THE MNE7 OBJECTIVE 3.4 CYBER SITUATIONAL AWARENESS LOE

FIRST IMPRESSION EXPERIMENT REPORT (FIER)

1. Introduction

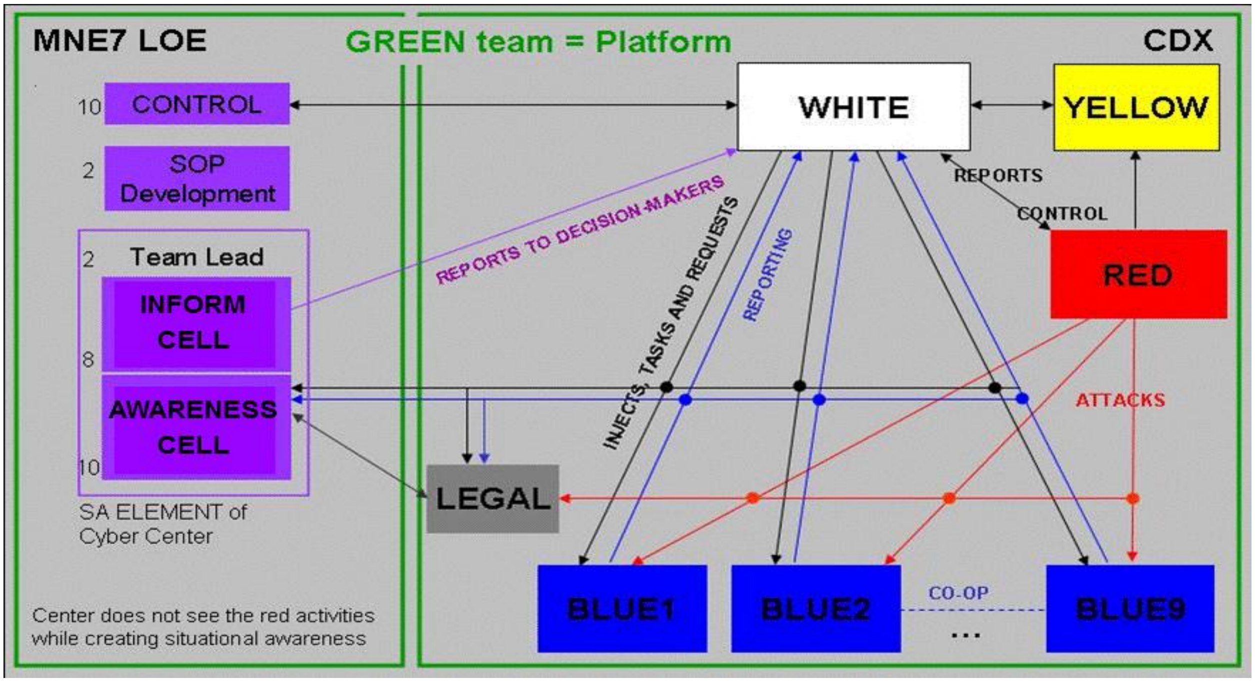
The Finnish Defence Forces Concept Development & Experimentation Centre (FDF CD&E Centre) organised the MNE 7 Cyber Situational Awareness (SA) Limited Objective Experiment (LOE) in Riihimäki 26 – 29 March 2012.

The Multinational Experimentation 7 (MNE7) campaign consists of several work strands, each dealing with different aspects of the theme “Access to the Global Commons”. Cyberspace is one of the core study areas. It consists of five objectives each studying different aspects of Situational Awareness (SA) in the Cyber domain. Objective 3.4 (SA enabling technologies) is lead by Finland and supported by contributing nations Austria, Denmark, Germany, Italy, Norway, Switzerland, United Kingdom and United States of America and by NATO ACT.

Objective 3.4 has been drafting a Cyber Standard Operating Procedure (SOP) to set a proper framework to study SA technologies in cyberspace. The Aim of this experiment was to support the early phase of the SOP development by discovering solutions and investigating related issues. The next version of to SOP will be available by the end of April 2012 and further refined in a SOP workshop in Denmark 8-10 May.

2. Experiment Overview

The LOE was executed ‘virtually’ alongside a technical Cyber Defence Exercise (CDX) which was lead by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia but distributed to several nations. The CDX was focused on training; Cyber specialists were to work in a virtual environment, where nine ‘Blue’ teams defended their partially prebuilt computer systems against ‘Red’ team attacks. The participants originated from both CDX contributing countries and MNE 7 nations. The MNE experiment design had the CDX providing a rich activity environment with adequate and suitable information feeds to support the requirements of the MNE Cyber experiment to study Situational Awareness. A schematic of the experiment design incorporating the CDX information feeds is shown below.



Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **08 JUL 2013**	2. REPORT TYPE **N/A**	3. DATES COVERED

4. TITLE AND SUBTITLE

THE MNE7 OBJECTIVE 3.4 CYBER SITUATIONAL AWARENESS LOE FIRST IMPRESSION EXPERIMENT REPORT (FIER)

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

The Multinational Experimentation 7 (MNE7) campaign consists of several work strands, each dealing with different aspects of the theme "Access to the Global Commons". Cyberspace is one of the core study areas. It consists of five objectives each studying different aspects of Situational Awareness (SA) in the Cyber domain. Objective 3.4 (SA enabling technologies) is lead by Finland and supported by contributing nations Austria, Denmark, Germany, Italy, Norway, Switzerland, United Kingdom and United States of America and by NATO ACT. Objective 3.4 has been drafting a Cyber Standard Operating Procedure (SOP) to set a proper framework to study SA technologies in cyberspace. The Aim of this experiment was to support the early phase of the SOP development by discovering solutions and investigating related issues.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**6**	

LOE participants were divided into two organisational functions each with a different SA purpose; an **Awareness cell** and an **Inform cell.** These cells would address the different working time spans within a fictitious **Cyber Centre** – current and future. The cells were further divided into smaller functions (roles) as follows.

Awareness cell (collects, combines, visualizes, and comprehends).
Role A-1 Understand ”Us” (Our services, operations and business, white team reports)
Role A-2 Collect (reports, pulling from logs, blue team reporting)
Role A-3 Analyse (categorize, combine, situation assessment, impact to us)
Role A-4 Visualize, present, share (Information push)

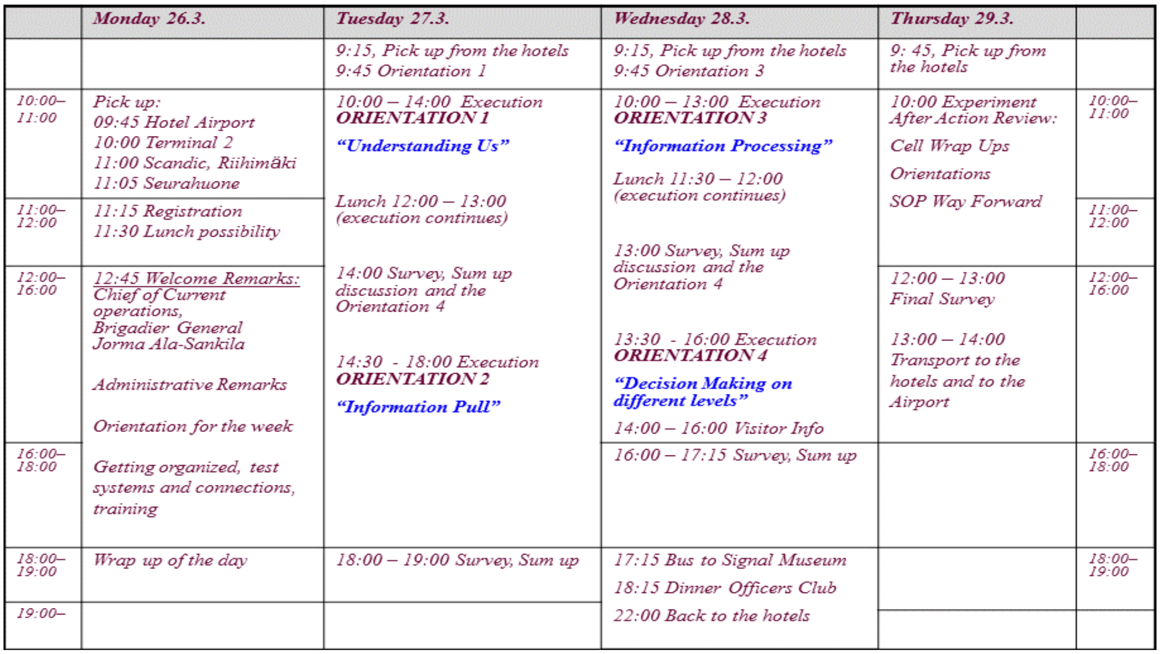
Inform Cell (estimates, projects, shares, informs)
Role I-1 Understand ”Them” (Intelligence)
Role I-2 Estimate and project (Future Impact to us, make recommendations)
Role I-3 Visualize, Present, Share, Inform (What can be done, what is expected?)
Role I-4 Media perspective (What is needed? What can be offered?)

It was not the intention to evaluate the structure being played during the event, rather its structure was intended to catalyse thinking and discussions during the event. A key part of the experiment design would be to ensure that the participants were from appropriate backgrounds to speak with authority and experience. In a traditional experiment the audience would have just played the game in an artificial environment under analysts' observation. In this discovery event the audience followed the exercise activities closely (especially 'Blue' team reporting), and at the same time actively contributed to the experimental research objectives through structured discussions and surveys.

3. Experiment Play

The experiment audience assessed the situation in the CDX i.e. tried to comprehend the situation and project the (future) impact to the operations and businesses. The main focus was to bridge the gap between the infrastructure level actors and the strategic leaders. The obvious limitation here was that higher echelons (senior leaders in the political and media interface) were not simulated in the experiment. Instead - the challenge was addressed in briefings, orientations, sum-ups and surveys.

The execution was paused regularly to discuss, assess, review or survey about any important activity, situation or other topic. This meant that the audience was regularly asked to change their focus (mindset) from the exercise and to start thinking in more generic terms. Four different orientations (as on the agenda below) were used to focus into the most important topics.



	Monday 26.3.	*Tuesday 27.3.*	*Wednesday 28.3.*	*Thursday 29.3.*	
		9:15, Pick up from the hotels *9:45 Orientation 1*	*9:15, Pick up from the hotels* *9:45 Orientation 3*	*9: 45, Pick up from the hotels*	
10:00–11:00	*Pick up:* *09:45 Hotel Airport* *10:00 Terminal 2* *11:00 Scandic, Riihimäki* *11:05 Seurahuone*	*10:00 – 14:00 Execution* ***ORIENTATION 1*** ***"Understanding Us"*** *Lunch 12:00 – 13:00 (execution continues)* *14:00 Survey, Sum up discussion and the Orientation 4* *14:30 - 18:00 Execution* ***ORIENTATION 2*** ***"Information Pull"***	*10:00 – 13:00 Execution* ***ORIENTATION 3*** ***"Information Processing"*** *Lunch 11:30 – 12:00 (execution continues)* *13:00 Survey, Sum up discussion and the Orientation 4* *13:30 - 16:00 Execution* ***ORIENTATION 4*** ***"Decision Making on different levels"*** *14:00 – 16:00 Visitor Info*	*10:00 Experiment After Action Review:* *Cell Wrap Ups* *Orientations* *SOP Way Forward*	*10:00–11:00*
11:00–12:00	*11:15 Registration* *11:30 Lunch possibility*				*11:00–12:00*
12:00–16:00	*12:45 Welcome Remarks: Chief of Current operations, Brigadier General Jorma Ala-Sankila* *Administrative Remarks* *Orientation for the week*			*12:00 – 13:00 Final Survey* *13:00 – 14:00 Transport to the hotels and to the Airport*	*12:00–16:00*
16:00–18:00	*Getting organized, test systems and connections, training*		*16:00 – 17:15 Survey, Sum up*		*16:00–18:00*
18:00–19:00	*Wrap up of the day*	*18:00 – 19:00 Survey, Sum up*	*17:15 Bus to Signal Museum* *18:15 Dinner Officers Club* *22:00 Back to the hotels*		*18:00–19:00*
19:00–					

The intention was that there would be a 50/50 split between ‘real’ play and informed critique and discussion of the SOP and general concept. As stated previously, this would only work with high calibre participants.

The technical set-up was simple for usability reasons. A portal environment to follow Blue team reports and other CDX related information, a chat tool, exercise email and one analysis tool (VS_Room) were available within the CDX environment. FacilitatePro was used to gather ideas and insights during the experiment using both structured data gathering (tailored surveys) and unstructured forms.

3. Achievement of Experiment Aim

The primary aim of the experiment was to support the SOP development, but also to exploit the opportunity to study MNE 7 related cyber SA issues in CDX.

Combining an exercise and an experiment is always a trade-of between training objectives in the exercise and research objectives in the experiment. The exercise provided the experiment with an environment with rich reporting from the Blue teams and adequate number of other cyber activities that catalysed discussions in the Cyber Centre. The most serious limitations from the experiment perspective were twofold: The experiment audience could not interfere with the game (communicate with other teams) and the exercise scenario was simplified to serve the training goals. For example all the Blue teams – and their reporting – were similar entities (ISPs with equal services). Therefore, the efficiency of different reporting mechanisms could not be observed. Neither were higher echelons (senior leaders) and their business needs adequately present in the scenario. That made the evaluation of executive level reporting more difficult. However, all these issues were well understood and anticipated prior to the event and incorporated into the design accordingly.

An experiment is often about evaluating or testing a hypothesis or a solution and it should provide insights for that purpose. Additionally, as an event where new solutions are explored, an experiment should also be about education for the participants and their critical feedback. Based on the exit survey and other responses, the latter goal has been accomplished.

The primary goal was to support the SOP development. Based on the SOP development team understanding, that goal has also been achieved. It can be expected that after the thorough analysis of the collected material – we’ll have much better understanding of the SOP scope, focus and content, which helps us to use the remaining MNE 7 events (2 workshops and the collective experiment for the outcome) more effectively.

4. Assessment of Experiment Execution

Based on the exit survey, other responses of the audience and the general feeling, the execution of the experiment was successful.

The core idea of using 50% of the time to participate/follow CDX and another 50% of the time to discuss more in generic terms about the SA-challenge between the different layers (actors) in cyberspace, seemed to be a viable approach. However, several ideas to improve such an effort were learned during the experiment. For example the 50-50 split of the audience energy – together with technical issues of the VPN-tunnelling in the beginning, limited the CDX contribution quite dramatically. Actually, during a short 2-day execution, the audience was not really capable of producing useful SA-products in the exercise environment. On the other hand – through orchestrated discussions and surveys – the ideas and insights beyond the CDX were effectively collected and recorded. From the brainstorming perspective, we might have been better off with smaller audience.

The experiment construct with the control cell, two operational cells (Awareness and Inform) and the SOP development cell was understood and accepted by the audience. However – because of the limited time to play in the experiment – the information flows and interfaces between the two operational functions were not properly investigated. It was seen important to work specifically for the immature SOP development during the experiment. However – the SOP cell worked too much in isolation most of the experiment.

The FacilitatePro tool was used to collect the ideas, insights and observations from the participants – in addition two analysts recorded their observations. Data collection was based on both a standing opportunity to post ideas and comments to a structured discussion forum, and on five surveys – conducted after each orientation and after the AAR (After Action Review). The next survey was always revisited based on the audience response and the quality of previous survey answers. After the first survey it became clear that all surveys need to be explained to the audience to get useful answers. The collected material is both quantitatively and qualitatively good.

The technical environment and the facilities – with known limitations – served the experiment well. 20+ preconfigured workstations were used with the possibility to use own laptops. The use of own tools was encouraged, but no actual new tools were introduced by the audience. The only substantial problem rose when the access to the CDX environment (VPN, Virtual Private Network) slowed down dramatically for the first execution day after more users started using the collaborative environment. The network configuration was changed in the evening and the problem was solved.

5. Initial Findings and Preliminary Conclusions

The implications from the experiment for the SOP development effort will be assessed over the coming two weeks and reported separately.

The experimental setting, notably the constraints imposed through the exploitation of the CDX, meant that the focus for the event was the study of procedural aspects to Situational Awareness development within a Cyber Centre. Also, there was no ongoing play of 'higher' levels above the Cyber Centre. This meant that the focus, naturally, was placed on the lower 'Operator' level inputs to the Cyber Centre and the related and achievable SA aspects. It is recommended that full cycles of activity between all levels are studied in the future.

Key findings included the following:

Information Timeliness

Information timeliness emerged as a key imperative for achieving requisite SA within a Cyber Centre. This included both information processing and information sharing aspects. It is suggested that a more thorough study of such things as information processing loading & tolerances under different operational conditions would be useful.

Decision-making

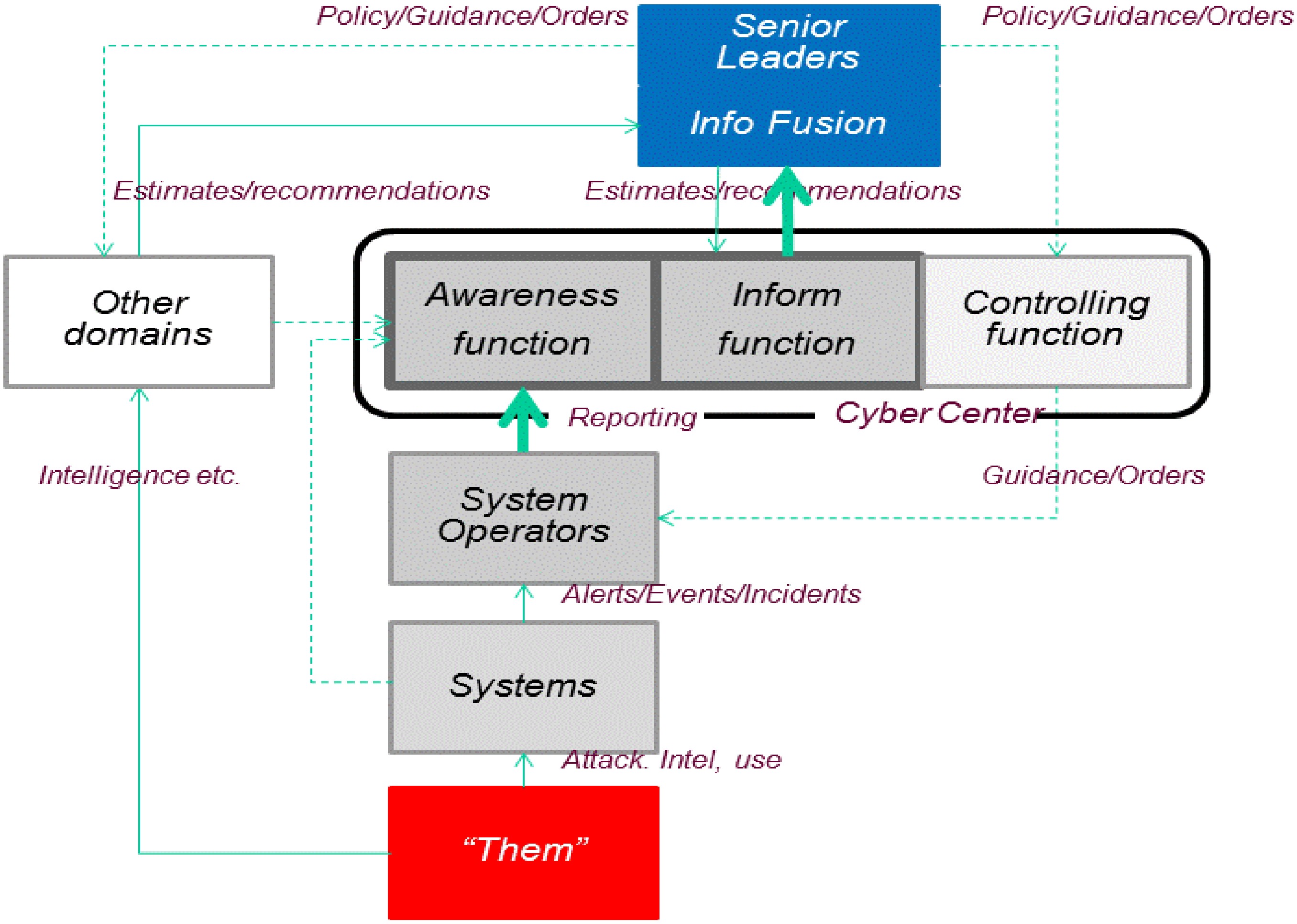
It is suggested that decision-making across the organisational architecture should be studied more fully. The link between SA and decision-making was not explored rigorously during the event (this was anticipated from the outset and was a result of the CDX constraints).

Socio-Technological Aspects

Although an emphasis was, naturally, placed on information processing, many of the issues that arose fell into what could be called 'softer' aspects of tool support; the socio-technological aspects of tool support. So, issues relating to Cyber Centre staff behaviours, competencies & capabilities, incentives & rewards arose as well as aspects like cultural and multinational issues, mandates, success indicators, organisational interdependencies etc. These ‘softer’ aspects should be considered in the ongoing investigations of Cyber SA and incorporated into the associated Tool requirements and the SOP.

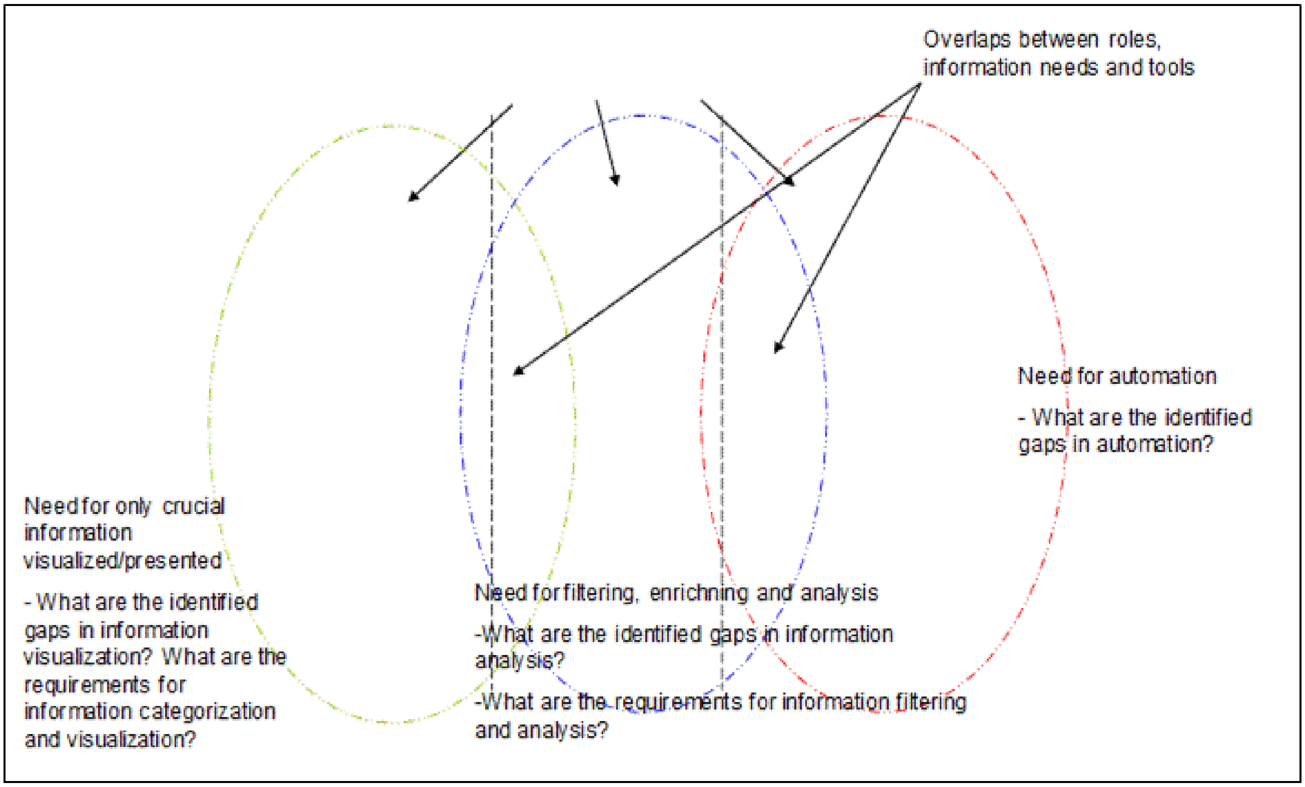
Relevance of findings and data to broader Outcome 3 (Cyber SA) aspects

The experiment was focused on Objective 3.4 and Cyber SA technologies and tool support. However, much of the findings and data gathered would be of interest and utility for MNE7 peer sub-objectives (such as 3.5 Cyber SA) and, indeed, the Outcome 3 Cyber strand as a whole. It is suggested that the findings and data relating to the structures and functions played during this event (see diagram below) could be exploited directly in the planning for the upcoming Objective 3 integrating experiment.



Technology Scope

The experiment allowed the team to understand the extent of technological support required or, at the very least, where it might be applicable. The experiment was, quite deliberatley, not a tool or technology heavy event. Still, it became apparent that, for this objective, many practical tools and their capabilities need to be studied. The picture (next page) gives a broad idea of the tool related challenges.



Overlaps between roles, information needs and tools

Need for automation

- What are the identified gaps in automation?

Need for only crucial information visualized/presented

- What are the identified gaps in information visualization? What are the requirements for information categorization and visualization?

Need for filtering, enrichning and analysis

-What are the identified gaps in information analysis?

-What are the requirements for information filtering and analysis?

6. Annexes

Annex A: The Experiment Attendance Roster

7. Points of Contacts

Experiment Lead
Auvo Viita-aho
Commander
Finish Defence Forces CD&E Centre
auvo.viita-aho@mil.fi
+358 (0)299 569 600

Analyst Lead
Anne Koskinen-Kannisto
Chief of Systems Development
Navy Command Finland
anne.m.koskinen@mil.fi
+358 (0)299 303 626