11th ICCRTS COALITION COMMAND AND CONTROL IN THE NETWORKED ERA		
Title: Social Network Analysis in Joint Experimentation: Analysing Organizational Robustness in JFCOM Multinational Experiment 4		
Topic: Experimentation		
Author 1 (POC):	**Author 2:**	**Author 3:**
Mark Round	Hannah State-Davey	Peter Goillau
QinetiQ plc	QinetiQ plc	QinetiQ plc
Alan Turing 208	Alan Turing 208	Alan Turing 208
St Andrew's Road	St Andrew's Road	St Andrew's Road
MALVERN	MALVERN	MALVERN
WR14 3PS	WR14 3PS	WR14 3PS
United Kingdom	United Kingdom	United Kingdom
+44 1684 894450	+44 1684 897552	+44 1684 894250
mdround@QinetiQ.com	hmsdavey@QinetiQ.com	pjgoillau@QinetiQ.com

© QinetiQ 2006

ABSTRACT

(DSTL/QinetiQ Paper 10)

The work reported in this paper was largely conducted under funding from the UK Ministry of Defence: *Contract AES/N05501 Report on the Analysis of Organisation at MNE4.*

Social network analysis (SNA) techniques offer great promise for researchers investigating the new command and control issues arising in the age of network-centric warfare. They provide a potential approach to the study of the organization-level properties that emerge from individual-level behaviours. Of these properties, organizational robustness and resilience are of particular interest to many militaries and governments facing modern threats. This paper documents the results of an application of SNA techniques to the analysis of such properties in an experimental distributed multinational headquarters (JFCOM MNE4). Observations are made about the success of the techniques in uncovering organizational structure as it evolved during the experiment. Indicators of robustness were surprisingly good, as were indicators of virtual co-location (shared role awareness): in particular, evidence was found of a bimodal network in virtual co-location patterns, an especially robust structure. Strengths and limitations of the data sources and techniques are discussed.

Introduction

USJFCOM Multinational Experiment 4

US Joint Force Command is currently developing concepts for future operational-level headquarters through a campaign of multinational experimentation. Multinational Experiment 4 (MNE4) was conducted between 27th February and 17th March 2006, and involved approximately 200 players[1] from seven nations (Canada, Germany, Finland, France, Sweden, UK and USA) representing an operational-level military headquarters and associated staffs. This organization was directed to conduct an effects-based operation within a simulated Afghanistan scenario, including the management of an extant operation and re-planning to cope with major scenario injects. InfoWorkSpace (IWS) was the main software collaboration tool deployed in MNE4.

The multinational analysis team was directed to assess the robustness of the Effects-Based Approach to Operations (EBAO) developed by JFCOM and the international community participating in MNE4. This robustness was broken down by JFCOM into three components: that of the processes, the organization that conducted them and the technologies that supported them. The UK analysis team took on the task of analyzing the organizational component. Within the UK contingent, the QinetiQ team was asked by JFCOM and UK MOD – Directorate of Analysis, Experimentation and Simulation (DAES) to trial the use of social network analysis (SNA) techniques in this analysis, based on previous work by the team examining its applicability in the analysis of organizational robustness.

Organizational robustness

Extensive research has been published on the properties of networks that make them robust or vulnerable when under conditions of targeted or random failure[2]. In order to make the assessment of robustness a tractable problem, the following definitions were used[3]:

1. *Structural organizational robustness* is the persistence of organizational structures in the face of a specified assembly of events;
2. *Functional organizational robustness* is the ability of the organization to maintain function in the face of a specified assembly of events.

Note that there should be no confusion with *resilience*, here – which we would define as the demonstrated ability to *recover* from damage caused by an insult within a specified timeframe. By the definitions above, robustness is shown when there is not even a temporary loss of structure/function in response to the event.

Social network analysis

Social Network Analysis (SNA) describes a set of techniques that enable visualisation and analysis of formal and informal relations between individuals. When

---

[1] The exact number of 'players' was hard to define – many staff occupied a 'grey cell' role, responsible both for exercise 'play' and for injecting stimulation into the processes.

[2] Watts (2003) is recommended as an accessible introduction to the area.

[3] There are many definitions of robustness in common usage, with no agreement on which is most appropriate. A comprehensive list of alternatives can be found at the website of the Santa Fe Institute. The following definitions are based on that by Allen, quoted at http://discuss.santafe.edu/robustness/stories/storyReader$9 (RS-2001-009. Posted 10-22-01).

applied as *organizational* network analysis (ONA), these techniques promise the ability to bring to light aspects of organizational structure and behaviour that influence the performance of the enterprise. On the basis of such information it is possible to recommend interventions that will deliver improvements in enterprise-level properties such as productivity, efficiency, robustness and resilience.

Based on graph theory, SNA techniques employ a formal mathematical approach to the study of all forms of social relations (Harary, 1969). As such, they bridge the gap between individual-level analysis techniques (e.g., measures of command intent, workload and situation awareness); and how these states and behaviours are influenced by their direct (*dyadic*) relationships with other individuals, the structure of sub-groups within which they operate, and their position within the entire network.

Individual-level measures cannot capture the organizational strengths and vulnerabilities that emerge from low-level interactions, or how these two levels of the system are mutually constraining and enabling. SNA is unique in addressing *self-organization* – how interactions and flows (in information, knowledge and tasks, for example) change to meet the functional demands of the situation. As such, it is an ideal tool with which to study robustness.

Method

Data collection and processing

Several networks were extracted from the experimental data made available by JFCOM, as – for the UK – the experiment was also a pilot study in integrating techniques of organizational analysis[4]. Additionally, it was not known in advance quite how users would employ the variety of collaborative tools at their disposal.

Those used[5] in the final analysis were: an **expected virtual co-location** network, mapping the degree to which individuals were expected to communicate, based on expected co-attendance at meetings; an **expected task collaboration** network, mapping the degree to which individuals were expected to collaborate, based on expected co-involvement in process steps; **virtual co-location** networks, mapping the extent to which individuals were virtually co-located in rooms, based on an analysis of co-attendance data culled from electronic logs of virtual room use[6]; **information flow** networks, mapping the results of player questionnaires on the players with whom they exchanged information; and **role awareness** networks,

---

[4] UK MOD's NITEworks program is developing a suite of such techniques for integrated analysis of military organizations.

[5] Other networks were generated during the data analysis phase, but the analysis of these is yet to be completed. It is intended that the results of the analyses of the following data sets will be available by September 06:

- room chat co-location networks – mapping the extent to which individuals were virtually co-located through shared participation in in-room chat, also based on logs;
- private chat co-location networks – mapping the extent to which individuals were virtually co-located through shared private chat;
- e-mail flow networks – mapping the flow of email through the headquarters; and
- reported meeting co-attendance networks – mapping meeting co-attendance links inferred from player questionnaires on meetings attended.

[6] InfoWorkSpace™ (IWS) version 3.0.

mapping the results of player questionnaires on the players of whose roles and responsibilities they were aware.

Structural analysis of robustness

The standard network measures used for assessing robustness depend on a few simple network concepts. These measures are useful in robustness analysis because they give an indication of how well messages (information, analyses, direction, and command intent) can be transmitted through the HQ:

- The **characteristic path length** (CPL) of the network – the mean path length of the shortest paths between all nodes– gives one measure of the diameter[7] of the whole network, and therefore message-passing success for the entire network – a good indicator of connectivity and therefore robustness[8];

- The **clustering coefficient** of the network – to what extent nodes are formed into clear sub-groups;

- The **degree distribution** within the network – to what extent nodes differ in the number of links they have in the network, which indicates to what extent the network's connectivity is based on key individuals;

- **Reach centrality** (Borgatti et al, 2002) was used to measure the proportion of all others in the organizational network an individual can reach in a given number of steps (e.g. one step, two steps, three steps etc). The higher the proportion of the network the individual can reach in the fewest amount of steps, the more highly connected they are.

Although robustness depends on having a highly connected network, it is not just any kind of highly connected network that determines level of robustness but one with a unique pattern of connectivity – the clustered or *scale-free* network (Thompson, 2005). The robustness properties of some common network topologies are well-established. Scale-free networks are characterized by having no *typical* scale of connectivity. A random network will show a distribution of links per node that is approximately normal – there will be a large number of nodes in the network that will have a near-average number of links. Scale-free networks have no such tendency – a large number of nodes will have very few links, and a decreasing number will show increasing numbers of links, forming a 'long tail' in graphs of degree distribution[9]. This long tail provides robustness to random failure more efficiently (with fewer links) than a comparable random network. It is the targeting of this long tail that is the surest way to cause such networks to break down.

By simulating the loss of nodes and links from the network, the team intended to derive an indication of how well the organization would cope in the short term with

---

[7] Note that *diameter* is sometimes defined instead as the length of the *longest* of all shortest paths.

[8] It gives a good indication of the connectivity of the network. A greater proportion of connectivity to others in the network reduces the level of dependency an individual has on another within the organization. It also enables individuals to reach others in the network quickly and easily without having to go through too many intermediaries. This has advantages for rapid information transferral and information is more likely to pass from sender to receiver without becoming distorted. A short CPL between any two individuals also enables greater visibility of what is happening at any given time in the rest of the organizational network (Krebs & Holley, 2002-2005).

[9] This decreasing distribution can be described by a power law, and this is commonly regarded as a diagnostic feature for scale-free networks.

the loss of critical staff (either permanently or through the effects of high workload, sickness, shift-changes etc.). Robust networks will show smaller changes in CPL and diameter than fragile networks when similar sets of nodes are removed.

Two types of node failure were considered – **random failure** and **targeted attack**. The former scenario represents a situation in which a set number of individuals are suddenly unable to participate in HQ activity. The latter might seem an unlikely scenario, but susceptibility to such attacks is now a widely-known property of real-world networks[10], and it is a useful way to simulate the effects of localized high staff workloads on the wider HQ.

In addition, the project team were interested to see if the organization showed evidence of resilience where the designed organization showed indications of poor structural robustness. In order to do this, the networks derived from 'expected' data were compared with the organizational network structures observed. While the link types in the networks were too different to allow direct mathematical comparisons to be made, it was possible to collect observations on changes in user roles and look for these in the observed networks.

Analysis of 'shadow' organizational structure

While not directly related to issues of robustness, the team were also interested to see whether the network data could be used to discover informal sub-groups within the whole – sometimes called 'shadow' organization. Topological patterns such as cliques, clusters and k-cores are often used for this purpose. Given the size of the data, and the lack of existing research practice into the application of such techniques to two-mode (e.g. actor-meeting) data, the analysis was mostly exploratory, but Johnson's hierarchical clustering procedure (Borgatti et al, 2002) was used to build an alternative hierarchy from the Week 3 data (see Figure 7 in the Appendix).

Homophily analysis – localization of information flow as a contra-indication of resilience

The theory of 'homophily' states that communication is more likely to occur between a sender and receiver who are alike (Lazarsfeld & Merton, 1954) or are similar on certain attributes such as demographic variables (Touchey, 1974). The opposite of homophily (i.e. that ties exist between individuals who are different in certain attributes) is known as 'heterophily'. Although communication can be more effective between individuals who are homophilous (Rogers & Bhowmik, 1971), it can limit information flow to localised groups. This negatively affects the permeation of information across the whole network required to support EBAO. In terms of efficient maintenance of robustness within the network, excessive homophily could be seen as an unhealthy organizational behaviour. The wider MNE4 analysis team was also interested in whether co-location would be a major determinant of the likelihood of staff being aware of each others' roles and responsibilities.

By using statistical techniques to explain variation in the relations between individuals, it is possible to determine the factors that affect the likelihood that two individuals within the organizational network will have a relationship. A structural blockmodel[11] statistical test was used to determine the extent to which interactions

---

[10] The standard introduction to these issues is that by Barabasi (2002).

[11] The 'structural blockmodel' method tests whether different classes have significantly different interaction patterns and whether this lies within-group or between-groups.

occur between individuals who share the same attribute through examining differences in group tie density (i.e. differences in the number of ties within-group vs. between-group) (Hanneman and Riddle, 2005). The degree to which ties based on information sharing or awareness of roles and responsibilities display homophily or heterophily was tested through correlating each of these networks with both function and location attribute data. Data from the information flow and role and responsibility questionnaires was used for this analysis.

The results of the analysis need to be considered in light of the constraints and artificialities of the MNE 4 experiment, including technical problems, tool constraints and an artificial operational tempo. IWS connectivity issues and Battle Rhythm disturbances limited working time across all functions, particularly in Week 1. This not only resulted in some process steps being temporally compressed or missed out of the EBAO cycle altogether, but also distorted data. IWS enables relational data for SNA to be captured quickly, accurately and automatically. However, although all event logs including room text chat entries can be captured, private chat entries are limited to logon/off. Voice chat event logging is also not currently possible in IWS. Activity logging should be a user requirement for future CIS. Due to technical difficulties with IWS players reverted to face-to-face working, especially at the start of experimental play when significant technical difficulties were experienced with the tool. As a direct result of a lack of pre-defined systematic observation of face-to-face interactions, this data could not be captured and included in the SNA analysis. This highlights the limitations of over reliance on gathering quantifiable, objective data for experimentation purposes from IWS and systems tools.

Results

Robustness analysis results

The Week 3 IWS event log data was selected for this analysis, as it would be most representative of the state of a mature HQ performing the EBAO processes. It was also expected that IWS Week 3 data would fall into one of the standard network types - a *scale-free network*. Two versions of the data were produced – *GT18* and *GT50* – with a number of the lower-value connections removed, as a noise-reduction measure[12].

Both of these networks were compared with an artificial random network of matched node number and link density (the percentage of possible connections that are present in the network), to assess whether they showed standard differences characteristic of known network topologies. Figure 1, below, shows the degree distributions for the two slices through the Week 3 data, GT18 and GT50, compared with distributions from matched random networks.

[12] The networks produced by IWS data event data were *valued*: the value between any two individuals being set by the minimum number of interactions recorded in rooms shared by those individuals within each of the three–hour work periods. In this way, the strength of each link was intended to represent the degree to which staff were virtually co-located. In order to conduct the various robustness analyses, it had to be dichotomized. In this process, lower-valued links are removed from the network so that only more frequent collaboration is represented, and all remaining links are treated as being of equal value. In order that the effects of this data processing did not introduce artefacts into the results two different networks were produced, at different thresholds. One network was created from links having mean or above-mean value (the 'GT18' network – for 'greater than 18', where 18 was the mean link strength) and another at the highest level before which the network would split into components of significant size (the 'GT50' network).

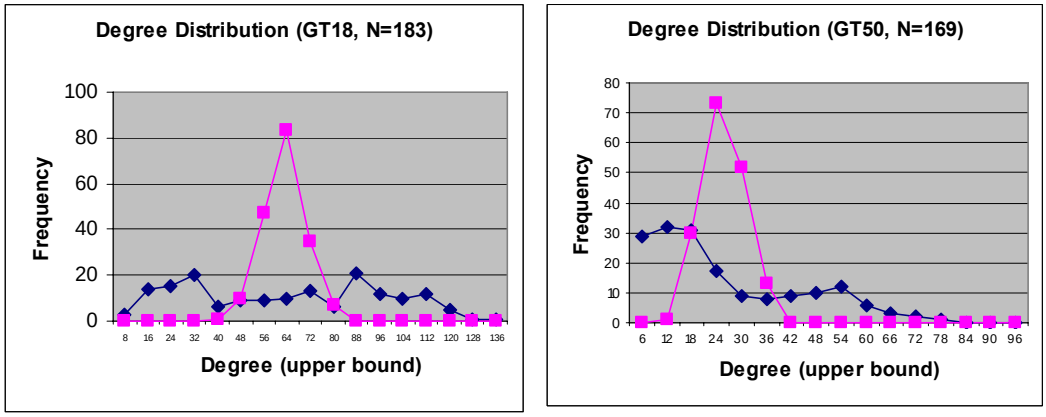

Figure 1. Degree distribution for the IWS Week 3 log data (GT18 and GT50 sets - dark blue diamonds) against matched random networks (pink squares).

	Nodes	Links	Density	Mean Degree	Cluster Co-eff.	CPL	ΔCPL
	N		d	K	C	L	ΔL
Random network (matched N,d)	183	10,958	.329	59.88	.330	1.67	--
Wk3 IWS: (GT18)	183	10,968	.329	59.93	.740	1.74	--
GT18, 20% targeted by degree	147	4,530	.211	30.82	.667	2.01	+15.6%
Means for GT18, 20% random failure, (10 trials)	--	7,143	.333	48.63	.738	1.74	+.3%
Std deviation	--	362	.017	2.47	.009	.03	+7.9%
Random network (matched N, d)	169	3,890	.137	23.02	.141	1.90	--
Wk3 IWS (GT50)	169	3,898	.137	23.07	.752	2.40	--
GT50, 20% targeted by degree	135	1,378	.083	10.68	.729	3.25	+35.7%
Means for GT50, 20% random failure, (10 trials)	--	2,500	.138	18.52	.750	2.43	+1.5%
Std deviation	--	127	.007	.94	.009	0.05	+2.1%

Table 1. Robustness properties of two different *m-slices* through the same IWS Wk3 event log dataset (the GT18 and GT50 networks).

While the Week 3 distributions are clearly not random, and both show a ‘long tail’ of higher-density nodes compared to the random networks, they do not follow the power-law curve expected of a scale-free network. Both distributions are in fact *bi*modal, with second modes occurring in both networks at about 55% of the degree maximum. This is a strong indication of the presence of a recognised type of network structure in the pattern of IWS use, known as a *bimodal network*. In such networks there are two typical scales of connectedness for nodes (shown by the two arithmetic modes in the distributions).

A more direct way to measure this robustness is by simulating such attacks and failures on the network by removing sets of nodes and measuring the degree to which the network disintegrates. A standard procedure for this (Lusseau, 2003) is to simulate a targeted attack by removing the 20% of nodes with the highest degree, and random attacks by removing randomly-selected sets of 20% of the network. The results of these analyses are given in Table 1. Figure 2 and Figure 3 show the shape of the GT50 network before and after the simulated targeted attack.

It can be seen from the table that the CPL for both the GT18 and GT50 slices is higher than that of a random network, which is not consistent with the properties of scale-free networks. The increase in CPL under conditions of attack – even for the GT50 network – is not as high as might be expected. As the graphs in Figure 2 and Figure 3 show, the network remains a single, relatively well-connected component, with the internally-redundant EBP group taking most of the damage. Scale-free networks, unlike random networks, will generally disintegrate under such conditions (Barabasi, 2002). Neither the GT18 nor the GT50 slice of the Week 3 data show such vulnerability, although they both suffered worse from targeted attack than from any of the random failures.

Emergent organizational structures observed

Evidence of functional robustness (the ability of the HQ to maintain function through changes in the internal structure) is provided in the changes seen in roles and groups in response to internal and external changes throughout the experiment. Figure 6 in the Appendix shows a the results of an analysis of one topological correlate of groups (k-cores). The CTF organizational structure evolved to cope with the demands of the process at both a role and subgroup level.

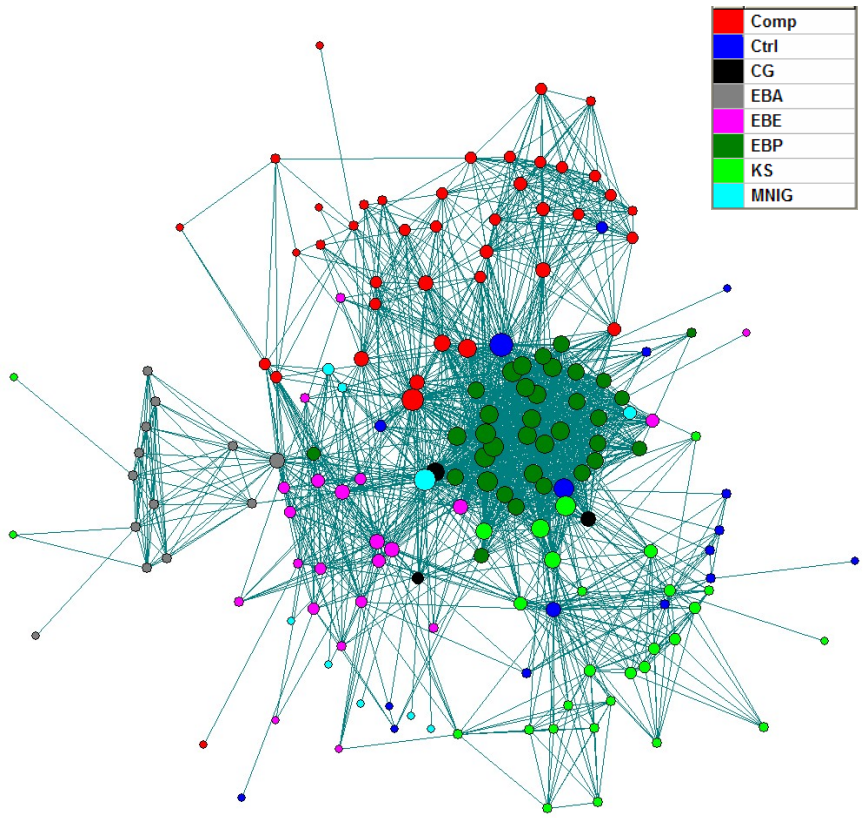

Figure 2. The Week 3 IWS co-location network (GT50 slice) – nodes sized by degree

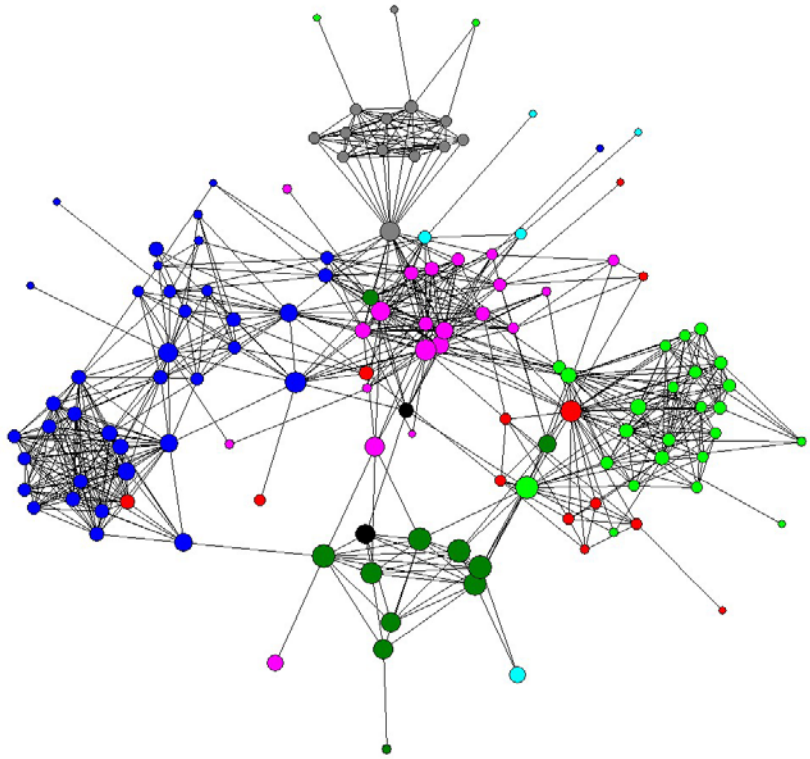

Figure 3. The Week 3 IWS co-location network (GT50 slice) after a simulated targeted attack on the most-connected 20% (by degree) – nodes sized by degree, pre-attack.

Role-level changes observed.

Over the course of the experiment, cross-functional roles evolved to suit the task, providing evidence of the resilience of the staff in self-organizing. Network analysis makes these changes clear. Comparison of the actual patterns of collaboration with data from the 'expected' networks (compare with Figure 8 in the Appendix) shows the roles that changed in response to the demands of the event. For example, the KM Records Management Officer's (RMO) role evolved to bridge between KM and EBE to help the over-tasked EBE Knowledge Management Officer (KMO) (Figure 4):

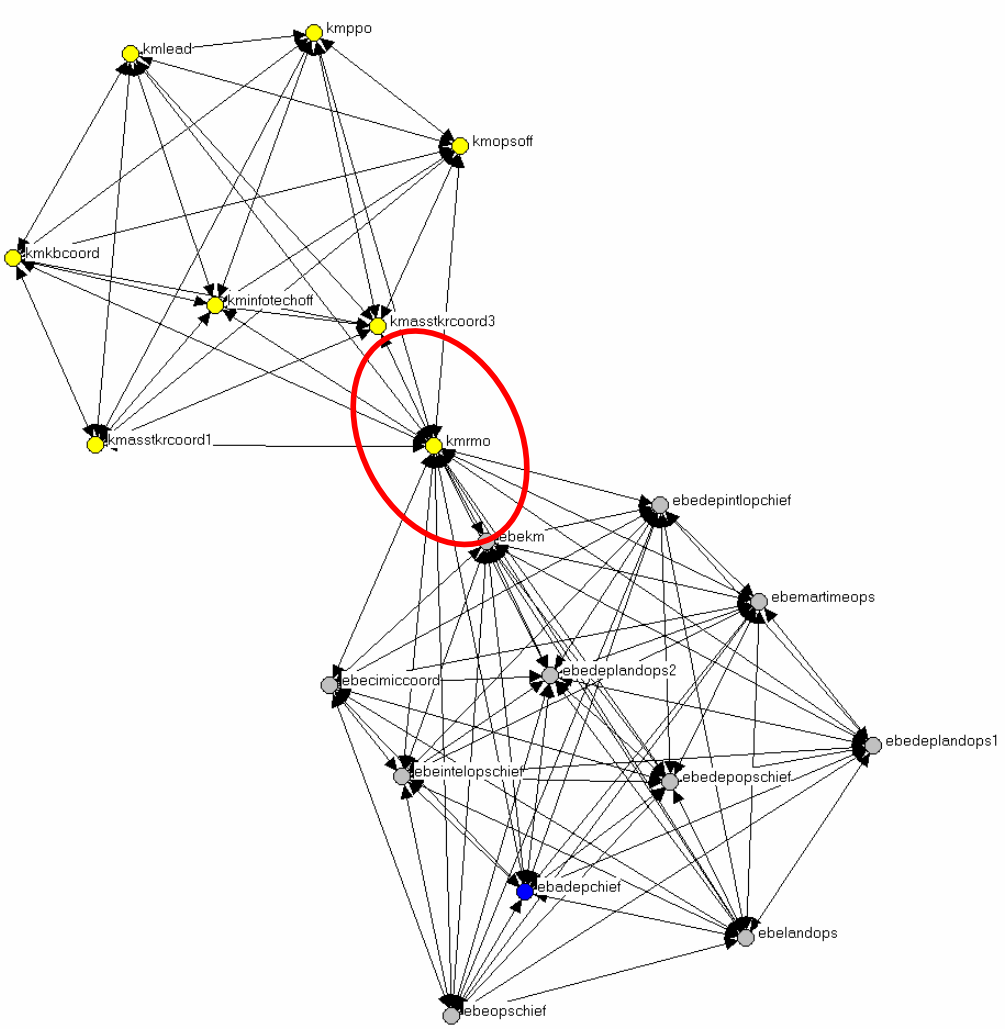

Figure 4. Evolved cross-functional role of the KM KMO to support the EBE KMO taken from IWS logs from Day 11 Week3.

The KM Training Officer was also redeployed to help the EBA KMO to help with standing knowledge request (KR) issues. These two roles continued to conduct their original roles whilst also facilitating the KMOs. The existence of these roles helped to facilitate information flow between functions by absorbing some of the workload from the KMOs in other groups.

Subgroup-level changes observed.

At the subgroup level, large meeting structures proved inefficient for conducting tasks and enabling valuable inputs to be made by all experts present. As the functional group with the largest membership, this was particularly the case for EBP who provided a rapid response to this. During week 1, EBP broke down into two subgroups to conduct parallel planning and in order to conduct collaborative planning more efficiently, forming subgroups in EBP Breakout Room (BO) 1 and EBP BO 2. This is shown in Figure 5.

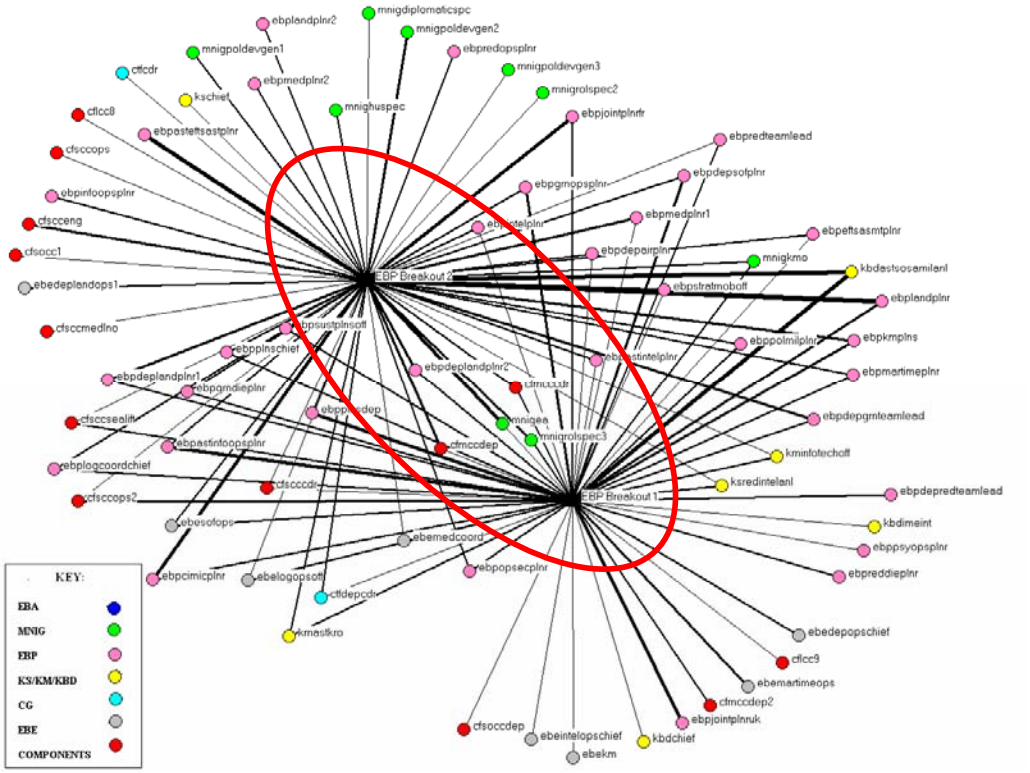

Figure 5. Evolution of two subgroups over week 1 and 2 to support the efficient conduct of EBP tasks in EBAO, taken from a snapshot of IWS logs from Day 9, Week 2. The mixing of teams attending the two rooms is very visible, as is sub-group of staff that attended both rooms.

These subgroups proved effective for conducting tasks across the whole experimental period. EBP BO 1 at the beginning of week two was used for continuing work on EB Plan 1A with active participation from MNIG, and Red and Green teams. EBP BO2 subgroup was formed to work on SITREPS in the first week and completion of the Action Development and Resource Matching (ADRM) in the second week.

One of the aspirations of the analysis was the detection of an emergent (or *shadow*-) organization developing within the HQ in response to the experimental conditions. Although this has, in part, been addressed in the section on bottom-up reorganization above, an exploratory analysis was conducted to see if an organizational structure could be inferred from patterns of association in IWS rooms using the Week 3 data.

The patterns of association were used as an index of the *similarity* of each pair of nodes from the network, and Johnson's hierarchical clustering procedure (Borgatti et al, 2002) was used to generate a representation of the clusters to which each actor belonged. This analysis often generates highly complicated representations: a simplified tree-map was used to make these sub-groups comprehensible. Figure 7 in the Appendix shows the results of this analysis represented as a tree-map[13], although it is a reflection of the degree of cross-group working that this is still a highly complicated structure, with many logons that seem to be out of place with regard to their formal group affiliation. The map is included as it may be useful in determining alternative structures to the one used in the experiment, as a basis for future development and experimentation.

Results of homophily analysis (within- vs. without-group communication)

The results of the analysis (see Tables 4-5 in the Appendix for information sharing tie densities for within and between-groups) show that all but EBP have significantly stronger within-group ties than between-group ties (p-value = .0000[14] across all weeks). This indicates that in these groups, individuals conducted significantly more localised information sharing within their own function. Although EBP was found to have moderately strong within-group information sharing ties in all weeks (0.078; 0.089; 0.095) this was not significantly different from those between EBP and the other groups in weeks 1, 2 or 3 (p-value = .5928; .6460; and .7994 respectively). EBP was also found to have stronger information ties with the Command Group and EBA consistently across all experimental weeks. However, EBP had fewer information ties with the KS/KM/KBD group than any other E-Function (tie density of 0.020; 0.023; 0.033 in weeks 1, 2, and 3 respectively). The significant between-group information sharing relationships are identified in Table 2, below.

WEEK 1		P-Value	WEEK 2		P-Value	WEEK 3		P-Value
CG	EBA	0.0392	CG	MNIG	0.0058	CG	EBE	0.0268
EBE	CG	0.0308	MNIG	CG	0.0136	CG	EBA	0.0284
						CG	MNIG	0.0284
						MNIG	CG	0.0126

Table 2. Significant between-group information sharing ties across all experimental weeks.

Across both weeks 2 and 3, the CG and MNIG displayed strong reciprocal information ties. However, the results did not show any significantly strong information sharing ties between the MNIG and any other functional group. This has implications for an expected organizational structure that emphasises inter-agency communication, required to support EBAO.

[13] Tree-maps are representations of tree-structured data (such as file structure) as if viewed 'from the ground'. Actors who commonly associated together are located together within sub-groups, which are themselves contained by larger groups.

[14] 'P' stands for probability and measures how likely that any observed difference between groups is due to chance. P can take any value between 0 and 1. The closer the value is to 0, the more unlikely the observed difference is due to chance.

Correlation of awareness ties with Function.

A similar pattern of within- and between-group ties was also found through correlation analysis between the 'Awareness of Roles & Responsibilities' network and the 'function' attribute data. Tie density values for within and between groups is shown in Tables 4-5 in the Appendix.

In weeks 1 and 2, a significantly greater level of awareness of others' roles and responsibilities was found within the CG (p-value = .0002; .0000 respectively), EBE (p-value = .0000 for both weeks), EBA (p-value = .0000 for both weeks), KS/KM/KBD (p-value = .0000 for both weeks), MNIG (p-value = .0000 for both weeks), and the Components (p-value = .0000 for both weeks). In week 3 however, only the CG reported stronger within-group awareness ties (tie density = 0.850; p-value = .0300). All other groups reported greater awareness of the roles and responsibilities of those in other groups to themselves. Table 3 below shows the significant between-group awareness ties for weeks 1, 2 and 3.

WEEK 1		P-Value	WEEK 2		P-Value	WEEK 3		P-Value
EBE	CG	0.0092	EBE	CG	0.0000	CG	EBP	0.0300
EBA	CG	0.0010	EBE	EBA	0.0412	CG	EBE	0.0300
EBA	MNIG	0.0274	EBE	MNIG	0.0042	CG	EBA	0.0300
MNIG	CG	0.0000	MNIG	CG	0.0000	CG	KS/KM	0.0300
Comp	CG	0.0038	Comp	CG	0.0008	CG	MNIG	0.0300
						CG	Comp	0.0300
						EBP	CG	0.0300
						EBE	CG	0.0300
						EBA	CG	0.0300
						KS/KM	CG	0.0300
						MNIG	CG	0.0300
						Comp	CG	0.0300

Table 3. Significant between-group awareness ties across all experimental weeks.

Although density of information sharing ties reported by members of EBP did not significantly differ across within- and between-groups, they did report across all weeks a higher level of awareness of the roles and responsibilities of the CG (tie density = 0.086; 0.081; 0.135 respectively) and the least awareness of the roles and responsibilities of those in KS/KM (tie density = 0.014; 0.014; 0.018 respectively).

Effects of distribution on information sharing and on awareness of roles and responsibilities.

Co-location was not found to have a positive significant effect on information sharing tie density across any of the experimental weeks for any of the groups (p-value = 0.9996). The MNIG however displayed a slightly stronger tendency for co-located

information sharing within their own group across all weeks, although this was again not found to be statistically significant (p-value = 0.5584; 0.5814; 0.6538 respectively). Co-location was also not found to be a positive significant driving factor in reported awareness of others roles and responsibilities across any of the experimental weeks (p-value = 0.9996). Again, the MNIG were found to have a slightly greater awareness of the roles of responsibilities of other MNIG members that were co-located at the same location, although this was found only to be statistically significant in experimental week 1 (p-value = 0.02088; 0.5010; 0.5066 respectively for weeks 1, 2 and 3).

Conclusions

In the context of this experiment, social network analysis techniques delivered results that were verified by subject-matter experts, for example in identifying role changes that had independently been described by players. They also delivered results that would not have been apparent at the level of the individual participant, such as an unexpected level of robustness to simulated threats, and an apparent success in overcoming some of the limitations of physical distribution through the use of virtual co-location technologies.

The identification of a bimodal network in the Week 3 IWS data was a particularly surprising discovery, given the expectation that evidence of a scale-free network would be found. It is particularly interesting as some artificial networks with bimodal degree distributions have shown a level of robustness superior to all other network types. This robustness has been seen in response not only to single insults of targeted attacks *and* random failures, but also to combinations of a single attack followed by a single failure (Tanizawa, 2005).

This prediction of improved robustness was confirmed by the results of the simulated attacks. Both of the IWS networks performed better than would be expected of a scale-free network – to the targeted attack in particular. Further work is required to identify the precise source of this robustness, but it is likely that redundancy in the internally well-connected EBP group was one source, combined with the existence of links between non-EBP groups. All the results (including eigenvector centrality measures not reported here) point to the EBP team as being central to the performance of the headquarters throughout the experiment. It is significant that this team were unusual in showing no significant preference for sharing information within the team rather than within the larger headquarters. This might have been expected to be a vulnerable source of network connectivity in the targeted attack scenario. It seems that the homophily shown by other teams was not so extreme as to render them disconnected when the removal of the EBP team was simulated.

Further work would also identify whether targeting by measures other than degree (such as eigenvector centrality, as an indicator of an actor's influence) would generate the same robustness result. Work by Goh et al (2002) suggests that it may be possible to classify networks universally using the exponent of the distribution of betweenness centrality scores instead of degree centrality. In the future, it might be useful to develop a corpus of results from analyses of this type on military and civilian[15] collaboration networks with which new networks could be compared.

[15] QinetiQ has already performed analyses of this type on electronic logs of its own corporate activity, with promising results (unpublished, as yet).

The organizational structure was under-specified before the experiment, but the headquarters showed evidence of functional robustness in that low-level structures emerged over the course of play that enabled the effective conduct of the process. This was in part due to adaptation by individuals in response to the demands of the new process. Network analysis was effective in identifying these changes, but failed to provide an adequate visualization of the analysis of emergent structure at higher levels of organization. Developing techniques for discovering and displaying emergent structure is now a key research area for the team, and it is intended that the same dataset will be used to test any new developments[16].

Initial indications are that these techniques have uncovered unexpected properties in the organizational structure of a military headquarters. There is fertile ground here for further work observing real military groups and testing hypotheses, specifically on adaptations to random failure and targeted attack. The collection of a corpus of such data would provide a valuable resource with which to address significant research problems, such as the diagnosis of large-scale enterprise properties (robustness, resilience) and modelling the dynamics of organizational networks under stress.

References

1. Barabási, A-L (2002) *Linked: The New Science of Networks,* Perseus Books Group.

2. Borgatti, S.P., Everett, M.G. and Freeman, L.C. (2002). *UCINET for Windows: Software for Social Network Analysis*. Harvard, M.A: Analytic Technologies.

3. Goh et al (2002) Classification of scale-free networks. *Proc. Natl. Acad. Sci. USA* **99**, 12583.

4. Hanneman, R.A., and Riddle, M. (2005) *Introduction to social network methods*. Riverside, CA: University of California, Riverside. URL: http://faculty.ucr.edu/~hanneman.

5. Harary, F. (1969) *Graph Theory*. Reading, MA. Addison-Wesley.

6. Krebs, V. and Holley, J. (2002-2005) Building Smart Communities through Network Weaving, at http://www.orgnet.com/BuildingNetworks.pdf, accessed 30 July 2006.

7. Lazarsfeld, P.F., and Merton, R.K. (1954). Friendship as a social process: A substantive and methodological analysis. In M. Berger (Ed.), *Freedom and Control in Modern Society* (pp. 18-66). Van Nostrand, New York.

8. Lusseau, D. (2003) The emergent properties of a dolphin social network. *Proceedings of the Royal Society of London-Series B (Supplement)*: DOI 10.1098/rsbl.2003.0057

[16] Further work is also required to address the apparent data-loss in some of the techniques used. The dichotomization of valued relational data (even where performed around a range of thresholds to produce several networks for analysis) undoubtedly hides valuable data about the differences between low- and high-strength links. This limitation on the possible value that can be gained applies both to the identification of sub-groups and to the analysis of structural robustness.

9. Rogers, E.M. and Bhowmik, D.K. (1971). Homophily-heterophily: Relationship concepts for communication research. In L.L. Barker and R.J. Kibler (editors). *Speech communication behaviour: Perspectives and principles*. Englewood Cliffs, N.J.: Prentice-Hall, pp. 206-225.

10. Santa Fe Institute, http://www.santafe.edu/research/robustness.php accessed 22 May 2006.

11. Tanizawa, T. (2005) Optimization of network robustness to waves of targeted and random attacks. *Physical Review E*, **71**, 047101.

12. Thompson, K. (2005). Virtual team connectivity – three action rules from nature. *Bioteams Feature*, **38**.

13. Touchey, J.C (1974). Situated Identities, Attitude Similarity, and Interpersonal Attraction. *Sociometry*, **37**, 363-374.

14. Watts, D. J. (2003) *Six Degrees: The Science of a Connected Age*. New York: Norton.

APPENDIX – Social Network Analysis diagrams

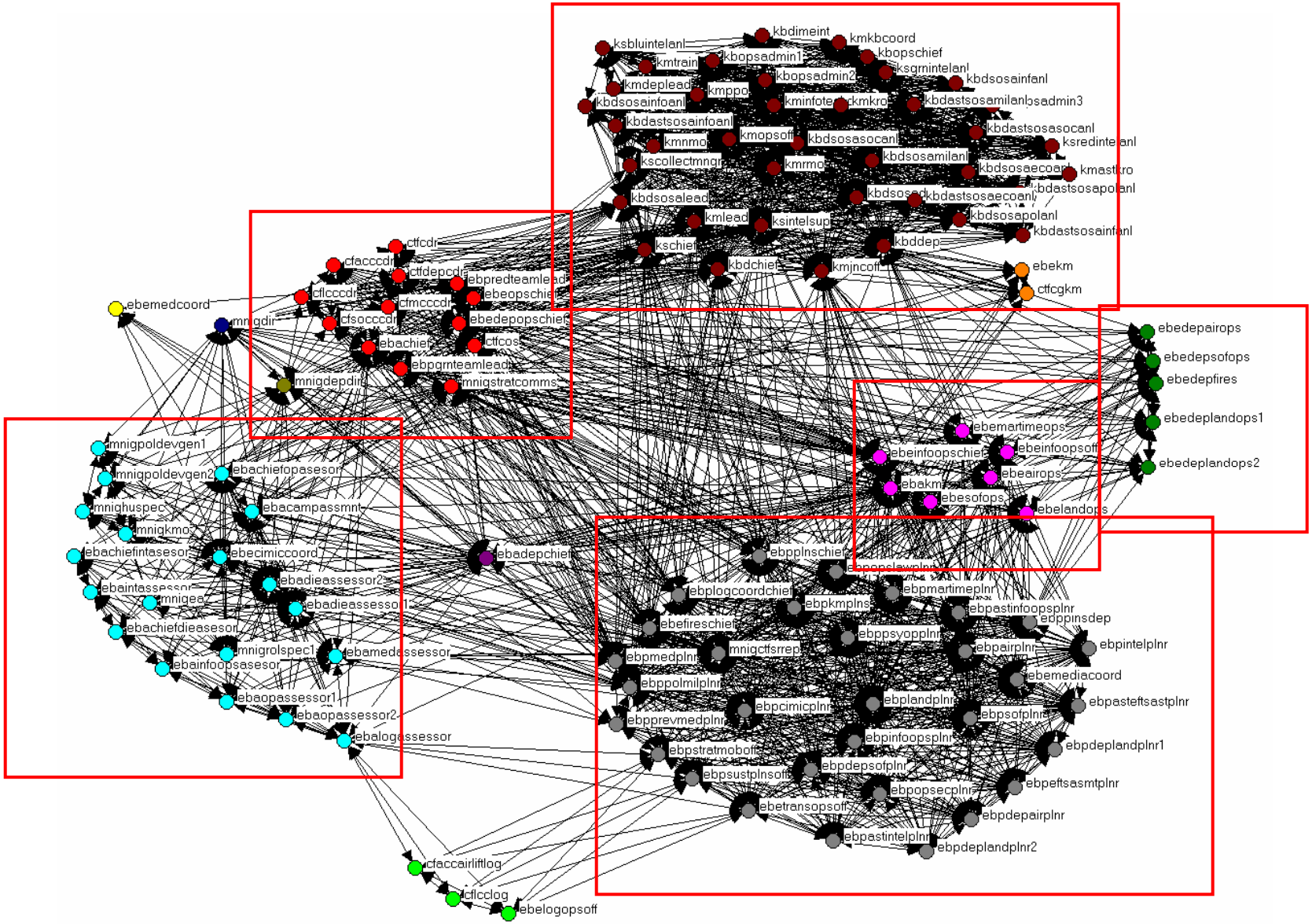

Figure 6. Analysis of subgroups in the expected meeting attendance network structure based on a classification of *k-cores* to which players belonged

Figure 7. A tree-map of the results of Johnson's hierarchical clustering procedure applied to the IWS Week 3 data: the diagram shows staff (by logon) clustered by amount of time spent virtually co-located.

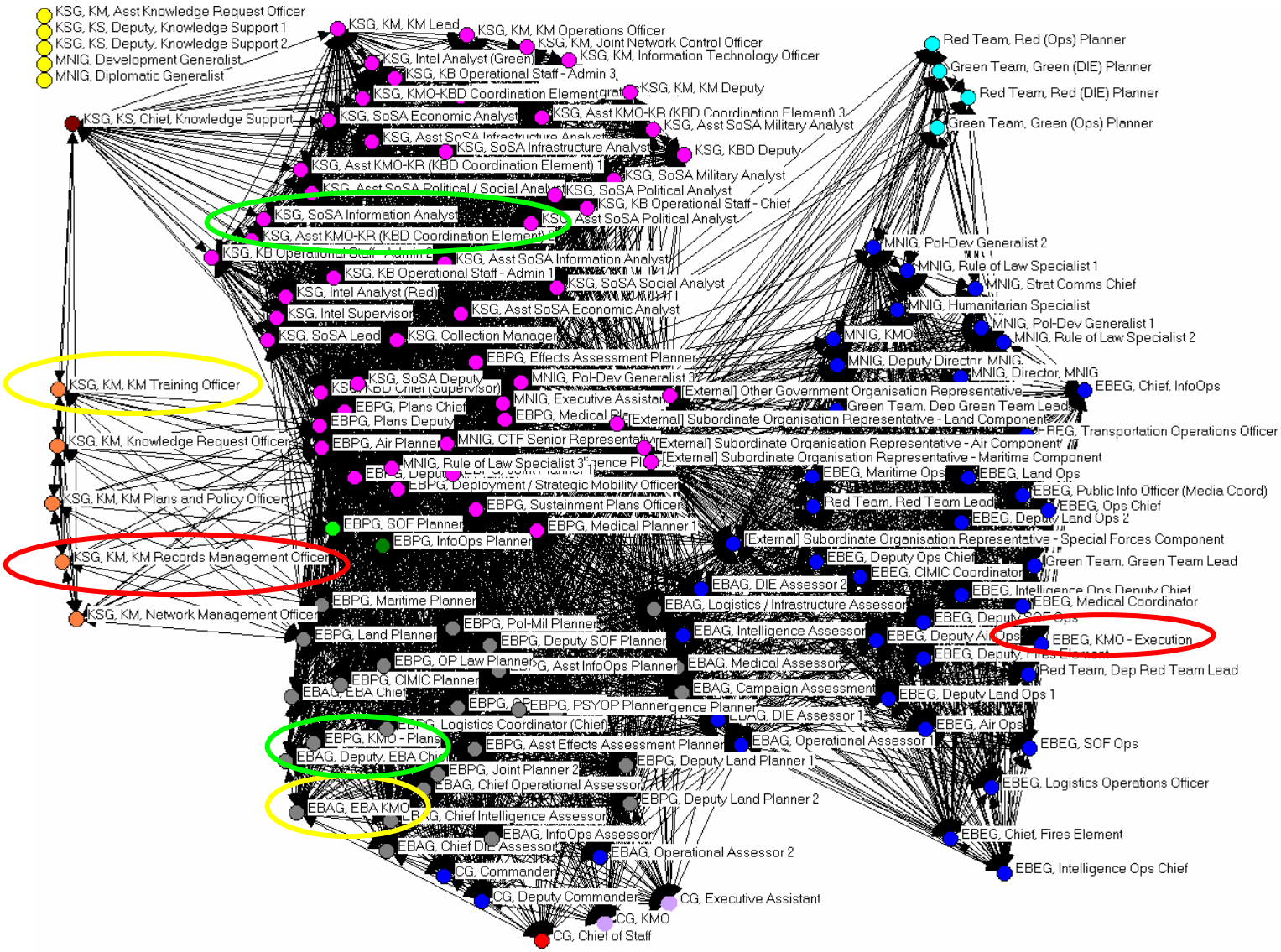

Figure 8. Expected interactions based on participation in the EBO process steps showing no pre-defined requirement for direct co-ordination between the KM Training Officer and the EBA Knowledge Management Officer (coloured yellow); the KM Assistant Knowledge Request Officer.

WEEK 1							
	CG	EBP	EBE	EBA	KS/KM	MNIG	Components
CG	0.667	0.095	0.159	0.198	0.136	0.155	0.160
EBP	0.117	0.078	0.064	0.088	0.020	0.037	0.041
EBE	0.197	0.061	0.359	0.111	0.051	0.088	0.069
EBA	0.146	0.091	0.134	0.654	0.111	0.138	0.106
KS/KM	0.110	0.042	0.054	0.114	0.230	0.034	0.010
MNIG	0.155	0.033	0.110	0.134	0.031	0.588	0.027
Components	0.123	0.045	0.065	0.100	0.008	0.019	0.189
WEEK 2							
	CG	EBP	EBE	EBA	KS/KM	MNIG	Components
CG	0.567	0.126	0.189	0.177	0.068	0.298	0.167
EBP	0.099	0.089	0.071	0.095	0.023	0.042	0.039
EBE	0.144	0.081	0.392	0.119	0.060	0.120	0.093
EBA	0.125	0.100	0.125	0.592	0.118	0.134	0.104
KS/KM	0.076	0.029	0.074	0.114	0.296	0.034	0.013
MNIG	0.250	0.041	0.120	0.143	0.029	0.863	0.028
Components	0.167	0.061	0.114	0.119	0.030	0.060	0.203
WEEK 3							
	CG	EBP	EBE	EBA	KS/KM	MNIG	Components
CG	0.833	0.180	0.265	0.271	0.129	0.357	0.210
EBP	0.180	0.095	0.086	0.108	0.033	0.077	0.058
EBE	0.212	0.097	0.463	0.148	0.058	0.097	0.106
EBA	0.177	0.110	0.145	0.658	0.121	0.165	0.108
KS/KM	0.140	0.063	0.099	0.141	0.319	0.062	0.046
MNIG	0.286	0.124	0.094	0.183	0.054	0.863	0.063
Components	0.180	0.062	0.099	0.124	0.025	0.060	0.246

Table 4. Structural blockmodel of differences in group tie density for information sharing.

WEEK 1							
	CG	EBP	EBE	EBA	KS/KM	MNIG	Components
CG	0.467	0.063	0.061	0.083	0.045	0.083	0.060
EBP	0.086	0.051	0.026	0.019	0.014	0.017	0.022
EBE	0.167	0.052	0.271	0.063	0.038	0.091	0.054
EBA	0.229	0.084	0.102	0.521	0.097	0.134	0.086
KS/KM	0.110	0.028	0.032	0.036	0.208	0.026	0.003
MNIG	0.381	0.031	0.039	0.054	0.013	0.549	0.019
Components	0.153	0.032	0.050	0.038	0.012	0.033	0.157
WEEK 2							
	CG	EBP	EBE	EBA	KS/KM	MNIG	Components
CG	0.600	0.086	0.129	0.115	0.053	0.190	0.105
EBP	0.081	0.068	0.041	0.020	0.014	0.031	0.033
EBE	0.348	0.140	0.392	0.153	0.099	0.198	0.119
EBA	0.219	0.100	0.122	0.575	0.101	0.161	0.107
KS/KM	0.148	0.036	0.055	0.065	0.242	0.055	0.013
MNIG	0.405	0.050	0.058	0.080	0.018	0.698	0.024
Components	0.242	0.055	0.075	0.063	0.018	0.049	0.204
WEEK 3							
	CG	EBP	EBE	EBA	KS/KM	MNIG	Components
CG	0.850	0.130	0.155	0.122	0.064	0.171	0.104
EBP	0.135	0.061	0.041	0.022	0.018	0.044	0.030
EBE	0.391	0.079	0.370	0.063	0.043	0.091	0.075
EBA	0.275	0.105	0.119	0.521	0.092	0.152	0.101
KS/KM	0.177	0.051	0.071	0.072	0.252	0.070	0.034
MNIG	0.557	0.093	0.107	0.107	0.034	0.604	0.039
Components	0.308	0.069	0.081	0.068	0,024	0.054	0.215

Table 5. Structural blockmodels of differences in group tie density for awareness of roles & responsibilities