Multinational Experiment 7

Cyber Domain Outcome 3

Cyber Situational Awareness

Limited Objective Experiment Report

Version 1.0

28 February 2013

UNCLASSIFIED

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

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

4. TITLE AND SUBTITLE
Multinational Experiment 7 Cyber Domain Outcome 3 Cyber Situational Awareness Limited Objective Experiment Report Version 1.0 28 February 2013

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 MNE 7 Cyber Situational Awareness Limited Objective Experiment (LOE) was conducted from 29 October to 02 November 2012 in the Boeing Defence (UK) Portal facility, in Fleet, UK. The aim of the experiment was to test the proposition that situational awareness could be obtained from shared cyber information, that came from multiple different sources, and that such situational awareness provided significant benefits to the strategic level (senior government official, senior executive) decision maker. The experiment focused on what elements of cyber information gave value to the cyber situational awareness, the willingness of organisations to share such information and the associated mechanisms for doing so, and the most appropriate/efficient way to display the situational awareness for specific decision makers.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**83**	

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

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

4. TITLE AND SUBTITLE **Multinational Experiment 7 Cyber Domain Outcome 3 Cyber Situational Awareness Limited Objective Experiment Report Version 1.0 28 February 2013**	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 MNE 7 Cyber Situational Awareness Limited Objective Experiment (LOE) was conducted from 29 October to 02 November 2012 in the Boeing Defence (UK) Portal facility, in Fleet, UK. The aim of the experiment was to test the proposition that situational awareness could be obtained from shared cyber information, that came from multiple different sources, and that such situational awareness provided significant benefits to the strategic level (senior government official, senior executive) decision maker. The experiment focused on what elements of cyber information gave value to the cyber situational awareness, the willingness of organisations to share such information and the associated mechanisms for doing so, and the most appropriate/efficient way to display the situational awareness for specific decision makers.

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**	**83**	

Executive summary

The MNE 7 Cyber Situational Awareness Limited Objective Experiment (LOE) was conducted from 29 October to 02 November 2012 in the Boeing Defence (UK) Portal facility, in Fleet, UK. The aim of the experiment was to test the proposition that situational awareness could be obtained from shared cyber information, that came from multiple different sources, and that such situational awareness provided significant benefits to the strategic level (senior government official, senior executive) decision maker. The experiment focused on what elements of cyber information gave value to the cyber situational awareness, the willingness of organisations to share such information and the associated mechanisms for doing so, and the most appropriate/efficient way to display the situational awareness for specific decision makers.

In addition it was assumed that you are unable to protect against the first attack from any (malicious) source (zero-day attack). Therefore in order to reduce the risk in the time period between detecting that first attack and a solution to it being found, it was proposed that basic cyber information regarding the attack should be shared as rapidly and widely as possible. To this end the LOE was a test bed for sharing of information across industry sectors and government departments as well as national borders.

The LOE also brought together the other key work strands from within the Outcome 3 Cyber situational awareness:

- a resilience methodology, the key element of which is to be able to identify an organisation/nation’s critical assets/infrastructure and their dependence on cyberspace;

- an Information Sharing Framework providing the guidance to establish the capability to increase an organisation’s cyber situational awareness enabled by sharing information across a trusted community of interest;

- guidance for Decision Makers, to provide structure and consistency in formulating legal responses to malicious cyber activity; and

- a review of enabling technologies to support the fusion and display of cyber situational awareness information in a manner appropriate to the decision maker.

There were about 60 participants in the LOE from industry, academia and government departments as well as representation from the Defence departments of the MNE 7 Nations. The LOE was based on four Sector ‘Nodes’ (Air Traffic Management, Power/Energy, Telecommunications and Defence) and a national ‘Hub’ - all the scenario/vignette material was developed by experts from the respective sectors, and within the Nodes and Hub there were representatives from the relevant sector. Over five, two-and-a-half hour sessions information regarding cyber incidents, together with more generic contextual information, was fed into the Nodes and Hub. Within each Node/Hub there was a designated decision maker who was ultimately responsible for maintaining the capability/services provided by that Node/Hub. On receipt of information each Node/Hub had to consider whether to share all/some information with others, or not. The aim was to gain sufficient awareness of potential threats to continuous operation, in time to implement any mitigation required – to avoid any physical/real world impact. In the first and last

sessions the only sharing permitted was via the national Hub, in sessions 2, 3 and 4 all sharing was permitted – the only constraints being issues of trust and deep rooted culture.

Insights:

- The overarching proposition would appear to be correct. Sharing information between sectors led to better situational awareness (some surprise at the value of information received from other sectors).

- The visualisation technology provided, significantly enhanced the ability of decision makers to grasp the impact of information received.

- Clear need for an Information Sharing Agreement (ISA) was reinforced – particularly in regard to taxonomy/protocols to enable cross-sector/international sharing.

- Establishing trust was a critical enabler to information sharing. Players (as requested) brought their real world culture to the LOE and found many reasons not to share.

- The Hub role was seen as vital and it has to be responsive – session 5 was particularly testing and the Hub became overloaded.

- Participants were not high level decision makers and tended to react based on their real-world experience/position in their own organisation. (A distributed experiment may a better way of encouraging higher level participation.)

- The legal aspects were not tested to the level hoped for.

- In reality additional Information Management tools would be required to manipulate information.

The large amount of data collected provides the opportunity to conduct further analysis for greater strength of conclusion. There is more to be extracted concerning the contributions of the players to the likely demands and implications of setting up a real-world solution along the lines represented within the LOE, but the fact that many players were not truly representative of the roles they were asked to perform undermines to some degree the value of those opinions.

Contents

Chapter 1 – Introduction

Purpose

0101. This report documents the results of an initial analysis of the data generated and collected in Multinational Experiment 7 (MNE7), Outcome 3: Cyber Situational Awareness, Limited Objective Experiment (LOE) activities conducted in the UK from 29 October to 2 November 2012.

Background

0102. MNE 7 is the seventh in a series of multinational and interagency Concept Development and Experimentation (CD&E) campaigns designed to improve coalition interoperability. The MNE7 problem statement addressed the issue of ensuring access to, and action within, the global commons (the air, maritime, space and cyber domains). The cyber domain (Outcome 3) strand of work focused on generating and understanding cyber situational awareness, within the context of cyber defence operations. The MNE7 nations/organisations participating in the LOE were: Austria, Canada, Finland, Germany, Italy, Norway, Spain, Netherlands, Sweden, United Kingdom, United States, and NATO. The LOE was conducted at the unclassified level.

MNE7 Cyber domain outcome problem statement

0103. Decision makers can gain sufficient understanding (including legal) from situational awareness of their own networks and relevant parts of wider cyberspace, drawing upon integrated and collaborative information. This will improve their ability to make timely, informed and effective decisions on the actions that allow us to anticipate, deter, prevent, protect, respond and rapidly affect an adversary's ability to disrupt or degrade our access to and freedom of action within the global commons. There is currently a gap in our ability to generate national and international situational awareness across the cyber domain of sufficient quality and timeliness to be of value to a decision maker. There is a requirement for a generic and comprehensive framework that details the processes for generating such situational awareness.

Experiment Outcome

0104. The aim of the experiment was to understand how the degree of shared cyber situational awareness affects the ability of our decision makers to make timely and informed decisions on actions in and through the cyber domain global common. The LOE examined the concept of cyber situational awareness, in an immersive experimentation environment using representative scenarios and vignettes to enable the interaction of decision makers and operators with network and systems representations.

0105. In addition to addressing the concept of cyber situational awareness, the LOE leveraged the relevant outputs derived from the other key work strands from within the MNE7 cyber domain Outcome:

- a resilience methodology, the key element of which is to be able to identify an organisation/nation's critical assets/infrastructure and their dependence on cyberspace;
- an Information Sharing Framework, providing the guidance to establish the capability to increase an organisation's cyber situational awareness enabled by sharing information across a trusted community of interest;
- guidance for decision makers, to provide structure and consistency in formulating legal responses to malicious cyber activity; and
- a review of enabling technologies to support the fusion and display of cyber situational awareness information in a manner appropriate to the decision-maker.

Experiment proposition

0106. Decision makers can gain sufficient situational awareness of their own networks and relevant parts of wider cyberspace, by drawing on integrated and collaborative information. This will improve their ability to make timely, informed and effective decisions on the actions that allow one to anticipate, deter, prevent, protect, and respond to an adversary's ability to disrupt or degrade our access and freedom of action in cyberspace.

Experiment study issue

0107. How does the degree of shared cyber situational awareness affect the ability of our decision makers to make timely and informed decisions on actions in and through the cyber domain global common?

Chapter 2 – Experiment description

Experimental environment

0201. The LOE event was conducted at the Boeing Defence UK, Portal facility, based in Fleet, Hampshire, UK. The event scenario was based on a nation within which 4 sectors were selected (military, power/energy, telecommunications/critical national infrastructure, and air traffic management) together with a national Hub and neighbouring countries. Each sector was represented by a central Node through which all external communications were routed. The Hub represented a central government grouping with responsibility for national infrastructure and crisis management. Both the Hub and Nodes were to generate and maintain their own situational awareness from cyber related information that would be fed to them such that the decision makers in each (senior executives/ senior government officials) were able to make the necessary decisions to ensure the continuous operation/delivery of their respective capability/service. The Hub as a 'national' Hub, had access to information from other government departments/agencies, and acted as a conduit to other national Hubs (represented by Experiment Control (EXCON)). The key to generating sufficient situational awareness that was appropriate for each of the decision makers was in how any information received at a Hub or Node was shared further.

0202. This experimental construct tested the utility of the Hub and Node construct and the Information Sharing Framework proposed by the MNE7 Objective 3.2 work, and highlighted the issue of how to present the information gathered to a high level decision maker – how to place cyber information in context.

0203. The live part of the experiment consisted of participants conducting their roles within these cells; four Nodes and the Hub. Figure 2-1, illustrates the organisational structure of the experiment, including EXCON roles.

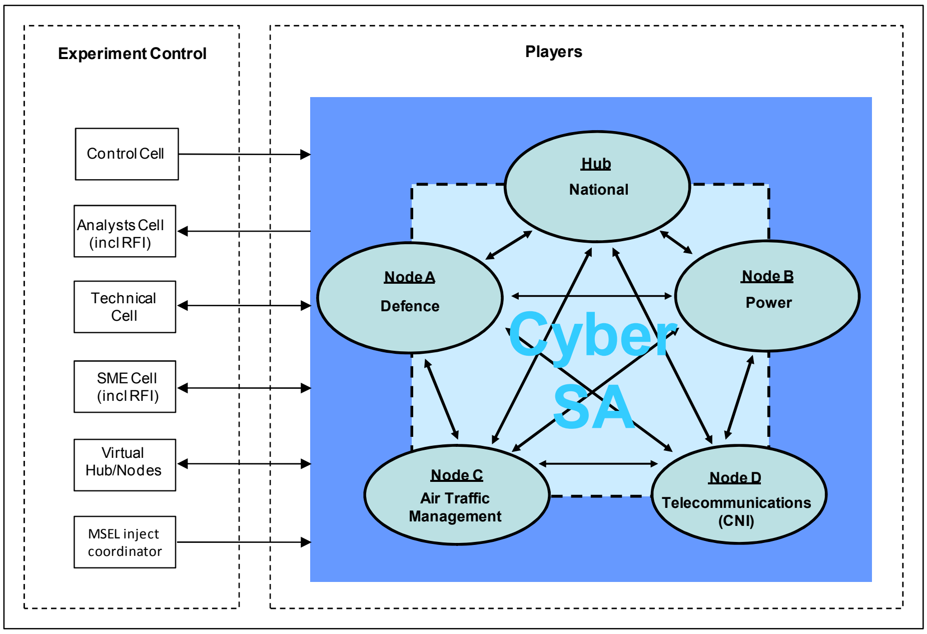


Figure 2-1 – Hub & Node organisational construct for MNE7 cyber situational awareness LOE

0204. The role of EXCON was to coordinate and provide participants with inputs (stimulus injects from a Master Scenario Events List (MSEL)) and interaction through responses to requests for information (RFI). Requests For Information would be answered by subject-matter experts (SMEs) within EXCON, who understood the overall scenario, Main Scenario Event List, and both physical and cyber infrastructure. EXCON also provided injects/responses to represent the lower control (LOCON) elements of each Node, and also virtual Hubs and Nodes as required. In addition to the playing of the scenario, EXCON had a controlling role, to ensure the experiment was executed as intended and within the rules set as part of the design. A facilitator/controller embedded in each cell ensured this function and guidance. Facilitators/controllers were precluded from influencing players, but were allowed to clarify and ensure adherence to the rules. Data collection by EXCON was essential if the event were to provide useful output. Two EXCON observer/analysts were also embedded in each cell.

0205. Each Node typically comprised of the functional roles: Decision-maker; Incident handler; Threat and vulnerability analyst; Legal advisor; and sector/infrastructure SMEs. The Hub differed slightly as it included SMEs from each of the sectors represented by the Nodes. Participants were allowed to organise, plan activities and make decisions themselves relating to their responsibilities and share of effort. In total there were 24 participants (‘players’); Table 2-1 shows the number allocated to each cell.

Cell type	Cell	No. of participants
Node	Defence	4
Node	Power	5
Node	Air Traffic Management	4
Node	Telecommunications / CNI	4
Hub	National	7

Table 2-1 – Number of participants in each Cell

0206. Figures 2-2 to 2-7 show cell players and embedded EXCON members during the experiment. The Hub and each Node had separate rooms within the Portal facility. Players conducted planning and discussion activities using dedicated information technology workstations but also had use of maps/graphical representations of relevant (and dependent) physical and cyberspace infrastructure. The suite of tools available on the workstations comprised: digital text and video communications; streaming information feeds; and infrastructure visualisation - all cell teams were provided identical tools with assured connectivity. The information sharing application supported a degree of weighting information including ‘source’ and ‘information confidence’. Cell observers and controllers also had identical workstations physically dislocated away from players, and were expected to roam within the cell to observe and capture intimate player interactions and general observations.

Figure 2-2 – ATM Node

Figure 2-3 – Military Node

Figure 2-4 – Power Node

Figure 2-5 – Telecom Node

Figure 2-6 – National Hub

Figure 2-7 – EXCON

Experiment scope

0207. The event was a human-in-the-loop experiment under controlled conditions. It was recognised that as a **limited** experiment, inherent design artificialities would cause difficulty in achieving a truly realistic representation of the operational environment expected in Nodes and Hubs. For example, all activities were driven by invented inputs (injects) from either EXCON or the experiment environment itself, which were more limited in range than real life (although in all cases the inputs were generated by experts from the respective sectors of: ATM, Power, Defence and Telecomms). Other real-life elements such as errors and breakdowns were not intentionally included, as they have little bearing on providing a better understanding cyber of situational awareness. The visualisation technology and experiment environment were a first attempt at trying to represent the collated cyber information in a real world context – appropriate to a high level decision maker.

0208. The processes needed to gain and maintain cyber situational awareness were considered through three interdependent layers, namely: *perception*; *comprehension*; and *prediction*. These were given narrow definitions for the purposes of the LOE, as follows:

- **Perception** – Noticing an event or piece of information. This is a step onwards from merely receiving it, but falls short of understanding it. It provides information about the status of elements.

- **Comprehension** – Appreciating the relevance of a piece of information. This encompasses how people combine, interpret, store and retain information. It includes the integration/fusing of multiple sources of information and determination of their significance. It yields an organised and composite picture of the situation as it evolves.

- **Prediction** – Having a view of possible future courses of events based on the understanding of past ones. This is the precursor to deciding on mitigating action and/or sharing information.

Experiment design

0209. An immersive synthetic environment was created within the Portal facility to stimulate player interaction. The live play part of the LOE was conducted over a three-day period with five discrete two-and-a-half-hour run sessions, each representing a different stage of the overall scenario. This allowed players to receive inputs in the form of events represented as external in origin and to communicate with each other according to the pre-arranged Information Sharing Agreements and the formatted incident reports. Communications between cells was controlled, in the first and last sessions (1 and 5), Nodes were prevented from sharing information/situational awareness directly with each other, but had to go through the Hub (representative of the current situation in most countries). The Hub and Node construct in conjunction with the Information Sharing Framework provided a means of anonymising (hiding the source) particularly sensitive information. A ‘repeat’ of session 1 in session 5 allowed the offsetting of any learning effects. In sessions 2, 3 and 4, Nodes were allowed to communicate and share with each other freely, though cognisant of the security and commercially sensitive pressures and barriers that might exist to prevent sharing (introduced into the LOE by using SMEs (participants) from the respective sectors). Comparison of the outcomes of sharing versus non-sharing sessions should provide insight into the value of such arrangements.

0210. Information sharing solutions may comprise of a number of trust domains that link security management with risk, policy, operations and assurance. Online collaboration is enabled by sharing information, driving the need to be able to trust others with your information and have confidence in information received from others. The tools and technologies to support information sharing were developed to ensure the integrity and provenance of information, keeping it confidential yet available.

0211. As the experiment environment and tools were new and unfamiliar to participants, a training process was built into the experiment schedule. EXCON were briefed and trained on the experiment and tools a week prior to the LOE enabling them to assist in the training of players in the afternoon of Day 1. In the morning of Day 2 EXCON and players undertook further training through a representative (no-sharing) session, and enacting specific roles and responsibilities including control and data collection. Session 1 was run in the afternoon of Day 2. Sessions 2 to 5 were played through the next two days, with Day 5 serving as contingency for any session, but also an opportunity to explore initial experiential insights through the EXCON LOE Hot-wash. The schedule is at Table 2-2; the contingency session for Day 5 was not required as all sessions were executed as planned.

	Day 1	Day 2	Day 3	Day 4	Day 5
AM	EXCON briefing	- Pre-briefing scenario/vignette.	- Pre-briefing scenario/vignette.	- Pre-briefing scenario/vignette.	EXCON Hotwash
		- Training session (No Sharing).	Session 2 (Sharing).	- Session 4 (Sharing).	
		- Post-briefing. - End of session questionnaire.	- Post-briefing - End of session questionnaire. - Semi-structured interviews.	- Post-briefing. - End of session questionnaire. - Semi-structured interviews.	
PM	Player briefing	- Pre-briefing scenario/vignettes.	- Pre-briefing scenario/vignette.	- Pre-briefing Scenario/Vignette.	
		- Session 1 (No Sharing).	- Session 3 (Sharing)	- Session 5 (No sharing).	
		- Post-briefing. - End of session questionnaire. - Semi-structured interviews.	- Post-briefing - End of session questionnaire. - Semi-structured interviews.	- Post-briefing. - End of session questionnaire. - Semi-structured interviews. - End of expt questionnaire.	

Table 2-2 – Experiment schedule

Scenario design

0212. A fictitious unclassified scenario immersed players into the experiment environment, providing a contextual awareness framework for players by feeding them with consistent and coherent information. The scenario was designed to stimulate cell players into initiating crisis action planning, sharing information about attacks (as much as they felt able to), and identifying emerging threat trends and possible courses of mitigation action on national infrastructure. This play was against a backdrop of a mildly troubled period in the history of a fictional country and its attempts to introduce economic reforms, preparations to host a high profile trade fair and increasing tensions with neighbouring states. A sense of urgency was generated while constraining players to realistic responses to the problems faced. The scenario also included contextual information from other domains (media) and 'background noise' that was injected throughout the LOE.

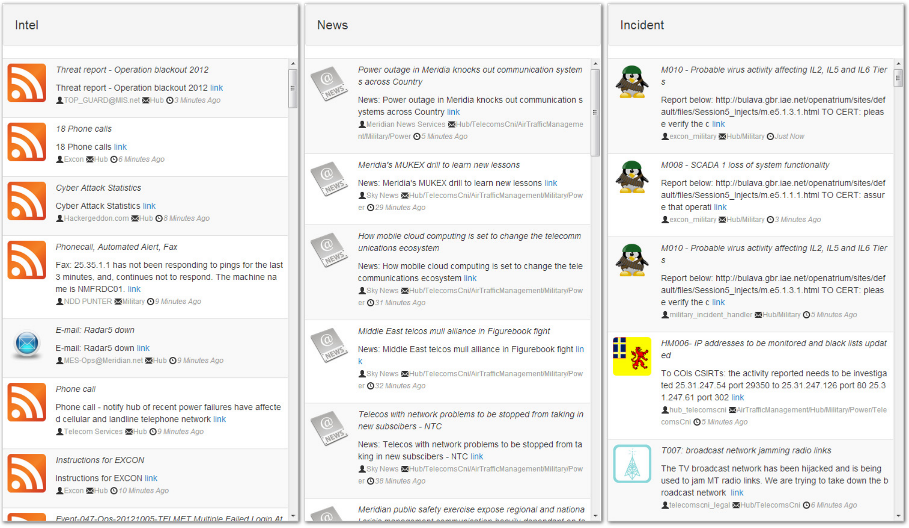
0213. Against the background scenario, four vignettes were generated that reflected the sectors represented by the nodes (Defence, ATM, Telecomms, Power). These vignettes comprised an overarching theme for each session and a series of information injects. The majority of injects from all the vignettes (a combined total of about 90/session) were designed so that they could **realistically** be sent to any Node but reaching the relevant Node was dependant on the inject information being shared. From this information the Nodes (and Hub) developed their situational awareness. The injects for each session followed an accepted 'kill chain' that built up to a specific incident, ranging from non-malicious activity to deliberate attack on part of the infrastructure. A typical chain of events could include: passive reconnaissance; active reconnaissance; perimeter probing; initial insertion; exploitation; and extraction. Cell players might only see 2 or 3 phases of this chain. The vignettes were balanced to reflect the type of information sharing protocol but also the loading on the Nodes. Support for the development of these vignettes varied considerably; ATM and Power had significant external expert contribution, this was less so for Defence due to time constraints and expertise availability, whilst the Telecomms/CNI vignettes were the least-well developed.

Experiment process

0214. Each of the five sessions followed a similar process. Players received a pre-session 'scenario brief' describing the wider socio-political situation within which the activities of the session would be set. This ensured all players shared a common context for the events of that session. EXCON SMEs who had developed and written the Main Scenario Event List briefed the rest of the EXCON team on what the injects would be stimulating, and what responses would be expected from the players for each session. This brief also guided the embedded observer/analysts to track for these events and possible player responses.

0215. Immersion in this fictitious environment was encouraged using a variety materials relating to aspects of society and events, placed within the cell rooms, along with senior national leader briefings given by broadcast voice to the players. Although such events appeared to be trivial or even frivolous, they were essential in helping to immerse participants in the scenario and generating realistic concerns among the players, fo example the benefits and adversities of sharing information between different or across similar sectors.

0216. Following the session pre-briefs, STARTEX announced by the Experiment Controller signalled the commencement of live play - driven by injects from the Main Scenario Event List Manager. Injects had a prescribed inject time and destination. Receiving cells were to track and manage incidents (injects) on the dedicated workstations using a combination of the information gleaned from streaming information feeds, logical or network/geospatial visualisations, and an incident management reporting tool that could help seek further information. Figures 2-8 to 2-10 show the typical screen displays that would be seen by players and EXCON.



Intel

Threat report - Operation blackout 2012

Threat report - Operation blackout 2012 link
👤TOP_GUARD@MIS.net ✉Hub 🕒*3 Minutes Ago*

18 Phone calls

18 Phone calls link
👤Excon ✉Hub 🕒*6 Minutes Ago*

Cyber Attack Statistics

Cyber Attack Statistics link
👤Hackergeddon.com ✉Hub 🕒*8 Minutes Ago*

Phonecall, Automated Alert, Fax

Fax: 25.35.1.1 has not been responding to pings for the last 3 minutes, and, continues not to respond. The machine name is NMFRDC01. link
👤NDD PUNTER ✉Military 🕒*9 Minutes Ago*

E-mail: Radar5 down

E-mail: Radar5 down link
👤MES-Ops@Meridian.net ✉Hub 🕒*9 Minutes Ago*

Phone call

Phone call - notify hub of recent power failures have affected cellular and landline telephone network link
👤Telecom Services ✉Hub 🕒*9 Minutes Ago*

Instructions for EXCON

Instructions for EXCON link
👤Excon ✉Hub 🕒*10 Minutes Ago*

Event-047-Ops-20121005-TELMET Multiple Failed Login At

News

Power outage in Meridia knocks out communication systems across Country

News: Power outage in Meridia knocks out communication systems across Country link
👤Meridian News Services ✉Hub/TelecomsCni/AirTrafficManagement/Military/Power 🕒*5 Minutes Ago*

Meridia's MUKEX drill to learn new lessons

News: Meridia's MUKEX drill to learn new lessons link
👤Sky News ✉Hub/TelecomsCni/AirTrafficManagement/Military/Power 🕒*29 Minutes Ago*

How mobile cloud computing is set to change the telecommunications ecosystem

News: How mobile cloud computing is set to change the telecommunications ecosystem link
👤Sky News ✉Hub/TelecomsCni/AirTrafficManagement/Military/Power 🕒*31 Minutes Ago*

Middle East telcos mull alliance in Figurebook fight

News: Middle East telcos mull alliance in Figurebook fight link
👤Sky News ✉Hub/TelecomsCni/AirTrafficManagement/Military/Power 🕒*32 Minutes Ago*

Telecos with network problems to be stopped from taking in new subscibers - NTC

News: Telecos with network problems to be stopped from taking in new subscibers - NTC link
👤Sky News ✉Hub/TelecomsCni/AirTrafficManagement/Military/Power 🕒*38 Minutes Ago*

Meridian public safety exercise expose regional and nationa

Incident

M010 - Probable virus activity affecting IL2, IL5 and IL6 Tiers

Report below: http://bulava.gbr.iae.net/openatrium/sites/default/files/Session5_Injects/m.e5.1.3.1.html TO CERT: please verify the c link
👤excon_military ✉Hub/Military 🕒*Just Now*

M008 - SCADA 1 loss of system functionality

Report below: http://bulava.gbr.iae.net/openatrium/sites/default/files/Session5_Injects/m.e5.1.1.1.html TO CERT: assure that operati link
👤excon_military ✉Hub/Military 🕒*3 Minutes Ago*

M010 - Probable virus activity affecting IL2, IL5 and IL6 Tiers

Report below: http://bulava.gbr.iae.net/openatrium/sites/default/files/Session5_Injects/m.e5.1.3.1.html TO CERT: please verify the c link
👤military_incident_handler ✉Hub/Military 🕒*5 Minutes Ago*

HM006- IP addresses to be monitored and black lists updated

To COIs CSIRTs: the activity reported needs to be investigated 25.31.247.54 port 29350 to 25.31.247.126 port 80 25.31.247.61 port 302 link
👤hub_telecomscni ✉AirTrafficManagement/Hub/Military/Power/TelecomsCni 🕒*5 Minutes Ago*

T007: broadcast network jamming radio links

The TV broadcast network has been hijacked and is being used to jam MT radio links. We are trying to take down the broadcast network link
👤telecomscni_legal ✉Hub/TelecomsCni 🕒*6 Minutes Ago*

Figure 2-8 – Streaming information feeds

0217. Figure 2-8 shows real-time streaming information feeds of intelligence alerts, news items and incident reports. A number of viewing options were available to help decision makers understand 'health' of the infrastructure. Figure 2-9 shows a 'logical' relationship or network map of the (physical) infrastructure - displaying the physical relationships between entities. Players could individually choose between the logical display or switch to a geospatial version (Figure 2-10), where infrastructure entities were overlaid onto a geographical map according to their relationship and location.

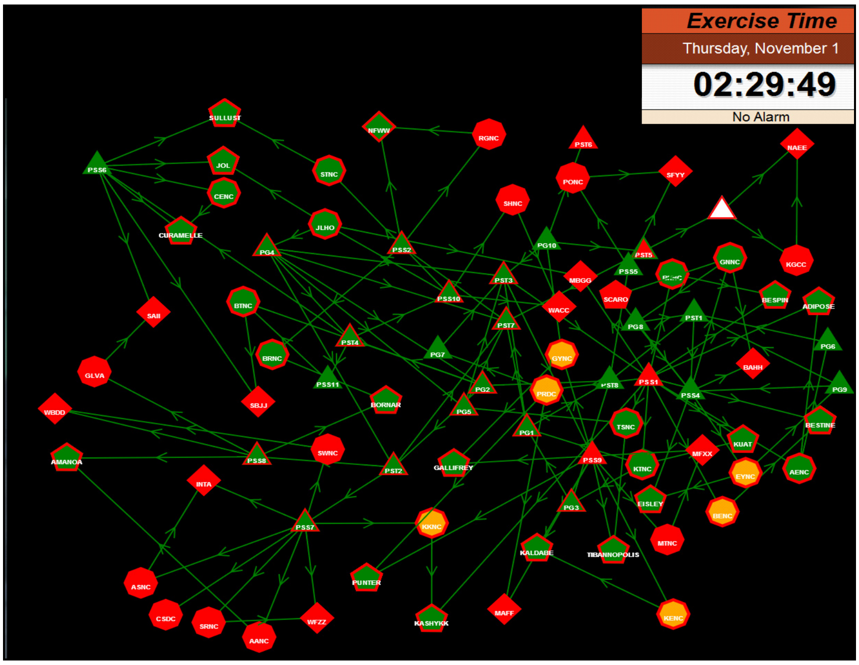


Figure 2-9 – Overall Network view

0218. The logical view was the most used by the Nodes. The view shown in Figure 2-9 is the ground truth – showing all infrastructures – as seen by EXCON; within each Node they would ideally see only their own infrastructure (that for which they were responsible) in the LOE other infrastructures could only be 'greyed out' as in the

ATM display – Figure 2-12. The colours on the infrastructure elements represented both the physical and cyber health of each element. The inner section represents the physical status of the element (e.g. is it functioning as expected) the outer ring represents the 'cyber vulnerability' of that element based on cyber information received and compared with the recorded cyber dependencies of that element. The operator could obtain additional information by placing the mouse cursor on an element to reveal the table shown in Figure 2-11. Figure 2-13 shows an opened incident report.

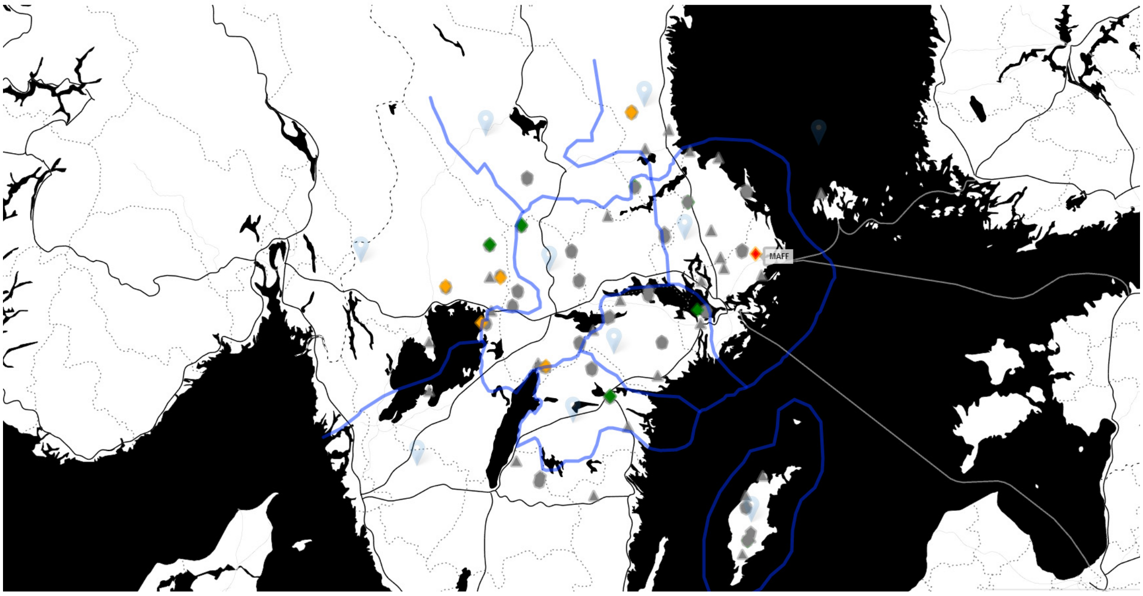
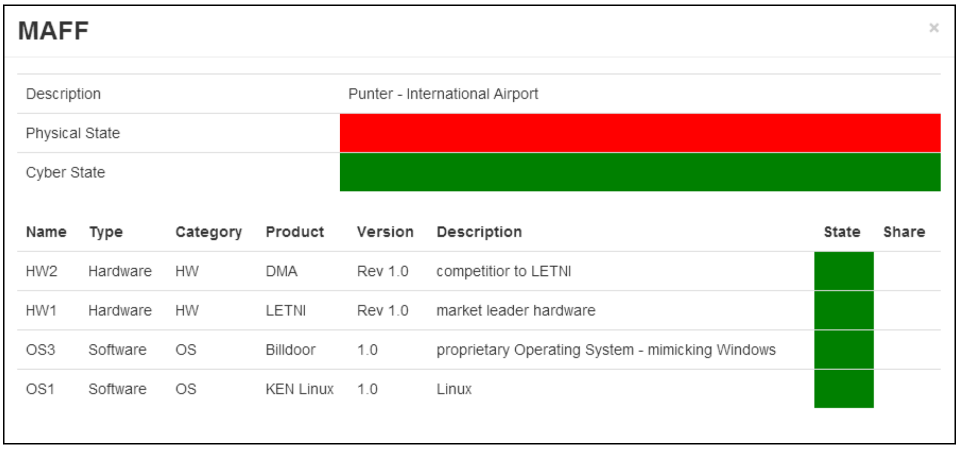


Figure 2-10 – Geospatial view

0219. Incident reports or responses to input information were generally received by the Incident Handler. Other cell members, led by the Decision-maker, would either investigate further, dismiss, record, or share information relating to this or related set of incidents with other Nodes or the Hub, in accordance with the sharing protocols. Sharing would entail preparing incident reports followed by dissemination to specific recipients outside the sector. If the players required more information, either from external sources, or from subordinate elements, a request for information to LOCON would elicit a response as if from an appropriate organisation, using the knowledge of the EXCON SMEs.

0220. Players were able to communicate face to face within a cell, or by using Instant Messaging (either to specific individuals or groups) in other Nodes/Hub – moderated by the sharing protocol. Request for information messages were ticketed directly using the Incident Management Reporting tool as well as Instant Messaging communication to EXCON Virtual Hub/Node and LOCON teams.



MAFF ×

Description	Punter - International Airport
Physical State	🟥
Cyber State	🟩

Name	Type	Category	Product	Version	Description	State	Share
HW2	Hardware	HW	DMA	Rev 1.0	competitior to LETNI	🟩	
HW1	Hardware	HW	LETNI	Rev 1.0	market leader hardware	🟩	
OS3	Software	OS	Billdoor	1.0	proprietary Operating System - mimicking Windows	🟩	
OS1	Software	OS	KEN Linux	1.0	Linux	🟩	

Figure 2-11 – Infrastructure element 'Drill Down'

0221. EXCON could flex the timing of injects, to either increase or decrease the stress placed on players, but generally they were delivered according to pre-arranged timings as shown in the MSEL in Figure 2-13. The announcement of ENDEX by the Lead Controller after two hours-and-half hours confirmed the end of the session; the input of injects would cease well before this stage to allow them to be observed by players.

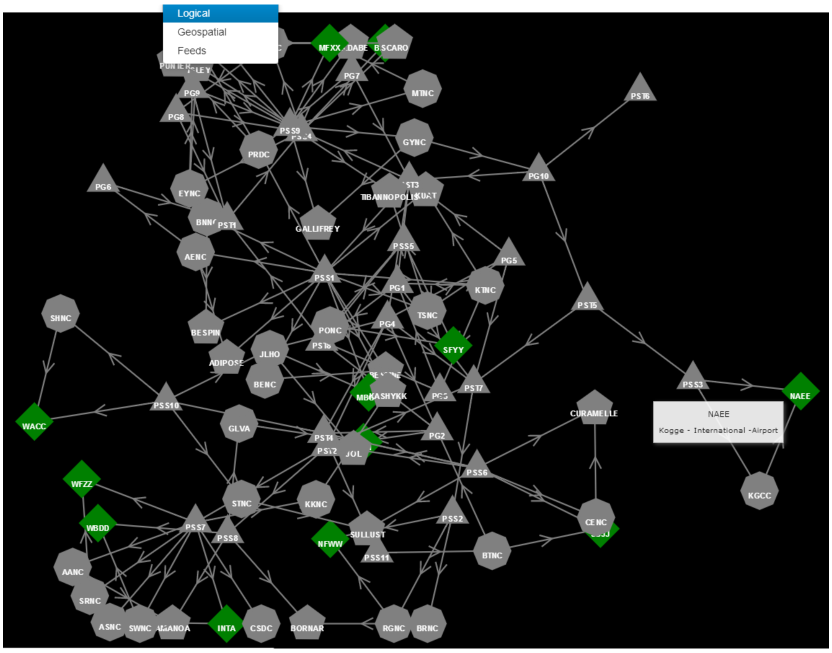
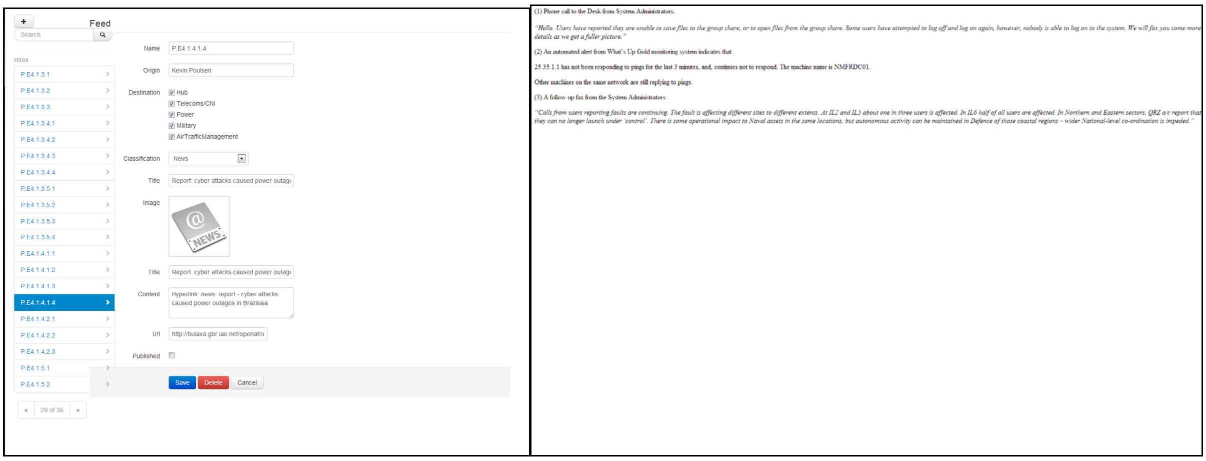


Figure 2-12 – Network view for ATM

0222. Session 1 was slightly delayed by technical issues arising from the preceding training period, in which case a late start forced a shortening of the live phase to only two hours. The end of each session witnessed an identical 'End-of-session questionnaire' to be completed by all players on the workstation. On completion of this questionnaire, a brief semi-structured interview, led by either the cell facilitator/controller or observer/analyst was undertaken with all cell participants.



Name: P.E4.1.4.1.4

Origin: Kevin Poulsen

Destination:
☑ Hub
☑ Telecoms/CNI
☑ Power
☑ Military
☑ AirTrafficManagement

Classification: News

Title: Report: cyber attacks caused power outage

Title: Report: cyber attacks caused power outage

Content: Hyperlink: news: report - cyber attacks caused power outages in Braziliaia

Url: http://bulava.gbr.iae.net/openatri

Published: □

(1) Phone call to the Desk from System Administrators:

"Hello. Users have reported they are unable to save files to the group share, or to open files from the group share. Some users have attempted to log off and log on again, however, nobody is able to log on to the system. We will fax you some more details as we get a fuller picture."

(2) An automated alert from What's Up Gold monitoring system indicates that:

25.35.1.1 has not been responding to pings for the last 3 minutes, and, continues not to respond. The machine name is NMFRDC01.

Other machines on the same network are still replying to pings.

(3) A follow-up fax from the System Administrators:

"Calls from users reporting faults are continuing. The fault is affecting different sites to different extents. At IL2 and IL5 about one in three users is affected. In IL6 half of all users are affected. In Northern and Eastern sectors, QRZ a/c report that they can no longer launch under 'control'. There is some operational impact to Naval assets in the same locations, but autonomous activity can be maintained in Defence of those coastal regions – wider National-level co-ordination is impeded."

Figure 2-13 – Incident report

Chapter 3 – Data

Data collection

0301. Data collection was an integral part of the experiment design, and the mechanism by which the design was translated, through data analysis, to worthwhile and auditable conclusions. Seven main sources of data were recorded prior and during the LOE, as follows:

- pre-experiment questionnaires, filled in by players prior to the experiment execution;
- analysts' observations, recorded throughout the sessions, aimed at capturing cell planning, discussions and decision making;
- Instant Messenger logs from discussions and communications patterns conducted over the synthetic environment;
- a situational-awareness survey sheet, completed by the decision maker throughout each session, to record the way additional inputs either supported or refuted their working hypothesis;
- end-of-session questionnaires, completed by all players at the end of each session, so that a consistent set of questions could be used to compare across the sessions;
- semi-structured interviews, conducted at the end of each session within a cell, with all players to capture their insights; and
- end-of-experiment questionnaire, filled in by each player having completed the entire experiment, to capture their own insights and lessons identified that could be taken forward.

In addition to these formal sources, player workings/annotations, and other outputs from individual cells also provided a source of raw data for potential analysis.

0302. The data-collection process for the analyst/observers entailed recording player behaviour during the live session play, in accordance with the guidance given in the MNE7 Analyst Guidance document, shown in Annex A. A sample situational awareness survey sheet and the instructions for completion by players are detailed in Annex B. At the end of sessions, players were directed to complete individual end-of-session questionnaires (questions listed in Annex C), after which the cell observer/analyst would then guide players through plenary a semi-structured interview (again following the guidance note). Audio recordings from the interviews allowed accurate notes to be transcribed. At the end of the final session, players completed an individual end-of-experiment questionnaire (questions listed in Annex D) before the cell plenary interview.

Data collected

0303. The experiment generated a large amount of quantitative and qualitative data, collected according to the collection plan outlined. Every player completed the pre-experiment questionnaire, providing the analysis with demographic data to be used as both a description of the type of player participating but also as a potential correlation to other effects.

0304. End-of-session questionnaire responses were collected for 23 players (two Hub players contributed to a single survey in collaboration). At least two responses were missing due to players completing the wrong questionnaire due to an error in the synthetic environment. Despite such minor problems, this gave a good richness of responses from across the cells and across the sessions.

0305. Audio recordings were made of all five post-session semi-structured interviews in each of the five player cells. All of the instant-messaging chat logs was recorded by the synthetic environment, with a significant amount of individual entries recorded. Several of the situational awareness survey sheets were completed during the sessions.

Chapter 4 – Analysis

Demography analysis

0401. A total of 24 players from nine nations participated in the experiment, all, but one, of whom were male, and generally aged over 40 years, with 40-to-45 years being the most populated age group. Players were not homogenous in training, background or performance. A sufficient mix of industry (nine) and military (12) players were distributed across the Nodes/Hub, three players were not affiliated with these groups. Almost all players had graduate-level education with a significant majority with post-graduate qualifications; the mean experience (in their field relevant to the node) was 13 years. Players were distributed across the cells such that each cell contained a range of background, education, and ages, some evidence showed that experience may not have been as extensive or evenly distributed as desired. The Military Node was the exception, which by design excluded participants without relevant background or knowledge. Players showed a slight inclination towards 'conclusive and decisive' and 'deliberate and rational' thinking styles. A high level of confidence of relevant domain knowledge was indicated by players; although the ATM Node appeared to be lower than average.

End-of-session questionnaire

0402. **Situational awareness overview - cell comparison**. A key question for the LOE was the level of awareness of the situation as a whole, which was documented using the questionnaire at the end of each session – the higher the answer value the better the perceived level of situational awareness. Figure 4-1 shows a comparison of the perceived level of situational awareness according to the role of the participants using the answers to the question *"Rate your awareness of the situation as a whole - to what degree you felt you understood what occurred in the session".* Each chart shows, for a given cell, the responses to this question in each of the five sessions. Note that not all cells contained the same roles.

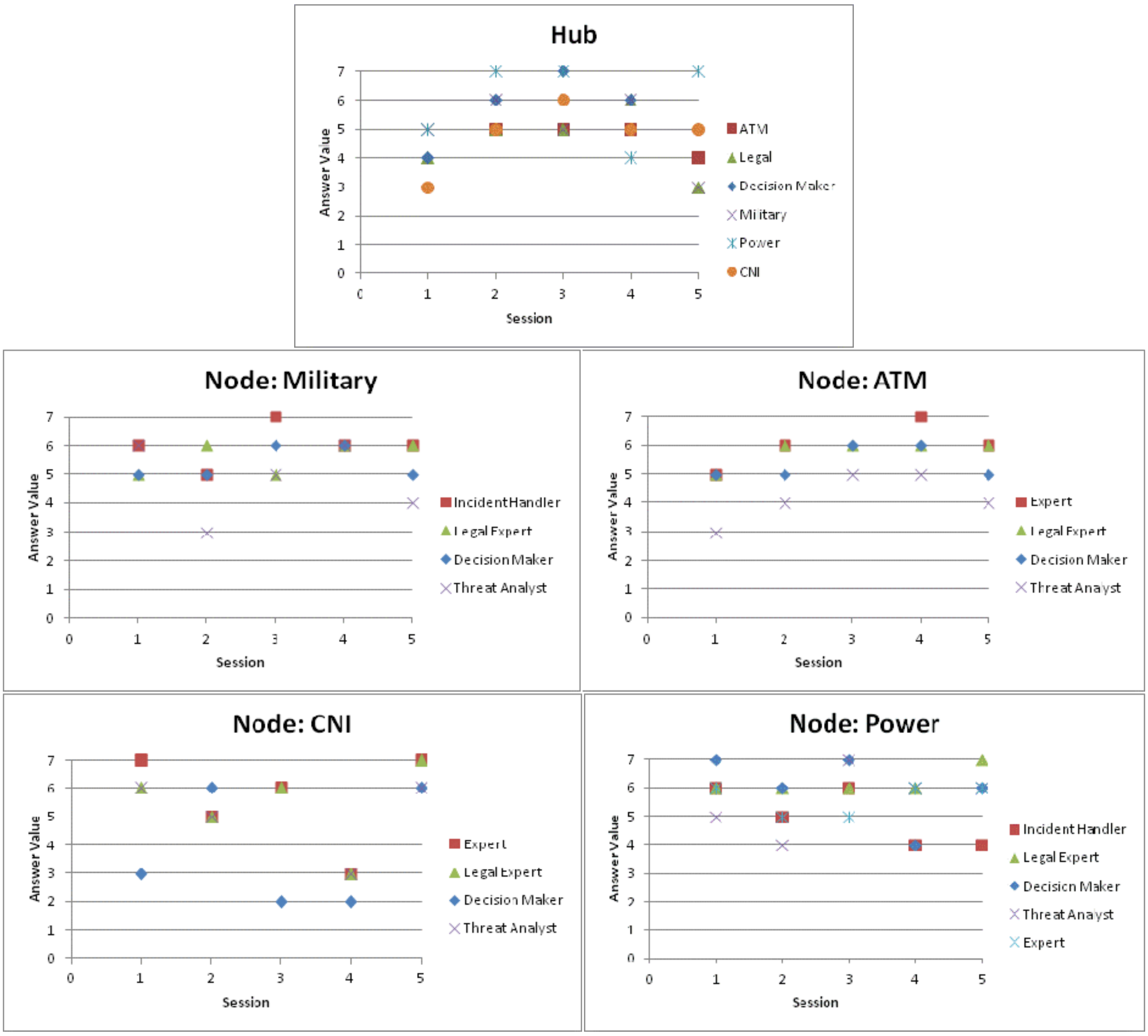


Figure 4-1 – Cell comparison of the perceived level of situational awareness by role

0403. In general, the players' (perceived) level of situational awareness was consistently high and reasonably clustered within each cell for each session, though the Telecomms/CNI Node appeared to deviate from this pattern. This deviation may be attributed to several reasons:

- variable level of relevant experience (cell SMEs appeared to be technical in background and operating at a lower level than the intended strategic role of the Node);

- differences in understanding coupled with language and cultural barriers between players, and exacerbated by the high technical content of discussions within the Node - specifically for session 4 where the main scenario event list placed higher demands on this cell.

0404. Furthermore, the injects developed for the Telecomms/CNI Node were least well-developed due to difficulties in obtaining sufficient contribution from external expertise.

0405. **Does the information sharing policy affect the perceived level of situational awareness?** Across the five sessions two distinctly different information-sharing policies were applied. Sessions 1 and 5 restricted information/situational awareness exchange amongst the individual Nodes, shifting the responsibility of sharing to the National Hub, whilst for sessions 2, 3, and 4, information exchange between Nodes was permitted. Question 1 of the end-of-session questionnaire, *"Rate your awareness of the situation as a whole - to what degree you felt you understood what occurred in the session",* best captures the perceived level of situational awareness. The following analysis compares the results across roles and by cell type.

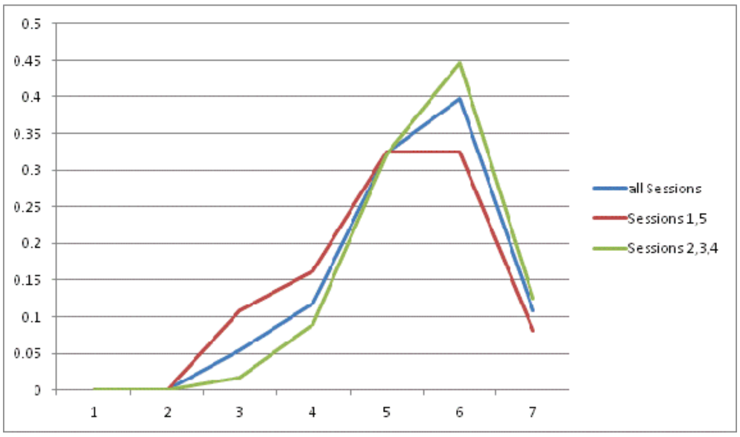


Figure 4-2 – Perceived situational awareness: all roles, all nodes except Telecomms/CNI; grouped by sessions

0406. **Individual role**. Figure 4-2 shows normalized[1] results for question 1, where "7" on the horizontal axis indicates the highest level of perceived situational awareness. The chart includes all participating function roles (i.e. decision maker, Infrastructure SME, Legal adviser, Incident handler, and Vulnerability and threat analyst) for all Nodes except the Telecomms/CNI node. Although a slight distinction is observed amongst the depicted groups (Group 1: all sessions; Group 2: sessions 1 and 5; Group 3: sessions 2, 3, and 4), it can be inferred that the information sharing policy had little influence on an **individual** player's perceived level of situational awareness.

[1] The vertical scale on this chart, and subsequent charts up to and including Figure 16, is simply the frequency of the score divided by the total number of all scores – this allows for missing data and unequal numbers of roles.

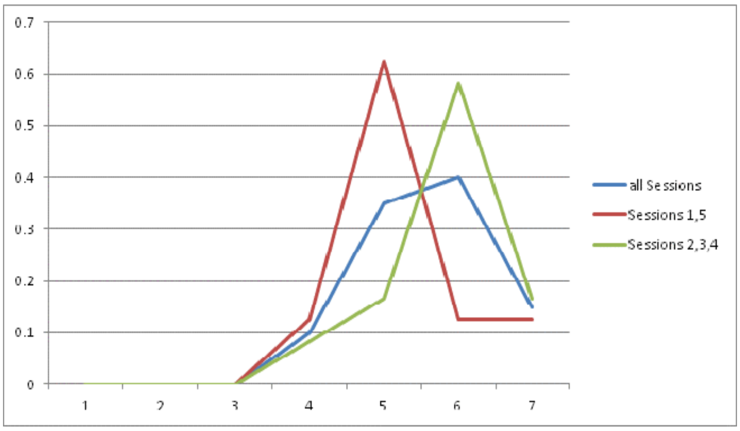


Figure 4-3 – Perceived situational awareness: role Decision-maker, all nodes except Telecomms/CNI; grouped by sessions.

0407. Further analysis focusing on the ‘Decision maker’ role (see Figure 4-3) indicates a different insight. For the Decision maker role, the perceived level of situational awareness was lower when the information sharing policy limited the flow of information solely to the National Hub (sessions 1 and 5), and higher when information could be shared amongst the Nodes (sessions 2, 3, and 4).

0408. **Individual cell**. Figure 4-4 depicts normalized counts of all roles within the Hub, grouped by the information sharing policy for the sessions. The perceived situational awareness appears to be lower when information sharing is only permitted through the Hub (Sessions 1 and 5). A combination of factors are likely to contribute to this effect, particularly as the Hub has two key operating modes – information management/exchange gateway and as an authoritative adviser based on assimilated processed information to provide guidance on protection and best practice. During Sessions 1 and 5, an increase in workload can be expected for the Hub with a shift towards information management/exchange gateway rather than authoritative adviser. This consequently lacks the processing of information and increase in content value. However, for Sessions 2, 3 and 4, a higher level of information intelligence is ascertained by better-informed Nodes (attributed to sharing amongst Nodes), and in turn provides an improved ingest for the Hub, thereby increasing the level of situational awareness in the Hub.

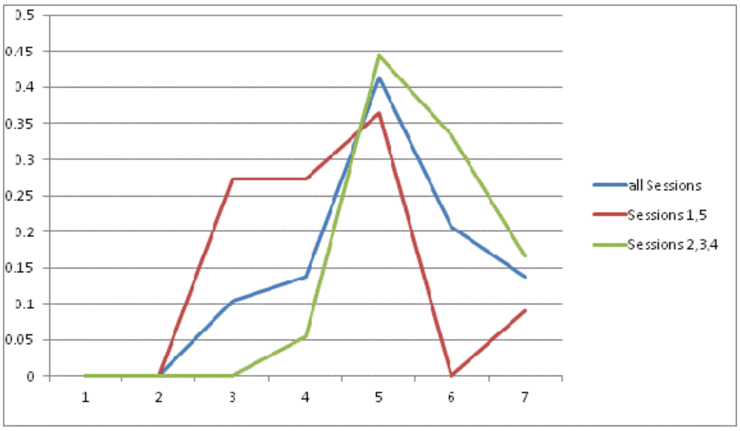


Figure 4-4 – Perceived situational awareness: all roles, Hub; grouped by sessions

0409. The respective graphs depicting the level of perceived situational awareness for the remaining cells are shown in Figure 4-5. The ATM Node appears to be the only Node reflecting a similar trend to that of the Hub, indicating a lower level of perceived situational awareness when the restrictive information sharing policy is applied. This is likely to be due to the strong tie developed with LOCON during the LOE development. Alternatively, this effect might be explained by the higher level of experience within the cell and by how coherently the team as a whole performed. The levels of perceived situational awareness for the Telecomms/CNI Node are similarly erratic to that previously seen in Figure 4-2. This reflects the level of resources available in the time frame to support development of the vignette injects. For the Power and Military Nodes the different information sharing policies seems to have very little effect on individual perceived level of situational awareness.

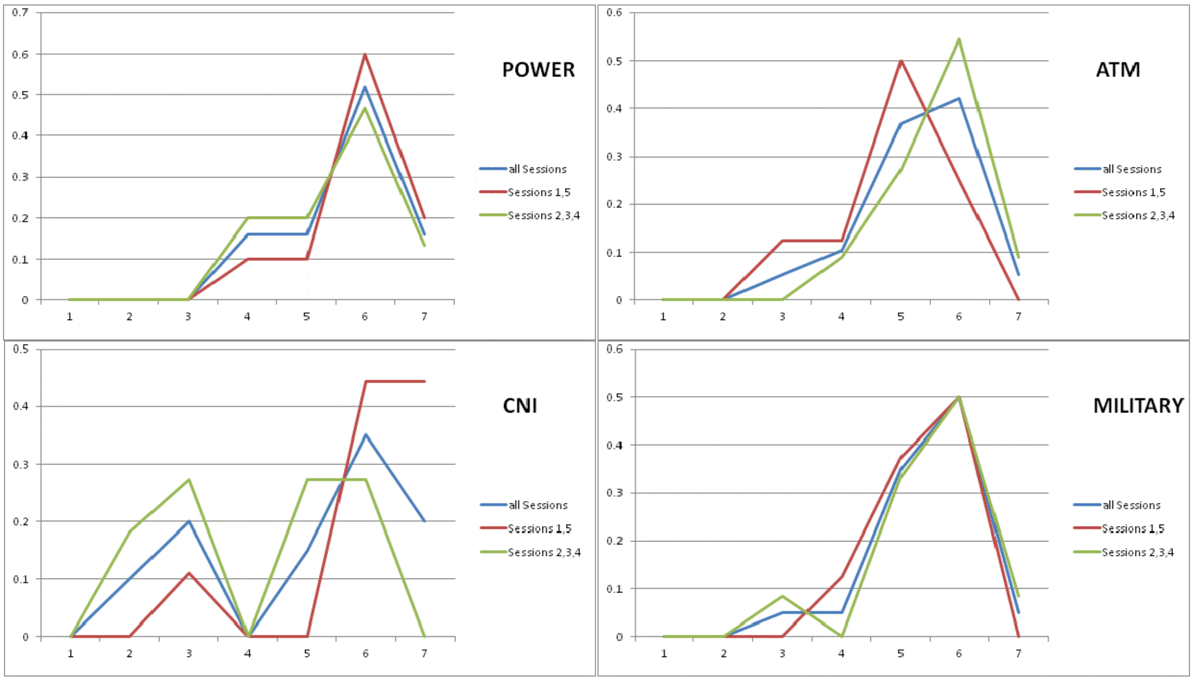


Figure 4-5 – Perceived situational awareness; all roles, by cell: grouped by sessions

0410. **How effective was the system (experiment environment) regarding noticing new information?** Normalised results of the question, *“Rate how soon, on average, you felt that you noticed new information entering the environment”* are illustrated in Figure 4-6. Overall trends are consistently low, indicating room for improvement for noticing new information. A valuable follow-up question is whether the expected volume of injects and incident reports due to different information-sharing policies has an effect on players noticing new information. As depicted in Figure 4-6, there is no discernible distinction among the two information sharing policies (sessions 1 and 5, versus sessions 2, 3, and 4).

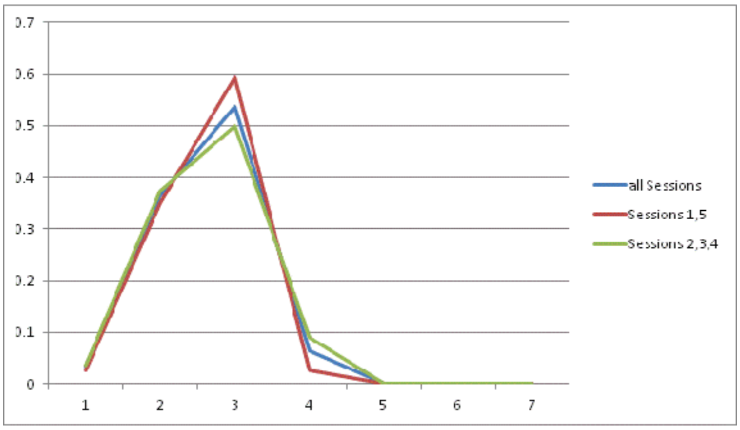


Figure 4-6 – Perceived timeliness of new information: all roles, all cells except Telecomms/CNI; grouped by sessions

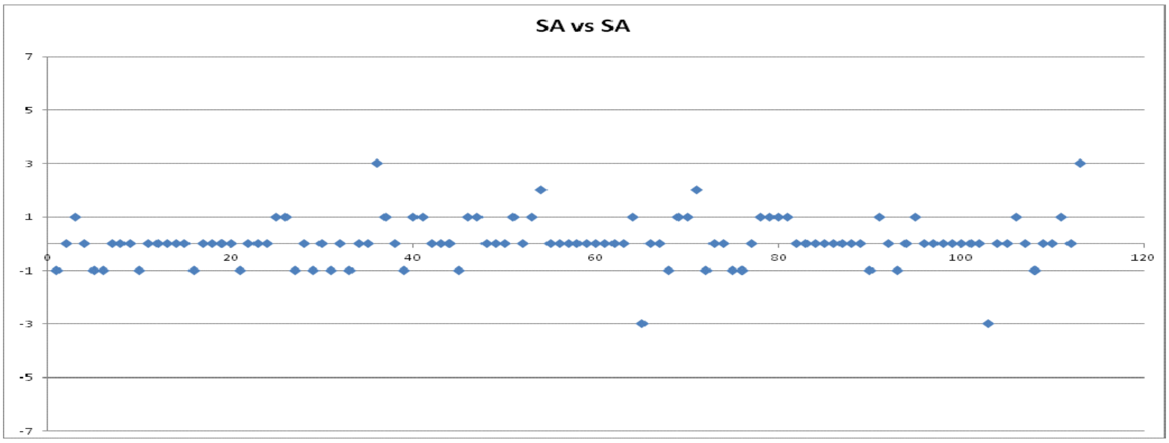


Figure 4-7 – Comparison of two situational awareness related questions

0411. **Survey participation effort**. The End-of-session questionnaire allowed two pairs of questions to be used to deduce an indication of the survey participation effort. Firstly, two questions that were aimed at the perceived level of situational awareness: Q1, *“Rate your awareness of the situation as a whole - to what degree you felt you understood what occurred in the session,”* and Q15, *“Overall, please rate your level of situational awareness for this session”.* The assumption is that the answer values should be the same. Figure 4-7 shows there are only four answer values that deviate by more than two classes, suggesting a good level of player answer consistency.

0412. Secondly, there were two mutually-exclusive aspects regarding the predictability of the scenario development: Q11, “Rate how often you were able to predict how the scenario was going to develop”, and Q12, “Rate how frequently you were surprised by the direction the scenario developed”. **Assumption**: the answer values should be complementary. Figure 4-8 shows only three answer values deviating by four classes or more, and additionally six values that deviated by more than two classes, suggesting a good level of player answer consistency.

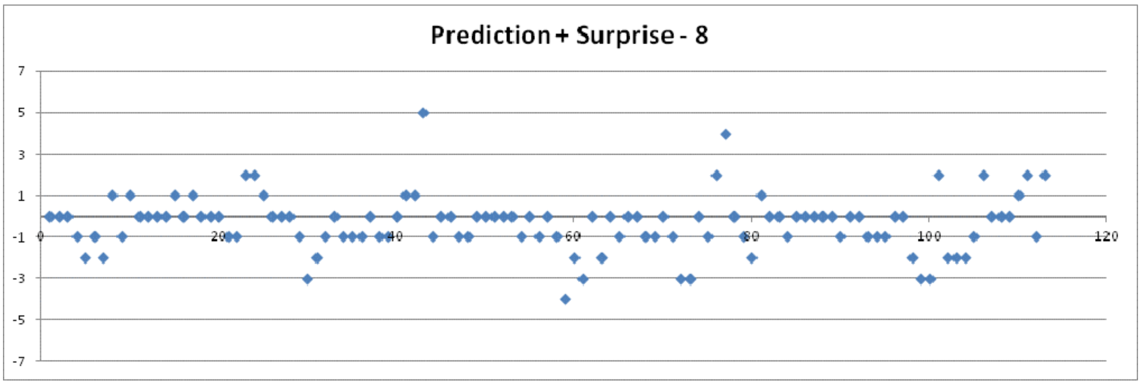


Figure 4-8 – Comparison of two questions about predictability of scenario development

4.3 Semi-structured interviews

0413. Annex E presents a capture of the individual semi-structured interviews. This section draws out the common themes from those summaries.

- **Cell roles and responsibilities**. Every cell except ATM noted initial performance challenges, generally due to a lack of understanding about the roles of LOCON and the other cells. There was some confusion surrounding each cell's roles and responsibilities within the national framework – the internal organization and processes were uncoordinated. Every cell except ATM reported improved group performance in the ensuing sessions; by session 3 and 4, internal cell interactions and processes had matured to good working levels.

- **Non-intuitive toolset**. The knowledge and practice time allocated for operating and understanding the tools was deemed limited. Cells were unable to fully understand the situational awareness visualisation tool health (colour) status indications, along with a lack of 'real-world' data richness/reality.

- **Incident tracking and review**. The Hub and Telecomms/CNI Node used alternative methods (from the toolset) to resource manage and track incidents. Nodes prioritised incidents by local SME subjectivity, tackling the most serious problem first. No formalised prioritisation method was developed. The need to prioritise and track incident was observed as key feature absent from the experiment toolset.

- **Effective situational awareness**. The Hub and ATM Node clearly recognised that information sharing provided improved situational awareness; however the Military Node were 'starved of information' when information was not shared across Nodes in the final session. All Nodes expressed generally poor or non-existent situational awareness concerning the status of the other Nodes.

- **Filtering of information**. Nodes appreciated the aspect of interacting through the Hub, but also that of the Hub 'filtering' incoming information.

- Nodes indicated they had a good idea of what information was required by the other Nodes, though with the exception of ATM, some deficiencies in the information received from the other Nodes was observed. The Power and Telecomms/CNI Nodes suggested this spread of misinformation could be mitigated through a liaison position.

- **Inject/Vignette credibility**. A review of the injects for real-world credibility would be required. The timelines were designed to test specific elements of the system with a steadily increasing severity of problems; it is possible they were viewed as being unrealistically severe.

End-of-experiment questionnaires

0414. The questions for the End-of-experiment questionnaire are listed in Annex D. Annex F presents graphical summaries of the answers to questions that did not require written answers. This section summarises some of the main points that arose.

- **Incident tracking, management and review**. Relatively poor scores for both the tools and facilities (Q.1 to 5) and could be attributed to the lack of information/incident tracking and prioritization tool, but also confusion over the interpretation of infrastructure ‘Status Display’ symbol colours. Similarly associated low scores were observed with the Decision-makers’ score on system support of situational awareness (Q.41). The need to modify or adapt processes and system tools/environment for handling information was a key issue raised by players. Figure 4-9 shows use of the value of an ad-hoc incident board for plotting information to visualising incidents and establishing patterns.

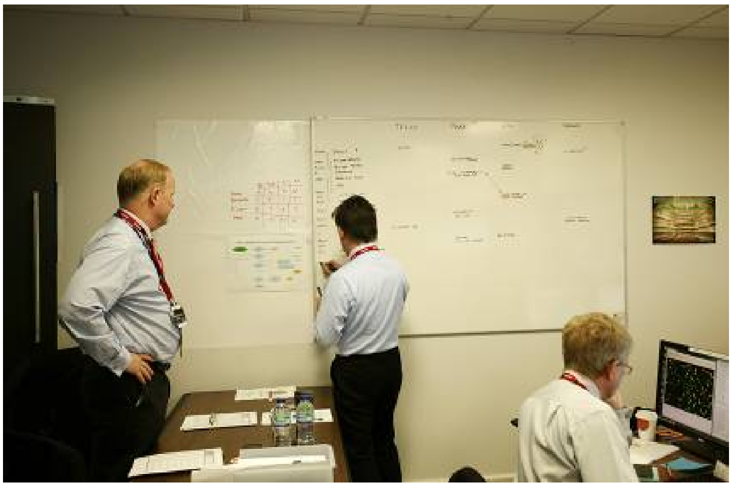


Figure 4-9 – Use of alternative methods to track incidents in the Hub

- **Scenario/vignette maturity**. Minor discontent on unrealistic injects and scenarios was observed, however a good response concerning system realism/workability (Q. 14). A high score for scenario / vignette sufficiency (Q.56) providing additional credibility to the overall experiment. In general, it appears there was enough perceived ‘realism’ to go forward with credible general conclusions.

- **Information sharing**. Good Node coordination (Q.29) which supported the experiment's basic premise. There were also calls within the SSIs for Liaison personnel to enhance information sharing effectiveness.

- **Role of the national Hub**. The Hub appears to be vital (Q.30) information exchange gateway, able to filter information and add value (intelligence) for the Nodes.

- **Mode of communication**. Communication preferences (Q.48) favour direct contact through Instant Messenger. The Hub showed a higher preference for the Incident Management Reports, probably due to the Hub's need to track overall situational awareness, whilst the cell SMEs and Decision maker need the Incident Management Reports for tracking and prioritisation.

Observations

0415. **Structured data sharing**. A gap for a structured data sharing mechanism to encapsulate host/network status information to drive more assets was identified by the Military cell.

0416. **Incident tracking, management and review**. The need to develop additional tools to aid the tracking, management, and responses to incidents was identified by players. Effective management and response to incidents requires applying detective and corrective controls to minimise adverse impacts, gather evidence, and learn from previous situations. Real-time analysis of the information technology and incident events will be required; the speed with which an organisation can recognise, analyse and respond to a security incident will limit the impact of the damage and potentially lower the cost of recovery. Another risk to mitigate will be the introduction of sudden or progressive changes of the threat landscape, creating unexpected volumes of new events to be managed. Such management requires being accessible by all players – essential for individual and collective situational awareness.

0417. The Incident Management and Reporting tool and streaming information feeds presented information in real-time, though without any provision for storage, search and retrieval capability, or tracking a sequence of incident events. Other functions absent from the suite of experiment environment tools included the ability to manage incident reports - either to prioritise (by criticality), or discard (due to redundancy or lack of applicability). Some cells resorted to assigning incidents to individual players for status tracking and mitigation responses, using flowcharts to depict the mitigation process along with analysed and prioritised options. Further analysis identified infrastructure with the susceptible[2] components with these options. Incident reports required to be systematically labelled to enable

[2] The term vulnerability was to mean a specific instantiation of a technical weakness, whilst susceptibility used to in the sense of host(s)/network(s) being open to compromise by a specific instantiation of a technical weakness.

easy archiving, searching and retrieval to find past events; this categorisation and labelling was demonstrated by the Military and Power Nodes. A further step recognised but not undertaken was to document the incident description, mitigation plan, actions and lessons learned for future reference, searches, and trend analysis.

0418. The implications of these observations is to provide explicit requirements for future design – i.e. reviewability. The tools supplied did not provide the ability to store, search, retrieve and examine historical events; a significant oversight when dealing with scenarios that required participants to build up awareness of the events occurring. Situational awareness is not simply spatial or temporal, it is also historical and contextual – decision-makers require an understanding of what has previously occurred in order to make informed decisions in the present time.

0419. Cell Decision makers were provided with situational awareness Survey sheets (shown in Annex B) to track their decision making and confidence, with which they could theoretically track their thinking. In practice these were frequently abandoned, annotated post-hoc or lacking in detail. It was anticipated that these surveys could allow the review of the incidents that occurred, but in reality fell short of this purpose. This appears to have been for two reasons. Firstly they were limited to the Decision maker and provided no awareness for the rest of the cell. As a consequence they did not provide mutual reference points that the improvised tracking systems did. Secondly, they were not revisable – they were fixed in time where the improvised lists were modified, edited and updated as new information became available. As a method for maintaining situational awareness, they demonstrated the necessity of timeliness.

0420. **Modifications**. Players made frequent adjustments to their individual or cell working environment through developing additional spreadsheets, and notes to facilitate optimised workflow process to their specific needs. Efforts should be made to allow system flexibility around core requirements to enable this cognitive offloading. This need will be more pronounced if the tools designed for real world activities as different sectors and industries will have their own standards and methods, and be impractical to design a fully integrated holistic system.

0421. **Incident awareness and saturation**. Players were generally aware of incidents that affected them, although there were also a large number of incidents which they did not become aware of. This may be attributed to a lack of sharing at times, and due to the lower operating level of players. Players were observed to engage with one particular problem and then become unaware when another issue arose, or if a previous issue re-emerged as more significant. This supports the observation that players were sometimes lowering their intended (strategic) level of operations, and actually missing a significant amount of information because they had a task to occupy them and unaware of other tasks to engage with, hence the level of perceived situational awareness may have been lower than reported. This also demonstrates the potential for situational awareness to become potentially too focused; the system did not afford awareness of the wider situation when an event/incident was prioritised.

0422. **Player experience**. Player experience levels may not have been sufficiently high for the tasks they were expected to perform. Some players focused largely on problem-solving, although the tasks were intended to require a strategic overview of events. Players with higher levels of experience, and those more accustomed to management-level strategic decision-making, may have been less distracted by detailed information, and aware of the additional problems, and shared information more effectively. The effect of experience on the establishing situational awareness should not be underestimated; greater experience should enable more effective discrimination of information.

Messaging data

0423. Instant Messaging was a form of point-to-point (individual-to-individual or individual-to-group) communication between cells; a log of all messages allowed to record the frequency of contact. Message totals were assembled for all players shown in Figure 4-10, providing a view of where the *directed* conversation was occurring during the course of the experiment.

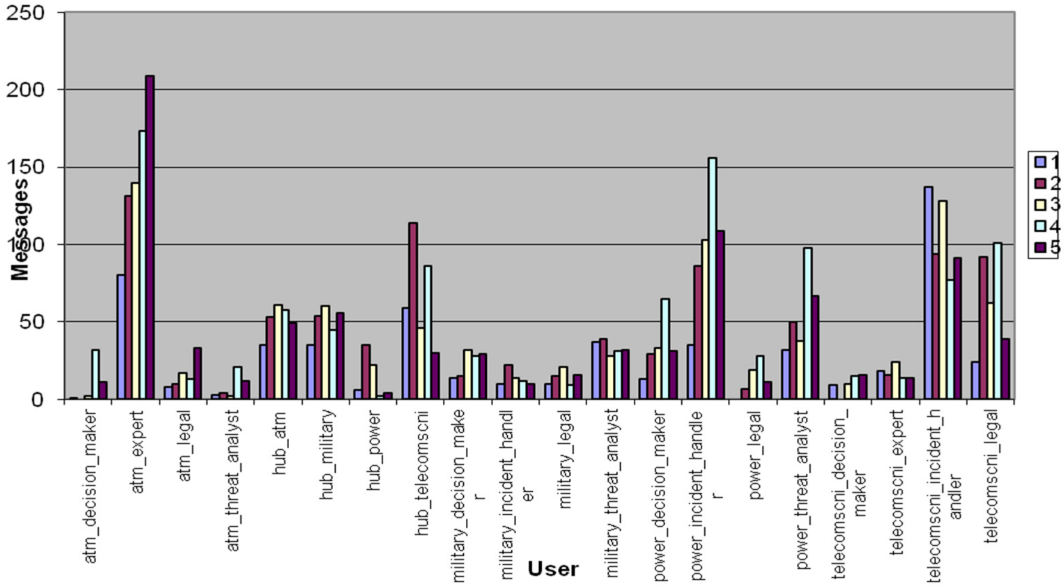


Figure 4-10 – Total number of messages sent (y-axis) by user (x-axis) and session (see legend)

0424. The chart demonstrates the significant differences between, both users and cell groups in terms of Instant Messenger tool use. It illustrates the variability of which user role was communicating the most, supporting previous observations of how cells managed their workload, and not necessarily assigning effort according to role function. As an illustration, the ATM cell expert was communicating substantially compared to the rest of the ATM cell. Further consideration of cell roles and functions is required in terms of work load and not just aligned to experimentally-assigned roles.

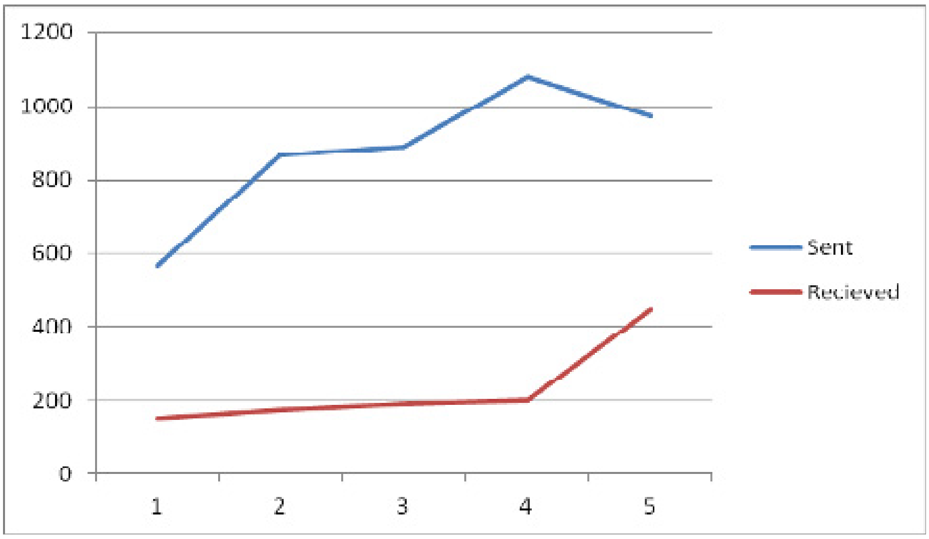


Figure 4-11 – Total messages (y-axis) sent or received by session (x-axis) for all cells and players

0425. A comparison of the volume of messages sent and received by players is shown in Figure 4-11, illustrating a simple metric of player behaviour as the experiment progressed. The high volume of messages sent indicated that players were communicating and sharing more often as the sessions proceeded, however, the number of messages received generally remains constant and low over the same period. Players during sessions 1 to 4 were actually communicating more with EXCON rather than each other. This could be attributed to the increase in sharing, but also that players may have had more challenges to address, and communicate with EXCON. Figure 4-12 provides further evidence by illustrating the number of messages sent/received for EXCON. During session 5 (no sharing), an increase in messages may have resulted due to EXCON significantly communicating more with players, a low point is observed during session 3 where sharing between Nodes should be fully established.

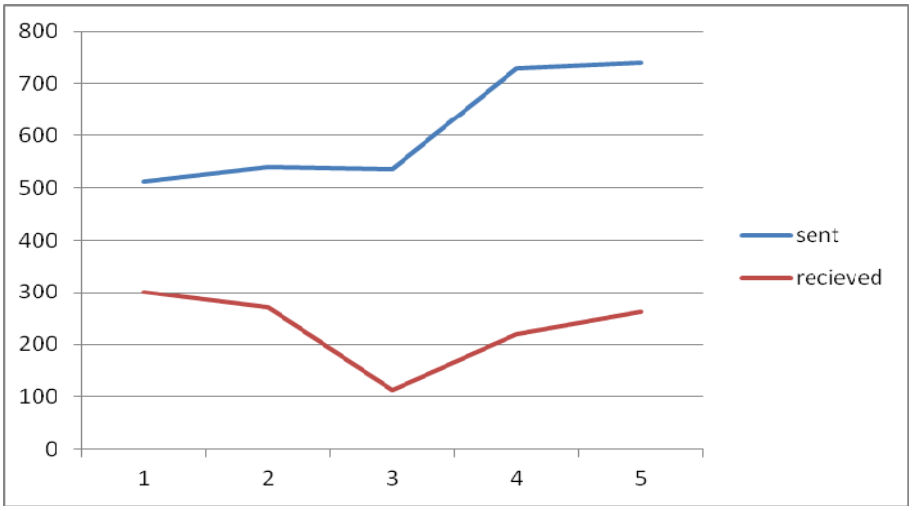


Figure 4-12 – Total messages (y-axis) sent or received by experimental session (x-axis) for EXCON

0426. Detailed analysis (shown in Figure 4-13), suggests that during the second restricted sharing condition (session 5), increasing player-hub communications were observed than previous sessions. Cognisant that players had become used to sharing and receiving more information from other Nodes, the restrictive sharing condition resulted in players seeking alternative sources (Hub) to maintain or enhance the level of situational awareness.

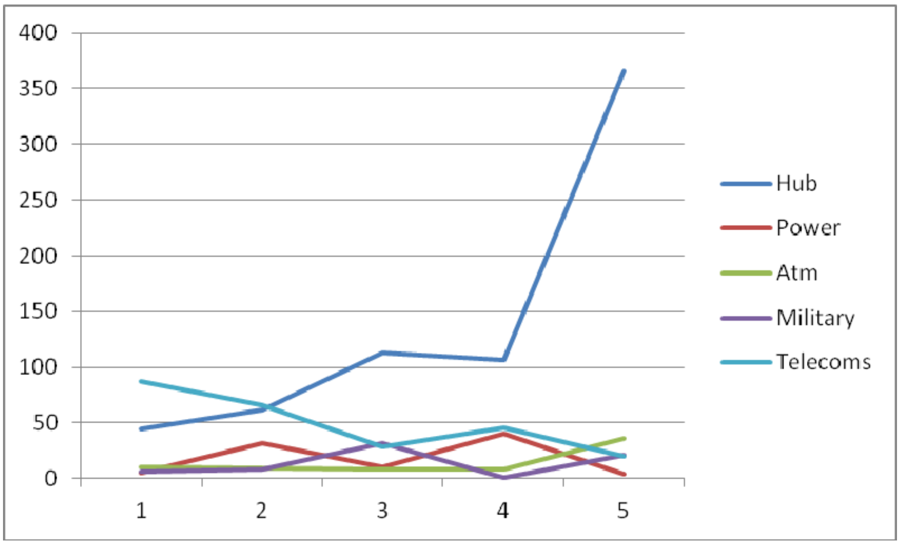


Figure 4-13 – Total messages received (y-axis) by experimental session (x-axis) and cell

0427. The volume of messages 'sent' can also be further analysed by cell (Figure 4-14). Firstly, the Hub was unable to match the tempo of messages sent by players during session 5, indicating that that Hub players may have struggled to cope with sudden increases in workload and attention. Secondly, the overall number of messages sent by the Military Node remains relatively low and constant across all sessions, whilst other cells increased communications significantly.

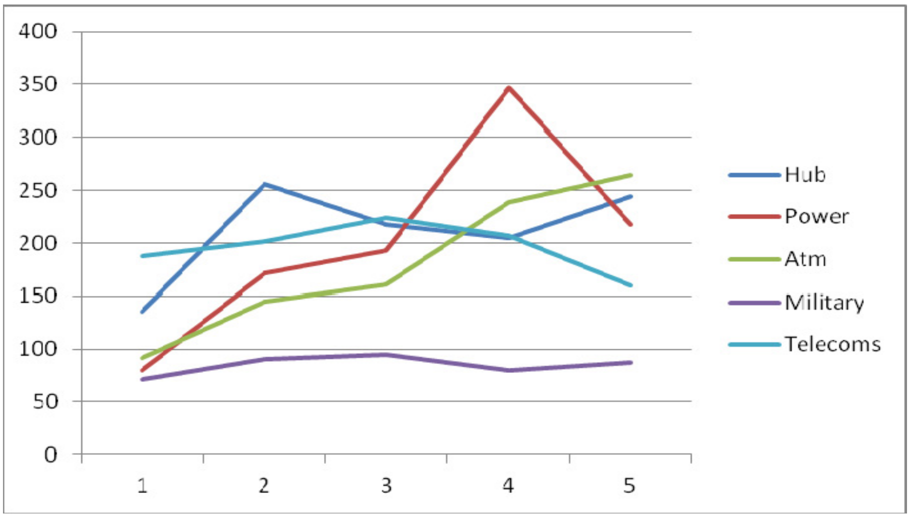


Figure 4-14 – Total Messages sent (y-axis) by experimental condition (x-axis) and cell

0428. Although the Military Node appeared not willing to sharing/transmit information readily as much compared to other Nodes, this may be due to national sensitivities, but also a low susceptibility of the infrastructure. This has implications on establishing a national system where the objective would be to foster better cooperation and awareness between different national sectors.

Chapter 5 – Experiment questions

0501. The LOE was designed to generate sufficient data to evaluate the draft (v0.5) Concept of Employment and the draft (v0.5) Framework of Processes for gaining and maintaining collaborative and integrated situational awareness of nations'/ organisations' own networks and relevant parts of wider cyberspace, which describes the key tenets and attributes of perception, comprehension and prediction, and to evaluate leveraged inputs from the other four cyber domain objectives. The high-level experiment study issue is stated as: "*How does the degree of shared cyber situational awareness affect the ability of our decision makers to make timely and informed decisions on actions in and through the cyber domain global commons?"* This was broken down into a number of more specific questions – Study Issues and Essential Elements of Analysis. This section takes each Study Question and assesses the degree to which the experiment and the analysis conducted so far answers it.

Study Issue 1: Does the solution provide a concept of employment for cyber domain situational awareness?

- Essential Element of Analysis 1.1: Does the solution inform the cyber strategic context within which the problem of cyber domain situational awareness resides (Ends)?

- Essential Element of Analysis 1.2: Does the solution inform the conceptual approaches to delivering cyber domain situational awareness (Ways)?

- Essential Element of Analysis 1.3: Does the solution inform the financial and organisational implications for delivering cyber domain situational awareness (Means)?

0502. This experiment does not really provide a strategic context in which Cyber situational awareness resides, nor was it designed to. *To achieve this representative participants (SMEs) must be of the appropriate level.* Some interviews with players may provide insight into this matter, but real-world operational contexts lay beyond its scope. It does provide some context for the means in which it can be delivered, however. It establishes the need for real-world relationships and agreements to be seen as a vital part of the solution, and not just the technical system. It also creates some confidence that the basic approach of feeds and incident tracking is a viable model, although there were comments that it would require extensive modification for use in the real world.

0503. The role of the Hub was the most directly illuminating for financial and organisational implications. Once sharing was removed (Session 5), players started to turn to the Hub for information, as evidenced by player comments, analyst observations and analysis of message data. Relative frustration with this process identifies it as a key enabler in this context, particularly if logistical obstacles stand in the way of establishing a more comprehensive system which enables direct sharing. Several questions asked how a system might be established in the real world. The answers to these have yet to be analysed, and may provide further useful SME perspectives.

Study Issue 2: What are the information requirements and processes required to gain and maintain situational awareness?

- Essential Element of Analysis 2.1: What are the cyber situational awareness tenets and attributes that deliver perception?

- Essential Element of Analysis 2.2: What are the cyber situational awareness tenets and attributes that deliver comprehension (defined for the LOE as the appreciation of relevance)?

- Essential Element of Analysis 2.3: What are the cyber situational awareness tenets and attributes that deliver prediction?

- Essential Element of Analysis 2.4: What are the cyber situational awareness tenets and attributes that deliver perception, comprehension and prediction each combined within a decision making process?

0504. As a first pass at data analysis, the specific questionnaire answers that dealt with perception, comprehension and prediction have not been assessed yet, and therefore there remains work to be done which could serve to illuminate best practice for supporting these principles.

0505. This report does, however offer some potential answers for the overall establishing of situational awareness. Messenger data indicated that participants missed the additional information that had been available when sharing, and looked for it in other locations when it was unavailable. The overall scores of situational awareness supported this view, where perceived situational awareness was higher on average in the sharing sessions than non-sharing, and player comments reflected this too.

0506. When considering where situational awareness failed in this experiment, it should be noted that a lot of the problems arose from cultural and working-practice considerations (which are discussed more fully elsewhere). This should underline that it cannot be assumed that a technological solution alone will solve the problem of Cyber situational awareness. No design can overcome a lack of information being placed into a system.

Study Issue 3: What are the roles and responsibilities for key stakeholders?

- Essential Element of Analysis 3.1: What are the relationships, partnerships and dependencies required across key stakeholders?

- Essential Element of Analysis 3.2: What are the attributes and characteristics associated with responsibility, sphere of action and prioritization of resource and effort associated with delivering cyber situational awareness?

0507. This experiment offers some qualified information about relationships and responsibility in obtaining Cyber Situational Awareness. What it does not offer is formalised advice about the way in which relationships should be established, nor about the specific challenges that might be encountered and difficulties addressed. This was an artificial setting and solution, which was representative, but not predicative in that manner and should not be taken as such.

0508. However, the reaction of participants in the scenario can tell us about the issues that are likely to arise. From analyst observations and the semi-structured interviews it was clear that participants put far more of a premium on information than the experiment did, and addressing problems was often hindered more by a lack of willingness to share (for whatever reason). In particular, the relatively low level of messages sent from the military cell typifies this attitude. This was an attitude that they brought with them from real-world experience and therefore is likely to reflect a real-world problem: the willingness to share. A related problem was the lack of understanding of what might have been useful for other cells to know, as evidenced from all cells failing to share pertinent information. The establishment of sharing protocols, and an environment which encourages it, will be essential and a non-trivial accomplishment.

Study Issue 4: Does the solution improve the ability of decision-makers to gain and maintain situational awareness?

- Essential Element of Analysis 4.1: What is the impact of social attributes such as confidence and uncertainty on a situational awareness process and system?

- Essential Element of Analysis 4.2: How well did the available technical means and user interfaces contribute to gaining and maintaining cyber situational awareness?

- Essential Element of Analysis 4.3: What gaps in knowledge were highlighted that could contribute to future requirements for research and development (in information management rather than specific tools) with respect to cyber situational awareness?

0509. This analysis does not yet include systematic study of the variables dealing with confidence and therefore there are limited conclusions that can be drawn. Analyst observations and the semi-structured interviews suggested that familiarity with the system brought increased confidence. However, since players were still missing elements of the problems generated it might be that this was unfounded confidence.

0510. The technical solution was found to work acceptably on the whole, as evidenced by participant responses, although there were indications that there existed serious reservations for bringing it into the real world; a matter which again requires further analysis of the questionnaire responses. There was evidence of the limitations of the system, as found in the observations of players generating their own methods of incident tracking, and adopting conventions for naming and tracking incidents in the system itself. However, these were relatively light modifications, and the majority of the system worked as intended.

0511. Some gaps in knowledge were highlighted, particularly in methods for bridging cultural conventions (as previously noted) but also in best practice for information displays. The maps, news feeds and incident tracking system were all the subject of specific feedback from participants in the interviews, and questionnaire responses should help to highlight additional flaws.

Study Issue 5: Does the solution leverage the outputs derived from the other four MNE7 cyber domain objectives?

- Essential Element of Analysis 5.1: Does the solution define improved methodologies for determining criticality, dependency, vulnerability, resilience and threats (CDVR&T) assessments?

0512. Yes. Analysis of critical infrastructure/assets was embedded in the situational awareness tools – representation of sector infrastructure together with a list of hardware/software configurations for each critical element (within the each infrastructure) enabled automatic visual highlighting of potential threats resulting from cyber activity.

- Essential Element of Analysis 5.2: Does the solution define a capability for collaborative information sharing?

0513. Yes. The generic Information Sharing Agreement (ISA) and the Hub and Node construct were taken from the Information Sharing Framework and enabled information sharing to evolve throughout the experiment.

- Essential Element of Analysis 5.3: Does the solution define a capability for a clear legal analysis?

0514. Although lawyers / legal experts were placed in each cell and EXCON, the experiment did not generate sufficient international cyber legal issues to engage them appropriately. The Guide to Decision Making was made available within each cell, but there was little recourse to it given the manner in which the vignettes developed. (The Guide to Decision Making was tested in a separate Objective 3.3 LOE held in Mar 12).

- Essential Element of Analysis 5.4: Does the solution define a capability for enabling technologies?

0515. The visualisation technology drew on the requirements identified in the Objective 3.4 LOE and subsequent Standard Operating Procedure as well as the NATO Cooperative Cyber Defence Centre of Excellence – Cyber Defence Exercise 2012. A number of modifications / additions to the requirements were identified.

Chapter 6 – Discussion

0601. At a technical level, the LOE was very successful. In terms of live play conducted against that planned, only 30 minutes were lost to technical issues, and the contingency provision for any overrun was not required. In view of the complexity of the synthetic environment and the requirements of such a large number of players (56 including EXCON, from 11 countries, plus representatives from NATO) this was very impressive.

0602. The training period was effective in familiarising the players with the environment and processes, including the questionnaires and interviews that formed a major part of the data collection. As would be expected, there was still some further player settling-in as the experiment progressed, as evidenced from the differences in behaviours noted between the first and last sessions, in which the rules of play were identical. This issue seemed to stem from the fact that having shared more freely in Sessions 2, 3 and 4, the ‘no-share’ Session 5 seemed very different to the opening session. Missing the ability to share as in the earlier sessions caused a much higher desire to push information through the Hub in the final session.

0603. Overall appreciation of cyber situational awareness across the run sessions did not change in the way that might have been expected. Some of the cells found it easier to cope under the more information-austere Sessions 1 and 5. This highlights the difference between perceived and actual situational awareness, and may also reflect to a degree one aspect of the LOE that fell short of intention - the level of the participants available to play the roles in the cells. In many cases players were not those who regularly operated at the strategic level, and were frequently observed to be trying to fix the problems illustrated by the injects, considering them at the technical rather than a strategic/political level.

0604. A very good response rate was recorded through the questionnaires and interviews, generating an enormous data set that could be mined for ever deeper analysis, though with diminishing returns. What is reported in this document is the ‘initial findings’, and provides a pointer to further analysis that could usefully be conducted, such as a deeper study of the responses to specific questions in the End-of-session questionnaires that were focused on perceived situational awareness.

0605. Despite a narrowing of the scope of the experiment from that originally envisaged (driven mainly by limitations in time and cost), the LOE still covered the Study Questions (see Chapter 5). Most of the insights at the higher level arise from the questionnaire responses, further informed by the emergent behaviour of the cells in developing appropriate ways of working. The fact that common themes and common solutions emerged across the cells adds to the confidence that they are valid and relevant. The independent variables of timeliness, accuracy and richness were not applied as treatments onto the stimulant injects delivered to the cells.

0606. The conduct of the experiment was delayed from the original plan by one month, and on extremely critical deadlines for the technical support team to deliver the experiment environment and tools. The reason for shortage of time in the build up to execution was largely due to the relatively late stage at which sector SMEs were brought together with experimental designers and analysts, so that each could understand the other’s requirements. Before that period, development work had been limited to at the abstract level. The need to integrate this development work sooner is therefore the main lesson to be taken to any future similar event. Other aspects of the design and development of the experiment progressed sufficiently well.

Chapter 7 – Insights

Overall LOE insights

0701. The overall initial LOE insights are as follows:

- The overarching proposition would appear to be validated that sharing information between public and private sectors led to improved situational awareness, with significant value on the information received from sectors.

- The visualisation technology provided enhanced ability of decision makers to grasp the impact of information received.

- Clear need for an Information Sharing Agreement (ISA) was reinforced – particularly in regard to taxonomy/protocols to enable efficient cross-sector/international sharing.

- Establishing trust was a critical enabler to information sharing. Players (as requested) brought their real world culture to the LOE and found many reasons not to share.

- The role of the Hub was seen as vital and it has to be responsive – session 5 was particularly testing for Nodes but also with the Hub becoming overloaded with management and requests for information.

- Participants were not high level decision makers and tended to react based on their actual experience/position in their own organisation. (A distributed experiment may a better way of encouraging high level participation.)

- The legal aspects were not tested to the level hoped for.

- In reality additional Information Management tools would be required to manipulate information.

Detailed experiment issues

0702. This section summarises the issues generated by the conduct of the experiment.

- Cyber situational awareness in the various cells was affected by the sharing protocol, but to a lesser extent than that might have been expected. The fact that many of the players were thinking and operating at a lower level than their role demanded is the main obscuring factor.

- The greatest difference was noted for the Decision-Maker role, where an improvement in situational awareness was seen during Sessions 2, 3 and 4, when compared with Sessions 1 and 5.

- The visualisation and communication technologies represented in the LOE are a major improvement to the current cyber situational awareness provision. Players felt the technologies would need to be focused at the right level and prevent information overload through good information mechanisms. There was also popular belief that barriers to any such collaborative working would need to have pre-agreed sharing protocols over a wide range of public and private sectors and across nations.

- Visualisation and communication technologies would need a mature and capable method, and agile process for management of events/incidents tracked over various periods of time.

- Most players appeared to be immersed in the experiment environment, although some felt that their role was not particularly clear or fully stimulated. Players were satisfied that most of the external agencies they envisaged interacting with were represented. However some players with an indifferent relationships were cautious of the interface with police and other law-enforcement agencies.

- Players were at times unaware of activities/events. This suggested that the level of perceived cyber situational awareness was often better than actual cyber situational awareness.

- Sessions 2, 3 and 4 entailed sharing information between all Nodes and the Hub. However, non-sharing during Session 5 resulted in a great increase in information being fed to the Hub, with which they were unable to cope. This suggested that efficiencies are to be found in facilitating cross-sector sharing at the Node level, but these depend upon the agreement of sharing protocols. Further, for a (national) Hub to be effective it must be responsive particularly to requests for information, and well resourced to cope with the operating mode of information management and exploitation.

- Players realistically assessed the benefits of sharing information across all sectors, with all real-world considerations (constraints and benefits) apparent. This often led to a decision not to share, which caused frustration

0703. The large amount of data collected provides the opportunity to conduct further analysis for greater strength of the conclusion. There is more to be extracted concerning the contributions of the players to the likely demands and implications of setting up a real-world solution along the lines represented within the LOE, but the fact that many players were not truly representative of the roles they were asked to perform undermines to some degree the value of those opinions.

Annex A – MNE7 analyst guidance

Qualitative analysis can seem simple, but it is actually a highly skilled and delicate undertaking. Observing and gathering relevant information without interfering in a task, influencing subjects or biasing their decisions is tricky to balance. This sheet has been prepared assuming no experience on the part of the analyst, but analysts of all levels of knowledge are encouraged to read and absorb the information - if only as a refresher course.

This guide contains a brief explanation of how to conduct qualitative observations and semi-structured interviews, followed by a summary of the experimental setup and guideline questions to be considering.

Qualitative Data Collection

The objective of good observation is to obtain an objective record of the behaviours and actions that are seen whilst participants are taking part in the experiment. Analysts should aim to gather information about behaviours whilst taking care to influence the actions being taken as little as possible. In this experiment, the aim should be to observe mostly passively and look for patterns and significant actions, asking appropriate questions where necessary but *staying out of the way as much as possible*. An analyst should never be the centre of attention. Analysts are free (and encouraged) to ask participants questions to clarify their state of mind, or reasons for decision making etc. Care should be taken however to ask open-ended, non-leading questions. As an example, a participant might be observed to miss, or not react to a particular inject. Analysts should avoid asking questions which directly identify this such as “Why didn’t you open that inject?” In such a case the analyst would then be cuing the subject to undertake behaviour they otherwise would not have and potentially biasing the results. Instead they should seek to ask questions which provide insight into the situation without necessarily prompting new actions, “Do you feel on top of your work?” for example, or “How do you feel your perception is of the environment?” Questions such as these can be asked at any time, and should be, including moments where nothing is occurring. That way, participants will become used to answering generic questions and not take them as a cue that they have missed something.

Alternatively, an analyst might be interested in why something was done and therefore it is appropriate to ask about that behaviour directly - but avoid prompting any responses. If the node decision maker made the choice to take action on information but not share it, “I take it you didn’t share that because it wasn’t relevant to anyone else” is an example of a leading question. “Could you explain how you just dealt with that information?” should get the same information but without presupposing reasons.

A “rule of thumb” for analysts is that you should strive to be as invisible to the node participants as possible.

Note Taking

For this experiment, analysts will be supplied with a clipboard and paper, a time synch sheet for each session, and a workstation with information management and email facilities for coordination with EXCON and other analysts. Given that the analyst is expected to move around the cell to hear conversations and ask questions, the majority of their observations will be recorded by taking notes.

Analysts should feel free to organise their notes as best suits their style, but any format should try to contain the following information when an observation is made if possible:

- Time of observation (experiment clock)
- Session Number
- Observed participants involved
- Participant roles
- Behaviour observed
- Explanations given by participants (if any).
- Theories of analyst (If appropriate)

Analysts are encouraged to give their informed opinion about patterns and decision-making reasons, but should make it clear in their notes the difference between their observations, factual actions and participant explanations. Analysts should feel free to speculate about participant behaviour if appropriate.

When making notes, analysts are urged to bear in mind that they will have to write them up later. Notes can be as long or short as necessary, but it is wise to write them as though someone else would need to understand them in the future with no knowledge of what had occurred other than that notepad. It is very easy to make vague notes and find a few hours later that you have no idea what you meant or what is being referenced!

Semi-Structured Interviews

Semi-structured interviews are a technique that consists of having a set of pre-prepared questions covering topics of interest, but being able to divert from these if something interesting is said, and to follow-up intelligently and appropriately.

Semi-structured interviews will be conducted at the end of each session, lasting 10-15 minutes, after participants have filled in their questionnaires and will be answered as a group. A suggested set of initial questions is provided below.

Baseline SSI Questions

How do you feel you performed as a group in the last session?

Where do you feel mistakes were made?

Where do you feel you performed strongly?

Given what happened, do you think you should have acted differently?

What information might have prompted you to act differently?

How do you feel your Situational Awareness was?

Can you give examples of where it was poor? Where it was good?

How did you interact with the other nodes?

What were your opinions on the sharing of information from other nodes?

Do you think you shared appropriately? If so, in what way? If not, why not? How did you decide that?

Experimental Questions

The following are a list of some of the research questions that are being asked in this experiment. They are included here as an aid to prompt thinking, but should not be attended to at the expense of all other observations. Analysts should be ready to adapt to the situation as it presents itself.

These questions are NOT intended to be answered or posed directly to participants, but rather to prompt analyst thinking. Directly interrogating participants about these ideas is likely to bias their results.

"*How does the degree of shared cyber situational awareness (situational awareness) affect the ability of our decision makers to make timely and informed decisions on actions in and through the cyber domain global commons?"*

This is the "exam question", as defined in the DCAP. In particular analysts should be looking for behaviour that demonstrates awareness of what is going on, confidence in decision making, accurate identification of necessary information and the ability to look ahead and make plans as a result.

NOTE: Participants may get things right, but have bad situational awareness. Alternatively they make have good situational awareness but make bad decisions – do not assume one necessarily means the other (although they generally correlate)

Situational Awareness

Situational awareness is generally defined as the combination of three separate ongoing processes: Perception, Comprehension and Projection. Observations should look to link behaviours to these three levels where possible, and analysts should use them as a paradigm within which to answer questions.

The three stages are independent and do not require each other to occur – you can project a future state without necessarily being aware of something or correctly understanding what it might mean. However it is *generally* the case that good situational awareness will involve all three building on each other, so it is useful to look for perception leading to comprehension leading to projection – or there being a failure at a stage.

- **Perception:** The act of actually noticing something in the environment. Does not mean that something has been understood or is dealt with appropriately. If something is completely missed, that implies poor perception

- **Comprehension:** Understanding what something means. Accurately identifying that an inject relates to a power plant, or alternatively accurately noticing that something is irrelevant. Again, USE of this information does not have to be good for comprehension to be high.

- **Projection:** understanding the system and the interacting properties sufficiently to make accurate predictions about what is coming next. Would imply getting ahead of the curve, making the connection between different injects to see what was coming. Could involve being wrong if comprehension is poor or things have been perceptually missed.

Additional questions

This list contains relevant questions for the analysis. They should be used as a prompt for what you should be looking for in your nodes.

- How is the group making decisions?
- Is information being shared between group members as well as other nodes?
- How is working style affecting the gaining of situational awareness?
- Are people taking the task seriously? Is there fatigue or boredom?
- What hypotheses are participants forming?
- Is there a command structure? Are there natural leaders?
- Who is talking to whom? What seems to be their priorities?
- How are they using the system? Are they struggling with it? Are they using it to its full potential?

Annex B – Cyber situational awareness survey sheet

This Form should be used as an aide memoire to help you keep track of events and make hypotheses about the possible cyber threats occurring in your cell during each session. The forms should be filled in by the Cell Decision Maker and will help EXCON to capture the situational awareness in each of the cells.

Procedure:

1. When a piece of relevant evidence comes to your attention (i.e. information that is relevant to you and will affect your decision) a new row should be started, beginning with the time of identification.

2. The ***Source Reliability*** and ***Information Confidence*** scores should be entered when evidence is identified, either using the ratings on the Incident Report forms or your own estimate. Guidance on the scales employed is as follows:

Source Reliability (%) *How reliable do you think the source of the information is?*		**Information Confidence (%):** *What is your level of confidence in the accuracy and completeness of the information?*	
100%:	Completely reliable	100%:	Complete confidence
80%:	Usually reliable	80%:	High confidence
60%:	Fairly reliable	60%:	Reasonable confidence
40%:	Not usually reliable	40%:	Low confidence
20%:	Unreliable	20%:	Minimal confidence
0%:	Reliability cannot be judged	0%:	No confidence

3. At some point during the session, you might begin to get an idea of what is happening, i.e. a possible threat to your system. These should be entered as ***Hypothesised Enemy Threats*** at the top of the form along with the time you first identify them. Throughout the session you may add, change or discount these hypotheses as your situational awareness changes. Additional pages will be provided.

4. Next, the evidence should then be rated in terms of how well it ***supports*** *or* ***refutes*** each of your threats using the following scale:

Evidence Support
SS: Strongly Supports
S: Supports
N: No Effect
R: Refutes
SR: Strongly Refutes

Note: If for any reason you go back and amend the evidence support, please indicate the time of correction in the comments box.

5. The second page of the form should be completed when prompted or just before you make your decision to share your mitigating strategy with EXCON (or at the end

of the session if you do not have time). Based on the evidence you have collated, two actions are required for each threat identified:

(i) **Threat Likelihood**: how likely (%) do you think your hypothesis is to occur?

(ii) **Threat Impact**: what is the negative impact of this threat to your systems? Using the scale below:

Likelihood
VL: Very Low L: Low M: Medium H: High VH: Very High

Tip: Only evidence that is relevant to making your decisions should be captured in the forms (i.e. the evidence should support/refute at least one of your threats).

Session: 1 / 2 / 3 / 4 / 5 **Node**: Hub / ATM / Power / CNI / Military **Incident No./Ref**:

Evidence					Hypothesised Enemy Threat		
#	Time	Description	Source Reliability (%)	Information Confidence (%)	Threat 1 Description:	Threat 2 Description:	Threat 3 Description:
					Time Threat Identified:	Time Threat Identified:	Time Threat Identified:
1			100 □ 80 □ 60 □ 40 □ 20 □ 0 □	100 □ 80 □ 60 □ 40 □ 20 □ 0 □	SS S N R SR □ □ □ □ □ Comments:	SS S N R SR □ □ □ □ □ Comments:	SS S N R SR □ □ □ □ □ Comments:
2			100 □ 80 □ 60 □ 40 □ 20 □ 0 □	100 □ 80 □ 60 □ 40 □ 20 □ 0 □	SS S N R SR □ □ □ □ □ Comments:	SS S N R SR □ □ □ □ □ Comments:	SS S N R SR □ □ □ □ □ Comments:
3			100 □ 80 □ 60 □ 40 □ 20 □ 0 □	100 □ 80 □ 60 □ 40 □ 20 □ 0 □	SS S N R SR □ □ □ □ □ Comments:	SS S N R SR □ □ □ □ □ Comments:	SS S N R SR □ □ □ □ □ Comments:

Time:		Hypothesised Enemy Threat		
		Threat 1 Description:	Threat 2 Description:	Threat 3 Description:
Estimated Likelihood of Threat Occurrence (%) (Very Low -Very High) VL L M H VH 0 20 40 60 80 100		Value (%)	Value (%)	Value (%)
Negative Impact of Threat (Very Low-Very High)		VL L M H VH □ □ □ □ □	VL L M H VH □ □ □ □ □	VL L M H VH □ □ □ □ □

ANNEX C – END OF SESSION QUESTIONNAIRE

“Rate” questions generally provided a 7-point scale running from “very low” to “very high” and the respondent simply had to click on a bullet beside the appropriate number on the screen.

1 Rate your awareness of the situation as a whole - to what degree you felt you understood what occurred in the session.

2 If you feel your awareness was lacking in some respect, or if you feel you were fully aware of everything, please explain why.

3 Rate to what degree you were aware when new information (items in the feeds, new messages in the conference and chat boxes) appeared in your display.

4 Rate how often you think that you may have missed some new information.

5 Rate how soon, on average, you felt that you noticed new information entering the environment.

6 Please specify when you felt you may have missed information and why. Alternatively, if you are fairly confident that you didn't miss anything, say how you organised your work to achieve this.

7 Rate how well you were able to identify which information was relevant to your tasks.

8 Rate how often you did not understand information that you saw.

9 Rate how confident you are that you correctly assessed and dealt with the information you encountered.

10 Please specify when and why you were not able to understand the relevance of the information provided. Alternatively if you felt you did understand, please explain how you determined what was relevant and if there were any techniques that you employed.

11 Rate how often you were able to predict how the scenario was going to develop.

12 Rate how frequently you were surprised by the direction the scenario developed.

13 Rate how confident you are that you made the right predictions and took the right actions based on the information that you saw.

14 Please specify what was easy / difficult about predicting events and the ability to plan a course of action.

15 Overall, please rate your level of situational awareness for this session.

16 Overall, please rate your confidence in your performance in this session.

17 Overall, please rate your confidence in your ability to meet the task demands in the future.

18 If you have any additional comments about this session and your participation in it, please detail them here.

ANNEX D – END OF EXPERIMENT QUESTIONNAIRE

“Statement” questions were answered on a 7-point scale running from “strongly disagree” to “strongly agree”. “Rate” questions used a 7-point scale running from “very low” to “very high” and in both cases the respondent simply had to click on a bullet beside the appropriate number on the screen. Question 6 was a two-way choice.

Some questions asked almost the same thing at different points in the questionnaire, for use as a test of consistency of response.

Please answer all these questions based on your overall impression from the whole experiment.

1. I found the tools and facilities easy and intuitive to use.
2. The tools and facilities supported all the actions I needed to perform.
3. The tools and facilities contained all the information I needed to perform my role.
4. The tools and facilities gave me easy access to the information I required to perform my role.
5. Rate how effective the presentation/ visualisation of the tools and facilities was at providing a good overview of the information.
6. Did you prefer to use the logical or geospatial situational awareness picture?
7. Please explain your preference for logical or geospatial situational awareness picture.
8. Please provide examples of things the tools and facilities did well
9. Please provide examples of things the tools and facilities did not do well.
10. Please provide examples of things the tools and facilities should be capable of.
11. Was there any specific information that the tools and facilities did not supply that you would have liked to see?
12. Do you have any additional comments about how usable the tools and facilities were? When answering these next questions about the system, please assume any usability issues you have highlighted have been addressed.
13. I would like to see an equivalent system in place in the real world.
14. The basic principles of the system seemed realistic and workable.
15. From your experience, what would be the major technical issues around bringing this system into the real world?
16. From your experience, what would be the major political or organisational issues in bringing this system into the real world?
17. Were there any issues or responsibilities you felt were not represented in this system that would be critical in the real world for this sort of task?
18. Please specify your role during MNE7, e.g. Power Node - Incident Handler.
19. Within your role, to what degree were you involved in 'advising'?
20. Within your role, to what degree were you involved in 'coordinating'?
21. Within your role, to what degree were you involved in 'planning'?
22. Within your role, to what degree were you involved in 'liaising'?
23. Within your role, to what degree were you involved in 'analysing'?
24. Within your role, to what degree were you involved in 'commanding'?
25. Within your role, to what degree were you involved in 'sharing information'?
26. I found it easy to contact the people I needed to talk to that were not in my node.
27. I felt my responsibilities were representative of those that would exist in the real world.

28. I felt the responsibilities of the other nodes and players reflected those that would exist in the real world.
29. My node coordinated well with the others (during sessions where that coordination was possible)
30. Which node aside from your own did you see as the most important to be in contact with and why?
31. Please list the three main people you were in contact with outside your node in the course of the experiment.
32. Was there anyone that you would have contacted in a real-world situation that was not represented in this exercise? What position and responsibilities do they hold?
33. The next questions address your overall situational awareness and where it was helped or hindered by the technology available.
34. Through all the sessions, how could the system better have helped your perception?
35. I could easily understand the meaning of the information.
36. Throughout all the sessions, how could your comprehension have been improved?
37. I found it easy to see where a situation was leading to.
38. Through all sessions, how could the system have helped you project future states?
39. I found there were some types of situation that were easier to predict than others.
40. Through all the sessions, what type(s) of situations, if any, were you able to predict with more accuracy?
41. I felt that overall the system helped me to gain the maximum possible situational awareness of any developing problems.
42. How do you feel the system could have better aided your overall situational awareness?
43. Overall the system helped me have confidence in the decisions I made.
44. What improvements would you make to the process used at MNE7, within and between nodes?
45. My decisions would have been influenced by the ready availability of non-cyber threat intelligence.
46. I would consider authorising the active use of reconnaissance and pacification of an adversary's CIS infrastructure during a confirmed attack given the legal and organisational approval to do so.
47. Given legal and organisational approval I would consider authorising the pre-emptive use...
48. Which of the communication methods did you prefer to use for communication between nodes, and why?
49. How effectively do you think you maintained situational awareness of the other nodes' status by information sharing?
50. To what degree did you feel that you had an incentive for your node to share information with other nodes?
51. What was your incentive to share information with other nodes?
52. What aspects of the system and setup aided your situational awareness the most?
53. What information did you find the most useful for aiding good situational awareness and why?
54. What information was least useful for maintaining good situational awareness

and why?

55. Were there any situations where the same information could be either useful or a hindrance depending on the context?

The next three questions address the experiment design.

56. The scenario and vignettes were sufficiently detailed and realistic to make the experiment a realistic test of process and systems.

57. The session timelines adequately supported system and process evaluation.

58. The audience manning and composition was adequate to support system and process evaluation.

59. If you feel you have any final observations or comments about this system and the experiment that were not addressed elsewhere, please note them here.

Thank you for completing this questionnaire.

ANNEX E – SEMI-STRUCTURED INTERVIEW SUMMARIES

ATM Node – Semi Structured Interviews

- **Session 1**
- **DM**
  - DM thought it was helpful having Legal run the first check on injects for legal issues and bring the team's attention to an inject.
  - DM felt team was better able that during Training Session to overlook spurious injects.
  - Thought it was very difficult to determine if they maintain situational awareness because they were too busy.
  - Felt the team needed more info, but could not tell us what information she would ask for.
  - PAS and PASCAL injects seemed like two different issues at times but at other times they seemed like the same issue. They consulted the paper copy of hardware and software that they were given to learn what was on the ATM systems and what might be vulnerable.
  - Thought they did ok recognizing what was really happening, but it was hard to predict what was happening. She was more interested in getting a task off her list of issues to work. She was not sure something was going to happen, rather wanted to get rid of any threats.
  - Thought they were getting useful information from other nodes/hub.
  - Due to speed, decided that if an inject required some sort of action, the team had to respond immediately and not defer to later. This risked having a later inject reverse her decision, but in the end she decided that was just tough.
- **Legal (LE)**
  - Felt better about being in the loop on what was happening.
  - Felt he got an important bit of information directing him to know that one Intel inject was more important than another
- **SME**
  - Was typing away in chat constantly for 2 hrs.
  - Session was more intense
  - He relied upon DM a great deal to maintain his situational awareness. situational awareness was maintained by team, he couldn't do it alone.
  - Seemed like there were 4 people doing 6 different jobs.

  - Regarding predicting, he said they were not predicting, rather being proactive in an engineering sort of way to remove risk to the ATM systems.
  - Inject icons all look the same so he is losing information and its taking a lot of work and time to find the specific, prior inject he is looking for. Requested a tag, wastebasket, colour coding, etc. (COP SW metadata requirement).
  - Used both types of situational awareness displays (map and network), but network was useless at the end because it was wrong relative to what status airports were reporting. Map was more intuitive, but some airports were hidden.
  - Felt the team had kept up with the injects and issues. But in the end they had to rely on IH expertise in cyber issues, protocols, software issues.

- **IH**
  - Team did not do much sharing to airports and LOCON, but tried to keep hub informed. They shared by sending IRs and chat to hub_ATM. Some were duplicated, but they were getting to hub faster through chat. IR contained more information, however.
  - Since inject icons are all the same, he requested some type of filter or marker as a software feature so he could keep track of what's important. He was overloaded with information (COP SW requirement).
  - Thought it was strange to use IR to report to EXCON, but they didn't use IR to report to node.

- **Session 2**
- **DM**
  - Felt team dynamics were largely the same as Session 1, but higher workload.
  - A dynamic in Session 2 that was not in Session 1 was more legal issues outside of ATM, so LE had to address those; IH had to handle more injects.
  - Noted that before the session started, they had a discussion (captured on whiteboard) about cyber crime versus cyber attack and their definitions and distinctions.
  - Noted that anticipating sharing, they expected more chat rooms. They found that the person in the chat room had better knowledge of what information had already been shared. So DM couldn't keep up and had to rely on their advice. And the person holding a conversation, was the person who continued to do so, rather than someone else stepping in.
  - Irrelevant information received from other nodes was discarded quickly.
  - Noted ATM created many more IRs than yesterday, but wasn't sure they had done enough.

  - Felt something was mission, because she did not have situational awareness of the system as she would have expected (see SME's comment for this session).
  - They did as they were told in the experiment going through the hub for questions, but in reality she would have not hesitated to pick up the phone and call another node directly. Legal advised her that she had to go through the hub for certain info, but in reality she would not have hesitated to make a quick call to a node.
  - Didn't think team would do anything differently in another sharing session; largely because they have not received any feedback on their performance.
- **Legal (LE)**
  - Felt Session one had gone perfectly, but today was difficult because he had to address both legal injects and Intel/news injects at the same time. Felt he was missing a lot of information.
- **SME**
  - Felt team was better at handling injects, so the external legal issues did not add to workload much.
  - Had better situational awareness here than in Session 1 where ATM is concerned but "had no clue" what was happening to Meridian's infrastructure as a whole. There are two parts to situational awareness: in ATM and the rest of the system. DM and hub_atm should have great system-level situational awareness.
  - Same as Session 1, requested to tag the injects page.
  - Had to keep checking with airports for their status because the network display was not correct. And many injects came in this the header saying it was from one person/organization, but the message was signed by someone else. So the messages are suspect as well. A large part of sharing is trusting each other's information but the tools were not trustworthy.
- **IH**
  - Were using IR both to share information and to receive info. IH was curious if the information ATM shared was actually useful to other nodes.
  - Felt team received more information and more relevant information with direct node sharing rather than going through the hub.
  - Team did have discussions NOT to share certain information and some information was shared again only to hub.
- **Session 3**
- **DM**
  - Felt it went better than Session 2.

  - In the middle of Session 2 there was tremendous information coming in, much of it contradictory. She arrived at a point where she had “no idea what was going on” when the cross country conference was going on. Lasted about 10-15minute period.

  - Three times, she felt she needed to step back and review all the information the team had and redefine the status of issues. They reviewed all the injects and saw that they had read everything. The result was that there was no inject that they had missed, but during the cross country conference, they mention power issues, but there was no inject about any power issues. So there were gaps in ATM situational awareness of other nodes, but it didn’t seem to matter to what ATM was doing. Except for the mentioned 10-15 minutes, they thought they had about 50% situational awareness, better than Session 2.

  - Was tempted to just walk out of the room and down the hall at the point when the hub as trying to take over decision-making to close airports, when that was DM’s job.

  - The first few injects we didn’t share with everyone. Thereafter, they changed the nodes that they included in sharing, based on what was happening at the time.

  - The hub had different information than ATM had and at times it seemed that they had less of an understanding about what was happening than ATM had. But we weren’t sure. We double checked, and found they had poorer situational awareness.

- **Legal (LE)**

  - Felt he had solved the problem of needing to respond to legal injects and also evaluate the Intel/news injects for legal issues. Was able to do both just in time.

  - Felt they were working better together than Session 2, but that probably they will work even better in Session 4.

- **SME**

  - Sharing did not work as they expected.

  - They had another player making decisions on behalf of ATM based on information that ATM didn’t have. They weren’t supposed to be doing that and it caused some emotion (frustration, irritation).

  - Thought he had a bit better situational awareness about the common infrastructure than in Session 2. But he also questioned whether he really needed to have more understanding of what was happening in other industries in order for him to be able to do his job.

- **IH**

  - Just before session, received training on sharing tools.

- **Session 4**
- **DM**
    - Re group dynamics, we set up a conference used throughout for node DMs to use to share. This resulted in answers to questions being received more quickly.
    - Team felt that they really trusted each other today. For example, asking legal "Do I or don't I …." Without questioning the answer.
    - Felt she had good ATM situational awareness even though she was extremely busy. For situational awareness outside of ATM, she felt it was poor. But the question still remains whether or not it would have been beneficial to have it. For example, there were lots of power issues, but once ATM decided to put everybody on power generators, the power issues were much less important. So she would read the power issues, but note it was just not of concern.
    - As in previous sessions, the team would pause and review which issues they were aware of and which had to be acted upon. But even so, they missed the KEN LINUX issue today.
    - Regarding what approach was used to prioritize information, the first was the scenario descriptions given by Jordan from EXCON at the beginning of each session. Then the DM assessed the risk of each possible action. DM placed a high priority on the Intel (believing it was probably very credible). But essentially, the same thought process was used in each session.
    - When the May Day emergencies began, ATMs focus was on that as the highest priority. This reflects real life. Also, the cyber threats were less important that the aircraft in emergency status.
    - DMs decision to share with other node(s) was based purely on whether or not they thought the information would affect them. With the emergency going on, they shared more with the military.
    - About a half hour from the end it appeared on the DM conference, that ATM has solved a problem (a patch) that someone else was just beginning to observe and had missed.
- **Legal (LE)**
    - Felt he was really integrated with the ATM team and legal, both.
    - There were aspects of civil domestic and international law involved.
- **SME**
    - Send more updates to hub than previously and made them a bit more formal. He did this even though they didn't ask for it to give them a better picture.
    - Felt Session 4 situational awareness was really improved over previous two sessions.

  - There were so many events going on, that they took paper and drew matrices to track in pencil the status of each (Kathryn H collected these and gave to Mark).

  - The information priorities are largely held in the player's minds.

  - The news feeds, in particular, were not very valuable. When things get busy, the news feeds are the first to discard. Maybe another person should be added to focus just on those.

  - They held back sharing with Power until ATM knew they had a problem, and then they shared and chatted with power directly. This avoided cluttering the sharing.

- **IH**

  - He asked the DM, "Do you think having DMs in their own conference/chat, left teammates out of the loop?" And "Do you think the hub was left out since they were not a member of the DM-only chat?"

  - Thought they created far fewer IRs than previously, but at the same time, they used IRs created by other nodes to update with information ATM had.

  - Military had two incidents when they had information. In one case, they would not share it because it was classified! Number 5 incident referenced number 4, but when they asked for a copy of number 4, the military refused based on classification. They did come back and gave a bit of number 4s information - enough to act on.

  - The small tool improvement on the incident page of putting different icons on the Intel/news feeds was very helpful.

  - Re incidents, they had overlapping IRs addressing the same issue. Maybe some nodes were making too many IRs, for example, military was generating too many IRs.

- **Session 5**

- **DM**

  - It took longer to get answers back from the hub, but at the same time, once you submit a question, you can just forget about it and turn your attention to the next issue while waiting for an answer.

  - At first DM had no situational awareness of the Meridian infrastructure because it was taking so long for the hub to get back to ATM with answers. Session 5 was a lot more like acting on guess work. There was a bit more prediction from "what if" thinking and we were developing several roads of what could happen and checking on those roads.

  - We had to be very clear with the hub who to share information with; this was different from Session 1.

  - Comparing sharing and not sharing to the real world, sharing is definitely more valuable. You may want to look again at whether or not to put telephones in the experiment. They make it easier to get a straight answer (even if the answer is I don't know). Emails can sit there for hours without being read. For example, a telephone would have solved the MFXX Centre problem very quickly rather than having Kathryn Heimerman recognize we had an IT issue because SME never received an answer in that chat room (KATHRYN HEIMERMAN'S NOTE: ATM SME was typing IMs to MFXX Center in chat for at least an hour and did not recognize that he was not receiving replies. Working with Controller/Facilitator's Technical Chat, we learned that IT had not established, or closed, that chat room because it was not on the list of chat rooms IT had that were allowed for the session).

  - Comparing to real world, ATM has service level agreements with all service providers. So in reality, those vendor service providers are required to tell us if there is some issue with the quality of service. So having telecom as a separate node in the experiment is unrealistic for ATM. And in the real world, those service providers would restore quality service to their really serious customers before other customers. For example, if home telephone service is cut, while residents might complain, they might not get media coverage about it like an air traffic center would if its radar lines were cut. And if telecom was threatened they would tell us.

- **Legal (LE)**

  - Relative to Session 1, legal chat was closed then; now we have it.

  - Discovered it is possible to attach files in chat which he didn't know in Session 1.

  - Recommended it result in a better tool to integrate Spark within Chrome and integrate other tools as well. One integrated tool would be better. It would be faster to use and easier to double check information behind a single COP.

  - The course of information is essentially bottom up not top down.

- **SME**

  - Felt team had built on every preceding session. And gained more experience with tools and processes.

  - By sharing all information with the hub, you may be able to remove parts of the nodes. Rather than an ATM expert in the node, the hub could take on legal decisions, commercial decisions, and do double checking on information.

  - If someone were to do an evaluation of the benefits of a hub architecture, ATM was making pre-emptive decisions to protect the ATM infrastructure knowing that it would take extra time for the hub to get back to us with an answer. We wanted to protect the system, and then later find out why.

  - Because we knew the value of sharing from Sessions 2-4, we were explicit with the hub who to share with in the hopes of getting valuable information.

  - Regarding doing this in a global sense, the more detailed information and the more industries and the more people that are included will cause the human-computer interface to become un-usable due to clutter and complexity.

  - The very thing we are trying to protect is the very thing that can kill the whole operation, because if there is a cyber attack we won't be able to talk to each other since we are relying on technology to do it all.

  - In reality, the communication between telecom and ATM would have been much more than in this experiment. If an airport reported a problem, we would contact telecoms immediately. We track every fault with telecoms.

  - At one point regarding Billdoor, there were conversations about sending account logins and passwords; this was not realistic.

  - In reality, someone would put in place processes that would serve as railroad tracks to keep every role within its sphere of responsibility.

- **IH**

  - The reason they created more IRs this time was that they were not allowed to update IRs that some other node had created. Had to start a new one.

  - They sent (nearly) all IRs to the hub and thought the session must have generated a much heavier workload for the hub.

- **Comment by EXCON_ATM**

  - Now telecom is moving toward a control center who will contact ATM, but their representatives are less on site at ATM. So telecom is moving more towards this experiment.

Hub – Semi Structured Interviews

Session 1

Player Comments

- Performance was initially poor and "all over the place".
- The Hub did not identify roles, so no triage system. As time progressed, this got better with better coordinated roles and follow-up.
- Legal did not feel he had the "big picture."
- The ATM SME stated that as the session got busier, he was told to "deal with it." As a result, ATM/Hub situational awareness as a whole went down. He "zoned" into specific problems.
- Triage roles were splitting between the DM / Advisor with the DM monitoring the Military and CNI, and the Advisor monitoring Power and ATM. Technical problems were noted, but nobody in the room had a complete picture of what was happening (i.e. nobody was using the whiteboard to incident track.) Other players did not notice that the Advisor was using a flip chart.
- The DM was overwhelmed during the first hour and could not "connect the dots". He never had complete situational awareness.
- ATM expressed worries about overloading in the next session because of non-sharing.
- Mistakes included missed communications from EXCON due to very vague references, poor process flows which resulted in data arrivals being too late for player relevance.
- Overall DM / Hub situational awareness started at 0% and grew to about 60%

Analyst Observations

- The Hub players continued to improve in their understanding and usage of the toolset.
- The Advisor displayed only limited horizontal information integration.
- The DM appeared overwhelmed with information. Evidence of this could be found in limited to non-existent use of the LCW survey tool.
- The DM / Advisor developed a triage process and improved it over time.
- Group "storming" over preferred processes was noted, but the Hub Team displayed professionalism and appeared to take their roles seriously.

Session 2

Player Comments

- Performance was deemed significantly better, “no comparison to yesterday.”
- Mistakes contributed to the lack of a rich picture. When the Hub SMEs ask questions of each other, they catch one another by surprise; still not communicating horizontally.
- The players were still trying to “wrap their minds around” the scenario that the writers wanted. One player suggested that in the future, experts should review the injects /scenarios for real-world credibility. Telecom expressed frustration over the lack of sense and the apparent inability to influence map status colours which seemed to “snowball” no matter what actions were taken.
- In real life, they do not have to spend so much time asking questions. LOCON SMEs and processes are in place to eliminate this confusion.
- Legal and Telecom expressed frustration over EXCON’s disagreement with the mitigation strategy. Private firms legally “own” their decisions.
- As a group they would not change their overall approach. They were trying to “play the system” and “pump people for information.” The Hub felt that during this session they were just beginning to learn from the mistakes of others and not just their own.
- situational awareness was enhanced by the Advisor’s use of the whiteboard. situational awareness between Hub players was deemed good as well, enhanced by the periodic updates given to the DM. DM situational awareness ramped up to about 85%, but will never be much higher due to the “unknown unknowns.”
- ATM expressed frustration over the display screens which did not match the map status coloration. The DM suggested that it might be best to turn off the big map display at the front of the room.
- Roles have changed with experience. The DM agreed that the Hub acted efficiently, but more emphasis needs to be placed on the national strategic view in future sessions.
- EXCON was deemed to be unresponsive. “Careful prodding” was suggested as a possible way to enhance Hub responsiveness. Use of the IM tool was also discussed as a way to speed communications and decision-making. Some nodes were more responsive than others; the responsiveness varied greatly between the nodes.

Analyst Observations

- The Hub players exhibited group “norming” into predictable and understood behaviour patterns.

- The Hub team appeared to settle on the use of the whiteboard as a triage / horizontal information integration process.
- Perceived situational awareness increased across the group.
- Sharing procedures and the amount of sharing evolved.

Session 3

Player Comments

- Hub performance was deemed to be good with the group's triage now running on auto.
- Initially missed some issues which started as node-to-node communications that did not include the Hub.
- The Nodes and EXCON were still slow to respond. If they don't know the answer, they need to say so.
- The Hub could improve by prodding the nodes harder, although better node performance on status updates was noted. Nobody "on high" (Cabinet, President, Prime Minister) was asking for status updates. The Advisor thought that chaos would ensue when he saw the CFMU inject (projection).
- Few real-world political pressures were in play in the experiment. Legal asked the Hub DM, "Who are you?" wanting to understand his level in the government.
- DM situational awareness was deemed to be 85%, although MIL disagreed (55%) as did Legal (60%). MIL and Legal were forced to share a keyboard throughout the exercise, effectively halving their effective analysis / coordination time.
- Again, node data richness varied greatly.
- A discussion of player perception ensued. It was noted that perception of injects depended upon player workload. The Advisor helped by cueing the Team, but the pace forced "scan reading" which sometimes resulted in lost details.
- No good information handling tools / procedures were in place, confounding the perception challenges.

Analyst Observations

- The Hub players were communicating, appeared to be calm and "on top of it."
- The Hub consistently detected status colour changes (which were missed initially in the nodes) and noted several IT errors.
- Teamwork and situational awareness continued to improve.

Session 4

Player Comments

- Information prioritization:
    - Power SME: Information was prioritized by severity and criticality
    - ATM: Ad hoc prioritization.
    - One player stated that there was not enough information to effectively prioritize.
    - MIL was limited by keyboard usage time allocation with Legal.
    - Legal prioritized by need and Hub requirements
    - It was noted that prioritization varies between the SMEs and the DM.
    - Legal and the Advisor prioritized and coordinated Hub actions during this session.
    - It was noted that the serialization scheme used in the titles of Incident Reports helped greatly when status / tracking items were listed on the whiteboard.
- Performance:
    - Power did not communicate as much as during previous sessions.
    - DM stated that the nature of the incidents tended to stovepipe the information during this session.
    - The ATM SME felt that communication was more efficient. More was achieved by good communication.
    - The Advisor felt that autonomous cells resulted in some duplication of information. The role of Incident Manager was missing; it was hard to fill in the LCW survey and keep up with the experiment.
- Mistakes:
    - ATM felt that he could have reacted earlier to the Skycoach issue, but that would have been unrealistic since he did not yet have enough information.
    - The Power SME deemed the IM tool difficult to use, making it difficult to pay attention.
    - The group felt that they sometimes got “sucked into” non-cyber issues. More work stations were needed. In the real world, other people would work these tangential issues.

  - The Advisor felt that he should have “pushed back” on the airport fuel issue as this was not a Hub-level item.
  - Legal felt that cross-border issues should have been discussed for legal implications. Such discussions were missing during this session.

- Situational Awareness:
  - ATM felt he had good situational awareness over his area, but not the wider picture.
  - Power was “heads down” in his own area throughout.
  - SMEs did not listen to other 30 minute updates because the discussion was too long.
  - The DM’s situational awareness started at 60% and ended at 85 – 90%.
  - The MIL SME suggested a 30 minute synchronization report be prepared for each node, however this was deemed onerous by the group who relied on Instant Messaging updates.
  - Legal was looking for “matching pictures” at the 30 minute update and stated that 15 minutes is too long to get through the process.
  - ATM wanted updates to be related to incident numbers.
  - SME interactions were with their nodes only. ATM requested incident reports for everything he saw.
  - situational awareness on other nodes was not too good since the SMEs were focused on their own problems and issues.

Analyst Observations

- Once again, the Hub showed good working relationships, coordination and performance.
- situational awareness was especially good, ending at a perceived DM situational awareness of 85%
- The overall atmosphere was calm with some “joking around” noted. However, a couple incidents of player swearing indicated genuine involvement in the experiment.

Session 5

Player Comments

- The players developed their own terminology concerning the two sets of experiment ground rules. When all information sharing was conducted through the Hub alone, the Hub Players referred to that set-up as the “hierarchy”. Open sharing was referred to as the “mesh.” When asked what we learned from the MNE7 experiment, the Hub players quickly converged to the following:

  “Mesh is good, hierarchy is bad, but be sure to keep the Hub in the loop.”

- Lack of real-world data richness made it difficult to determine when it was best to share information.

- The “mesh” approach allows the National Hub to focus on the big picture situational awareness.

- The “mesh” also allows for faster initiation of a “fix” since the Hub and nodes are already “in the loop.” Node-to-node sharing allows “non-filtered” technical information to flow directly between SMEs, eliminating confusion sometimes injected by national level non-experts along the way.

- Data access control issues were noted by the MIL SME.

- The Hub’s situational awareness was deemed to be 40%, significantly lower than session four, but better than session one due to better familiarity with the tool set.

Analyst Observations

- The Hub players had obviously learned the power of sharing. More sharing was noted in this session than in session one.

- Additional evidence of the players’ commitment to sharing could be observed when they encountered some initial problems with the Instant Messaging tool early in the session. Spirited calls for a “Pause Ex” ensued, indicating a strong desire to be able to share with as few hindrances as possible.

Military Node – Semi Structured Interviews

Session 1

How do you feel you performed as a group this session?

- Initially everyone was trying to find out where we all fitted into it – especially on a national scene. The organisation outside the group was unclear – how should information be channelled? What level are they at?

- Communicating with the DM was difficult as he was over the other side of the room – the only way was to shout.

- Things were missing in the scenario – what resources are available to us (i.e. do we have our own analysis team?).

- The Military hub is blind – they don't understand the roles. Explained that the Military hub is a national Military rep.

Where do you feel mistakes were made?

- The general principles were there and along the right lines – i.e. searching for threats, but we were waiting for excon for answers. We didn't do anything in the meanwhile.

- The players thought the process was correct, they just weren't fast enough. Due to the unfamiliarity.

- A lot of tools and the workstation screen gets very cluttered. Need different screens.

- In the beginning they didn't divide up the incidents efficiently. The TA would be doing all the comms [advising DM on impact of incident], the IH would keep overall control of the situation [advising DM on status of incident].

- IH & TA felt their roles were overlapping. Defining the roles for the next session would be good.

- Legal was sat there on his own with not much to do but to watch colours change.

Was your workload as a DM balanced?

- Yes. Normally wouldn't be an unreasonable workload within this environment.

- The DM shouldn't be down in the weeds – hard to do if you have a technical background.

Would you have acted differently, given what happened?

- No. Apart from the communication between EXCON and the hub which could have been more streamlined if they had a better understanding of the organisation.

- Updating the tools – the technical issues were frustrating.

What was your situational awareness?

- Not good – a good situational awareness from what the scenario gave us within the confines of the scenario. Reasonable.

- Definitely lacking information about our own systems, the patch status and expected estimation times you'd have in a real environment.

- Lack of other media information (i.e. the register) and especially the source of the information.

- Not enough information on what was happening about the other sectors. We had to make assumptions.

- Didn't get any response from EXCON.

- Didn't hinder the DM process, but would have been able to make more informed decision if other information is available.

Question as to whether there were players involved in a power chat that weren't supposed to be sharing during this session. Telecoms CNI chat.

Session 2

How do you feel you performed as a group this session?

- The group process worked better – the group structure is better than the test session. The players are only reporting to the DM when needed (i.e. a summary). Players were confused during the training run, but this session helped to make responsibilities clear. DM was trying to stay out of the weeds and filter relevant information/requests to the hub – the DM decided the relevance but confirmed it with the team.

- Speed of LOCON delayed session players – there is a lag in the system about the colour changes on the situational awareness logical view. This is a falsity of the experiment. It is difficult to link the information to someone else (i.e. the nodes) when each have a different view. What is the point of the 'Share' button if it doesn't affect the colour change? The granularity of the experiment is not as rich as the real world. Also there is a stovepipe for RFIs to LOCON. EXCON SME advises to go to LOCON for more information.

- There was a lack of awareness about what was happening in the other nodes (e.g. Power). In the real world the Military would know what was happening. This information would normally be fed in sideways or when something goes wrong – not necessarily from top down.

- Incident report format is much better – they're starting to look more aligned to real life.

- ISA was followed more – legal advised which information to strip out (i.e. personal and IP).

What was impacting your ability to conduct the three exercise missions?

- Military had no specific intelligence about any of them. They only had information about the cyber incidents.

- There wasn't enough time to try to analyse what was going on in-depth. There was only just enough time to manage the incidents. Constant attention from start to end – no time to sit back and comprehend.

- Players were overloaded (TA and IH), then there were a few minutes to process, then more overloading. This is normal for a CERT.

- Reality of CVE announcements – really you'll only get a report one or two every couple of days, not a bunch in a short space. There is a lot of work to do for each so this was potentially a misunderstanding for the experiment designers. In real life, the configuration mgmt team would issue bulletins and request information as to how the system would be affected.

Did you make any wrong decisions?

- IH opened up too many tickets (9). He assumed that all the information was applicable to their procedures.

- Legal received many injects through chat – the DM didn't notice what legal was doing. It took him away from the wider situation – his situational awareness of what was going on. DM thinks legal should be more involved when something novel comes in.

- DM Military tried to share information with the others over chat to the hub, but not one replied. From LOCON it was a 'black hole'. They didn't get the information from others – they were just managing their information.

What was your situational awareness?

- Really good – the team dynamics worked really well to give a good picture of the Military situation.

- DM made decisions and then informed the team. He was happy with the decision and the information he had available. The information was lacking – firstly from the geo-display and from the other nodes.
- They had more relevant information from LOCON.
- They had a wider appreciation of the wider picture, but not really detailed.

What was the functional impact (effect) of everything that went on elsewhere to Military capability?

- DM: With additional information we had increased capability compared to if there was no information. E.g. the information from power allowed them to plan ahead and mitigate the effect. Not a direct impact to the other nodes.

Session 3

How do you feel you performed as a group this session?

- As a group it was okay, but the information was not as rich. There were a few technical issues that were restricting the information flow of IRs – had to resort to using chat. This impacted them on not being able to see the relevance – didn't have everything they needed to make a good assessment. This was telecoms info.
- The team managed the session accordingly in light of the tech issues.

How did you think when you were sharing information – i.e. what/when to share?

- The intel reports weren't detailed as the DM would have liked it to be, and 50-60% of the bits they could have done without, but because of the time constraints they often decided to share the whole thing (apart from desensitising the material if necessary) with the other nodes/hub.

Where do you feel mistakes were made?

- DM: Difficult to relate some injects to overall scenario. Difficult to separate what's happening in the scenario to what would happen in real life. I.e. you can cope without civilian aircraft for a while – you get around it by using what you have. In the scenario it was a big deal.

Did you perceive the larger picture adequately – relate to other sectors and the hub?

- Aware at a high level of what was going on, but indirectly. Not getting enough relevant information from other sectors.

Were you good at sending out information and assessing the relevance?

- Yes – tried not to spam the other nodes.

Did you perceive any larger threats (nationwide)?

- A Military node wouldn't look outside of the Military but would feed into the hub/central governmental organisation. If there was something that was common to everybody, we flagged it up. Military are the ultimate consumer, not a provider. Although they don't provide anything, they might have a reliance on the provision of a service – they provide impact statements for the other sectors (doesn't happen outside, but could happen with the lawyer in the session.

Did you receive anything else from outside Meridia that would affect your assessment of the situation?

- Only after ENDEX – a power employee who was affiliated with Southland. This shows that there is an active physical threat from Southland – this is the proof from rumours. In the real world, the threat alert status would change and additional hardening measures would be put into place.

How was your situational awareness?

- Could have been better had there been more information on the incident reports from outside Military.
- The middle section of the session, they were actively assessing threats from a national level (i.e. the telecoms issues and their impact on the other sectors).

Session 4

How do you feel you performed as a group this session?

- A well-oiled machine. The group dynamics were very good.
- By necessity, the IH and TA were more autonomous as the DM was more overwhelmed from all the alerts from all the different tools. This is the way it normally works.

- It was difficult to work out which things could be delegated because of the speed of incidents coming in, but the IH and TA picked up the things that were relevant. Was delegating to the others the issues only the DM was receiving.

Did you have a method of prioritisation?

- Gut instinct. Safety critical takes priority over patches.

Where do you feel mistakes were made?

- They stopped updating previous IRs due to the speed of the injects in the session – no time.

What was different in this session as opposed to the last in terms of causing information overload?

- We were getting information from other sectors – they ticked more boxes on the distribution list. Some technical issues on this point that might have stopped them from seeing it (i.e. multiple people opening up the same report).

- The icons on the feeds helped to provide situational awareness.

Level of situational awareness from other sectors?

- Getting more information from power and air traffic – had almost nothing from telecoms even when the questions were asked. Received a news article about being on the brink of radio silence – this surprised them as they'd heard nothing and got nothing back when requested further information.

What would you have done differently?

- Picked up more themes from the scrolling feeds – be more active looking at the incident reports and connecting them.

How was your situational awareness?

- Much better than the last session because we were getting more information from power and ATM. It wasn't perfect, but it was as good as it can get within the confines of the experiment.

- DM thought more about the strategic issues (i.e. festivals and geographical area).

- TA/IH was better than previous sessions.

Which were the events that affected your awareness/decision making?

- The aircraft.
- The power base going up and down.
- The exfiltration issues.

How did these effect your decisions?

- Power – we made sure to warn them that their power stocks were up and business continuity plans in action.
- Did offer assistance to ATM – some coordination over air traffic.

Facilitator briefs players on the actual events of this session.

What parts did you not pick up on?

- DM got most of the events – not totally 100% of it - but not from telecoms.

How do you feel about the information you received from the other nodes – did you trust it?

- We trust the information appropriately – i.e. patches. We wouldn't just role out the patch because they tell us it is a good patch for the software – we'd test it for our own infrastructure before we install it.
- It would not be different if it came from the hub – they've got to get their information from somewhere. Though for some information they might give it a higher confidence – but not if it is simply passed on.
- You build up trust relationships over time, but this cannot really be captured in an experiment. These personal relationships haven't been discussed in the experiment – situational awareness can be significantly changed from one piece of info from a trusted source.
- Some of the information was a little diverted – ATM hadn't informed hub directly so they got the information from another node after it had been passed on.

How do you think LOCON performed?

- Much better – LOCON didn't have to communicate with the facilitator a lot to prod players in different directions. The RFIs were spot on and in the right format for a node. The relationship worked better.
- Protocols about talking to LOCON weren't strictly specified.

Session 5

How do you feel you performed as a group this session?

- Group worked well, but it was really frustrating not being able to share with the rest of the nodes. They don't think they got all the information they were getting before. Starved of information this time.
- Compared to S1, the frustration is bigger now because they were used to sharing.
- They performed better through working with each other over the past 5 sessions.
- There are still some frustrations over not having what you would normally have doing this type of work.
- Performing much more efficiently – because they could see how capable the other team members were. Could see what other people could do and how they would get on with it at the end of each session.
- Legal: very good – took us off in a different tangent – requested more from J2 and J3.

Have you been true to your roles from the first session?

- The DM was getting a lot more involved than he needed to be, and even in this session, but it was a much better distribution.
- IH/TA were a little bit more technical in this last session because of the nature of the incidents.

How did you perceive your situational awareness?

- Starved of situational awareness by not being able to interact directly – they were getting information from feeds or via the hub directly. Not as much information available.

Facilitator briefs players on the actual events of this session.

What parts did you not pick up on?

- The data centre incident only happened minutes before the end. The sync of military injects for this session were very much out of sync with the rest.
- The ATM incident was in hand. They knew about that.
- The Power – no power was removed, just probed. They had some of that, not all, because DM expected power to shut it all down.
- Telecoms – effectively someone coming in and taking down network by misconfiguration. They were aware that it had gone down, not of the reasons behind it.

Power – Semi-Structured Interviews

Session 1

Player Comments

- Situation Awareness – Varied throughout the session, depending upon workload and wealth of information. situational awareness ebbed and flowed throughout the session. DM / Advisor complained about learning the tools. Not well organized as a team quite yet, but eventually sorted through the information. Early off, the Team suffered from redundant efforts due to lack of direction.

- Information confidence level at the point of decision to share information – Decision to share was driven the level of “emergency” associated with the information. Criteria: Is the information relevant? Was it available through other sources? Found a balance of when to / when not to share.

- Did you understand what happened in the other nodes? Absolutely not. Could only name one incident that another node faced.

- How did you feel about the LCW form? Terrible. The DM could not keep up with the session and fill out the form. Prompting might help, but the form-dedicated time might be 20 seconds.

- Do you know what you were supposed to be doing? Only in part.

Session 2

Player Comments

- How did the session go? Misleading information impacted the situational awareness. Should have gone back to get clarification. The (inject, other) documentation caused confusion. So a lot of time was wasted sorting out the information. 66% through the exercise before some of this was sorted out. Big issues concerning the relationship with power companies were only sorted out very late in the session. This session was slower than the first, not as much happening. Less pressure than expected.

- How did node reorganization help this session? Took some time to adjust, but sorted it out. Useful to the session. Splitting problems were handed off to individuals, still sorting out the Legal role.

- Did something surprise the DM? No. The proper information was flowing up to the DM. The national Hub responses were sometimes annoying, but kept them updated.

- How confident were you in the decision making process? Still learning roles, etc., so no discernable different yet. This session taught this node to communicate proactively.

- Did the other node know what they needed about the Power node? Legal aspects were coordinated with the other nodes. There was more structure with the new node organization. Legal felt more comfortable during this session.

- Did you get the needed information from other nodes? Telecom information to Power was limited. Did not know enough to prompt Telecom / ATM at the proper time. The information balance is not sorted out yet – there needs to be a one-on-one introduction across the nodes.

- How did you use SPARK in this regard? Don't know. IRs appeared to be the preferred method of contact throughout.

- How did the session go concerning the design of the experiment? Architectural problem concerning communication of the status colour changes. Different colour status data provided to the node than the experiment control caused confusion. Discrepancies will be addressed as an ad hoc fix out of ExCon in future sessions.

- Did anyone capture the "worm" out there? Yes. Nothing was actionable about that inject.

- How did you assign tasks? Geographically – north / south – on a regional basis. Common themes had to be assigned on an ad hoc basis.

Session 3

Player Comments

- How did it go overall in this session? Interesting. A lot of confusion and other-node ignorance about Power. The Hub did not do information validation.

- Was this a process problem or a lack of information problem? Cannot say, but overall the OS vulnerability story was not consistent. Not enough information available to provide a technical assessment. Telecom information in particular was missing; needed Telecom to provide more information in a timely manner. The displays of hardware status were confusing. Could not understand the nature of the vulnerability from the status displays, could not help the power company nodes.

- Status displays (red) – does this provide enough information? No. Highlights problem, but does not provide insight. There needs to be a way to highlight the important technical data. Need a way to retain and track the important data – need a technical tracking tool. Need to inform other nodes when status green (system restored) occurs as well. Certain data was classified and could not be shared without additional information. Again, more detail is needed. Things do not happen so fast in the real world, so we have more time to analyze. Risk is the sum of threat and vulnerability; both parameters must be separated and analyzed, then re-integrated.

Session 4

Player Comments

- How did the session go? A little bit less information than expected from the other nodes. Other DMs provided a lot of useless information. Situation reports did not come in from the other nodes.

- What did you specifically want from the other nodes? ATM did not provide airport locations for instance.

- Was there a case where they did not share? In general, the nodes did share enough detail.

- Did you share enough information to the other nodes? No – selective in information sharing. Process was to put together a complete picture before sharing to prevent confusion. Knew what other nodes needed; waited for sufficient detail before sharing. Again, confusing technical data made it difficult to sort out. Other nodes were guilty of sharing abstract information that did not help.

- At the operator level, did you understand the information coming in? Some detail was missing, but the overall picture was clear throughout the exercise. Provided information to the power plants with the proviso that they should go ahead and switch to manual ops if they begin to see anomalies, but they did not do so. In the real world, you'd re-qualify the company teams.

- What method did you use to prioritize information? Time pressures drove the team to address the "hottest" information first.

- How did you put the Legal piece into the session? Legal POV was to validate the legal sharing of information. Legal took the initiative to share some information to help the node team. Not a Legal task, but needed to help the node. DM asked for Legal help on some national issues.

- Did you want to focus more or less on national issues? Less. Not our job. We're supposed to maintain the power grid; not interested in politics. Legal needs evidence, not political whisperings.

- Do you feel you understood what was happening in the other nodes? Across the board, apart from some airfield problems, No. We were not aware of other nodes. ATM asked for SCADA tech data which should come from their vendors, not us. That information should be available from the national Hub / cert.

- Would it be useful to share such tech data? Or are the barriers presently in place for good reasons? You do not want to be distracted by questions which should be answered in other venues; we have a certain amount of time to do our own jobs. Currently privatized proprietary information is not shared for economic reasons. Cyber defence does not require sharing of unique proprietary information, just cyber system-level information. A genuine challenge to get companies to share anything.

- Information sharing is fine, but competition issues have to be addressed to cause sharing – correct? Yes. National standards in smaller nations may lead the way to starting. Technical people will naturally share when the Lawyers are not in the room. Legal agreed.

Session 5

Player Comments

- How did this session go? Well, in general. Missed a lot of information, but the team did well overall.

- How was this session different? Geo-political request directly to the node would NEVER happen in real life. We would only reply to the extent limited by company Lawyers. Normally dealt with at higher levels and trickled down.

- Awareness – did you what was going on in other cells? No.

- Did you have more awareness about other cells than in the past? This session was simpler due to the lack of information flowing from other nodes. Information sharing from the Hub was either very controlled or the Hub did not have awareness of what was important. It took more time to correlate and build situational awareness?

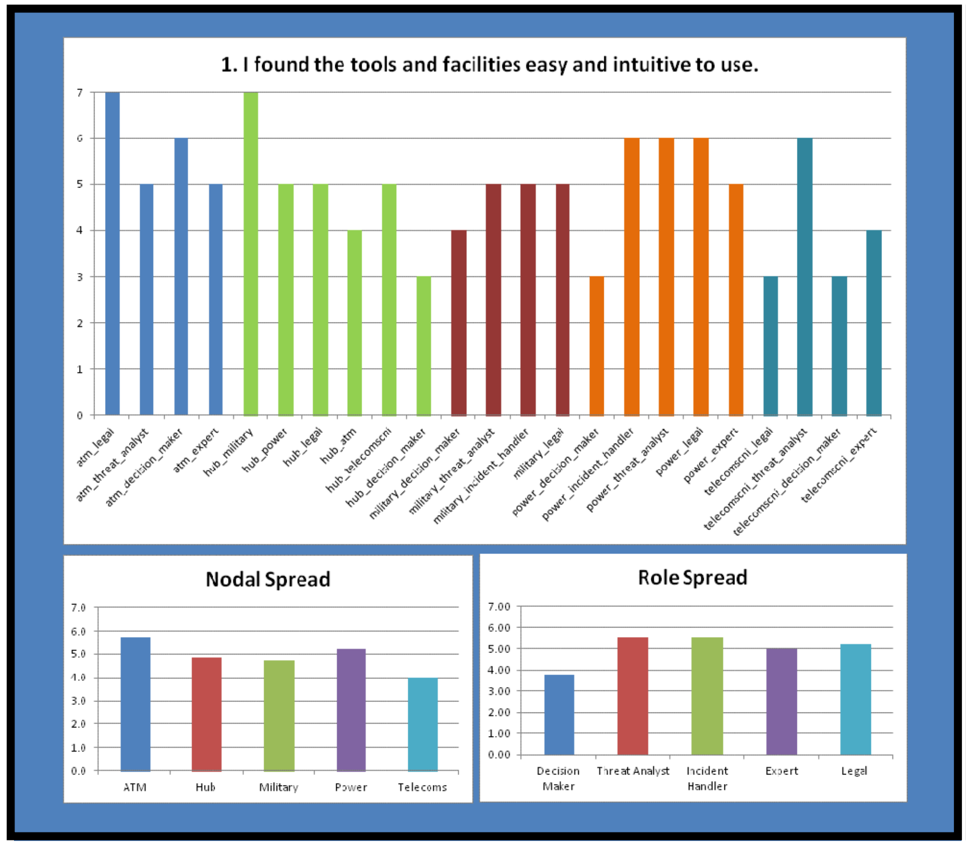
- Did the Hub provide what you needed? No. They needed to provide a better state status report. We needed half-hour updates. Not enough information. The system probably limited their ability to share, but hard to say because the limitations were not clearly defined. We cannot say whether the Hub was doing their job well or not. Maybe a liaison officer in the Hub would help the information flow.

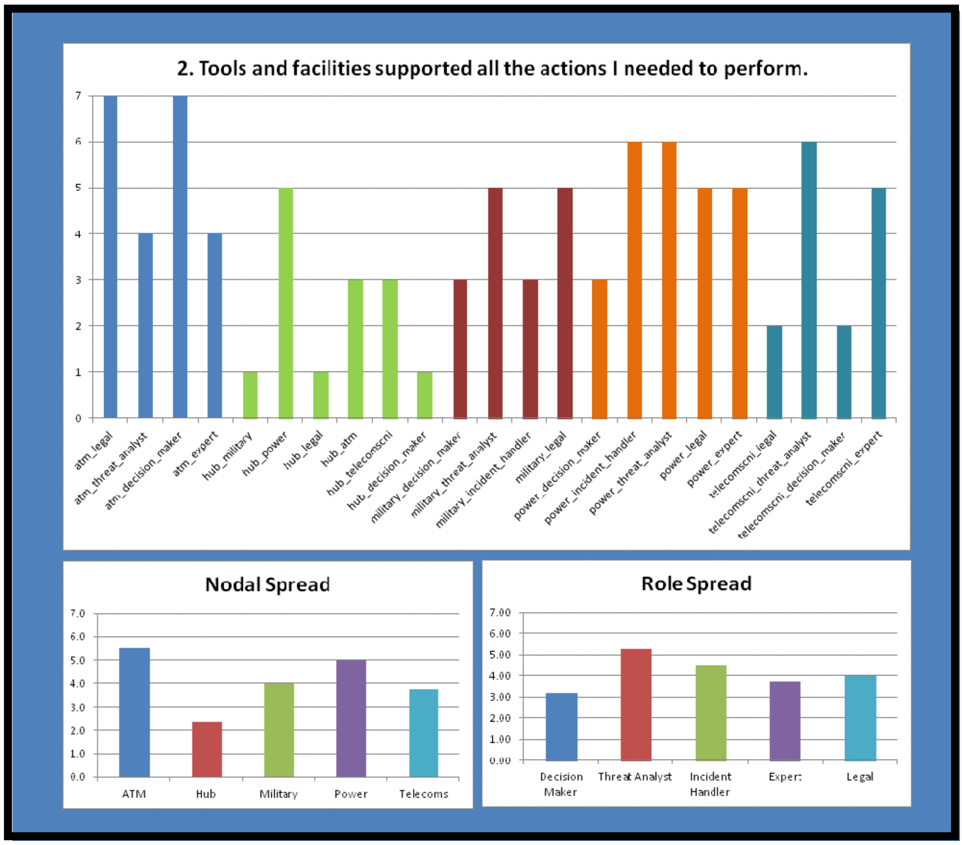
- When you made decisions, did you have confidence? Did our best based on the information available. Tried to inform others. Only one issue was discussed concerning whether it could be shared. Some early correlated information was shared immediately with the Hub. We told our own power companies, but they did nothing with it.

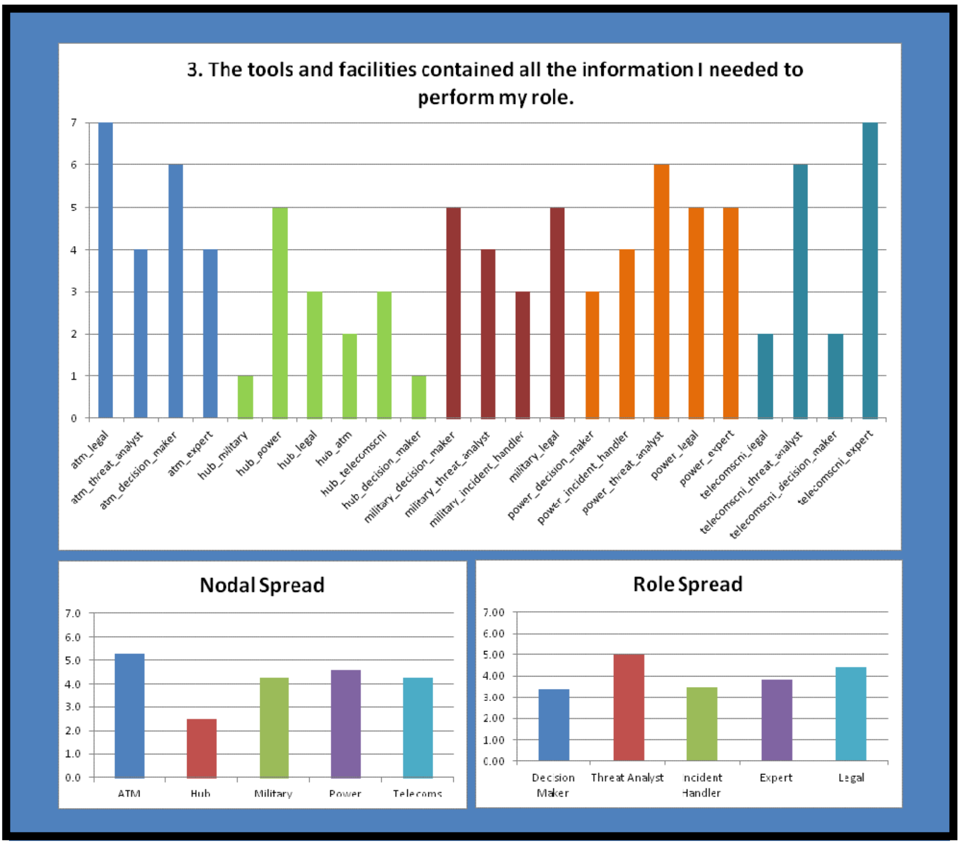
- Did you get similar correlated information from other nodes? No. Expected much more, especially from telecom and, to some extent, the military. The military did a bad job, or the Hub just did not push out the information.

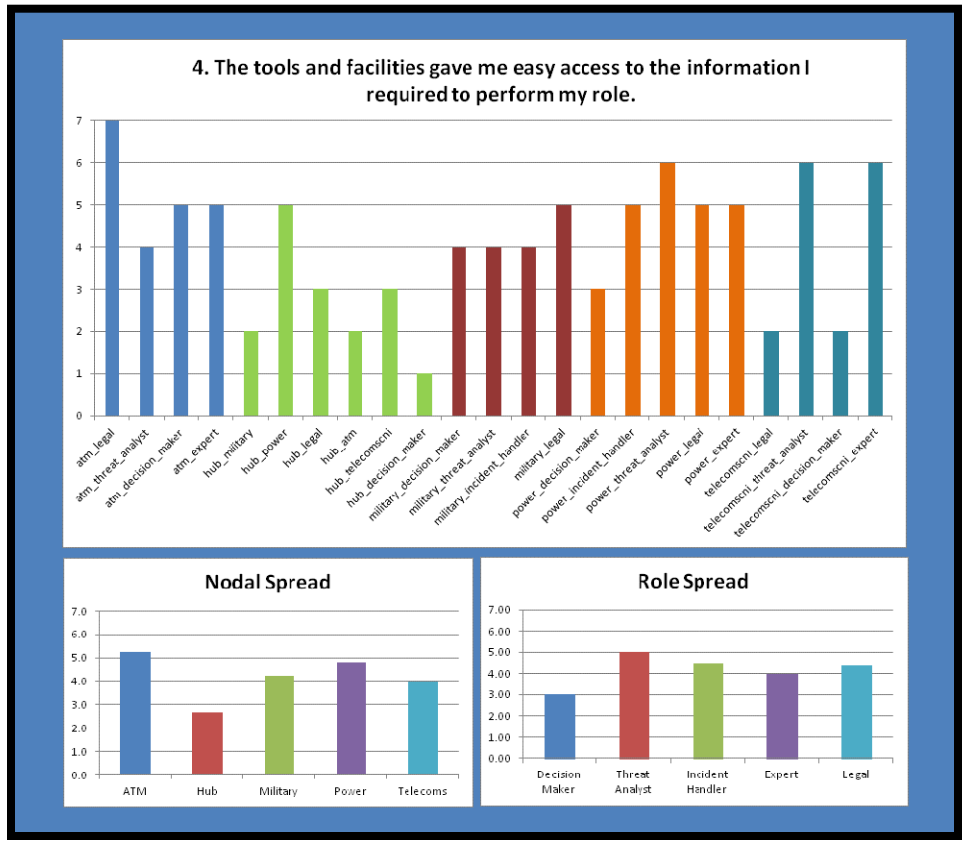
- Did you provide the level of information needed by the other nodes? Yes. We provided information up to the Hub and expected information back that did not come back.

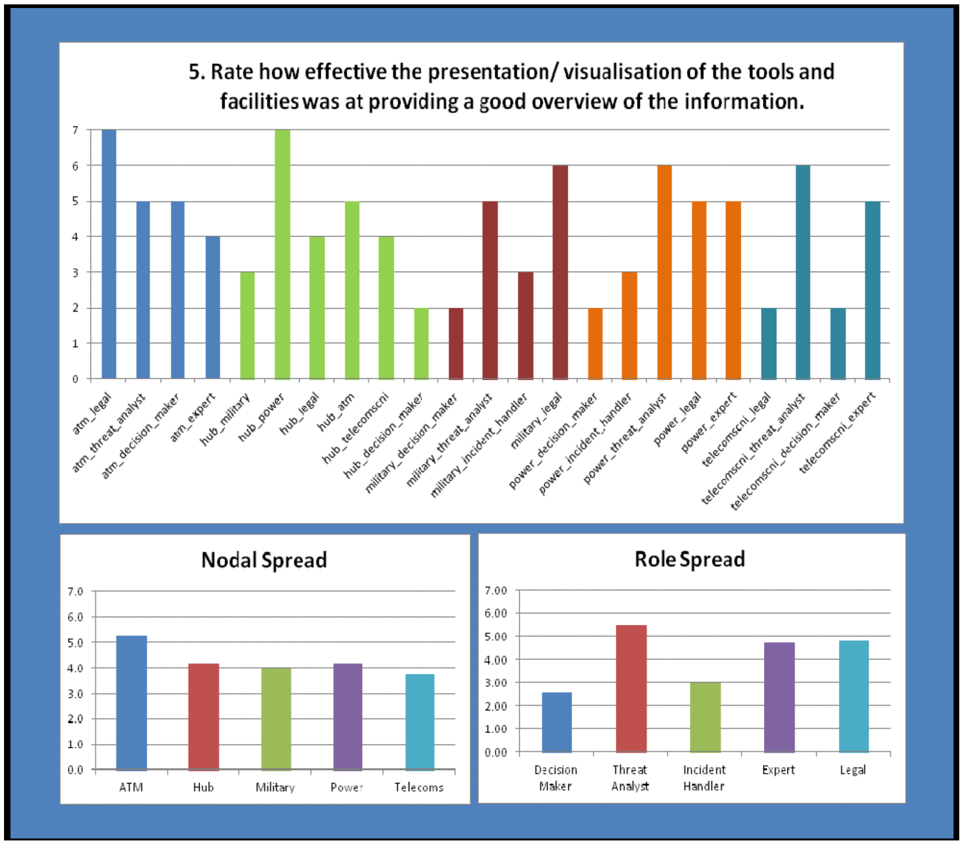
ANNEX F – END-OF-EXPERIMENT GRAPHICAL SUMMARIES

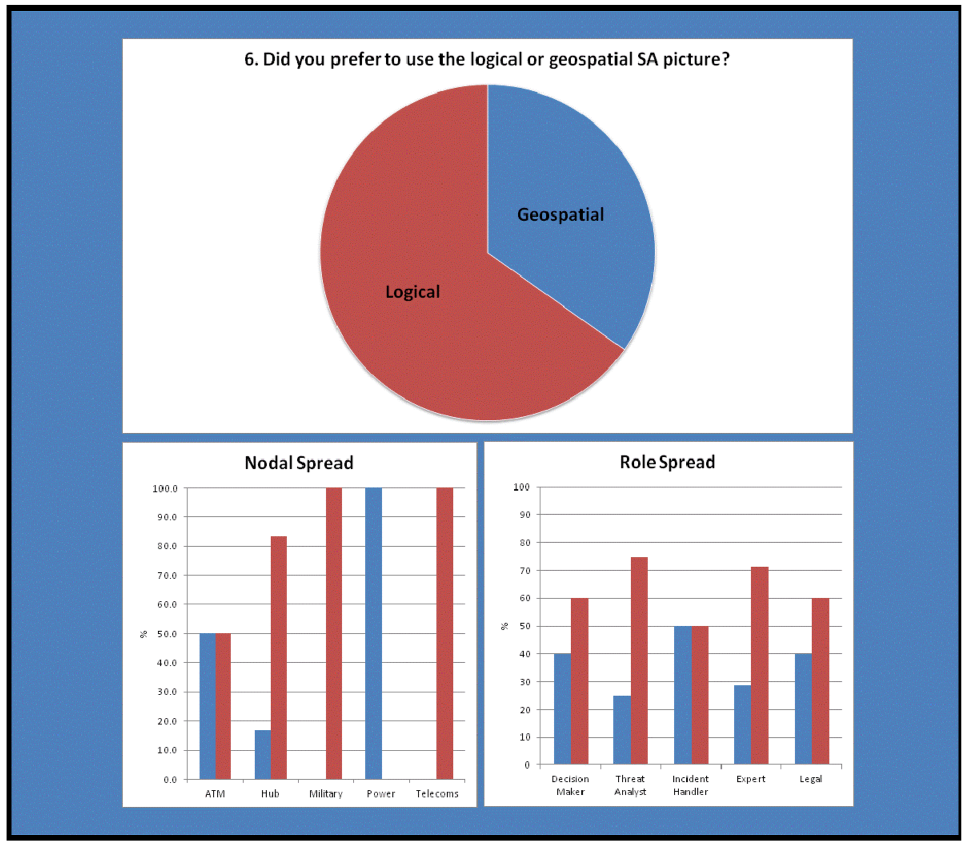


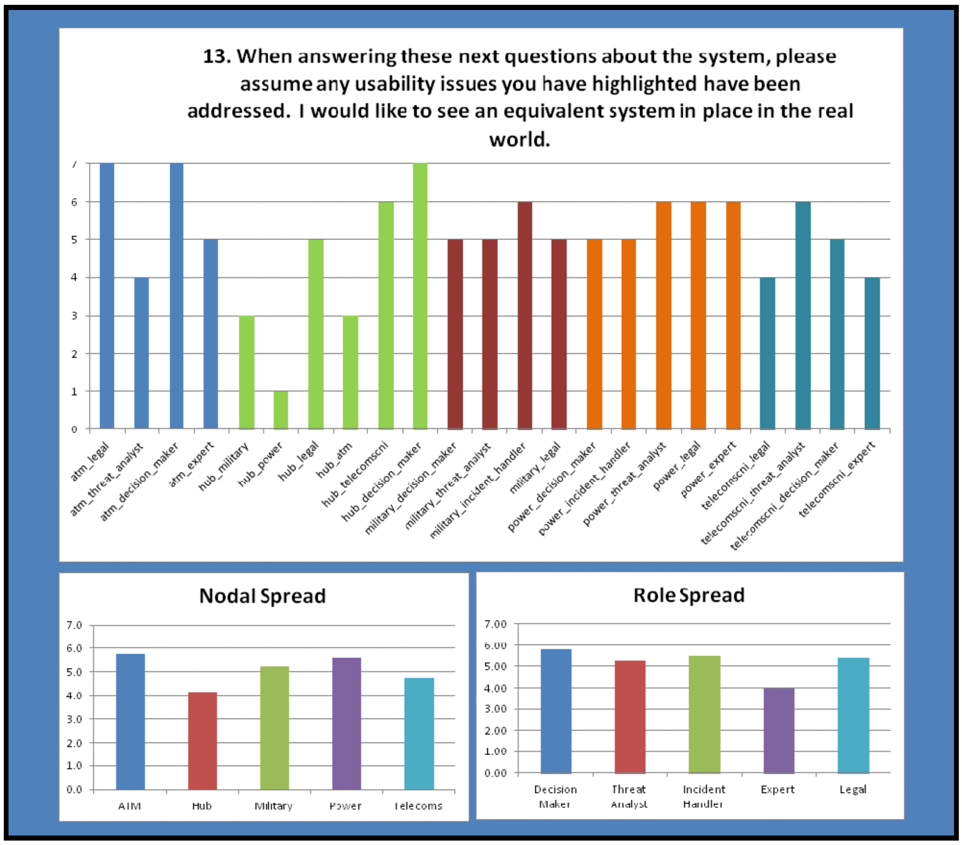


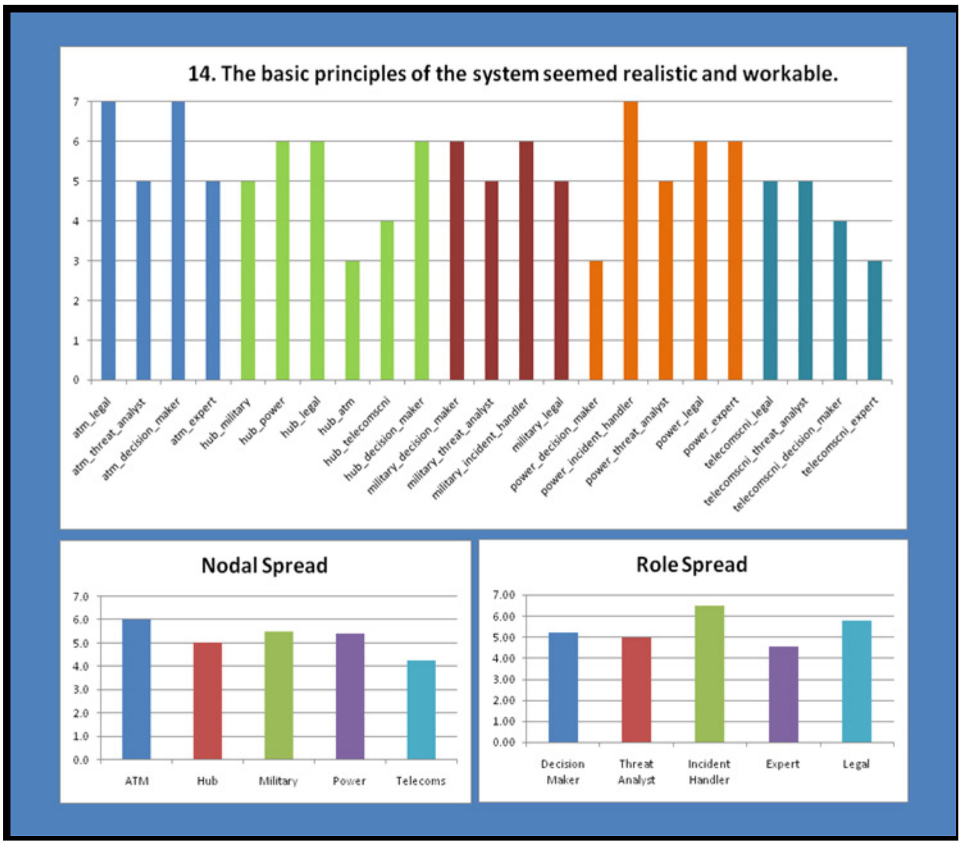


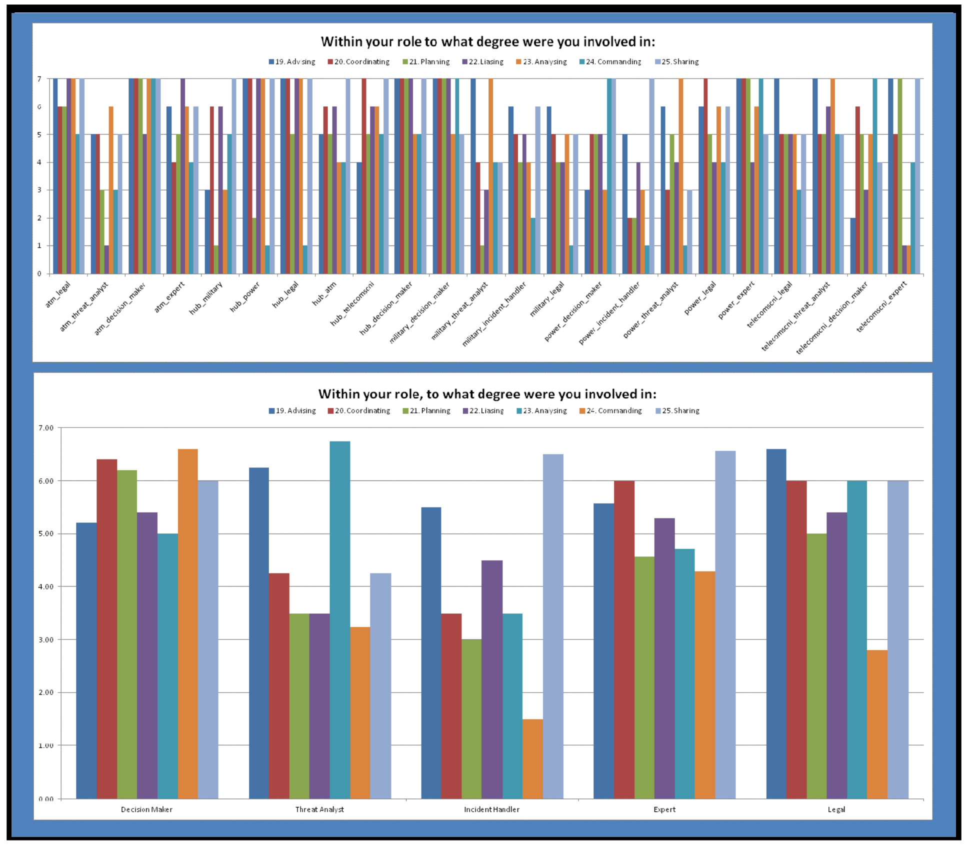


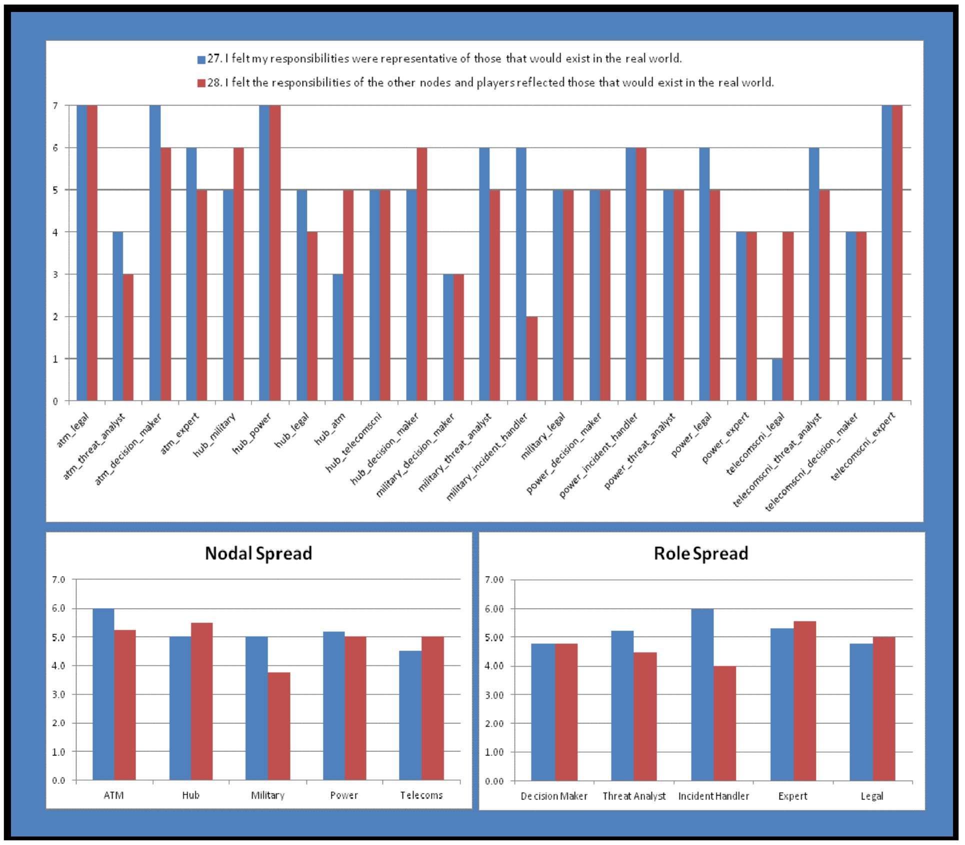


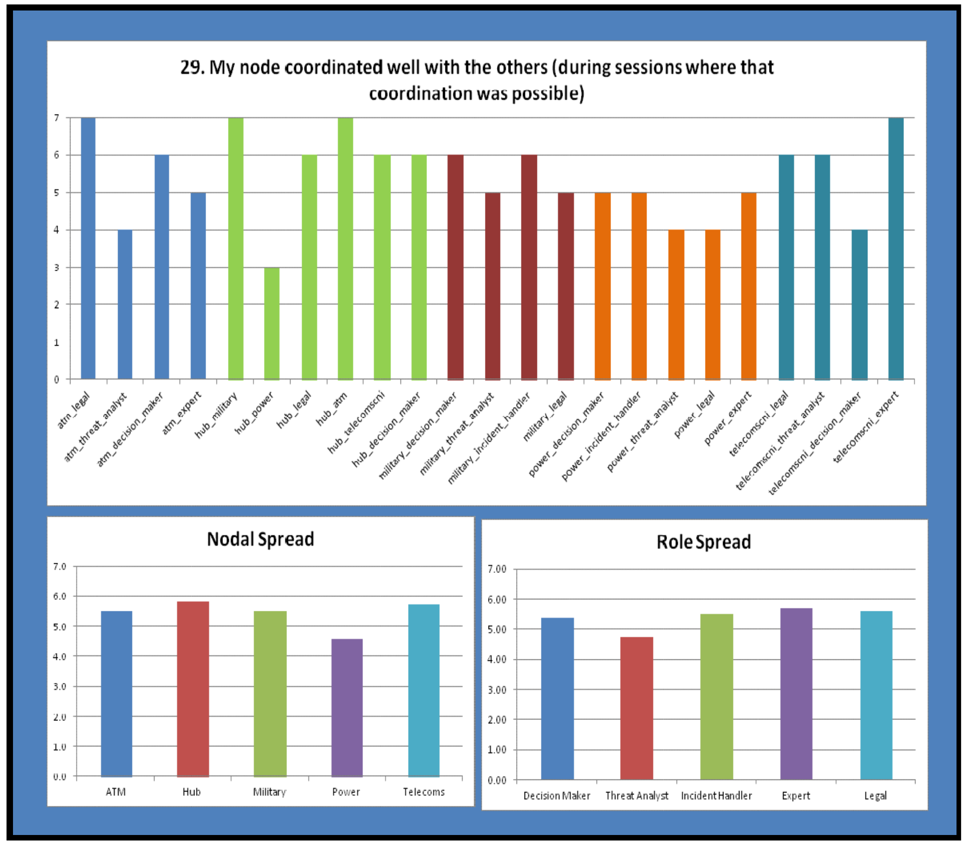

6. Did you prefer to use the logical or geospatial SA picture?
Geospatial
Logical
Nodal Spread
%
100.0 90.0 80.0 70.0 60.0 50.0 40.0 30.0 20.0 10.0 0.0
ATM Hub Military Power Telecoms
Role Spread
%
100 90 80 70 60 50 40 30 20 10 0
Decision Maker Threat Analyst Incident Handler Expert Legal

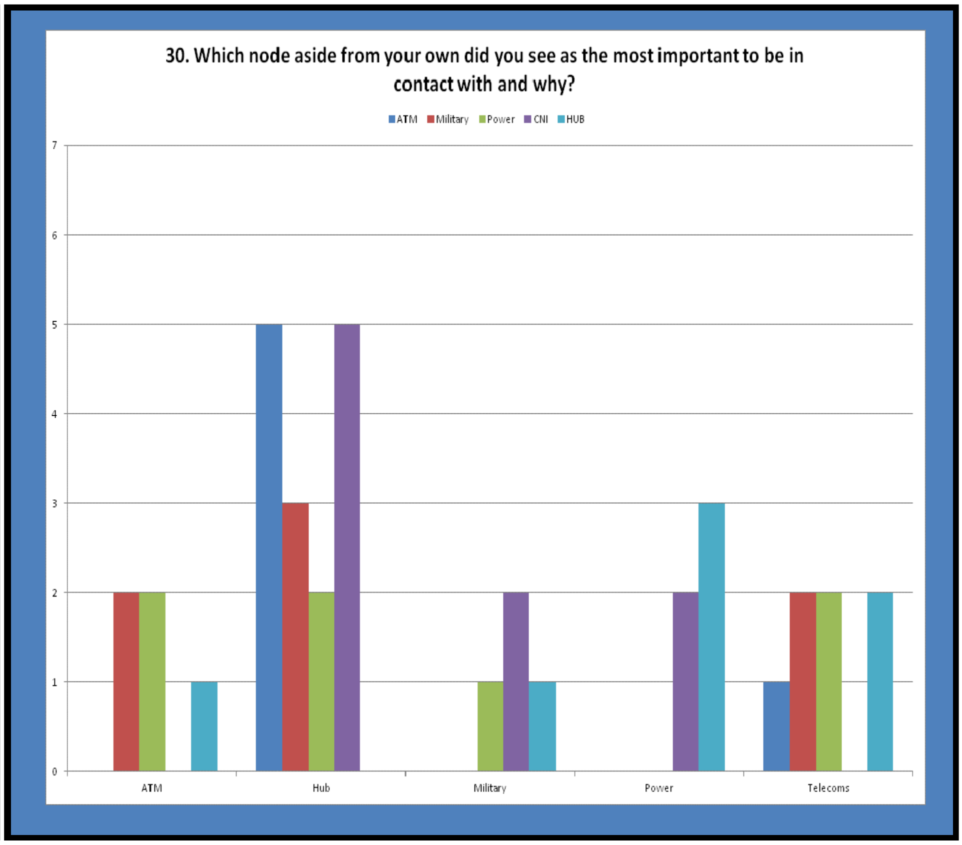

13. When answering these next questions about the system, please assume any usability issues you have highlighted have been addressed. I would like to see an equivalent system in place in the real world.
7 6 5 4 3 2 1 0
atm_legal atm_threat_analyst atm_decision_maker atm_expert hub_military hub_power hub_legal hub_atm hub_telecomscni hub_decision_maker military_decision_maker military_threat_analyst military_incident_handler military_legal power_decision_maker power_incident_handler power_threat_analyst power_legal power_expert telecomscni_legal telecomscni_threat_analyst telecomscni_decision_maker telecomscni_expert
Nodal Spread
7.0 6.0 5.0 4.0 3.0 2.0 1.0 0.0
ATM Hub Military Power Telecoms
Role Spread
7.00 6.00 5.00 4.00 3.00 2.00 1.00 0.00
Decision Maker Threat Analyst Incident Handler Expert Legal

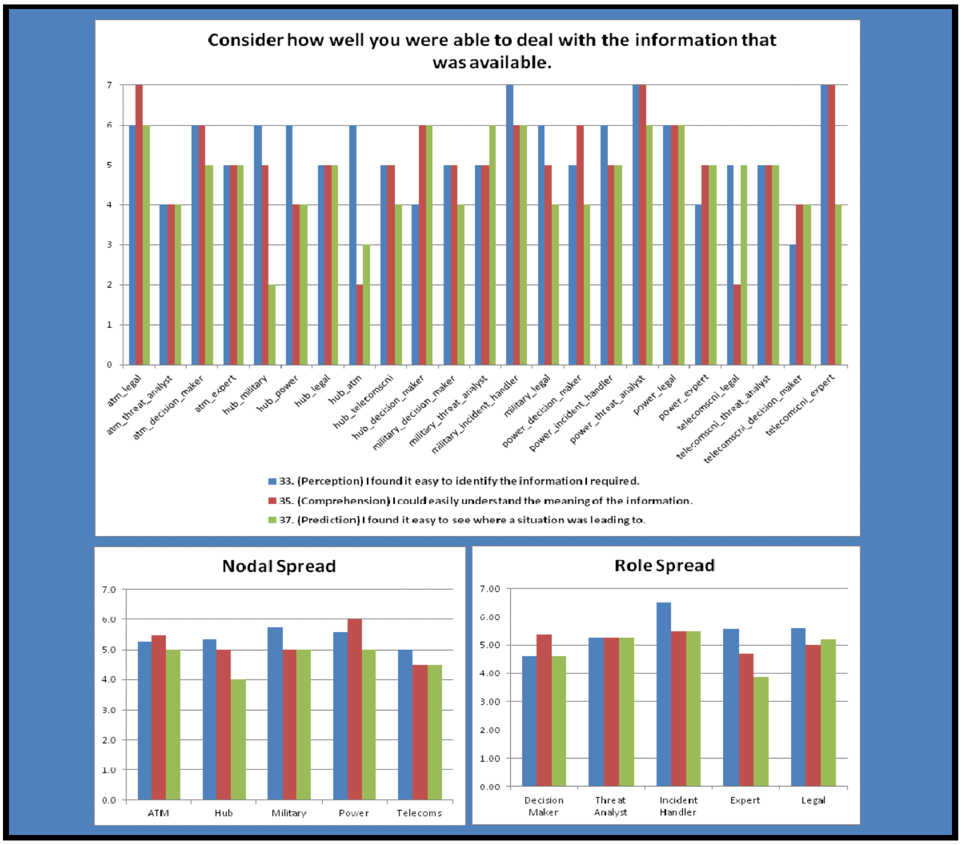

14. The basic principles of the system seemed realistic and workable.
7 6 5 4 3 2 1 0
atm_legal atm_threat_analyst atm_decision_maker atm_expert hub_military hub_power hub_legal hub_atm hub_telecomscni hub_decision_maker military_decision_maker military_threat_analyst military_incident_handler military_legal power_decision_maker power_incident_handler power_threat_analyst power_legal power_expert telecomscni_legal telecomscni_threat_analyst telecomscni_decision_maker telecomscni_expert
Nodal Spread
7.0 6.0 5.0 4.0 3.0 2.0 1.0 0.0
ATM Hub Military Power Telecoms
Role Spread
7.00 6.00 5.00 4.00 3.00 2.00 1.00 0.00
Decision Maker Threat Analyst Incident Handler Expert Legal

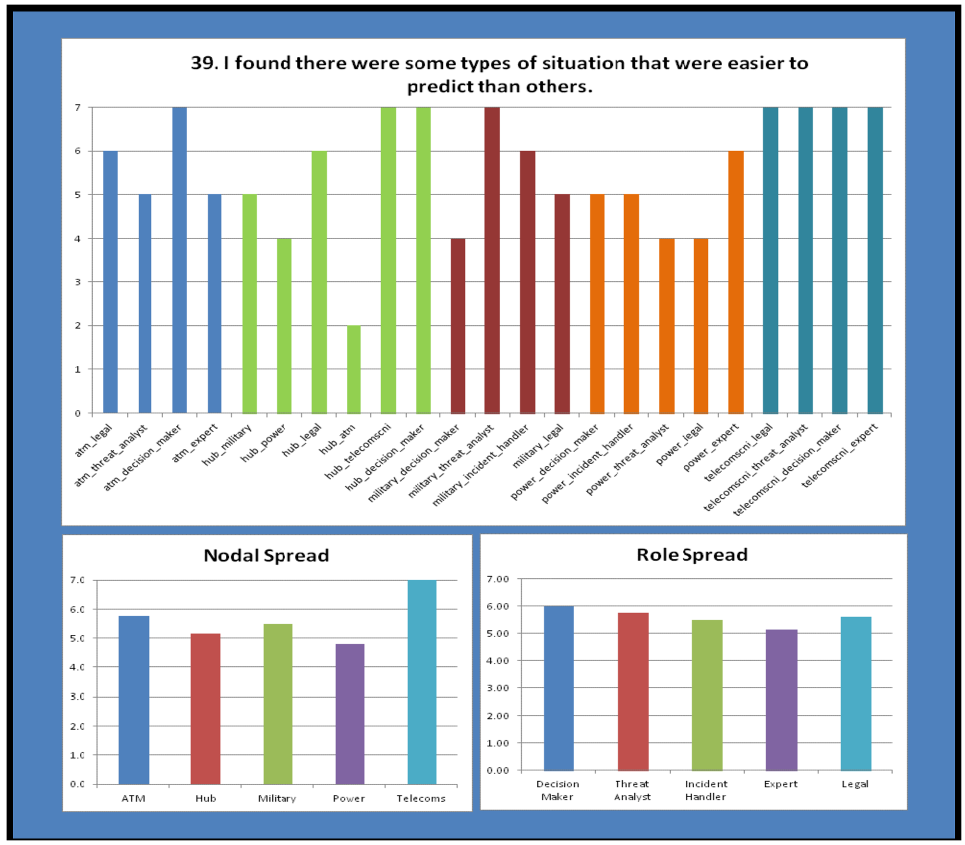

Within your role to what degree were you involved in:
19. Advising 20. Coordinating 21. Planning 22. Liasing 23. Anaysing 24. Commanding 25. Sharing
7 6 5 4 3 2 1 0
atm_legal atm_threat_analyst atm_decision_maker atm_expert hub_military hub_power hub_legal hub_atm hub_telecomscni hub_decision_maker military_decision_maker military_threat_analyst military_incident_handler military_legal power_decision_maker power_incident_handler power_threat_analyst power_legal power_expert telecomscni_legal telecomscni_threat_analyst telecomscni_decision_maker telecomscni_expert
Within your role, to what degree were you involved in:
19. Advising 20. Coordinating 21. Planning 22. Liasing 23. Anaysing 24. Commanding 25. Sharing
7.00 6.00 5.00 4.00 3.00 2.00 1.00 0.00
Decision Maker Threat Analyst Incident Handler Expert Legal

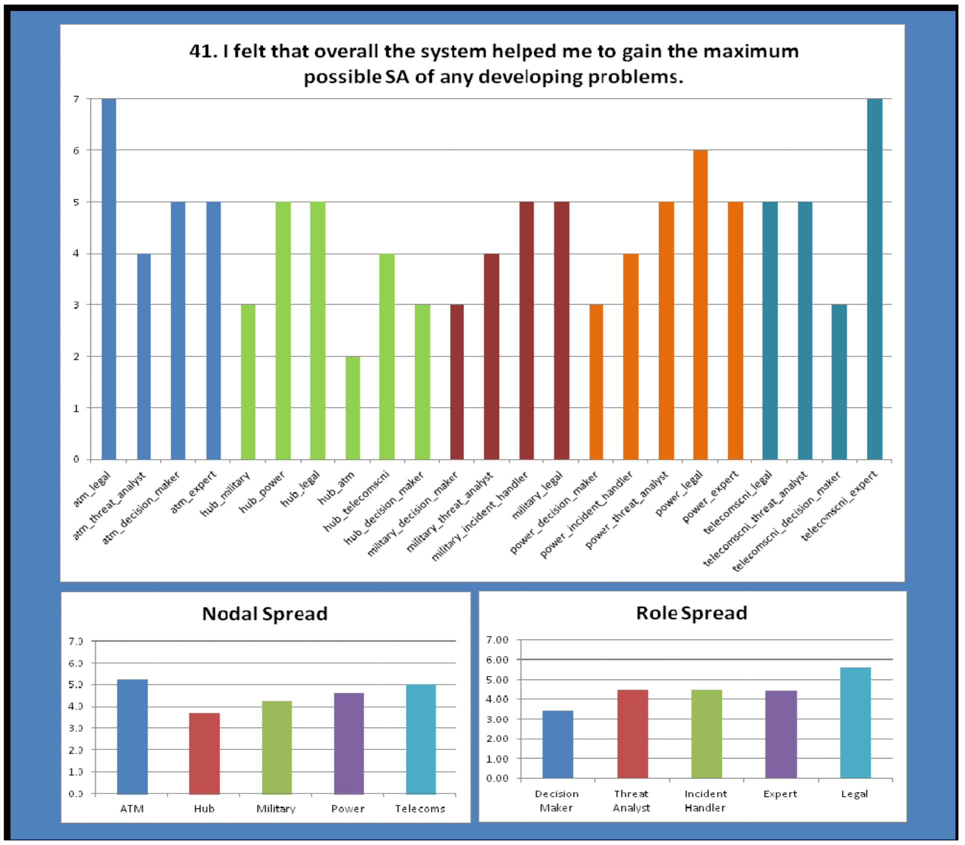

27. I felt my responsibilities were representative of those that would exist in the real world.
28. I felt the responsibilities of the other nodes and players reflected those that would exist in the real world.
7 6 5 4 3 2 1 0
atm_legal atm_threat_analyst atm_decision_maker atm_expert hub_military hub_power hub_legal hub_atm hub_telecomscni hub_decision_maker military_decision_maker military_threat_analyst military_incident_handler military_legal power_decision_maker power_incident_handler power_threat_analyst power_legal power_expert telecomscni_legal telecomscni_threat_analyst telecomscni_decision_maker telecomscni_expert
Nodal Spread
7.0 6.0 5.0 4.0 3.0 2.0 1.0 0.0
ATM Hub Military Power Telecoms
Role Spread
7.00 6.00 5.00 4.00 3.00 2.00 1.00 0.00
Decision Maker Threat Analyst Incident Handler Expert Legal

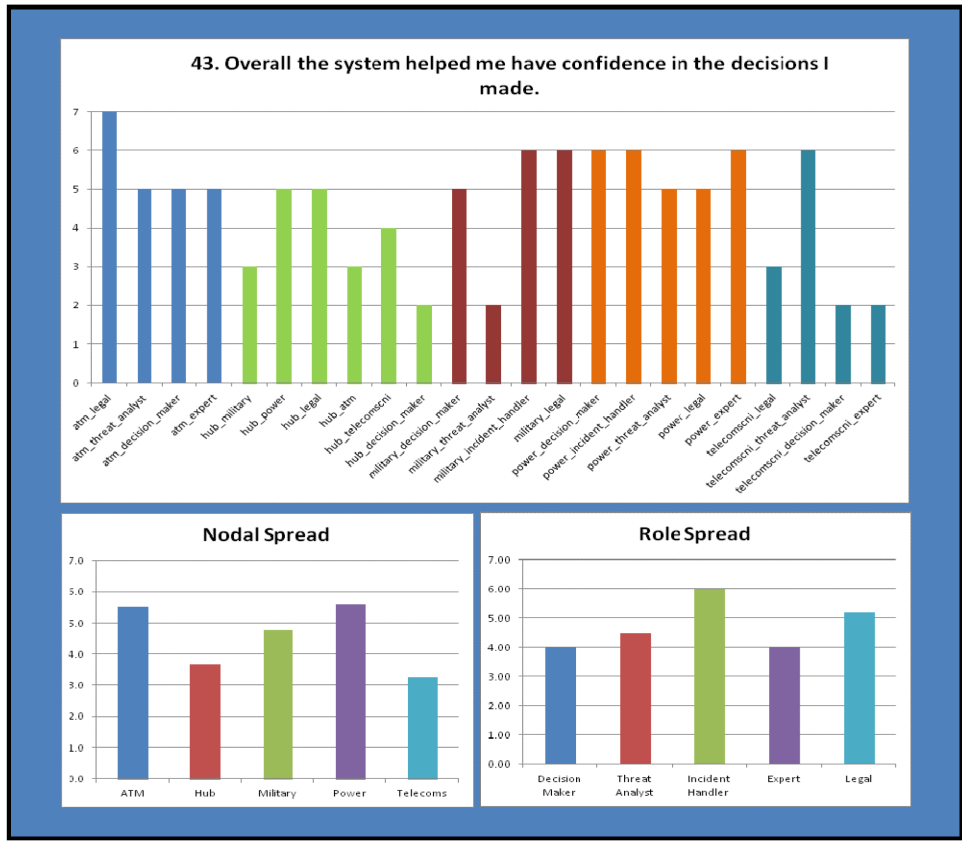

29. My node coordinated well with the others (during sessions where that coordination was possible)
0
1
2
3
4
5
6
7
atm_legal
atm_threat_analyst
atm_decision_maker
atm_expert
hub_military
hub_power
hub_legal
hub_atm
hub_telecomscni
hub_decision_maker
military_decision_maker
military_threat_analyst
military_incident_handler
military_legal
power_decision_maker
power_incident_handler
power_threat_analyst
power_legal
power_expert
telecomscni_legal
telecomscni_threat_analyst
telecomscni_decision_maker
telecomscni_expert
Nodal Spread
ATM
Hub
Military
Power
Telecoms
Role Spread
Decision Maker
Threat Analyst
Incident Handler
Expert
Legal

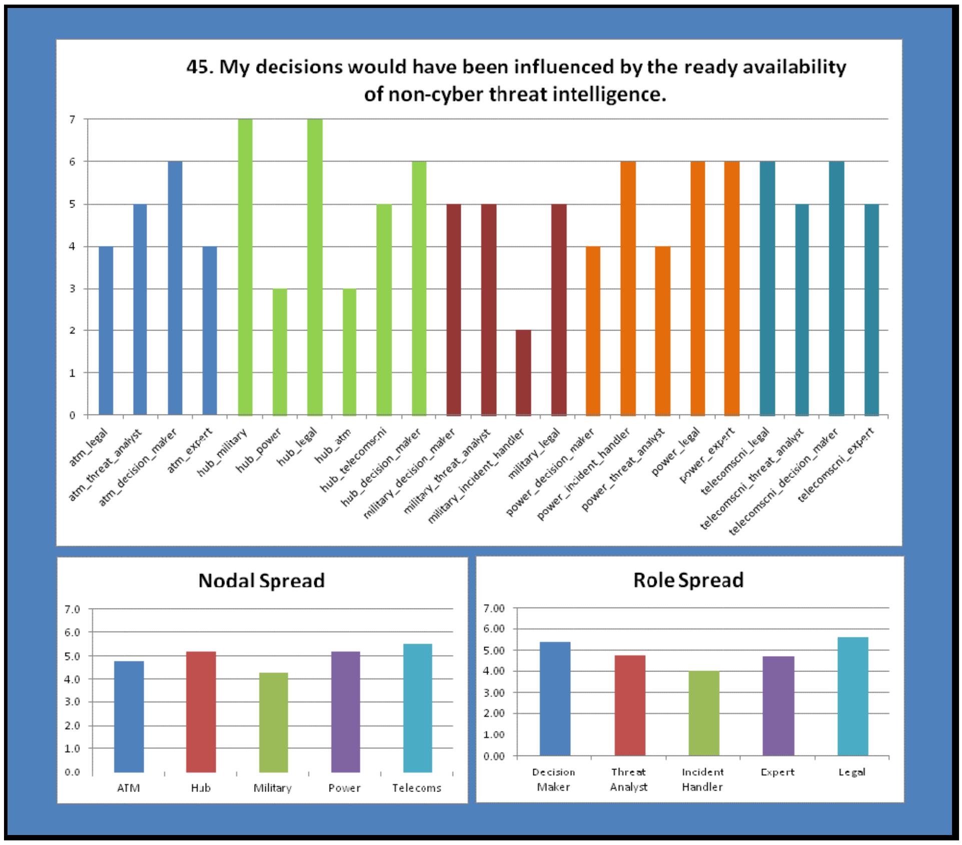

30. Which node aside from your own did you see as the most important to be in contact with and why?
ATM
Military
Power
CNI
HUB
0
1
2
3
4
5
6
7
ATM
Hub
Military
Power
Telecoms

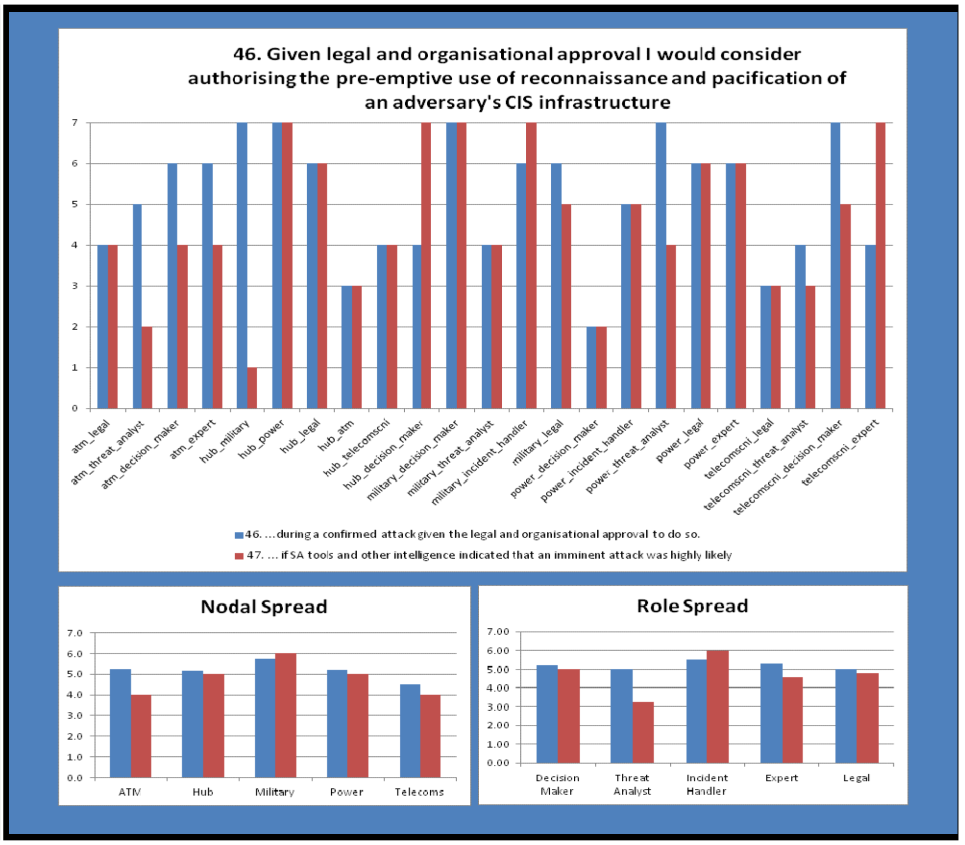

Consider how well you were able to deal with the information that was available.
atm_legal
atm_threat_analyst
atm_decision_maker
atm_expert
hub_military
hub_power
hub_legal
hub_atm
hub_telecomscni
hub_decision_maker
military_decision_maker
military_threat_analyst
military_incident_handler
military_legal
power_decision_maker
power_incident_handler
power_threat_analyst
power_legal
power_expert
telecomscni_legal
telecomscni_threat_analyst
telecomscni_decision_maker
telecomscni_expert
33. (Perception) I found it easy to identify the information I required.
35. (Comprehension) I could easily understand the meaning of the information.
37. (Prediction) I found it easy to see where a situation was leading to.
Nodal Spread
ATM
Hub
Military
Power
Telecoms
Role Spread
Decision Maker
Threat Analyst
Incident Handler
Expert
Legal

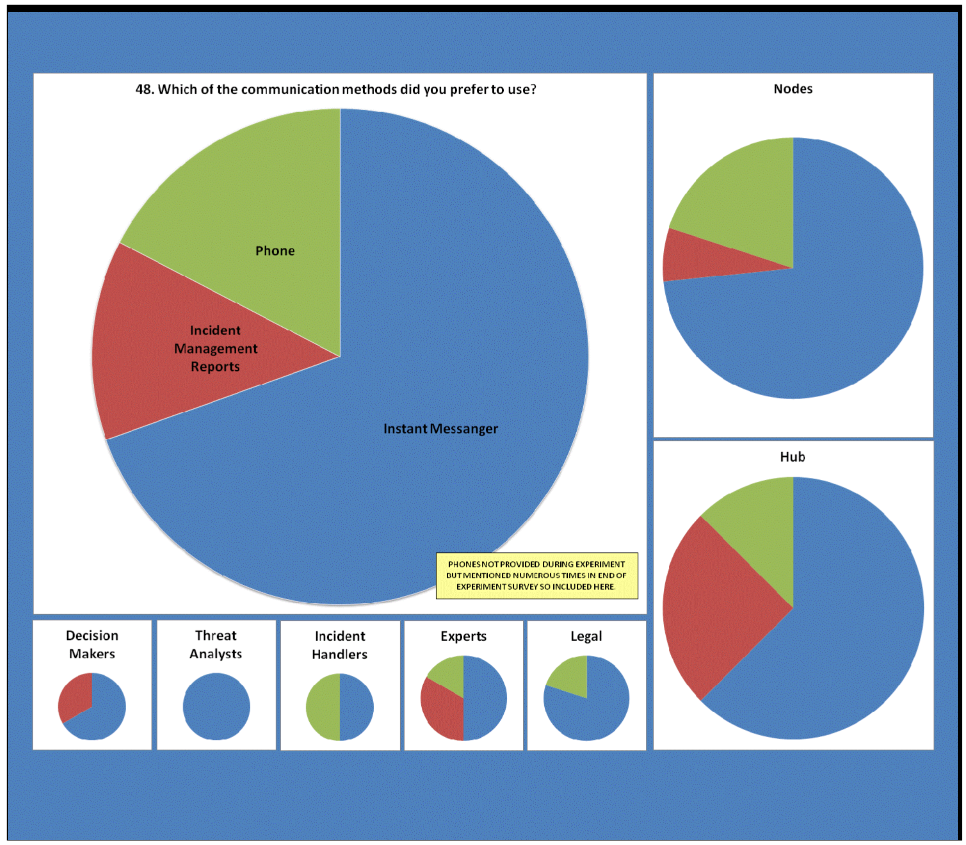

39. I found there were some types of situation that were easier to predict than others.
atm_legal
atm_threat_analyst
atm_decision_maker
atm_expert
hub_military
hub_power
hub_legal
hub_atm
hub_telecomscni
hub_decision_maker
military_decision_maker
military_threat_analyst
military_incident_handler
military_legal
power_decision_maker
power_incident_handler
power_threat_analyst
power_legal
power_expert
telecomscni_legal
telecomscni_threat_analyst
telecomscni_decision_maker
telecomscni_expert
Nodal Spread
ATM
Hub
Military
Power
Telecoms
Role Spread
Decision Maker
Threat Analyst
Incident Handler
Expert
Legal

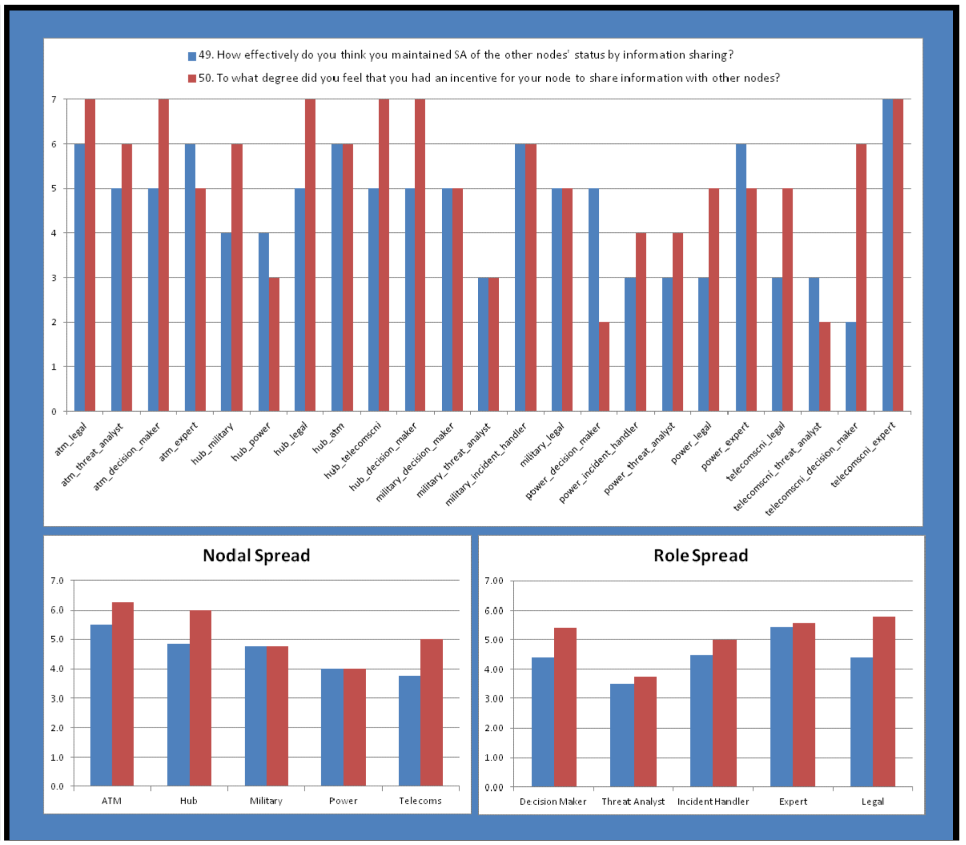

41. I felt that overall the system helped me to gain the maximum possible SA of any developing problems.
atm_legal
atm_threat_analyst
atm_decision_maker
atm_expert
hub_military
hub_power
hub_legal
hub_atm
hub_telecomscni
hub_decision_maker
military_decision_maker
military_threat_analyst
military_incident_handler
military_legal
power_decision_maker
power_incident_handler
power_threat_analyst
power_legal
power_expert
telecomscni_legal
telecomscni_threat_analyst
telecomscni_decision_maker
telecomscni_expert
Nodal Spread
ATM
Hub
Military
Power
Telecoms
Role Spread
Decision Maker
Threat Analyst
Incident Handler
Expert
Legal

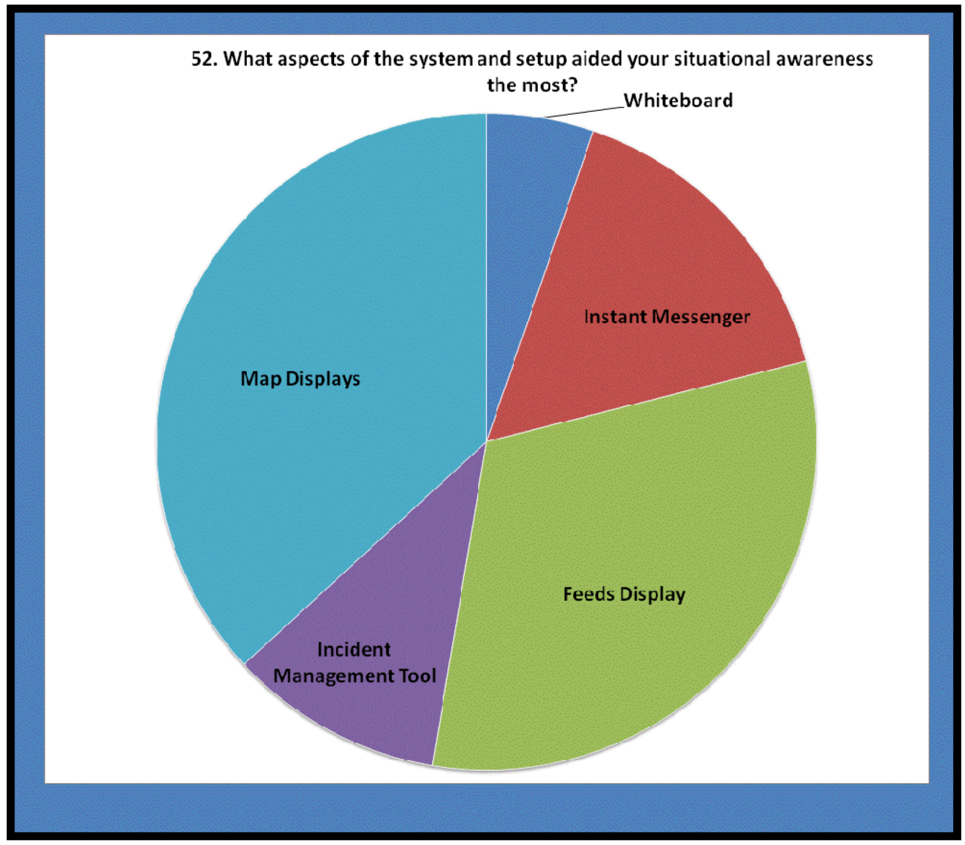

43. Overall the system helped me have confidence in the decisions I made.
0
1
2
3
4
5
6
7
atm_legal
atm_threat_analyst
atm_decision_maker
atm_expert
hub_military
hub_power
hub_legal
hub_atm
hub_telecomscni
hub_decision_maker
military_decision_maker
military_threat_analyst
military_incident_handler
military_legal
power_decision_maker
power_incident_handler
power_threat_analyst
power_legal
power_expert
telecomscni_legal
telecomscni_threat_analyst
telecomscni_decision_maker
telecomscni_expert
Nodal Spread
ATM
Hub
Military
Power
Telecoms
Role Spread
Decision Maker
Threat Analyst
Incident Handler
Expert
Legal

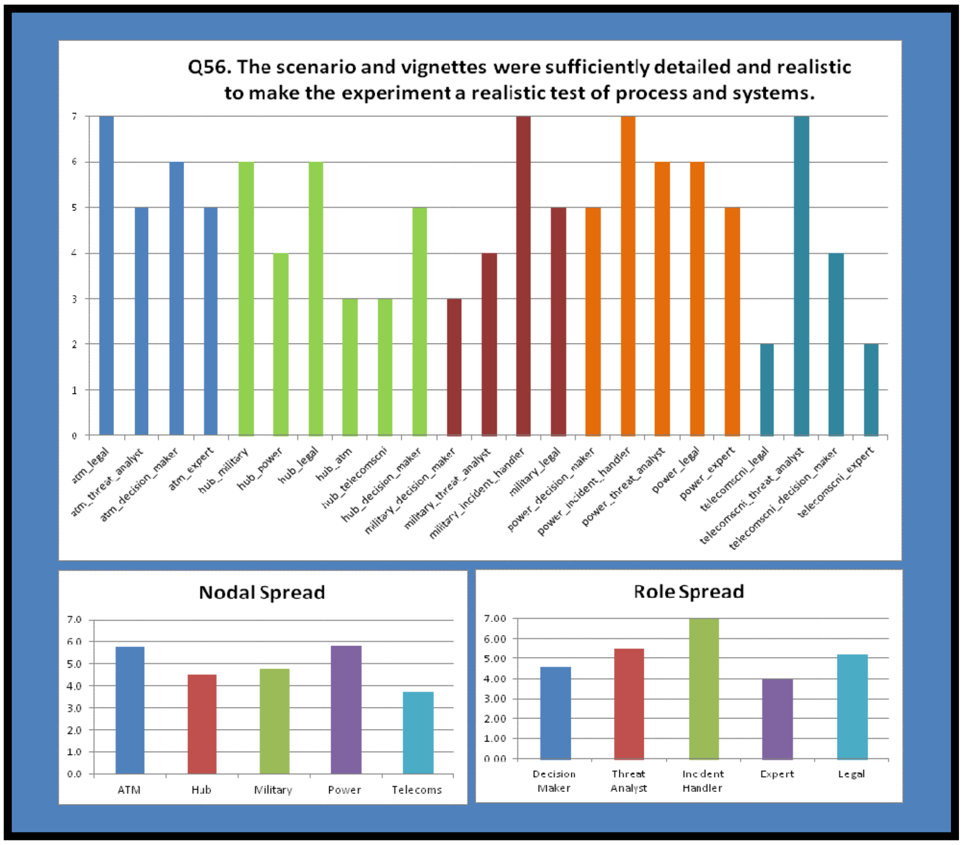

45. My decisions would have been influenced by the ready availability of non-cyber threat intelligence.
Nodal Spread
ATM
Hub
Military
Power
Telecoms
Role Spread
Decision Maker
Threat Analyst
Incident Handler
Expert
Legal

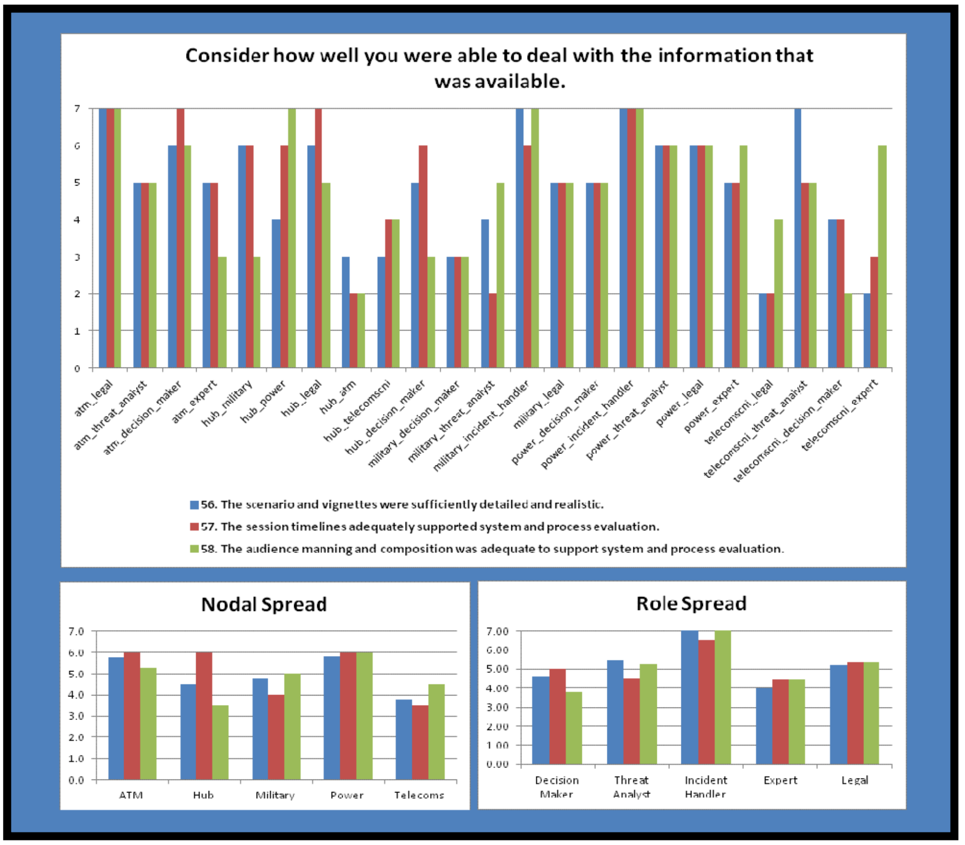

46. Given legal and organisational approval I would consider authorising the pre-emptive use of reconnaissance and pacification of an adversary's CIS infrastructure
46. ...during a confirmed attack given the legal and organisational approval to do so.
47. ... if SA tools and other intelligence indicated that an imminent attack was highly likely
Nodal Spread
ATM
Hub
Military
Power
Telecoms
Role Spread
Decision Maker
Threat Analyst
Incident Handler
Expert
Legal


48. Which of the communication methods did you prefer to use?
Phone
Incident Management Reports
Instant Messanger
PHONES NOT PROVIDED DURING EXPERIMENT BUT MENTIONED NUMEROUS TIMES IN END OF EXPERIMENT SURVEY SO INCLUDED HERE.
Nodes
Hub
Decision Makers
Threat Analysts
Incident Handlers
Experts
Legal


49. How effectively do you think you maintained SA of the other nodes' status by information sharing?
50. To what degree did you feel that you had an incentive for your node to share information with other nodes?
Nodal Spread
ATM
Hub
Military
Power
Telecoms
Role Spread
Decision Maker
Threat Analyst
Incident Handler
Expert
Legal


52. What aspects of the system and setup aided your situational awareness the most?
Whiteboard
Instant Messenger
Map Displays
Feeds Display
Incident Management Tool


Q56. The scenario and vignettes were sufficiently detailed and realistic to make the experiment a realistic test of process and systems.
0
1
2
3
4
5
6
7
atm_legal
atm_threat_analyst
atm_decision_maker
atm_expert
hub_military
hub_power
hub_legal
hub_atm
hub_telecomscni
hub_decision_maker
military_decision_maker
military_threat_analyst
military_incident_handler
military_legal
power_decision_maker
power_incident_handler
power_threat_analyst
power_legal
power_expert
telecomscni_legal
telecomscni_threat_analyst
telecomscni_decision_maker
telecomscni_expert
Nodal Spread
0.0
1.0
2.0
3.0
4.0
5.0
6.0
7.0
ATM
Hub
Military
Power
Telecoms
Role Spread
0.00
1.00
2.00
3.00
4.00
5.00
6.00
7.00
Decision Maker
Threat Analyst
Incident Handler
Expert
Legal


Consider how well you were able to deal with the information that was available.
0
1
2
3
4
5
6
7
atm_legal
atm_threat_analyst
atm_decision_maker
atm_expert
hub_military
hub_power
hub_legal
hub_atm
hub_telecomscni
hub_decision_maker
military_decision_maker
military_threat_analyst
military_incident_handler
military_legal
power_decision_maker
power_incident_handler
power_threat_analyst
power_legal
power_expert
telecomscni_legal
telecomscni_threat_analyst
telecomscni_decision_maker
telecomscni_expert
56. The scenario and vignettes were sufficiently detailed and realistic.
57. The session timelines adequately supported system and process evaluation.
58. The audience manning and composition was adequate to support system and process evaluation.
Nodal Spread
0.0
1.0
2.0
3.0
4.0
5.0
6.0
7.0
ATM
Hub
Military
Power
Telecoms
Role Spread
0.00
1.00
2.00
3.00
4.00
5.00
6.00
7.00
Decision Maker
Threat Analyst
Incident Handler
Expert
Legal