ACT) and the Austrian Ministry of Defence. The Conference was attended by 415 people from NATO, Nations, industry and international organizations, as detailed below.

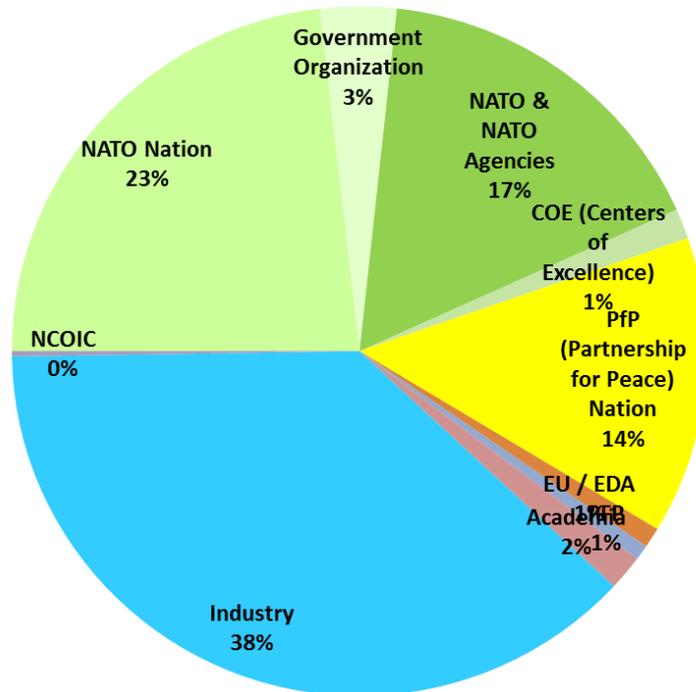
It is to be noted that despite the budget restrictions in the current difficult economic situation, attendance was high again, above 400, demonstrating strong enduring interest and support in NNEC and this year's theme of Future Mission Network.

A few key figures:

- 415 attendees
- 45 speakers
- 25 of 28 NATO nations represented
- 10 PfP Partner nations represented
- 167 Industry representatives
- 4 Representatives from the EDA

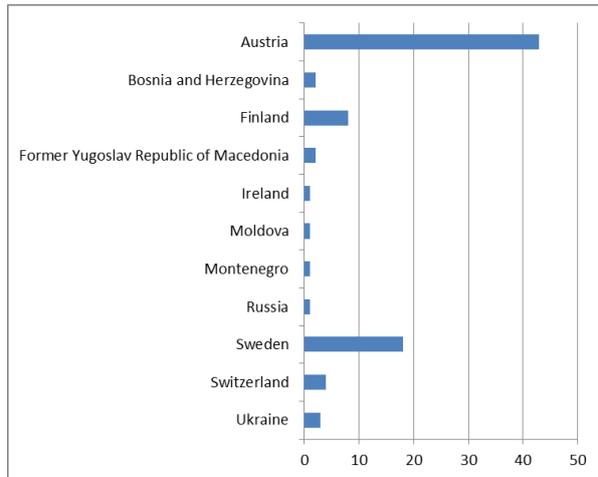
Attendee information on the 2012 Conference is listed and depicted below.

### Attendance by category:



**Attendance by Partner Nation location:**  
(includes national representatives, industry...)

Austria	43
Bosnia and Herzegovina	2
Finland	8
Former Yugoslav Republic of Macedonia <sup>1</sup>	2
Ireland	1
Moldova	1
Montenegro	1
Russia	1
Sweden	18
Switzerland	4
Ukraine	3
<b>Grand Total</b>	<b>84</b>

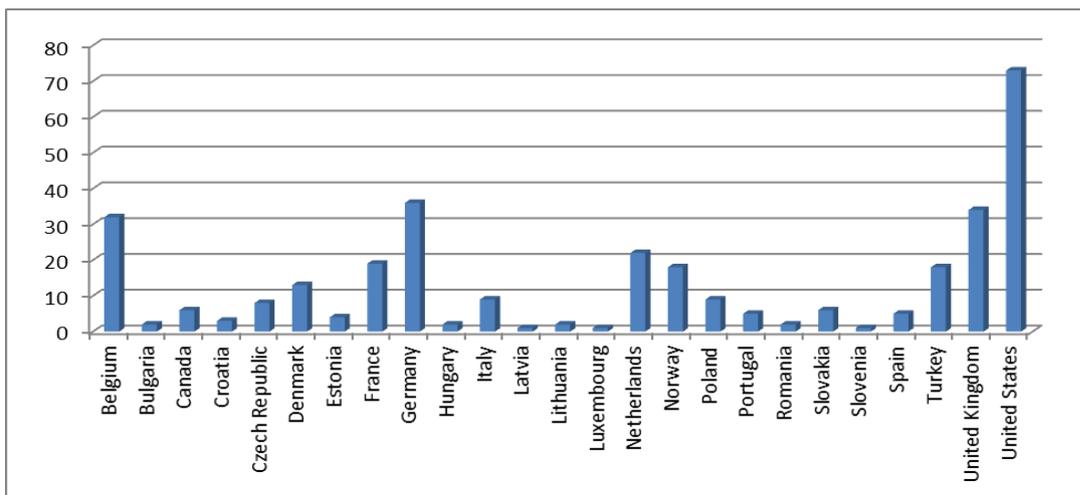


**Attendance by NATO Nation location:**  
(includes national representatives, NATO bodies, industry...)

Belgium	32
Bulgaria	2
Canada	6
Croatia	3
Czech Republic	8
Denmark	13
Estonia	4
France	19
Germany	36

Hungary	2
Italy	9
Latvia	1
Lithuania	2
Luxembourg	1
Netherlands	22
Norway	18
Poland	9
Portugal	5

Romania	2
Slovakia	6
Slovenia	1
Spain	5
Turkey	18
United Kingdom	34
United States	73
<b>Grand Total</b>	<b>331</b>



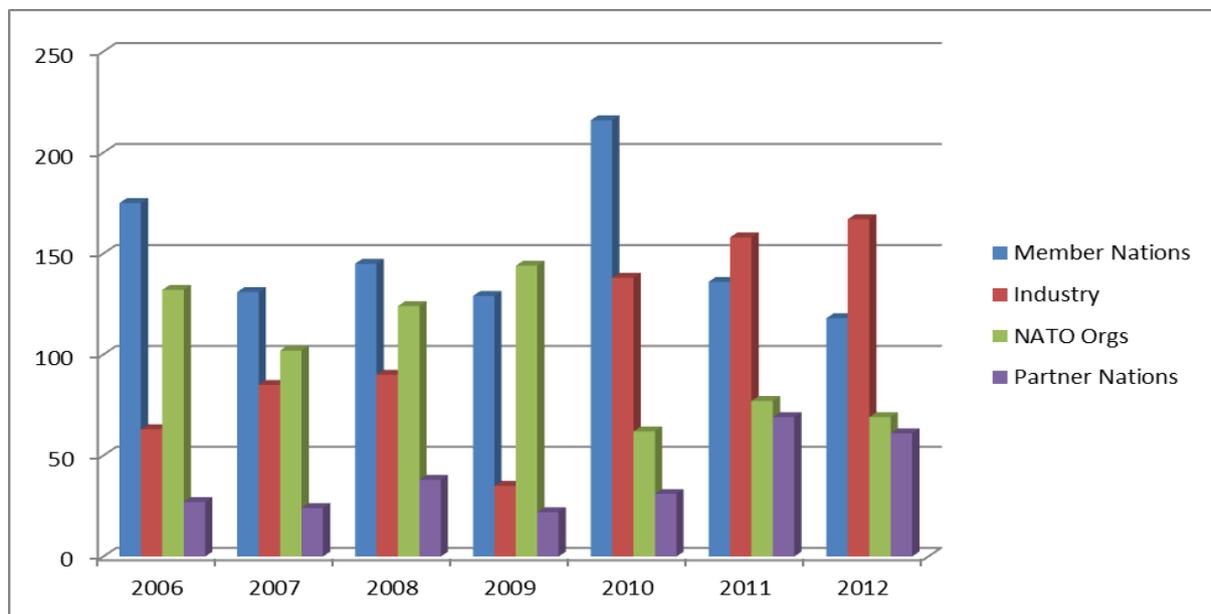
<sup>1</sup> Turkey recognizes the Republic of Macedonia with its constitutional name

**Yearly Comparison:**

Except for a slight decrease most certainly due to budget restrictions, the overall interest in the NNEC Conference remains very high, with again over 400 participants.

The following yearly comparison shows participation by main categories (smaller categories are incorporated by their location, in Nato nations or Partner nations):

	2006	2007	2008	2009	2010	2011	2012
Member Nations	175	131	145	129	216	144	118
Industry	63	85	90	35	138	158	167
NATO Orgs	132	102	124	144	62	72	69
Partner Nations	27	24	38	22	31	67	61
<b>Total</b>	<b>397</b>	<b>342</b>	<b>397</b>	<b>330</b>	<b>447</b>	<b>441</b>	<b>415</b>



The graph above depicts an increasing participation of industry as well as Partner nations, while the level of participation of member nations is rather constant once taken into account location effects (the 2010 Conference was held in Rome, Italy).

NATO organisations obviously suffered from budget cuts in 2010, nevertheless, participation stabilized for the 2012 NNEC Conference despite the ongoing agency reform, a further indication that NNEC remains a major topic of interest.

## Annex B: 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, 232 attendees provided responses to the survey, which makes it reliable, with highlights provided below:

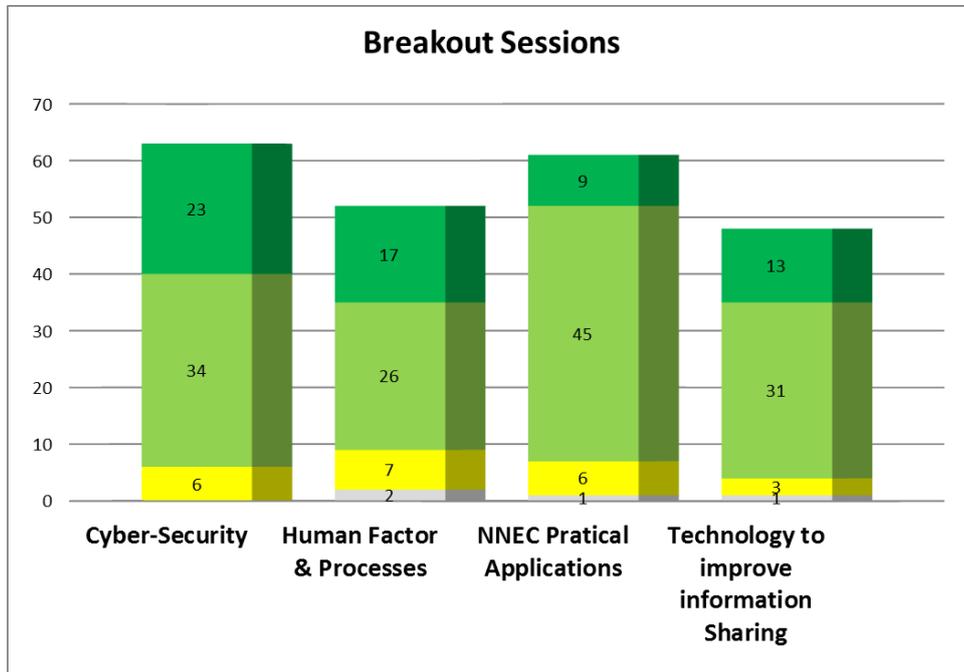
Attendees expressed a high degree of satisfaction for the conference as measured by the number of responses:

- Excellent 28%
- Good 60%
- Fair 10%
- No comment 2%

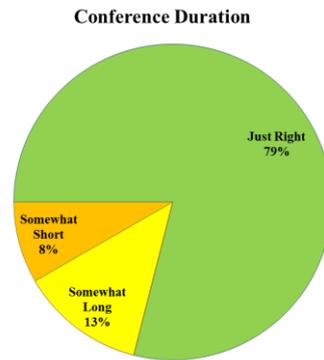
**Overall Conference Evaluation**



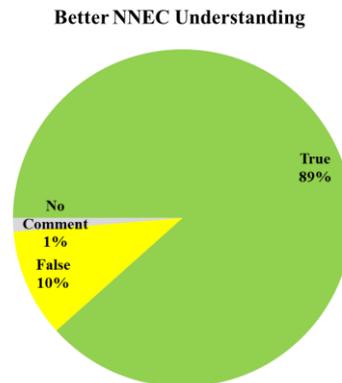
The satisfaction for the breakout sessions was similarly very positive:



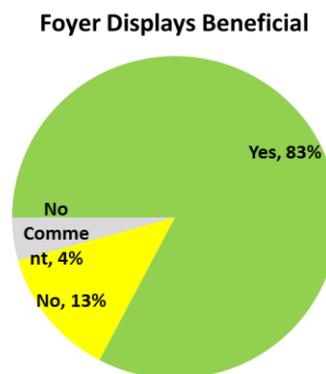
The duration of the conference was rated as “just right” by 79% of the attendees, with a split reminder of whether the conference was somewhat short (8%) or somewhat long (13%):



Almost 90% of participants thought the Conference reached its aim of better NNEC understanding:



Over 80% of participants thought the foyer displays by industry or government were beneficial:



Most of the participants appreciated the operational focus and the reminder that NNEC’s reason for being is to support those in the field, covering both technical and operational aspects.

Some participants also requested more practical examples of actual implementations as well as associated lessons learned.

All survey feedback is fully appreciated and taken into account in preparation for the following year’s NNEC Conference.

## Annex C: Memorable quotes and presentation captures

### ***Memorable quotes***

GEN Edmund Entacher – CHOD Austria

Recognized.....the **‘need to adopt a common information framework’**

Characterized the NNEC Conference as..... **‘important’** in terms of..... **‘information and the requirements to improve interoperability’**.

GEN Mieczyslaw Bieneck – DSACT

Described NNEC as..... **‘a way of doing business’** and **‘a multi-dimensional concept’**

Characterized NNEC as..... **‘part of a comprehensive process’** leading on..... **‘how we move forward with NNEC in the context of Future Mission Network(s)’**.

MGEN Patrick Fermier

Recognized.....that **‘transformation is taking a more important role in alliance business’**

Noting that..... **‘NNEC is being integrated’** in capability development and expressing the opinion that NATO..... **‘offers the best venue for collective efforts’**.

BGEN Jonathan Mullin

Recognized NNEC as ..... **‘The most important capability’**

As it is..... **‘the leverage effect of joining together’** and underlined the need to..... **‘emphasize the win-win nature’** of NNEC.

MS. Michele Weslander Quaid

Made the statement..... **‘Collaborate or Die’**

Focusing on the need to..... **‘innovate’** and **‘regulate the outcome not the technology’**, encouraging NATO to..... **‘have the courage to take the risk and make the best decision we can with what we know now’**.

MGen (ret) Georges D'Hollander

Recognized that NNEC needs to be.....' **ready to face new challenges**'

Characterized the NNEC Conference as..... '**an important opportunity**' in terms of building..... '**trust and a community among nations and industry and to collectively communicate the way-ahead**'.

LtGen (Ret) Jo Godderij

Informed the NNEC Conference that the AMN is..... '**supporting a lot of the NNEC Vision**' supporting the premise that..... '**Partnership with NATO / nations / partners is essential**'

NNEC Conference 2012 also provided a platform for discussions on Cyber Defence, NATO's Future Mission Network(s), Secure Information Sharing, Industry engagement, NNEC as a vehicle for FMN development, Social media and many other topics.

*disclaimer: This was a deliberate decision of the conference staff to provide some capture of the presentations and discussions. The captures are “a” record of briefs and discussions. They represent the interpretation of the writers and not necessarily the official views. Should there be any specific comment, please contact the NNEC Branch staff.*

**Tuesday, March 27<sup>th</sup>, keynotes and plenary presentations captures**

<b>Presentation Title:</b>	<b>Keynote</b>
<b>Presenter:</b>	<b>GEN Edmund Entacher, CHOD Austria</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Austria is a NATO PfP nation.</li> <li>- The military used to work with flags and hand signals - interoperability was simple.</li> <li>- However, we now operate on a much larger technological stage and interoperability has become more complex in the information age</li> <li>- Asymmetric warfare requires a different approach to provide a truly comprehensive common operational picture. We have to be aware of civilian requirements as well as military. Interoperability has become the central requirement and challenge of the 21<sup>st</sup> century. NNEC stands for C2 supported by state of the art. We need a common information framework and pursue a willingness to share a precondition for cooperation. This conference is important as it deals with information and the requirements to improve interoperability.</li> <li>- PfP goals are pursued in an active manner. Austria participates in the C3Board.</li> <li>- Pleased to host this year’s NNEC conference</li> </ul>

<b>Presentation Title:</b>	<b>Keynote</b>
<b>Presenter:</b>	<b>GEN Mieczysław Bieniek, Deputy SACT</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Recognition of the growing importance of industry and academia to NATO</li> <li>- As new threats emerge, having the ability to change and adapt in an agile way is essential</li> <li>- Today’s economic environment demands that we do the same work with fewer resources</li> <li>- NNEC acknowledged as a way of doing business, a multi-dimensional concept</li> <li>- This new way of working requires involvement of all partners</li> </ul>

	<p>resulting in a network that allows unprecedented flow of information</p> <ul style="list-style-type: none"> <li>- While AMN represents best current capability, room for improvement. We must work together to give free and unobstructed flow of information to enable soldiers and decision makers</li> <li>- In times when our children are communicating in real-time it should not be so daunting for the military to do the same, but we need to be aware of security needs. The next two days will give us the chance to look at how we move forward NNEC in the context of Future Mission Network.</li> <li>- It is the expertise of this audience that will benefit us over the next few days</li> <li>- We need to look at NNEC as part of a comprehensive process</li> <li>- More important than technical solution is the will of us all to improve information sharing</li> </ul>
--	---

<b>Presentation Title:</b>	<b>Keynote</b>
<b>Presenter:</b>	<b>MGEN Patrick Fermier, Director NHQC3Staff, for ASG DI</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- We live in a globalized world with international connectivity</li> <li>- Technology and Social networks are pervasive. The Arab Spring was powered by social networks without the reliable power and technical infrastructure that we are used to in the western world.</li> <li>- Current economic times requires us to be more flexible and efficient in our employment of technology</li> <li>- We need to get better at doing SMART business</li> <li>- Doing more by doing it together</li> <li>- NNEC is being integrated into NDPP</li> <li>- Following 2011 political guidance transformation is taking a more important role in alliance business.</li> <li>- NATO needs the ability to connect all forces, training education, joint exercises, better use of technology</li> <li>- Better use of NATO standards and the need to shift from a more theoretical approach to more practical approach</li> <li>- We need to plan for an all-inclusive effort at short notice. Robust scalable infrastructure</li> <li>- Collaboration and partnership are essential. Complex challenges affect all of our nations and require close international cooperation. NATO offers the best venue for collective effort but we need to and can do better</li> </ul>

	- Go beyond WWW. NATO needs a network where coalition can plug and play – in the context of FMN it should be possible. It is time to do what the rest of the word does and plug and play.
<u>Question (by)</u>	<u>Answer</u>
MGEN Willemse – CFI: isn't time for NATO to move away from STANAGS and toward industrial open standards to achieve PLUG and PLAY	The answer is not black and white because we have some unique systems such as the link 16. But we need to move toward open standards where feasible. We also need to protect, to analyse how civilian sector achieve the balance between protect and share. We may be protecting too much of our system. 75% standards should be civilian 25% need to be military
Mr. Mark Clark – Raytheon – in Afghanistan and Libya are there things where networks helped or where they fell short that you would like to tell industry NNEC is feasible if nations change policy. Has this changed?  NCSA - CIS systems have short duration. Are our decision making processes still appropriate	Libya was different to Afghanistan because we used the NCN infrastructure in Europe. This showed NATO network is valid. But would like to get some idea from industry how you work. Need closer link between old business and new one (internet companies). We need some experienced eyes to help benefit from new ways (younger). We need to adapt.  Short answer is no but maybe for a good reason. Money is limited decision on security lead to different way of spending money. We need to explain what is at stake without changes. What is the consequence of the change? If you design a system with security first the system is old, we need to think sharing first and then add security. The answer is balance. When AMN was put in place security was zero. After a while it was enhanced. We don't want to put in place a system with full security.  No. The cycle to acquire a new system is 6-7 years. Regulations do not allow to quickly put new systems in place. Today the rules in NATO cannot allow for quick wins. We use CUR for urgent requirements but it is three years instead of 7 years. Most of what is in ISAF is result of CUR. We need to explain why we want to change the process. We need help from industry to convince resource community and political leaders.

<b>Presentation Title:</b>	<b>Keynote</b>
<b>Presenter:</b>	<b>BGEN Jonathan Mullin, Capabilities Director, EDA</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Most important capability is NEC. Joining together leverage</li> <li>- Governance is critical in transformation.</li> <li>- For the EU NEC, the aim was to define the EU aspects in order to get away from the technical side by transforming the way information is handled and to enhance comprehensive approach</li> </ul>

	<ul style="list-style-type: none"> <li>- In theory if you join systems together it will all improve. People, processes, and technology all have their own challenges.</li> <li>- Concept was delivered in 2008 and was in the top 12 priorities</li> <li>- EDA carried out a NEC implementation study. Aim was to allow EU to define where to go. Addressing people, processes, and technology. Now report is being staffed</li> <li>- Maritime surveillance networking example: twin track with technical and people they developed a concept for the people track of NEC. A personality thing building trust with people in many agencies. Had to demonstrate a win-win for cooperation and building maritime operational picture. Have some tools to support development and tracking</li> <li>- Experimentation test evaluation – looking at civ mil information sharing</li> <li>- Operational aspects need to be addressed – cites McCrystal article and the need to move from layered military structure to network of people (empowerment, trust, initiative, competency) created a feedback loop.</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
MGEN Willemse – What challenges do you face as you engage in the EU about NEC	The first problem is the term NEC. It is seen as a military thing. You have to emphasize the win-win nature of it. Where we have been successful in engaging working level at workshops that you are achieving a good common cause. MARSUR has been a good example because it really engaged the working level.
MGEN Fermier – About FMN. Is there an EDA FMN initiative	In terms of the EU there is an operational WAN, but that is not the same as an FMN. I think we are at a pause where people need to decide what to take forward in the EU. The critical piece is that we don't duplicate but reinforce or add value.
Mr. Peter Hatchard – Some examples of governance as part of NEC	Political and Security committee, DG MARE in maritime. Question is how to bridge the gap between all of the parties.

<b>Presentation Title:</b>	<b>Secure Information sharing in support of Operations</b>
<b>Presenter:</b>	<b>Ms. Michele Weslander Quaid, CTO Google</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Collaborate or Die</li> <li>- AS CIO under Ambassador Negreonte saw the problems of multiple networks. One common network in unclassified world is internet</li> <li>- We must Innovate - Regulate the outcome not the technology. Need to rewrite policies to describe objective end state; we need</li> </ul>

	<p>mobile, social, cloud. Enterprise 2.0 (IT-consumers).</p> <ul style="list-style-type: none"> <li>- Consumer 3 times faster than business, business 3 times faster than government</li> <li>- Mobile: productive from any device, geo/location based awareness</li> <li>- Collaboration - share links at data level; trust (set permissions flexibly) add connections flexibly, inherently social fine-tuned sharing</li> <li>- Geo – providing context, more than just imagery, geo relevant search, visualization, RSS feeds, UDOP: User Defined Operational Picture (showed demo)</li> <li>- Cloud – host data centrally, key is hosting by company strong in cyber security, using modelling of normal and abnormal behaviour to find anomalies in the system, sharing data, keeping context or methods secret</li> <li>- Culture Policy, Technology. – Culture is hardest to change. Have to change culture to change policy</li> <li>- Accept commercial solutions, secure at data layer not network layer</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
LCL David Cathro – Do you think NATO has the culture and leadership to take on the challenges you highlighted	I see the vision and I see the will. The leaders are setting that vision. Don't analyse the problems for too long and don't wait for a 100% solution. Let people use what you have and innovate as they can. We must have the courage to take the risk and make the best decision we can with what we know now. Someone has to stand up and say I will buy the risk.

<b>Presentation Title:</b>	<b>Cyber Security Austria – Civil and Military Activities</b>
<b>Presenter:</b>	<b>BGEN Helmut Habermayer, Austrian MOD</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Cyber Security makes a complete picture of civilian and military possible.</li> <li>- Cyber-attacks can be used to reach a political goal, can be surprising and have immediate effect ,</li> <li>- Assessment of the future is impossible, but the threat is rising</li> <li>- Austria tries to be active with the European process of governments in the cyber security process (exercises) look to future cooperation with other nations and NATO)</li> <li>- Building up cyber security capability in all ministries. Defence leads because of already working on IT security</li> <li>- Working groups on cyber security</li> <li>- A risk matrix for cyber is being developed to helps guide</li> </ul>

	<p>capability</p> <ul style="list-style-type: none"> <li>- Working group on awareness to increase awareness of risk and measures for defence (anti-virus, back ups)</li> <li>- Objectives: be world innovator in cyber defence</li> <li>- Roadmap calls for agreement to strategy this summer and then development from there</li> <li>- Military activities: organizational structure for cyber, MNE cooperation, participate in COE, and Combined Endeavour, work with agencies and research (KIRAS – government with public to define requirements, industry to provide products)</li> <li>- MOD is working Cyber Attack Information System CAIS. Supposed to be a public/private cyber management tool, includes malware detection, traffic detection and infrastructure tracking. Main issue now is network</li> <li>- Currently strong divided between military and civilian, but would like to cooperate. Four options for working together: military nucleus, military assistance,</li> <li>- Need a cyberspace operations unit</li> <li>- Need whole of government approach, not just technology</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
MGEN Willemse – Is Austria pursuing offensive capability with others or on its own	If you want to defend you have to have offensive capabilities. We are working with other institutions and we don't want to have it all done alone. I don't think it is even possible alone.
LTGEN Hermann – How are you preparing personnel for continuity with knowledge in cyber defence	Military has its own education courses for ICT, so we are bringing up technically trained specialists. From our perspective in taking part in operations we have enough cyber security personnel already to provide specialists for these exercises. If it is needs we will bring up additional personnel.

<b>Presentation Title:</b>	<b>Operational Perspective on the NATO Future Mission Network</b>
<b>Presenters:</b>	<b>CAPT Horsefield (ACO) and CAPT Leca (ACT)</b>
Summary of major themes and points:	<p>CAPT. Mike Horsefield</p> <ul style="list-style-type: none"> <li>- Think of services as bricks. I don't want a federated network I want to create the ability to federate</li> <li>- What are the brick interfaces for FMN? Governance, Joining and Staying, Operational (together, organized, sensible), Technical, Future</li> <li>- CCOMC Comprehensive Crisis Operations Management Centre) – predictive horizon scanning, cyber security, Lessons</li> </ul>

	<p>Learned from OUP, better interaction with international partners CAPT. Jean-Francois Leca</p> <ul style="list-style-type: none"> <li>- FMN is to be able to connect people to be able to work together as necessary</li> <li>- Need core services</li> <li>- Not looking to create federated network but the ability to federate</li> <li>- Any capability should be tailored for a specific mission</li> <li>- Future operations will be coalition based FMN must deal with this</li> <li>- Must use the planning scenarios, use different assets, deal with threats, cope with changes in technology</li> <li>- Will be based on DOTMLPFI</li> <li>- Will need flexible organisations, Will need to address federated training audience, material asset, leadership support,</li> <li>- Lego's should allow the easy combination of partners and assets</li> <li>- FMN should be pragmatic, taking what we can and adding where we can</li> <li>- Next Step – Concept by mid-2012</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
<p>Mark Clark (Raytheon) – Do you see one network being able to go from major war to small operation</p> <p>Based on AMN how do you see all of these issues – STANAGs vs Commercial standards</p> <p>What about the UDOP from the Google presentation?</p>	<p>(MH) let's talk security domain instead of networks. You will have a different security domain for different operations. I think you are talking about a solution rather than a requirement. If nations have the ability to federate it doesn't matter because if they have the same rule set they will be able to connect to whatever network they want.</p> <p>(MH) we don't use STANAGs in AMN we use NISP NATO Interoperability Standards Profile. As an operator I don't have solutions I have requirements</p> <p>(MH) I think the answer is yes. They have militarized some Google solutions for AMN. The trouble is with different proprietary standards that keep you using the same product once you start.</p>

<b>Presentation Title:</b>	<b>Comprehensive Crisis Management</b>
<b>Presenter:</b>	<b>COL Luc Le Blanc For BGEN Booman, Director CIS, ACO</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- The joint brief gave the shared view of SHAPE and ACT</li> <li>- We must take into account new threats.</li> <li>- Economy requires us to work with 40% fewer personnel. New NATO C&amp;I agency will be stood up in 100 days</li> </ul>

	<ul style="list-style-type: none"> <li>- Modern crises cannot be handled by military alone. We have to utilize a comprehensive approach CCOMC is an operations centre where the UNCLAS network will become the business network. It is interesting to consider the consequences. Some nations are already using LL from ISAF and OUP to change their own ICT. If we do not address the NNEC challenge we will cease to be useful</li> </ul>
--	---

<b>Presentation Title:</b>	<b>Secure Information Sharing in NATO-led Coalition Operations, Operational Experiences from Managing Federated Networks in Coalition Operations</b>
<b>Presenter:</b>	<b>LTGEN Kurt Herrmann, Director NCSA</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Provision of end-to-end secure CIS services in a cost-effective way for ISAF, Maritime and other OPs</li> <li>- Implementation of a Service Management Framework based on industrial standards</li> <li>- Service Management Framework (SMF) covering toolset and training has been implemented for AMN</li> <li>- Operation &amp; Maintenance of the big variety of NATO and national Functional Area Services (applications) is demanding (Interoperability, SOA, Governance, Data Management)</li> <li>- Cyber Defence Services (System Engineering, Incident Response, and Vulnerability Management) are challenging in an integrated, federated environment. CD is structured top-down (centralized governance, decentralized execution)</li> <li>- FMN requires robust network (bandwidth, IP-based)</li> <li>- Adaption of current web-based and cloud-based services over an IP-based infrastructure</li> <li>- Consistent CD requires cooperation and collaboration with nations, NGO, IGO, etc.</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
What is your view on outsourcing in terms of the FMN? (IBM)	Mobile (deployed) part needs to be augmented by the NATO force structure. Central (stabilized) part is an ideal part for outsourcing solutions to provide cost-effective services. However, operational commanders need to maintain control.
MGEN Willemse. What is the No.1 issue in the implementation of FMN?	To make best use of existing capabilities and industry best practices while keeping the architecture open. Cyber Defence remains a focal point.

<b>Presentation Title:</b>	<b>Are the NNEC Challenges met?</b>
----------------------------	-------------------------------------

<b>Presenter:</b>	<b>MGEN (ret) Georges D'Hollander, General Manager NC3A</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Most of the NNEC challenges identified in 2003 (shift from need-to-know to need-to-share) were met, however we have to face new challenges</li> <li>- AMN was a quick-fix initiated by the in-theatre commander to overcome the pressure of war. NATO was not prepared to provide a capability off the shelf to support any of the recent operations. NATO needs to be prepared for future operations.</li> <li>- We should focus rather on key principals (how do we do things?) then on technology and details on the solution</li> <li>- NNEC Conference is an important opportunity to build trust and a community among nations and industry and to collectively communicate the way-ahead</li> <li>- We need more proven interoperability (testing) rather than STANAGs.</li> <li>- Next driver will be civil-military information sharing for TMD</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
What is the best way forward in working together with industry?	Engage with industry earlier. Industry is part of the solution. Implies that we need new procedures. Future C&I agency will be in a better position as they can consider the whole life-cycle of capabilities.
Quick fixes (CRONOS, AMN) have been dominating. Should we use the CUR process more frequently? (K. Hermann)	CapDev in NATO is not conducted in the most efficient way at the moment. CPs are difficult to manage. It would be better to define an end-state. The way to reach this end-state can vary and be accomplished in several spirals. (ACOS C4ISR)
What instead of STANAGS to have guidance for nations?	We need to make sure: <ul style="list-style-type: none"> <li>- That Industry delivers capabilities that are fully interoperable</li> <li>- to test interoperability (more focussing on distributed battle-labs infrastructure, rather than on exercises)</li> </ul>
Certification	NC3A is not resourced to conduct certification. Smart Defence (Multinational Initiatives where nations take the lead) implies problems.
How to remain national sovereignty in terms of Smart Defence? (Mr. Peter Rasmussen)	Basis of our procurement rules is competition. Mid-size national industries have a lot of expertize in particular areas and should be involved in the bidding process wherever possible. However most industry currently involved in C4ISR development are rather international than national.

<b>Presentation Title:</b>	<b>Operationalizing NNEC through FMN</b>
----------------------------	--

<b>Presenter:</b>	<b>Dr. Alberto Domingo, Deputy NNEC Branch Head, ACT</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Already achieved a lot through ACT PoW (Architectures, taxonomies, exercises etc.) as well as creation of Body of Knowledge. NNEC objectives and principles are well understood as seen in AMN (addresses more than 60% of NNEC criteria).</li> <li>- NNEC is still needed to integrate military/non-military partners, move information protection closer to the information, resolve non-technical interoperability issues and in general to address the effects and not the solutions</li> <li>- FMN can operationalize NNEC based on lessons learned in recent operations. It will be a top-down, scope-time compromise under resource constraints of the NNEC Vision. NNEC will provide FMN with key ingredients for information sharing.</li> <li>- FMN-NNEC Concept will be created along the DOTMLPFI strands of development</li> <li>- FMN shall be a single information domain, easy to join/operate and leave, flexible in terms of service/information provision, with no need for imposed applications.</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
Practicality? Have you captured the total costs in your lessons learned to identify a first price-tag? (Mr. Peter Rasmussen)	Total cost for AMN is not representative for FMN. Actually we are doing the opposite for FMN. We are considering how we can rely on capabilities we already have available and subsequently identify the gap.
FMN will influence the NDPP. Do you think the recent NNEC Force Goals will remain valid or change? (Italian MOD)	There will be more Force Goals (Targets) and they will be in more detail.

<b>Presentation Title:</b>	<b>From AMN to FMN</b>
<b>Presenter:</b>	<b>LTGEN (Ret) Jo Godderij, former DG IMS, ATOS</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Development of FMN should focus on the future users / war-fighter's point of view. Operators should decide which applications / products will be used.</li> <li>- Complex environment requires interoperability on an ad-hoc basis. AMN is currently supporting already a lot of the NNEC</li> </ul>

	<p>Vision (One Mission, one Network, one common database)</p> <ul style="list-style-type: none"> <li>- There will be a lot of challenges in terms of governance, legacy systems, complex environment with a great variety of stakeholders</li> <li>- FMN is not just a copy of AMN in a new environment.</li> <li>- Architectural blueprint consists of three components (All-nations cloud, nations' shared cloud on the edge of the network, national extensions)</li> <li>- NCIA has an essential role as an all-embracing service provider over the whole lifecycle.</li> <li>- Nations have to act like an Infrastructure Service Provider.</li> <li>- Nations / Nations local industry should be encouraged to deliver applications to enhance the software variety of the FMN</li> <li>- Cyber Defence Rules &amp; Policy has to be adhered by everybody involved.</li> <li>- Using Innovation in the broadest sense</li> <li>- Partnership with NATO / nations / partners is essential</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
Do the apps need to have common semantic definitions? (Mr. David Cameon)	If you look at one complete FMN this would be the ideal solution.
NNEC tenet 'impact on the nature of command' has not yet been met. How do we develop NATO command doctrine that considers NNEC? (UK NC3REP)	There have been discussions in the MC and the C3B but apparently there is a big variety of viewpoints. Especially as principles like information sharing and Comprehensive approach can significantly impact on the way we run our business.

<b>Presentation Title:</b>	<b>Lifting the Fog of War – Enabling the FMN</b>
<b>Presenter:</b>	<b>Prof. Wesley Rhodes, IBM, CTO Europe and VP, SG</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- FMN must not only access data, but must make sense of it – structured and unstructured data from all troop contributing nations, quickly and accurately.</li> <li>- Technologies to be considered are: Cloud, Collaboration, Mobile Computing, Watson (Natural Language Interpretation), Analytics, Streams and Sense Making (relevant information finding the user)</li> <li>- Sense Making on the FMN provides a mechanism to evaluate</li> </ul>

	<p>new observations against previous observations in order to determine if what is being observed is relevant. In this regard, more data (even bad data) is helpful while processing speed increases.</p> <ul style="list-style-type: none"> <li>- FMN must not only access data, but must enable soldiers to make sense of it.</li> </ul> <p>All processes that deal with implementation of technology (Procurement, governance, risk management, etc.) have to be streamlined.</p>
<p><u>Question (by)</u></p>	<p><u>Answer</u></p>
<p>Military decision making process is mostly hierarchical and not supporting a collaboration environment (LTGEN Kurt Herrmann)</p>	<p>Yes, but you're in a good position as the nations involved agree to the basic principles of information sharing.</p>
<p>Systems like Watson, are only as smart as their algorithms. Do you agree?</p>	<p>The algorithms can't be poor, but the quality of the outputs the available data is essential. Development of efficient algorithms like Watson can be achieved by collaboration among industry, academia, etc.</p>

## Wednesday, March 28<sup>th</sup>, plenary presentations captures

<b>Presentation Title:</b>	<b>Exploiting Social Media</b>
<b>Presenter:</b>	<b>Mr. Roger Mendham, Logica</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Increasing importance in social media having a dramatic impact on the way information is managed in the military domain</li> <li>- Facebook, YouTube, Twitter dominance</li> <li>- Common to all highly relevant to military domain – now embracing in imaginative way</li> <li>- Most military under 30 years old. Social media is instinctive for this group. Opens up a new range of possibilities for info exchange and used today.</li> <li>- Building blocks – search, analyse, share</li> <li>- Need sophisticated search engines to extract info from media for INTEL gathering</li> <li>- Social media can be manipulated for operational reasons</li> </ul>

<b>Presentation Title:</b>	<b>Enhanced Secure Information Sharing with Google</b>
<b>Presenter:</b>	<b>Mr. Tom Wojszynski, Google</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Intro to Google – Google maps most heavily used interface in the world. Translation services. Fundamentally changed the way the world uses data to extract knowledge. Have offices in 19 of 28 NATO nations</li> <li>- Secure user data – need customers to feel comfortable that it is safe</li> <li>- Information is under constant attack from Cyber activities</li> <li>- New attack vector social media</li> <li>- Costly to manage at the device level should control centrally</li> <li>- Have global infrastructure to support</li> <li>- Manage supply chain by assuming it is corrupt.</li> <li>- Chrome, Chrome Books, Android</li> <li>- If the data is secure rather than network – open up new possibilities</li> </ul>
SHAPE – What is main threat	What is Number 1 threat – majority of resources against one state sponsored threat
System accreditation	System accreditation – customers must have the ability to analyse google capabilities to gain confidence
Data security	Distributed data is more secure because do not introduce a single point of failure

Austria MOD – Access management?	Trust and Need to know are still key principles.
----------------------------------	--

<b>Presentation Title:</b>	<b>Evolution of NEC in Finland and future challenges</b>
<b>Presenter:</b>	<b>BGEN Harri Ohra-Aho, chief J6, Defence Command Finland</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- NEC – most important focus on “people” – trust /cognitive – as it is the most difficult area</li> <li>- Finnish Defence Forces (DF) under major reform. All tasks require a different approach but forced to use a single network and dealt with coherently.</li> <li>- Joint comprehensive and combined is the principle underpinning new DF concept</li> <li>- Achieving a develop network :             <ul style="list-style-type: none"> <li>· Strategy – structure, organisations</li> <li>· Objectives - adequate performance – determines results – need good metrics</li> <li>· Values – Human interaction</li> </ul> </li> <li>- Uncertainty is the norm – need agility – but more partners mean more risks</li> <li>- Goal is for the network to create more value and reduce risks</li> <li>- Challenge is how to achieve agility while maintaining control. Achieved through common values. Coherent IM and interoperable services.</li> <li>- What has Finland done and is doing - 5 year plan:             <ul style="list-style-type: none"> <li>· Series of domains ranging from defence force to government to public</li> <li>· Generate static , mobile and end user environment</li> <li>· Whole structure owned by the state.</li> </ul> </li> </ul>
<u>Question (by)</u>	<u>Answer</u>
ACT – How difficult to align stakeholders	Legacy is to work closely together. In times of budgetary constraints difficult to create the single network.

<b>Presentation Title:</b>	<b>How NNEC Changed our Business: Communication as a Service</b>
<b>Presenter:</b>	<b>Mr. Olivier Doerre, FREQUENTIS AG</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Major challenges of the transformation to NNEC as it impacts on a medium sized business</li> <li>- Growing relevance of information - mission critical</li> <li>- Impact of comprehensive approach – implies major changes to processes</li> </ul>

	<ul style="list-style-type: none"> <li>- Uncertainty including military spending decreasing</li> <li>- Market trend Capability Developments:             <ul style="list-style-type: none"> <li>· Capability based thinking</li> <li>· Growing importance of information</li> <li>· Service orientation</li> <li>· New ways of Communication – chat, video etc.</li> </ul> </li> <li>- MT Interoperability:             <ul style="list-style-type: none"> <li>· Convergent platforms</li> <li>· Variety of new interfaces</li> <li>· Emerging standards</li> <li>· Cyber security</li> </ul> </li> <li>- MT Mobility             <ul style="list-style-type: none"> <li>· Ubiquitous Access</li> <li>· Tailored to mission</li> <li>· Reach back</li> <li>· Advanced requirements</li> </ul> </li> <li>- MT Cost efficiency:             <ul style="list-style-type: none"> <li>· Shrinking defence budget</li> <li>· New procurement paradigms</li> <li>· Life cycle cost management</li> <li>· Rare project with development</li> </ul> </li> <li>- Communications as a service:             <ul style="list-style-type: none"> <li>· Modular user interface</li> <li>· SOA</li> <li>· Convergent hardware platforms</li> <li>· Flexile interfaces</li> </ul> </li> <li>- Practical examples             <ul style="list-style-type: none"> <li>· IP Based Secure Communications</li> <li>· Component framework</li> <li>· Agile Development and rapid prototyping</li> </ul> </li> </ul>
<u>Question (by)</u>	<u>Answer</u>
ACT - advice for NATO	Military asking for unachievable requirements Go for 80% solution.

<b>Presentation Title:</b>	<b>Train as you fight – Considerations for FMN development</b>
<b>Presenter:</b>	<b>Mr. Steve Moore – Booz Allen Hamilton</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Opening thoughts:             <ul style="list-style-type: none"> <li>· Must learn from experience</li> <li>· Troops must be fully trained for ops – must be contextual</li> <li>· CFI – training focus - how is this best done - thoughts later</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>- Theme – FMN – must be incrementally achieved - through an SOA modular approach. FMN needs a lead architect who must be agile to change. Done within a Capability Development framework.</li> <li>- Live virtual and Constructive (LVC). Offers support to distributed mil ops for training experimentation and testing (see slide for more detail).Technology improves realism, availability and reduces training cost. Today do not need permanence to get training persistence (important for SMART defence) technology unlocks possibility</li> <li>- FMN needs to consider training exercise and mission rehearsal in a cost effective and coherent way.</li> <li>- Lessons observed about training and exercises:             <ul style="list-style-type: none"> <li>· Need to provide proper context lead to Joint National Training capability</li> <li>· Need persistent training capability</li> <li>· Must join up training centres</li> <li>· Train from strategic to tactical level</li> <li>· Develop trust and relationships – trust must be earned not declared</li> <li>· Investment enabled innovation – unintended but positive consequence.</li> </ul> </li> <li>- Technology capabilities for consideration for FMN             <ul style="list-style-type: none"> <li>· Affordable and incremental</li> <li>· Use the cloud – public or private</li> <li>· Use SOA – SEE SIMPLE AND POWERFUL CHART</li> </ul> </li> </ul>
<u>Question (by)</u>	<u>Answer</u>
Who should be the lead architect	ACT /NATO – Capability Developer
What are the training metrics	What motivates leaders – ultimately reduced those killed in action. Difficult but relevant question.

<b>Presentation Title:</b>	<b>Enabling a national security strategy through a FMN</b>
<b>Presenter:</b>	<b>Mr. Stuart Whitehead – US Joint Staff</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- US wishes to achieve its security goals thru partnerships</li> <li>- Wide list of mission areas – C2 is the common thread</li> <li>- Need to overcome the friction of short term warning</li> <li>- Must be ready to go whatever the mission</li> <li>- World growing smaller and military more lethal</li> <li>- Commerce leads technical edge, not military</li> </ul>

	<ul style="list-style-type: none"> <li>- The destination – moving away from mission specific networks. COTS hold the key but security concerns remain.</li> <li>- Sharing is the default – emotionally and mentally some way to go</li> <li>- Operational needs often overrides security</li> <li>- The Landscape:             <ul style="list-style-type: none"> <li>· Who are the partners</li> <li>· Agree process</li> <li>· How does the FMN support decision making?</li> </ul> </li> <li>- How do apps replace business process/what is the impact on service needs</li> <li>- Standards:             <ul style="list-style-type: none"> <li>· Standardised interface is the really valued metaphor</li> <li>· Many point to point interfaces generating need for mediation. Creates</li> <li>· US developing open non- proprietary interfaces with ACT</li> <li>· Increases operational agility</li> </ul> </li> <li>- Conclusion:             <ul style="list-style-type: none"> <li>· Common standards</li> <li>· Connectivity</li> <li>· Train as partner</li> <li>· Cyber security</li> <li>· Consider national safeguards</li> </ul> </li> </ul>
<u>Question (by)</u>	<u>Answer</u>
Standards – do you include XML	Yes – working with XML based standards.
Mr. John Wiles – UK – enforcement of standards is key – how does that happen?	US view – certification only achieved if standards are used. PM is responsible. Captain Mike Horsefield (SHAPE) – Joining instructions are NATO’s way of standard enforcement.
The future – how do you envision the needs of the future?	<ul style="list-style-type: none"> <li>- Look to scenarios, CONOPS, then examine FMN in light of each scenario.</li> <li>- What are the likely missions</li> <li>- Use integrated architectures</li> </ul>

**Wednesday, March 28<sup>th</sup>, breakout sessions presentations captures**

Breakout 1: Technology

<b>Presentation Title:</b>	<b>RF Spectrum Awareness End-to-End Management of hybrid SATCOM/Terrestrial Networks</b>
<b>Presenter:</b>	<b>Mr. Stuart Daughtridge, KRATOS</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- The presentation focused on End-To-End Network-Management to achieve convergence of Hybrid Terrestrial and SATCOM Networks</li> <li>- Vulnerability of RF link may jeopardize mission success. E2E management of the full spectrum (RF/SATCOM) is needed, however IT and OT (Operational Technology) integration is challenging</li> <li>- RF Situational Awareness COTS solutions are available. KRATOS developed solutions to bridge the IT/SATCOM gap and provides IT/OT convergence taking into account Cyber security issues</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
You also have to consider lawful interferences in different locations. A spectrum investigation has to be conducted to prior to the assignment of frequencies (Austrian MoD)	The software was setup to identify errors and interferences once they occur to allow immediate responses.
Olympic Games / European Soccer Championships coming up. Must we expect interferences in the broadcast of those events? (Dutch Air Force)	The companies involved in the broadcasting of these major events are well aware of the critical factors and have identified network management as part of their risk management. They are also using our products. I would not expect any limitations

<b>Presentation Title:</b>	<b>Nanosatellites and Future Military Operations</b>
<b>Presenter:</b>	<b>Mr Coen O. Janssen, Student at Delft University of Technology,</b>

	<b>The Netherlands</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Nanosatellites (1-10kg) can be provided at low cost in large numbers with low vulnerability to support future operations and NNEC.</li> <li>- Concept considers usage in large swarms for identification, tracking and communication.</li> <li>- Currently still under development, but progressing rapidly. Many application operational in the near future</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
What is the lifetime of a nano satellite?	Typically four or more years at this stage. Given the concept of large swarms, failure of a single satellite is irrelevant. Global coverage requires approx. 70-80 satellites. Management of 200 or more satellites possible.
What are the means to launch a nano satellite?	Typically piggy-back with conventional satellites. Alternative launches via fighter-jets or ships may be possible in future.
What is the payload of a nano-satellite?	It currently carries a standard camera. It is however designed to be equipped with any potential future sensor. It is also currently tested with phased arrays in order to establish high data links.
Will nano satellites replace the current satellites?	Probably not. They will be used complimentary to standard satellites. For identification purposes, standard satellites are the better option. Nano satellites have benefits for tracking purposes as they are more agile and use a lower orbit. They are also more robust for communication purposes.

<b>Presentation Title:</b>	<b>Solving the challenge of providing effective Situational Awareness over challenged tactical networks - force protection</b>
<b>Presenter:</b>	<b>Mr Christian Norkjaer, Systematics A/S</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Systematics has developed a Tactical Communication Battle Management System (BMS) supporting FFT and achieving tracking of up to 1000 tracks with a latency of less than one minute.</li> <li>- Once integrated in a system of a vehicle, the software accesses the vehicles sensors. Each soldier is identified once he plugs his unique USB-stick into the system. The software contributes to the Tactical Situational Picture (SIT) by using the vehicles radios to broadcast the FFT data.</li> <li>- Therefore the system supports all IP/non-IP based radios (SATCOM, 3G, UHF/VHF,...), does not need point-to-point contacts or end-to-end routing</li> </ul>
<u>Question (by)</u>	<u>Answer</u>

Is the data submitted compatible with Coalition partners?	The data is sent to the HQ and can be sent from there to coalition partners by using MIP.
What is the precision of the tracks?	Precision relies on the accuracy of the connected sensors. Our system focuses on the distribution of the data.

<b>Presentation Title:</b>	<b>Advances in Network Mobility and Radio Aware Routing</b>
<b>Presenter:</b>	<b>Mr Joshua McCloud, CISCO</b>
Summary of major themes and points:	<p>CISCO concept for establishing ad-hoc networks among mobile devices is based on</p> <ul style="list-style-type: none"> <li>- Radio-Aware Routing</li> <li>- Ad-hoc Routing</li> <li>- Integration in Platforms</li> <li>- Exchanging App-Information (Routing of App Services)</li> </ul> <p>CISCO Mobile Access Networks (MAN) optimizes interfaces, address-usage, state information and flooding based on usage of current protocols.</p> <p>CISCO routers that support these concepts for Advanced Networking are already integrated in systems by Thales and others.</p>

Breakout 2: Human factors

<b>Presentation Title:</b>	<b>Strategic Management of Information – How Does Human Behaviour Impact Future Mission Networks</b>
<b>Presenter:</b>	<b>Dr. Nancy Houston, ACT</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Information sharing is a behaviour not a technology and is such a radical shift from traditional military practices that it should be addressed as a change management issue.</li> <li>- The 80/20 principle should apply to network development – 80% of effort should be on the human-related issues of policy, processes, organisation and training and 20% on the technology.</li> <li>- High-level support should be sought within NATO to shift the focus to address the human issues that inhibit human agility and the ability to fully exploit the benefit of a future mission network.</li> <li>- The cognitive limits of both humans and organizations are exceeded by vast quantities of information and thus require effective collaboration (e.g. the NATO federation or the collaboration of organization in a comprehensive approach).</li> </ul>

<b>Presentation Title:</b>	<b>The Role of Chat in Supporting the Human Network</b>
----------------------------	---

<b>Presenter:</b>	<b>Dr. Candace Eshelman-Haynes</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- A social network is best understood as the sum of shared experience, shared values, shared training, shared information, and shared interactions.</li> <li>- The role of a social network in human information behavior is the same as the role of a neural network or a technical network – it supports awareness, processes information to find meaning, moves information through the system, coordinates action.</li> <li>- Chat or some form of chat will be an important tool for as long as we have soldiers working in operations.</li> <li>- New technologies coming online will introduce different gaps between the field and the command center. Human Computer Interaction issues should be addressed to best understand how these changes will affect operator decisions regarding information flow and information management.</li> </ul>

<b>Presentation Title:</b>	<b>Human Factors Aspects of Shared Situational Awareness in Complex Missions</b>
<b>Presenter:</b>	<b>Ms. Corinna Semling, IABG mbH Systemic Analysis and Human Factors</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- The comprehensive approach is about establishing shared situational awareness between mission partners.</li> <li>- Shared situation awareness needs are determined by the degree of shared goals and impacted by level of trust and risk.</li> <li>- Germany has developed a model for assessing shared awareness among organisations that provides a reflective assessment, an overview of partner’s network, an analysis guidance suitable for making recommendations about how to improve civil-military cooperation.</li> </ul>

<b>Presentation Title:</b>	<b>Exploring the impact of Federated Mission Networks on Human Factors issues within a simulated Joint Fires Support Scenario</b>
<b>Presenter:</b>	<b>Dr. Fred Lichacz &amp; Dr. Dave Allen, DRC Canada</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Federated networks improve situation awareness and trust in a C2 environment.</li> <li>- The Joint Fires Support Technology Demonstration Project highlighted the value of experimentation activities to test and appropriately develop federated mission networks. Experimentation results show that a federated mission network provides a viable way for improving timely collaboration, meta-situation awareness and trust in military operations.</li> <li>- The system was judged by operators as more trustworthy. It provided better clarity of information and showed fewer blue-on-blue incidents in the targeting scenario.</li> </ul>

<b>Presentation Title:</b>	<b>Information Sharing Management: An Essential Enabler for NNEC and the Future Mission Network</b>
<b>Presenter:</b>	<b>Mr. David Kamien, CEO, Mind-Alliance Systems, LLC</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Information sharing does not just “happen” either on a technical or human level. As with other aspects of operations, information sharing and management should also be planned to minimize the impact of surprises.</li> <li>- Introduced a system to support planned information sharing that includes a model for how to assess information sharing needs.</li> <li>- NATO interoperability would benefit from a holistic approach to information sharing – need high-level mandate to address organizational, policy, procedural &amp; training issues</li> </ul>

Breakout 3: Information assurance and cyber defence

<b>Presentation Title:</b>	<b>A NNEC-compliant Information Assurance Model in Support of FMN</b>
<b>Presenter:</b>	<b>Dr. Hermann Wietgreffe, NC3A</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Discussed the difficulties of establishing trust in an information-sharing environment.</li> <li>- Highlighted the constraints on security labelling of information/documentation in NATO (only the author has the authority to change the classification level)</li> <li>- Discussed the use of Information Exchange Gateways (IEG-C) to facilitate initial information sharing across cross security domain environments. They are key instruments to create trust. They should look at the information flows, not just the services.</li> <li>- Desire to move from multiple security domains and instead operate on one single network. This would result in higher efficiencies and reduce overall threat to the network/information.</li> <li>- Mid-Long Term approach should take 6-12 years.</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
Dr. Bent (IBM): Who owns the release policies? Work is being done in the UK in researching this issue more in depth. Good opportunity for collaborative	The Nations own the policies. But more investigation needs to be made to address the details depending on the physical location of the data, who the author was and what effect policy has on the data.

endeavour.	
Have you looked into the details associated with trust of the labelling mechanism?	Yes, NC3A has looked into the details and continues to do research in this area to ensure that the results are not tempered and stay relevant over time.

<b>Presentation Title:</b>	<b>Cross Domain as an Enterprise Services</b>
<b>Presenter:</b>	<b>Ms. Sue A. Roddy, Director UCDMO</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- To meet the growing needs for cross domain point solutions data transfers, access management and multiple security domains need to be further refined.</li> <li>- The focus at the end of the day is to keep things out (Malware, etc.) while keeping secrets in.</li> <li>- Enterprise: Define the boundaries in terms of the mission instead of the physical network.</li> <li>- Access management is a very ambitious endeavour and needs to be addressed in a different manner as the human factor is changing the nature of what the conditions are.</li> <li>- Having just one enterprise is not realistic as not all enterprises are equivalent (Community-Wide, Mission Specific, etc.).</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
Why are you not using international standards instead of the DoD?	You are correct and I will adjust my slides to reflect the international standards instead of the US driven ones used.
Oracle: How are you handling the data replication security threats?	Special devices for data replication exist using a special set of criteria. The criterion is highly structured and allows for an enhanced level of support.
Is the US discussing the issues associated with the reduction of data centres?	3: The focus is to, with the reductions that are occurring across the board, maintain the same level of support and utilize the capabilities of the remaining centres more efficiently while not forgetting the important details that are often overlooked.

<b>Presentation Title:</b>	<b>Protected Core Networking for Future Mission Networks</b>
<b>Presenter:</b>	<b>Mr. Roland Schultz, THALES Communication &amp; Security</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Would like to see Protected Core segments implemented throughout the current network to act as a stepping-stone towards a future mission network.</li> <li>- Through the use of PCNs you reduce the overall footprint that you have while integrating the functional services that operate on the networks.</li> <li>- Network Management in Cyber Defence (NMCD)</li> <li>- The Service Level Agreements (SLAs) are managed by the PCN.</li> <li>- There is a necessity to provide different connectivity models inside the mission networks, not just use one standard model.</li> <li>- Lack the policies necessary to properly implement an FMN capability and more work needs to be done to address the issue.</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
ACT: Will the PCN have a deployable capability in the future	Of course the eventual plan is to have a deployable capability. Protected core segments will change to more stable deployable capability and work is currently being done to identify the requirements associated with that capability.
Canada IBM: Can you elaborate on centralized management?	Information management is not currently centralized. The nations are not going to turn over their management capabilities; the second point is asking the question of what the information being shared will actually be. The networks services need to be shared and the sensor data needs to be shared. But other areas need to be investigated as well.

<b>Presentation Title:</b>	<b>Smarter Cyber Defence</b>
<b>Presenter:</b>	<b>Mr. John Palfreyman, IBM</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- NNEC is a good example of smarter defence from a military standpoint.</li> <li>- Being faced with an overwhelming volume of data that is ever increasing, there is a need to face the control aspects of the data.</li> <li>- Smarter defence is about taking a cross lifecycle/holistic view across the supply chain.</li> <li>- The more connected we are the more vulnerable we become. Work should be done on mitigating the risk by taking the time to understand the vulnerabilities we face.</li> <li>- The tools being used to access data are mostly custom-made which brings another level of complexity to combating the</li> </ul>

	<p>threats.</p> <ul style="list-style-type: none"> <li>- Mobile devices are much harder to secure, not just from a software standpoint, but also from the human dynamic that is causing the bigger issue.</li> <li>- Fundamentally change the way we think about defence from a cyber-standpoint. Understand that the threat will get in, and anticipate how to react when it does. Stop making “throwing technology at it” the only solution and instead also focus on the human element.</li> <li>- Bottom line: Smarter defence does require that our systems are instrumented, interconnected and intelligent for information superiority, but a smart approach is needed to overcome the increased vulnerabilities.</li> </ul>
--	---

<b>Presentation Title:</b>	<b>Cyber-Protecting IP Networks: Implementation Models</b>
<b>Presenter:</b>	<b>Mr. Frederic Martinez, Alcatel-Lucent</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- A popular trend is the advanced persistent threats. Difficulty in preventing these attacks comes from the nature of the design. Long-term attack plans that are designed to gather certain data shows there is a serious threat growing in the community.</li> <li>- Sophisticated targeted attacks are another area that is becoming a growing concern. Stuxnet case study. Future threats may in fact be designed to trick the system into being more efficient thus hiding itself even better.</li> <li>- White lists and black lists are only a temporary (time sensitive) solution and will not likely protect future threats.</li> <li>- Single situational awareness is impossible. There will not be a single solution that solves the problem; it will have to be a combination of solutions that work together to form a common defence.</li> <li>- Optical infrastructure exposed security threat. Fiber optic cable can be bent and data can be leaked.</li> </ul>

Breakout 4: NNEC practical applications

<b>Presentation Title:</b>	<b>Resilient Command and Control Networks: Assuring the Mission by Countering the Cyber Threat</b>
<b>Presenter:</b>	<b>Mr. Fred Wright, Georgia Tech Research Institute</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Operational view for cyber attacks</li> </ul> <p>OV-1 discussion, attacker’s point of view using military mission</p>

	<p>analysis process. Persistence, covertness, steal data, deny use of data, change data, leave with no trace</p> <p>What targets are available to attackers</p> <ul style="list-style-type: none"> <li>- Key threat vectors</li> </ul> <p>Modern Malware, cloud and web vulnerabilities, wireless vulnerabilities, social engineering and insider threats. Proactive defence is the key.</p> <p>Static defences are easily overcome. Trend analysis essential component. Continual analysis of web presence – self-awareness. Know how your people are using wireless systems, be alert to vulnerabilities, scan the RF environment and actively manage your mobile devices. Insider threat is very tough – again, be proactive, id potential bad actors before they attack, multi-key authentication.</p> <ul style="list-style-type: none"> <li>- Holistic Defence</li> </ul> <p>Manage mission assurance; secure the info and not the network defence at every level, risk analysis and mission assurance, continual pen testing and red teaming. Assess risk by asking what is threat to mission. Mission assurance – network security is only part of the puzzle. Know potential impacts of attacks before they happen and develop countermeasures and recovery procedures.</p> <ul style="list-style-type: none"> <li>- Emerging Concepts</li> </ul> <p>Map IT services to missions – the so what issue; Freedom of manoeuvre in cyberspace; Cyber situational awareness, event correlation and cyberspace visualization.</p>
--	---

<u>Question (by)</u>	<u>Answer</u>
<p>LCL David Cathro ACT SEE</p> <p>Any potential for adoption by military networks of more secure web services?</p>	<p>Yes, and this has not really been explored. Some software products are known problems, potential to mitigate some risks here</p>
<p>Danish Defence Acquisition. Difference in security levels for mobile devices (operational vs. tactical issue)</p>	<p>Operational level is likely more valuable for exploitation, but the tactical level is much more vulnerable (outside the fence is easier to exploit)</p>

<b>Presentation Title:</b>	<b>US Coalition C2 Capabilities – Evolving to Future Mission Network</b>
<b>Presenter:</b>	<b>Mr. Ron Pontius, US DOD</b>

<p>Summary of major themes and points:</p>	<ul style="list-style-type: none"> <li>- US View of C2 – Joint Definition</li> </ul> <p>C2 includes data, people and processes, C2 is a human endeavour, and systems must support the people and not handcuff them.</p> <ul style="list-style-type: none"> <li>- C2 as a formal Joint Capability Area – dedicated and focused capability development effort</li> <li>- 4 Examples of C2 systems discussed</li> </ul> <p>CENTRIXS – in wide use in number of theatres, many small bilateral networks in use (over 50), not really cost effective anymore.</p> <p>CFBL – Combined Federated Battle Lab Network. Developmental network with many multinational partners. Can test out capabilities and concepts.</p> <p>UISS – Unclassified Info Sharing Services. For use in collaboration with traditional and non-traditional mission partners (IO, Civil Government, NGO, not a .mil domain. In wide use now. All Partners User Access Network.</p> <p>AMN – Afghanistan Mission Network. Much larger inclusive view of the word network.</p> <ul style="list-style-type: none"> <li>- Challenges</li> </ul> <p>Applications and services, data, infrastructure. Key is to leverage enterprise services and incrementally deliver capabilities. If you cannot trust individual users you cannot move from need to know to need to share. Identity and access management a key enabler. Can I trust the data? Also a challenge.</p>
<p><u>Question (by)</u></p>	<p><u>Answer</u></p>
<p>LCL David Cathro SEE. Do you think NATO will get with program in terms of FMN?</p>	<p>Very hopeful – I think we have a true partnership in place with ACT. We are being careful not to adopt a US-only perspective, ACT inputs are influencing US FMN concept. We need to work this forward together.</p>
<p>Mr. Mark Clark Raytheon. UISS – is this a cloud really? Identity and access management – I think industry already has this, what is the holdup.</p>	<p>ID and access management – NSA has lead here, they do involve industry, challenge is working through the policy aspects. UISS – not really a cloud service at all.</p>

<p><b>Presentation Title:</b></p>	<p><b>Enhanced SA through distributed and collaborative multisensory data fusion</b></p>
<p><b>Presenter:</b></p>	<p><b>Ms. Karna Bryan, NURC</b></p>

<p>Summary of major themes and points:</p>	<ul style="list-style-type: none"> <li>- NURC Program Overview</li> <li>- Focus on Maritime Situational Awareness Program.</li> </ul> <p>Cross platform interoperability of NATO maritime systems, focus at the sensor level. Building on EXTAC 790, specifically the data fusion problem.</p> <p>Challenge is bringing national info from various military and civilian agencies and then making sense of it all.</p> <ul style="list-style-type: none"> <li>- Data fusion and sense making</li> </ul> <p>Automation is key to utilizing all of the available information. We have seen increased info sharing, increases the need for automation. Collaborative Multi Sensor Source Fusion and Tracking. Common interfaces are a key here in order to enable data fusion.</p> <ul style="list-style-type: none"> <li>- Big challenge is facilitating collaboration.</li> </ul> <p>Work on a multinational collaborative framework.</p> <p>Tidepedia track correlation project. The vision is “fusion on demand” – network based data fusion. Development of very straight forward applications for use on NATO networks. “Simple Fusion Service” app as a baseline capability.</p> <p>Behaviour based anomaly detection to identify potential bad actors.</p> <p>Integrated sensor performance estimation – bringing sensors from different surveillance systems together to build a coherent picture – again, sense making.</p> <ul style="list-style-type: none"> <li>- Exploiting information for better decision making!</li> </ul>
<p><u>Question (by)</u></p>	<p><u>Answer</u></p>
<p>Correlation capabilities – can you provide some details? What can you leverage across the network?</p>	<p>That is exactly what the tracking and fusion elements will provide.</p>
<p>Mr. John Nankervis – SPAWAR. Comment on maintaining the context of data if most of the metadata is striped out.</p>	
<p>Denmark – I am working air domain. Please talk a bit about the accuracy of your sensors and do you prefer raw sensor data or processed data?</p>	<p>Answer – this is a challenge. It is better to first fuse the data and then do the tracking but this can be tougher to implement. Better picture but tougher process to implement.</p>

**Thursday, March 29<sup>th</sup>, plenary presentations captures**

<b>Presentation Title:</b>	<b>Linking Nations with the NATO Command Structure</b>
<b>Presenter:</b>	<b>MGEN Kjell-Ove Skare, Norwegian Armed Forces Defence Staff</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- 1987 – Robust Command Structure, NATO commands in almost every nation, well resourced, close linkages to each nation. This is no longer the case.</li> <li>- New guidance recently adopted, much reduced command structure, but a very robust level of ambition. NCS must be augmented with the Force Structure, linking nations to the NCS is key to success.</li> <li>- Regional Understanding through formalized cooperation with national entities.</li> </ul> <p>Norway is seeking to better link national defence HQ with NCS – how to best link with ACO and subordinate commands. Strategic and operational command and control using national elements (FMN, CFI, Smart Defence). Bumper Sticker – Plug and Play with NATO.</p> <ul style="list-style-type: none"> <li>- Review of new NATO command structure, role of SHAPE and CCOMC.</li> </ul> <p>SHAPE-ACO becomes a key element to link nations to the NCS, SHAPE is the key link. Need this to ensure the common security guarantee with nations. Again, plug out of national C2 structures and plug in to the NCS, major emphasis now on preparation and interoperability. Identify best practices for NATO nations and solve some of the existing barriers to plug and play.</p> <ul style="list-style-type: none"> <li>- Norway and NATO</li> </ul> <p>Assessment matrix – nation and NATO. Political to tactical, peace, crisis and conflict. Many gaps found in numerous areas as assessment was conducted. Each nation may wish to consider such an approach. As nations restructure they need to keep alliance interoperability in mind.</p> <ul style="list-style-type: none"> <li>- Information Exchange is a key shortfall, from both national and NATO perspectives</li> </ul> <p>Norway to SHAPE and NCS, with a view toward CCOMC and latest alliance guidance. C2 tools, renewed focus on training and exercises. Use NATO classified security domain as the national solution? Use NATO classification instead of NORWAY classification unless an issue is national eyes only. Change in habits and culture needed. TOPFAS example – use as national planning</p>

	<p>system, move into NATO classified domain. Norway does not have a NATO classified VTC capability, this is now being addressed. BICES distribution – this is a powerful tool.</p> <ul style="list-style-type: none"> <li>- Bottom line – Norway is looking at very serious changes to ensure interoperability with NATO.</li> </ul> <p>Serious attention is being paid to results of the gap analysis. Dual hatting national commanders with both a national role and a NATO role? Redefine operational and tactical roles from both a national and NATO perspective – will Norway need to provide component commanders for a NATO operation? Dialogue must begin now.</p> <ul style="list-style-type: none"> <li>- Change the way we train and exercise – distributed training needs to be an integral element of the FMN.</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
MGEM Willemse – dual hatting, can you formalize this as a national requirement?	If a NATO command was to operate on your territory that is a major national issue. In national interest for NATO to effectively operate on Norwegian soil. Essential to have a Norwegian integrated into the NATO structure in order to bring good regional knowledge to the NATO operation. Dual hatting can help to achieve this. This is nothing new for NATO. This should be considered before a potential crisis so yes, formalized.
IBM Question – standards and national systems. Do you see a mind-set change here (adopting NATO standards as national standards)	Norway is far down the path of adopting NATO standards as the National standards in the technical realm but this is not enough. It is about how we do business, thus the need for education and training.
	Comment – JFC Brunssum MA. This topic has been discussed by CDR JFC Brunssum. Brunssum intends to pursue this dual hatting approach in a formal conference with national commanders.
Question – the technology is here so the problems lie elsewhere like culture and behaviour. Your comments?	Answer – if technology is implemented from a national perspective we can have a problem so it is not so much a question of culture but a question of viewpoint as you adopt new technologies. Processes, technology, and organizations – we need to approach this the way that corporations do.

<b>Presentation Title:</b>	<b>EU NEC Briefing – practical support required for CSDP missions (common security and defence policy)</b>
<b>Presenter:</b>	<b>Mr. Marcel Staicu, project officer NEC, European Defence Agency</b>

<p>Summary of major themes and points:</p>	<ul style="list-style-type: none"> <li>- EDA is responsible to ensure that required capabilities are properly developed.</li> <li>- EU Lisbon Treaty 2009, effect of budget cuts. Cooperation with NATO is now a must, cannot afford separate NATO and EU solutions.</li> <li>- EDA roles. Prepare technical solutions, promote cooperation, share capabilities, promote cooperation and dialogue, maintain close working relationships with NATO, promote dual use technologies, promote robust European defence industrial base</li> <li>- Review of EU CDP – capability development process.</li> <li>- NEC is one of the key EU capability development priorities. Top down and bottom up approaches are being pursued. NEC as a core driver. Maritime Surveillance example discussed. NEC roadmap tracking tool.</li> <li>- EU NEC principles – federation; flexibility; one governance: communities of interest, information sharing, Ubiquity – one person, one information profile. Service orientation, information assurance, reusability, standardization.</li> <li>- Discussion of EU NEC maturity model</li> <li>- EU NEC capabilities assessment methodology introduced. Seeking practical and tangible outcomes, developing EU practical guidelines</li> <li>- Way ahead: practical tangible IM Tools; coherent set of design and implementation guidelines; use of online resources to guide project.</li> </ul>
<p><u>Question (by)</u></p>	<p><u>Answer</u></p>
<p>MGEN Willemse: where could EDA be of help to NATO? Is EDA considering a future mission network?</p>	<p>EDA can be of help – avoiding duplication and coordinating efforts; develop compatible systems; EDA has a strong link with the civilian world and can help NATO in this respect. Good cooperation is key. FMN – no, EDA is not so much involved in operations and EDA is not developing a FMN. This is answer at technicians’ level; political leadership has not weighed in yet.</p>
<p>UK C3 rep – is EU-EDA enforcing standards?</p>	<p>Yes EDA has standards and is looking at NATO standards like the Architectures and the NISP. EDA also has an eye toward commercial and civilian standards. EU has a robust standardization effort as well, and they work closely with NATO.</p>

<p><b>Presentation Title:</b></p>	<p><b>Implementing a Future Mission Network: Generation Y, Mission Assurance, and Modelling and Simulation</b></p>
<p><b>Presenter:</b></p>	<p><b>Mr. Angel San Jose Martin, ACT, Mr. Gerald Gendron, SimIS</b></p>
<p>Summary of major themes and points:</p>	<ul style="list-style-type: none"> <li>- M&amp;S as a capability</li> <li>Generations and Information security. Gen Y – is there a conflict</li> </ul>

	<p>between their wants and needs and the need for info security? Gen Y wants personal devices in the work place (this is an IA concern). Does this affect Gen Y productivity if devices are prohibited? Need to find the right balance.</p> <ul style="list-style-type: none"> <li>- M&amp;S and the Connected Forces Initiative. M&amp;S is now a mature capability that is widely available.</li> </ul> <p>People, process, technologies and the interactions between them. Do we develop processes and technologies with the people in mind? How do we look at the factors (pairwise or all together)</p> <ul style="list-style-type: none"> <li>- Change across generations. Generation Y 1981-2000. Soon to be our mid-level leaders.</li> <li>- Mission Assurance – this is a commercial information term that has been in use since the early 90s.</li> </ul> <p>Strong task focus – we will do the mission, may take some IA risks in order to complete the mission. Tension between mission accomplishment and IA.</p> <ul style="list-style-type: none"> <li>- M&amp;S in support of cyber defence and IA. Can help examine the balancing of mission accomplishment with cyber defence priorities.</li> <li>- FMN and how M&amp;S can support.</li> </ul> <p>Operational preparation – M&amp;S can provide support to help visualize different alternative approaches. Supports test, evaluation, and certification,</p> <p>Training – distributed training and LVC live virtual constructive. These are heavily dependent upon M&amp;S tools</p> <p>Lessons learned – M&amp;S tools can be used to recreate events and support the analysis.</p> <p>Future Mission Network User – digital natives want this to behave like their smart phones work, easy to use, always available, always in use</p> <ul style="list-style-type: none"> <li>- M&amp;S can provide a persistent tool set for the development of the FMN.</li> <li>- Gen Y and younger are different than Gen X and the Boomers – we need to change our training approaches, and M&amp;S can help.</li> </ul>
<p><u>Question (by)</u></p>	<p><u>Answer</u></p>
<p>Italian MOD OF-5. Our current leaders are Gen X. How can we accommodate both Gen X and Gen Y? How can M&amp;S help with testing and validation?</p>	<p>In experimentation we see how each generation uses the tools – they do indeed use the IT tools differently. Looks like the olders are becoming more technologically adept as well. M&amp;S – can build a cheap model of a system, a test bed. This can then be used in testing evaluation and validation.</p>

LTC David Cathro SACT SEE. We develop rigid processes for our technology development. How can we adapt more flexible approaches?	Current procurement system will not work, we must modify it to better enable innovation. M&S can be helpful here.
Can you use M&S tools in “real time” situations?	Yes you can! An example would be using an iPad to help with Mission Execution (Google maps and the associated tools, tactical decision aids, etc.)
Austrian MOD OF-5 and a Baby Boomer. How do you train people on legacy systems using modern training methods?	Gen Y will use the existing tools and legacy systems differently, and they learn differently. We must adapt the training style, but it is not really hard at all to adapt training for the Gen Y and younger audience.
Mr. John Nankervis SPAWAR. Reuse of capabilities – clear message that capabilities cannot “frustrate” the users. What kind of configuration changes is needed that can still balance mission accomplishment with IA imperatives?	This is real problem and something that our future solutions teams need to work on. Again, M&S is part of the solution for this.

<b>Presentation Title:</b>	<b>Knowledge Management - Austrian View – An enabler for interoperability</b>
<b>Presenter:</b>	<b>COL Klaus Mak, Defence Academy Austria</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- Challenges                             <ul style="list-style-type: none"> <li>· What is knowledge? Need a single definition</li> <li>· Support for Capability Development –take a holistic approach – knowledge is a product – must be measured</li> <li>· Enabler for Cap Dev/Interoperability – do we have a tool to evaluate?</li> <li>· Improvement of the evaluation quality – do we know what quality of human capital we have in the organisation – need to design a knowledge score card</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>- Determine the Common Denominators – develop a knowledge architecture model</li> <li>- Conclusion                             <ul style="list-style-type: none"> <li>· Documentation Communication and Transparency</li> <li>· Have established preconditions for discussion</li> <li>· Evaluate quality</li> </ul> </li> </ul>
<u>Question (by)</u>	<u>Answer</u>
Does this process bring value? Gen Skare	Hard work to implement, must be able to benchmark. Needs more time to take hold.

<b>Presentation Title:</b>	<b>MNMIS</b>
<b>Presenter:</b>	<b>CAPT Paulo Costa, ACT</b>
Summary of major themes and points:	<ul style="list-style-type: none"> <li>- NATO Strategic Concept, SMART Defence, MNA TF</li> <li>- CP 9C0107 – provides resources for operational functional services including Maritime (Project TRITON) to replace MCCIS and to develop MSA capabilities. NC3A is the Host Nation.</li> <li>- MNMIS – Multi-national solution to Maritime C2</li> <li>- MNMIS will enhance NNEC (situational awareness) through removing interoperability barriers.</li> <li>- MNMIS could be a component of FMN – need to identify a lead nation</li> <li>- MNMIS - will meet national Maritime C2 requirements – ACT has a facilitating role</li> <li>- MNMIS Workshop – held last month – achieved small victories</li> </ul>
<u>Question (by)</u>	<u>Answer</u>
What is relationship with EU Maritime initiatives - ACT	MARSUR is a different concept – linking point to point nation to nation
How do we de-conflict with ourselves?	Confusion over difference between TRITON and MNMIS. Clarified.
Involvement of industry? Mr. Frans Picavet	Industry will ultimately be involved in the competition

<b>Presentation Title:</b>	<b>The effects of CA on C2</b>
<b>Presenter:</b>	<b>COL Toine Visser, Director C2CoE</b>

<p>Summary of major themes and points:</p>	<ul style="list-style-type: none"> <li>- Traditional             <ul style="list-style-type: none"> <li>· Focus on military aspects</li> <li>· Importance of operational security</li> <li>· Planning and execution by military</li> <li>· Information sharing within military community – still difficult</li> </ul> </li> <li>- CA             <ul style="list-style-type: none"> <li>· 3D – defence diplomacy development</li> <li>· All partners involved including civilian components</li> <li>· Exchange of Information with all partners is essential</li> <li>· Military in supporting role</li> </ul> </li> <li>- Challenges             <ul style="list-style-type: none"> <li>· Military wanted to be in the lead</li> <li>· Civilians do not want to be coordinated</li> <li>· Security issues</li> <li>· Planning and executing together means that info must be shared</li> <li>· Must be trust</li> <li>· Short deployment for the military</li> <li>· Military look for short terms goals</li> </ul> </li> <li>- Examples             <ul style="list-style-type: none"> <li>· AMN/FMN – able to exchange all info/can we plan together</li> <li>· need to exchange info with NGOs et al</li> </ul> </li> <li>- Impacts             <ul style="list-style-type: none"> <li>· Staff process</li> <li>· Command posts</li> <li>· Information sharing</li> <li>· Trusted relationships with civilian actors</li> <li>· Paradigm shift on security</li> </ul> </li> </ul>
<p><u>Question (by)</u></p>	<p><u>Answer</u></p>
<p>Mr. John Nankervis – SPAWAR – trust relationship with Civilian actors when wish to remain anonymous?</p>	<p>Consider using social media. Must be done before the operation.</p>
<p>ATOS – what experience are we getting out of the field with civilian relationships</p>	<p>Arguable that the comprehensive approach is partly happening in Afghanistan. Cultural changes still required from military and NGOs.</p>

## Annex D: Conference Agenda

### Agenda overview

The general layout of the conference was over two and a half days, with registration and ice-breaker on the previous day:

26 March	27 March	28 March				29 March
Registration	Keynotes	Presentations <ul style="list-style-type: none"> <li>• Nations</li> <li>• Industry</li> <li>• ACT</li> </ul>				Presentation
	Introduction					Final remarks / Summary
	Hi Level Presentations	break out Technology	break out Human Factors & Processes	break out Information assurance and Cyber Defence	break out NNEC practical implementations	
ICE BREAKER		CONFERENCE DINNER				

**Tuesday 27 March – Day One – Keynotes and Plenary****Moderated by Major General Jaap Willemse, ACOS C4ISR & NNEC, HQ SACT**

08:15	Administrative Brief <b>LCL Michael Buttler, HQ SACT</b>
08:20	Opening Remarks <b>MGEN Jaap Willemse, ACOS C4ISR &amp; NNEC, HQ SACT</b>
08:30	Keynote <b>GEN Edmund Entacher, Chief of Defence, Austria</b>
08:55	Keynote <b>GEN Mieczyslaw Bieniek, Deputy Supreme Allied Commander Transformation, HQ SACT</b>
09:20	Keynote <b>MGEN Patrick Fermier, Director, NATO HQ C3 Staff (representing ASG-DI)</b>
09:45	Keynote <b>BGEN Jonathan Mullin, Capabilities Director, European Defence Agency</b>
<b>10:10</b>	<b>Networking and Coffee Break</b>
10:35	Keynote: Secure information sharing in support of coalition operations. <b>Ms. Michele Weslander Quaid, Chief Technical Officer, Google</b>
11:10	Cyber Security Austria – Civil and Military Activities <b>BGEN Helmut Habermayer, Austrian MoD</b>
11:45	Operational perspective on the NATO Future Mission Network <b>CAPT Mike Horsefield and CAPT Jean-François Leca, SHAPE NATO and HQ SACT</b> Comprehensive Crisis Management <b>COL Luc Le Blanc for BGEN Bert Booman, Director CIS, ACO</b>
<b>12:30</b>	<b>Lunch Break</b>
13:40	Secure Information sharing in NATO-led Coalition Operations <b>LTGEN Kurt Herrmann, Director, NATO CIS Services Agency (NCSA)</b>
14:15	NNEC Challenges Met? <b>MGEN (Ret) Georges D'Hollander, General Manager, NATO C3 Agency</b>
<b>14:50</b>	<b>Networking and Coffee Break</b>
15:15	Operationalizing NNEC <b>Dr. Alberto Domingo, NNEC Branch, HQ SACT</b>
15:50	From Afghan Mission Network to Future Mission Network <b>LTGEN (Ret) Jo Godderij, Former DG-IMS, ATOS</b>
16:25	Lifting the Fog of War – Enabling the FMN <b>Prof. Wesley Rhodes, CBE, IBM CTO Europe &amp; Vice President, Software Group</b>

**Wednesday 28 March – Day Two – Plenary and Breakout sessions****Moderated by MGEN Jaap Willemse, ACOS C4ISR & NNEC, HQ SACT**

08:00	Administrative Brief <b>LCL Michael Buttler, HQ SACT</b>
08:15	Exploiting Social Media for Defence advantage in the Operation Domain <b>BGEN(Ret) Roger Mendham, Logica</b>
08:45	Enhanced Secure Information sharing with Google <b>Mr. Tom Wojszynski, Google</b>
09:20	Evolution of NEC in Finland and future challenges <b>BGEN Harri Ohra-aho, Chief of J6, Defence Command Finland</b>
<b>09:55</b>	<b>Networking and Coffee Break</b>
10:20	How NNEC changed our business: Communication as a Service <b>Mr. Oliver Doerre, Frequentis AG</b>
10:55	Train As You Fight – Considerations for FMN to support Mission Preparation / Development <b>Mr. Steve Moore, Booz Allen Hamilton</b>
11:30	Enabling a National Security Strategy through a Future Mission Network <b>Mr. Stuart A. Whitehead (SES), US Joint Staff J8</b>
<b>12:00</b>	<b>Lunch Break</b>

**Breakout Session 1: Technology to improve information sharing****Moderated by COL Patrick Grelier, NNEC Branch Head, HQ SACT**

13:35	RF Spectrum Awareness End-to-End Management of Hybrid SATCOM/Terrestrial Networks <b>Mr. Stuart Daughtridge, Kratos Technology &amp; Training Solutions</b>
14:10	3D-positioning system for the 21 <sup>st</sup> Century soldier <b>Prof. Ulrich Walder, TU Graz and AIONAV Systems Ltd</b>
14:45	<b>Networking and Coffee Break</b>
15:10	Nanosatellites and Future Military Operations <b>Mr. Coen O. Janssen, Student at Delft University of Technology, The Netherlands</b>
15:45	Improving Force Protection <b>Mr. Christian Norkjaer, Systematic A/S</b>
16:20	Advances in Network Mobility and Radio Aware Routing <b>Mr. Joshua McCloud, CISCO</b>

**Breakout Session 2: Human Factor & Processes****Moderated by Dr. Nancy Houston, HQ SACT**

13:35	Strategic Management of Information – How does Human Behaviour Impact FMNs? <b>Dr. Nancy Houston, HQ SACT</b>
14:10	The role of chat in supporting the Human Network <b>Dr. Candace Eshelman-Haynes</b>
14:45	<b>Networking and Coffee Break</b>
15:10	Human Factors Aspects of Shared Situational Awareness in complex Missions <b>Ms. Corinna Semling, IABG mbH Systemic Analysis and Human Factors</b>

15:45	Exploring the impact of FMNs on HF issues within a simulated Joint Fires Support Scenario <b>Dr. Fred Lichacz and Dr. Dave Allen, Defence Research &amp; Development, Canada</b>
16:20	Information Sharing Management: An Essential Enabler for NNEC and the FMN <b>Mr. David Kamien, CEO, Mind-Alliance Systems, LLC</b>

### Breakout Session 3: Information Assurance and Cyber-Security

*Moderated by Mr. Jeff Salter*

13:35	A NNEC-compliant Information Assurance Model in Support of FMN <b>Dr. Hermann Wietgreffe, Nato C3 Agency</b>
14:10	Cross Domain as an Enterprise Service <b>Ms. Sue A. Roddy, Director, Unified Cross Domain Management Office, USA</b>
14:45	<b>Networking and Coffee Break</b>
15:10	Protected Core Networking for Future Mission Networks <b>Mr. Roland Schultz, THALES Communication &amp; Security</b>
15:45	Smarter Cyber Defence <b>Mr. John Palfreyman, IBM</b>
16:20	Cyber-protecting IP Networks: implementation models <b>Mr. Frederic Martinez, Alcatel-Lucent</b>

### Breakout Session 4: NNEC Practical Applications

*Moderated by Mr. David Burton*

13:35	Planning for an agreed Future Mission Network <b>Mr. John Neumayer, Joint Intelligence Surveillance Reconnaissance, HQ SACT</b>
14:10	U.S. Marine Corps Life Cycle Modeling Integrator (LCMI) program <b>Mr. Raymond Nelson, Concurrent Technologies Corporation</b>
14:45	<b>Networking and Coffee Break</b>
15:10	Resilient Command & Control (C2) Networks <b>Mr. Jeff Moulton, Georgia Tech Research Institute</b>
15:45	U.S. Coalition C2 Capabilities: Evolving to Future Mission Network <b>Mr. Ronald W. Pontius, U.S. DoD</b>
16:20	A Framework for Collaborative Multi-Source Sensor Fusion and Tracking <b>Ms. K. Bryan, M. S. Horn, M. A. Berni, NATO Undersea Research Centre (NURC)</b>

**Thursday 29 March – Day Three - Plenary****Moderated by MGEN Jaap Willemse, ACOS C4ISR & NNEC, HQ SACT**

08:00	Administrative Brief <b>LCL Michael Buttler, HQ SACT</b>
08:10	Linking Nations with the NATO Command Structure <b>MGEN Kjell-Ove Skare, Norwegian Armed Forces Defence Staff</b>
08:45	EU NEC Briefing <b>Mr. Marcel Staicu, European Defence Agency</b>
09:20	Implementing a Future Mission Network: Generation Y and Mission Assurance <b>Mr. Angel San Jose Martin, NATO HQ SACT &amp; Mr. Gerald Gendron, SimIS Inc.</b>
09:45	<b>Networking and Coffee Break</b>
10:20	Knowledge Management <b>COL Klaus Mak, Defence Academy Austria</b>
10:55	Maritime Activities – Multinational Approach (MNMIS) <b>CAPT Paulo Costa, HQ SACT</b>
11:30	The Effect of the Comprehensive Approach on Command & Control <b>COL Toine Visser, Director, Command &amp; Control Centre of Excellence (C2CoE)</b>
12:00	Summary and Closing Remarks <b>MGEN Jaap Willemse &amp; Austrian Rep</b>
12:30	<b>End of Programme</b>