CONNECTIONS 24(3): 93-103 http://www.sfu.ca/~insna/Connections-Web/Volume24-3/Dekker.web.pdf

Applying Social Network Analysis Concepts to Military C4ISR Architectures[1]

Anthony Dekker[2]
DSTO C3 Research Centre, Fernhill Park
Department of Defence, Canberra, ACT Australia

We discuss the application of Social Network Analysis concepts to military C4ISR (Command, Control, Communications, Computers and Intelligence, Surveillance, & Reconnaissance) architectures. In particular, we describe what we call the FINC methodology, which calculates a number of simple metrics for comparing and quantifying organisational network aspects of C4ISR architectures. This facilitates a more complete evaluation of the costs and benefits of various organisational structures. We have constructed a Java-based tool called CAVALIER, to carry out this and other forms of Social Network Analysis. After outlining the methodology, we apply it to a case study relating to a (hypothetical) military-led humanitarian assistance mission.

INTRODUCTION

Decoding "Milspeak:" What are C4ISR Architectures?

The term C4ISR architecture[3] is used by the US and other militaries to refer to the organisational structure used by military forces in carrying out a mission. Such a mission need not involve traditional warfare: increasingly military forces are involved in operations other than war, such as peacekeeping, humanitarian relief, flood control, etc. The key aspect of C4ISR is command (authority and responsibility) and control (exercising authority over subordinates). These two indivisible aspects of leadership are referred to as C2. Since communications and computer technology are important in carrying out these leadership functions in a large organisation, the acronyms C3 and C4 are used to include these facilities.

[1] The author is indebted to Jon Rigter, Moira Chin, Gina Kingston, and Pin Chen for many useful discussions on C4ISR architectures, and to two anonymous referees for comments on the paper.

[2] dekker@ACM.org

[3] C4ISR Architecture Working Group, US Department of Defense. *C4ISR Architecture Framework Version 2.0*.

Since leadership cannot be carried out without information of some kind, the acronyms C3I and C4I are used to include intelligence. It must be emphasised that this does not refer to the movie-inspired image of men in trench coats licensed to kill: it simply means the collection of information of every kind, increasingly from publicly available sources such as reference books, the Internet, and television news. The acronym C4ISR includes two specific sources of information: surveillance (systematic observations of something) and reconnaissance (observations on a specific occasion).

Traditionally military structures have been very hierarchical, but modern innovations in communications and computer technology have made a wide range of other structures possible. At the same time, an emerging emphasis on operations other than war may require more flexible non-traditional organisational structures. In this environment, there is a need for formal techniques for the evaluation of a wide range of organisational structure options. We believe that Social Network Analysis techniques are the obvious choice for such evaluation.

SOCIAL NETWORK ANALYSIS

Social Network Analysis is an approach to analysing organisations focusing on a network-based view of the relationships between people and/or groups as the most important aspect. Going back to the 1950's, it is characterised by adopting mathematical techniques especially from graph theory (Gibbons, 1985; Krackhardt, 1994). It has applications in organisational psychology, sociology and anthropology. A good summary is found in Wasserman and Faust (1994).

Social Network Analysis provides an avenue for analysing and comparing formal and informal information flows in an organisation, as well as comparing information flows with officially defined work processes. In previous work, we have applied Social Network Analysis to military organisations in more or less standard ways (Dekker, 2000).

The first goal of Social Network Analysis is to visualise relationships between people and/or groups by means of diagrams. The second goal is to study the factors which influence relationships (for example the age, cultural background, and previous training of the people involved) and also to study the correlations between relationships. The third goal is to draw out implications of the relational data, including bottlenecks where multiple information flows funnel through one person or section (slowing down work processes), situations where information flows does not match formal group structure, and individuals who carry out key roles that may not be formally recognised by the organisation. The fourth and most important goal of Social Network Analysis is to make recommendations to improve communication and workflow in an organisation, and (in military terms) to speed up what is commonly known as the observe-orient-decide-act loop or decision cycle (Allard, 1996).

In this paper, we extend traditional Social Network Analysis to the specific area of C4ISR architectures by introducing a specific methodology for evaluating and comparing organisational structures which we call FINC (Force, Intelligence, Networking and C2). This methodology combines Social Network Analysis techniques with military thinking about organisational structure. After outlining the methodology, we apply it to a case study relating to a (hypothetical) military-led humanitarian assistance mission.

THE FINC (FORCE, INTELLIGENCE, NETWORKING AND C2) METHODOLOGY

We will illustrate the FINC methodology using the simple and relatively traditional military structure shown in Figure 1 (the figure is produced by our Java-based CAVALIER tool). In this example, two brigade-level units (BDE 1 and BDE 2) are controlled by a divisional-level headquarters (DIV HQ),

which in turn is controlled by a joint headquarters (JNT HQ) which also controls strategic intelligence and air assets. We provide this example structure purely in order to describe the methodology, and are not suggesting that it is appropriate for any specific purpose. In the second part of this paper we provide an application of the methodology to a less traditional and more realistic structure for a military-led humanitarian assistance mission.

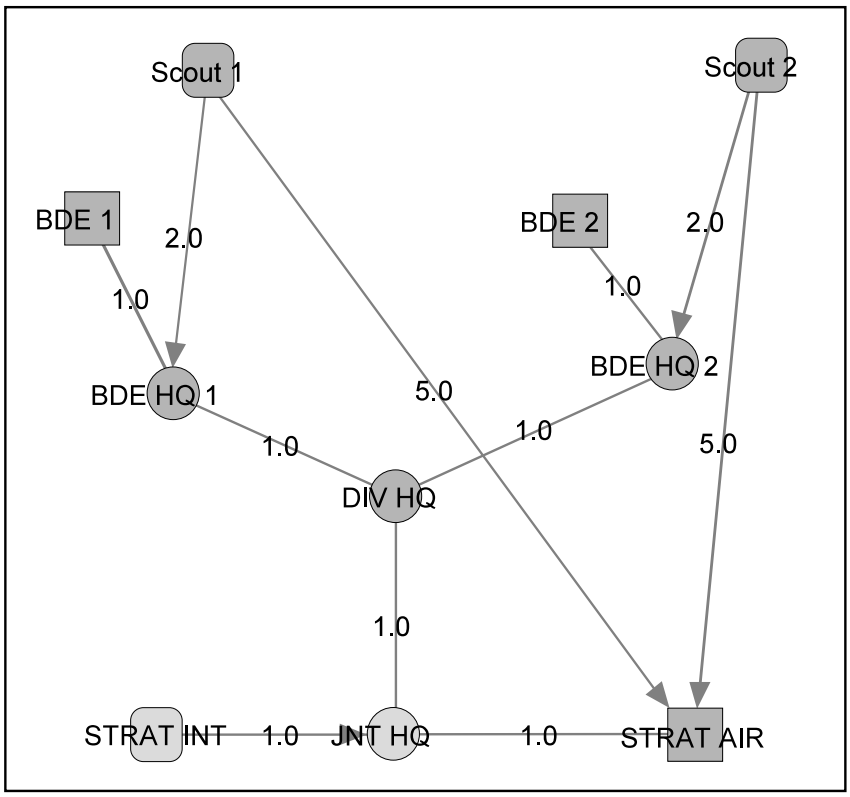

Figure 1. A Simple Military Organisational Structure

The FINC methodology analyses an organisational structure relatively simply in terms of force (assets which carry out any kind of military task, indicated by square boxes in Figure 1), intelligence (assets which collect any kind of information, indicated by rounded boxes in Figure 1), networking (which provides communication between assets, indicated by lines or arrows in Figure 1, depending on whether information flow is unidirectional or bidirectional), and C2 (command and control or decision-making, indicated by circles in Figure 1). The force and intelligence assets are often themselves organisations that can be subdivided in a similar way, if necessary.

Essentially, the FINC methodology models an organisation as an information-processing structure, together with the interactions between the organisation and its environment. The organisation receives information from its environment (intelligence), makes decisions, and produces some effect on its environment (force). In this way, it resembles a model of a biological organism. Ultimately, the performance of an organisation (or an organism) depends on the appropriateness of its response to its environment.

Our methodology need not of course be restricted to military organisations. For ordinary commercial organisations, the force assets include the sales force and business units; intelligence assets include research and development, market research, and recorded sales figures; and C2 assets include management and decision-makers.

Force and intelligence assets are associated with a particular area of operations, which for simplicity is assumed to be approximately circular. In Figure 1 these assets are:

Scout unit 1 (Intelligence), radius = 100 (in arbitrary units)
Scout unit 2 (Intelligence), radius = 100
Brigade BDE 1 (Force), radius = 100
Brigade BDE 2 (Force), radius = 100
Strategic air (STRAT AIR) assets (Force), radius = 400
Strategic intelligence (STRAT INT) assets (Intelligence) radius = 400

In cases where the areas of operation for intelligence and force assets overlap, there is benefit in providing a flow of information from the intelligence asset to the force asset. In Figure 1, candidate information flows are:

Scout unit 1 to Brigade BDE 1
Scout unit 2 to Brigade BDE 2
Strategic intelligence (STRAT INT) to Brigade BDE 1
Strategic intelligence (STRAT INT) to Brigade BDE 2

Scout unit 1 to Strategic air (STRAT AIR)
Scout unit 2 to Strategic air (STRAT AIR)
Strategic intelligence (STRAT INT) to Strategic air (STRAT AIR)

Different intelligence assets differ in the quality of information they provide. Although such differences can be quite complex, for simplicity we model this using a numerical quality score for various modes or bands. Given two intelligence assets in the same band, we prefer the highest quality information, while two intelligence assets in different bands are assumed to be complementary. If a single asset produces different kinds of information, we simply model it as multiple co-located assets. For Figure 1, quality (in arbitrary units) is taken to be:

Scout unit 1 (Intelligence), quality = 0.5
Scout unit 2 (Intelligence), quality = 0.5
Strategic intelligence (STRAT INT) assets (Intelligence) quality = 0.2

In other words, the strategic intelligence assets in this example provide information which overlaps with the information provided by scout units, and which is lower-quality but available over a wider area (we emphasise that this example is not realistic, and is provided merely to illustrate the methodology). The issue of how actual sensor characteristics are translated to numerical quality scores is outside the scope of the present paper.

Each communication link in the network has varying reliability and bandwidth characteristics which for simplicity we model as an average delay in transferring information across the link. Delays (in arbitrary units) are indicated on the links in Figure 1. Again, the issue of how actual bandwidth and reliability characteristics are translated to numerical delay scores is outside the scope of this paper.

Each C2 node in the architecture processes intelligence information and passes it on (as well as many other C2 functions). This introduces an additional delay factor which is added to the delay factor for communication links. In Figure 1, all delays for C2 nodes are assumed to be 1.0 (in the same in arbitrary units as for links).

Our model does not consider cognitive factors in the ability of C2 nodes to process and correlate information. Approaches similar to TASCCS (Verhagen, and Masuch, 1994) or ACTS (Carley and Prietula, 1994) would be required to examine this; we intend to include such modelling in future work.

The FINC methodology uses the information in this model to conduct three kinds of analysis: delay analysis, centrality analysis, and intelligence analysis.

DELAY ANALYSIS 1: THE INFORMATION FLOW COEFFICIENT

In delay analysis, we consider the combined delay (i.e. the combination of communication delays and C2 delays) for each candidate information flow. Where multiple communication paths exist, we take the one with the shortest delay. For Figure 1, the delays for the candidate information flows are:

Scout unit 1 to Brigade BDE 1, delay = 2.0 + 1.0 + 1.0 = 4.0
Scout unit 2 to Brigade BDE 2, delay = 2.0 + 1.0 + 1.0 = 4.0
Strategic intelligence (STRAT INT) to Brigade BDE 1, delay = 7.0
Strategic intelligence (STRAT INT) to Brigade BDE 2, delay = 7.0

Scout unit 1 to Strategic air (STRAT AIR), delay = 5.0
Scout unit 2 to Strategic air (STRAT AIR), delay = 5.0
Strategic intelligence (STRAT INT) to Strategic air (STRAT AIR), delay = 3.0

The first metric we use for assessing C4ISR architectures is simply the average of these delay values, which we call the information flow coefficient. It provides a measure of how effectively the military organisation can mobilise information to carry out a task. For the example in Figure 1, this coefficient is 5.0. For this metric, low values are desirable.

The information flow coefficient provides one simple way of assessing changes to to the military structure. For example, eliminating the direct links between scout units and strategic air assets in Figure 1 reduces the effectiveness of information flow, and increases the information flow coefficient to 5.86. Conversely, reducing the delay on those direct links from 5 to 3 improves the effectiveness of information flow, and will decrease the information flow coefficient to 4.43.

DELAY ANALYSIS 2: THE COORDINATION COEFFICIENT

The second metric we use for assessing C4ISR architectures is the coordination coefficient. It provides a measure of how effectively the military organisation can coordinate activities. This metric is calculated by averaging the delays along paths connecting force assets. For the example in Figure 1, these paths are:

Brigade BDE 1 to Brigade BDE 2 and vice versa, delay = 7.0
Brigade BDE 1 to Strategic air (STRAT AIR) and vice versa, delay = 7.0
Brigade BDE 2 to Strategic air (STRAT AIR) and vice versa, delay = 7.0

Consequently, the coordination coefficient is 7.0. For this metric, low values are also desirable.

CENTRALITY ANALYSIS

In centrality analysis, we try to identify the most "central" node in the architecture, which provides some indication of the "centre of gravity" (von Clausewitz, 1997) of the structure. Centrality is a traditional idea in Social Network Analysis, and there are several possible definitions of the concept (Wasserman and Faust, 1994), but a suitable definition for the degree of centrality of node *i* in a network where there is a concept of varying "distance" or "strength" of links is:

$$(\text{AVERAGE}_{j \neq i} \{1 / \text{delay}(i, j)\} + \text{AVERAGE}_{j \neq i} \{1 / \text{delay}(j, i)\}) / 2$$

i.e. the centrality score for a particular node is the sum of inverse distances to all the other nodes — the most central node is the one that he is "closest" to everything else.

For the network in Figure 1, the most central node is the divisional headquarters (DIV HQ), while the second most central node is the joint headquarters (JNT HQ). This provides an indication that the architecture in Figure 1 is indeed an army-focused rather than a joint-focused structure.

INTELLIGENCE ANALYSIS: THE INTELLIGENCE COEFFICIENT

Our third form of analysis measures the degree to which intelligence is used. For each candidate information flow from an intelligence asset to a force asset, we estimate the effective intelligence quality to be the intelligence quality discussed above divided by the delay factor for the path. This is a somewhat crude calculation, since some information retains its value even after considerable time has passed, while other information becomes useless almost immediately. However, this calculation provides a simple approximation to the way that information loses value over time.

For Figure 1, we calculate as follows:

Scout unit 1 to Brigade BDE 1, delay =4.0, quality = 0.5, effective quality = 0.125
Scout unit 2 to Brigade BDE 2, delay = 4.0, quality = 0.5, effective quality = 0.125
Strategic intelligence (STRAT INT) to Brigade BDE 1, delay = 7.0, quality = 0.2, effective quality = 0.029
Strategic intelligence (STRAT INT) to Brigade BDE 2, delay = 7.0, quality = 0.2, effective quality = 0.029

Scout unit 1 to Strategic air (STRAT AIR), delay = 5.0, quality = 0.5, effective quality = 0.1
Scout unit 2 to Strategic air (STRAT AIR), delay = 5.0, quality = 0.5, effective quality = 0.1
Strategic intelligence (STRAT INT) to Strategic air (STRAT AIR), delay = 3.0, quality = 0.2, effective quality = 0.067

These calculations are repeated for each intelligence band or mode.

For each force asset and intelligence band, we calculate an intelligence volume which is the product of effective intelligence quality and relative area (within the area of operations of the force asset) covered by the intelligence asset. In cases where the areas of operations of intelligence and force assets only partially overlap, we assume that there is sufficient flexibility of position to make this overlap total when needed.

For example, for the strategic air (STRAT AIR) asset in Figure 1, strategic intelligence covers the entire area of operations (radius = 400) with effective intelligence quality = 0.067, while the two scout units cover smaller areas (radius = 100) with slightly higher effective intelligence quality = 0.1 of the same kind of information. Figure 2 illustrates this:

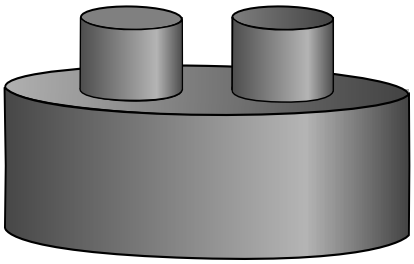

Figure 2. Intelligence Volume for Strategic Air Asset

In this diagram, the intelligence assets relevant to STRAT AIR are indicated by grey cylinders. The area of each cylinder indicates the physical area covered by the intelligence asset. The height of each cylinder indicates the corresponding effective intelligence quality, so that the two cylinders representing scout units stand out above the slightly lower effective intelligence quality of the strategic intelligence (STRAT INT) asset. The intelligence volume for the strategic air asset is simply the total

volume of the combined shape (divided by pi for simplicity):

intelligence volume for STRAT AIR
= 0.067 * 400 * 400 + (0.1 - 0.067) * 100 * 100 + (0.1 - 0.067) * 100 * 100
= 10720 + 330 + 330
= 11380

The intelligence volume for each brigade ignores strategic intelligence assets, since for this example we assume that the scout units provide exactly the same kind of intelligence and they have a higher effective intelligence quality of 0.125:

intelligence volume for BDE 1 or BDE 2
= 0.125 * 100 * 100
= 1250

The intelligence coefficient of the architecture is simply the total of the intelligence volumes for each force asset and intelligence band. For Figure 1 this is 11380 + 1250 + 1250 = 13800, approximately. For this metric, large values are desirable.

The intelligence coefficient can be improved either by improving the quality of individual intelligence assets, decreasing the delay on communication paths, or by adding intelligence assets (on new bands) which complement existing assets. We believe this metric provides a reasonable way of assessing the impact of such changes.

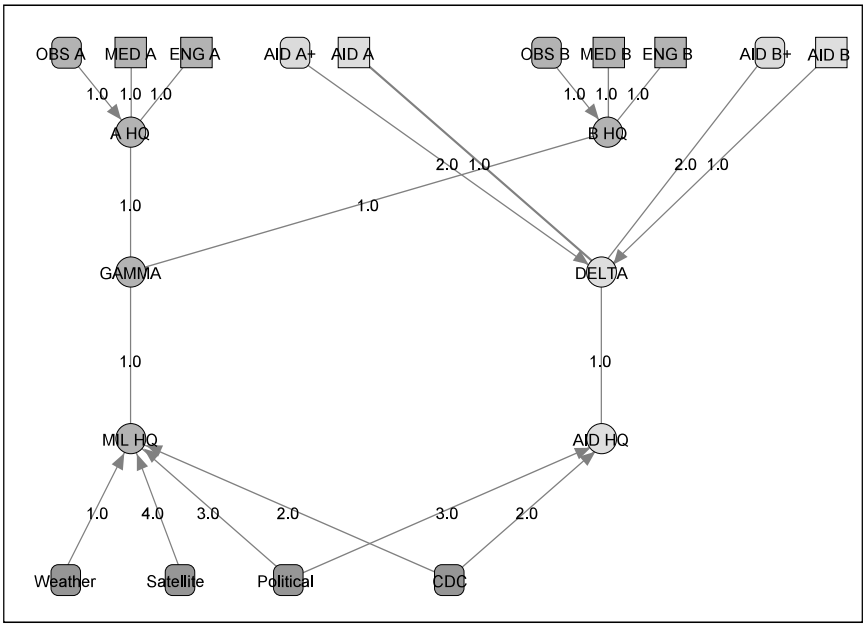

Figure 3. Flawed Architecture for Humanitarian Assistance

For example, eliminating the direct links between scout units and strategic air assets in Figure 1 not only reduces the effectiveness of information flow (as indicated by the increase of the information flow coefficient to 5.86), but it also reduces the effective intelligence quality of the scout assets as applied to strategic air assets to 0.0625, thus reducing the intelligence coefficient to 0.067 * 400 * 400 + 1250 + 1250 = 13200, approximately. Increasing the quality of strategic intelligence from 0.2 to 0.3 increases the intelligence coefficient to 18500, while adding a new strategic intelligence asset with quality = 0.1 in a different band increases the intelligence coefficient to 24100.

A HUMANITARIAN AID CASE STUDY

Having described our FINC methodology, we now turn to a practical application of it in a more realistic scenario. Figure 3 shows a C4ISR architecture for a hypothetical humanitarian assistance scenario. A volcanic eruption has occurred in the small third world country of Omega, particularly affecting the towns Alpha and Beta. A military assistance mission consisting of medical and engineering staff has been dispatched to render assistance, and an international aid agency is independently providing distribution of food and clothing.

The architecture for this mission in Figure 3 shows almost every possible design flaw. The force assets (square boxes) providing assistance here are military medical and engineering units in Alpha and Beta, and the independent aid units in Alpha and Beta. The military units are co-ordinated by small headquarters elements in the towns of Alpha and Beta, and by an intermediate headquarters in Gamma (the national capital), but are ultimately organised from a military headquarters back in the donor country. The independent aid effort, on the other hand, is co-ordinated from the mining town of Delta, which has the only suitable air strip for the agency's aeroplanes. The aid agency also ultimately organises its efforts from the donor country. There is no coordination of the military and aid efforts whatsoever.
There are five information sources (rounded boxes in Figure 3) in five different bands:

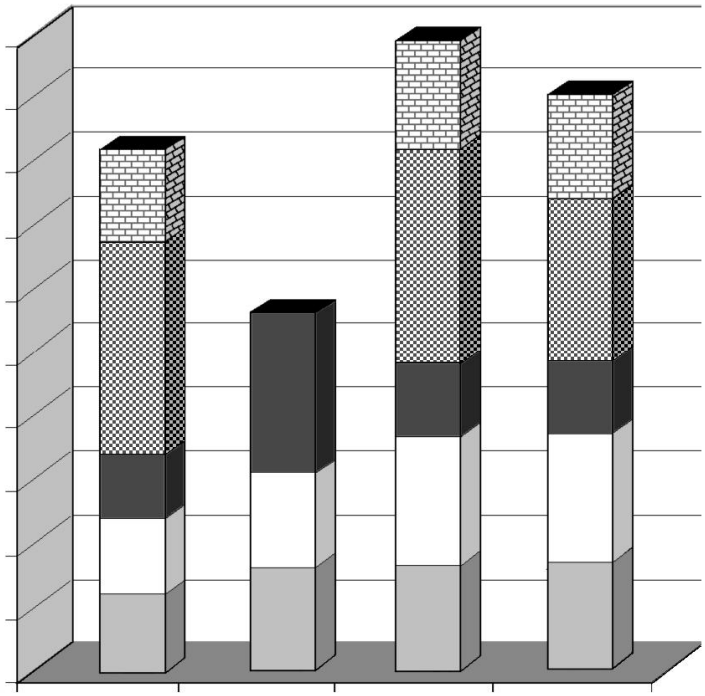

Figure 4. Comparison of Intelligence Volumes for Humanitarian Aid Architecture

1. Observers on the ground (independently for the military and aid teams). The delay factor for the aid organisation's observers is slightly greater, since they do not have a permanent presence at Alpha and Beta.
2. Weather reports provided to the military headquarters in the donor country.
3. Military satellite imagery, showing the extent of devastation in rural areas, lava temperature, etc. This is provided to the military headquarters with the substantial delay of 4, reflecting processing delays.

4. Political information about Omega's own response is provided to military and aid headquarters via the Omega embassy in the donor country (delay = 3).
5. Medical information about potential disease outbreaks is provided by the Centers for Disease Control and Prevention (CDC -- http://www.cdc.gov) in Atlanta, Georgia (delay = 2).

All information sources have quality = 1. For this architecture we have an information flow coefficient of 6.9 (reflecting the long path from information sources in the donor country to the affected areas), an infinitely large coordination coefficient (since there is no coordination between the military and aid contingents), and an intelligence coefficient of 41200.

The left-hand side of Figure 4 shows intelligence volumes for the military medical contingent (far left) and the humanitarian aid contingent (centre left). Here information in different intelligence bands is coloured:

1. GREY: medical information from CDC
2. WHITE: political information from Omega embassy
3. BLACK: satellite imagery
4. DOTTED: information from observers on the ground
5. BRICK PATTERN: weather information

The thickness of the DOTTED bands indicates higher effective intelligence quality for the military medical contingent since the observers are closer to the active units in the field.

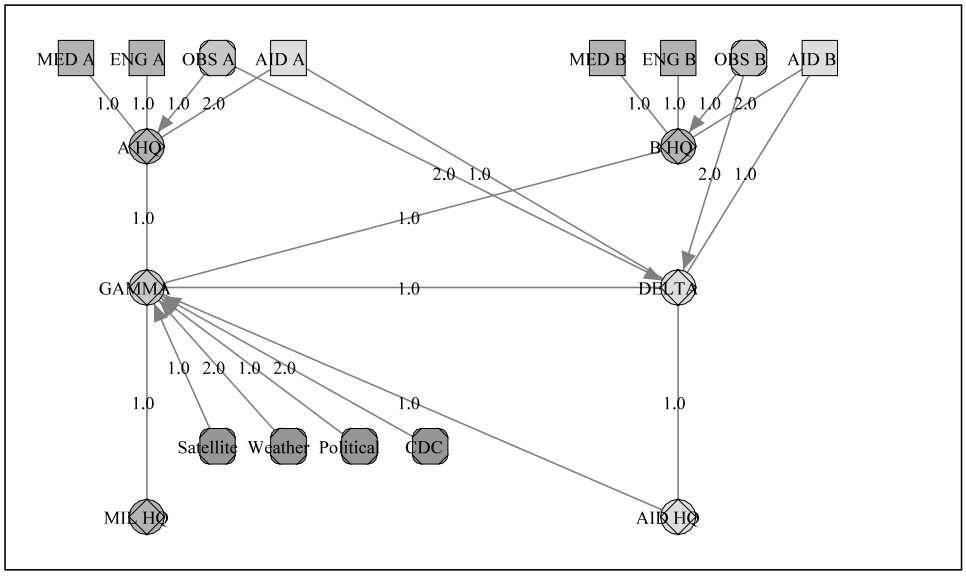

Figure 5. Improved Architecture for Humanitarian Assistance

Figure 5 shows an alternative architecture. Both military headquarters in Alpha and Beta and the aid agency air strip in Delta now receive the same reports from observers on the ground, and aid units in Alpha and Beta liaise with the military headquarters in those areas. The main coordination site is now in the national capital of Gamma, and planning is done there by military and aid staff together. This is a good choice, since Gamma was in fact the most central node in the old architecture. Staff at Gamma are in regular contact with headquarters back in the donor country and with the air strip at Delta. All information (other than reports from the field) is now provided directly to the shared headquarters at Gamma:

1. Weather reports are obtained from a neighbouring country and provided directly to the headquarters at Gamma (delay = 2).
2. Satellite imagery is now obtained from a commercial company at reduced quality (0.6) but this is more than compensated for by a substantially shorter delay (delay = 1).
3. Political information about Omega's own response is now provided directly from the Omega national government in Gamma (delay = 1).
4. Medical information about potential disease outbreaks is still obtained from CDC (delay = 2).

The substantial improvement in efficiency is reflected in our metrics, i.e. FINC analysis provides a way of quantifying the intuitive idea that this new architecture is better. The information flow coefficient is now 5.0 (28% better, i.e. lower), the coordination coefficient is now 5.4 (infinitely better, i.e. lower), and the intelligence coefficient is now 54200 (32% better, i.e. higher)

The right-hand side of Figure 4 shows the new intelligence volumes for the military medical contingent (centre right) and the independent aid contingent (far right). These have improved by 22% for military medical and 61% for independent aid. Military medical still has a slightly higher score than independent aid since the permanent establishments on the ground provides better access to observer reports (reflected by the thicker dotted band).

DISCUSSION

We can see that the FINC methodology provides a way of quantifying the benefits of the second architecture in Figure 5. Naturally, there may be costs associated with both architectures (particularly relating to communication across cultural barriers), and so the methodology does not prove that the second architecture is the best, but by quantifying the benefits it provides a clear starting point for discussions of cost/benefit tradeoffs.

In related work (Dekker, 2001), we demonstrate the utility of the FINC methodology in predicting organisational performance in a simple simulation scenario.

CONCLUSION

We have presented a methodology for evaluating and comparing organisational structures which we call FINC (Force, Intelligence, Networking and C2). This methodology combines Social Network Analysis techniques with military thinking about organisational structure, and provides three kinds of analysis: delay analysis, centrality analysis, and intelligence analysis. We have constructed a Java-based tool called CAVALIER for carrying out this and other forms of Social Network Analysis.

We have illustrated the FINC methodology with a case study involving humanitarian relief in conjunction with a non-government aid organisation. The FINC methodology provides a way of evaluating the efficiency of organisational structures for military (and also non-military) organisations, particularly in relation to the flexible structures required when military forces carry out non-traditional activities.

REFERENCES

Alberts, D.S., J.J. Garstka and F.P. Stein. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd ed.* US Department of Defense C4ISR Cooperative Research Program Publications Series. Available electronically at: http://www.dodccrp.org/Publications/pdf/ ncw_2nd.pdf

Allard, K. 1996. *Command, Control, and the Common Defense*, rev. ed. Washington: National Defense University.

C4ISR Architecture Working Group, US Department of Defense. *C4ISR Architecture Framework Version 2.0.*

Carley, K.M. and M.J. Prietula. 1994. ACTS Theory: Extending the Model of Bounded Rationality. In *Computational Organization Theory*, K.M. Carley and M.J. Prietula, eds., 55-87. Hillsdale, NJ: Lawrence Erlbaum Associates.

Dekker, A.H. 2001. *C4ISR Architectures, Social Network Analysis and the FINC Methodology: An Experiment in Military Organisational Structure.* Internal report, available as HTML at: http://www.acm.org/~dekker/FINCX/

Dekker, A.H. 2000. Social Network Analysis in Military Headquarters using CAVALIER, in *Proceedings of 5th International Command and Control Research and Technology Symposium*, Australian War Memorial, Canberra ACT, Australia, 24-26 October 2000. See also: http://www.dodccrp.org/2000ICCRTS/cd/papers/Track6/039.pdf and http://www.dodccrp.org/2000ICCRTS/cd/index.htm

Gibbons, A. 1985. *Algorithmic Graph Theory*. Cambridge University Press,

Krackhardt, D. 1994. Graph Theoretical Dimensions of Informal Organizations. In *Computational Organization Theory*, K.M. Carley and M.J. Prietula, eds., 89-111. Hillsdale, NJ: Lawrence Erlbaum Associates.

Verhagen, H. and M. Masuch. 1994. TASCCS: A Synthesis of Double-AISS and Plural-Soar. In *Computational Organization Theory*, K.M. Carley and M.J. Prietula, eds., 39-54. Hillsdale, NJ: Lawrence Erlbaum Associates.

von Clausewitz, C. 1997. (translated by J. J. Graham and F. N. Maude). *On War*. Wordsworth. See also: http://www.clausewitz.com/CWZHOME/On_War/ONWARTOC.html

Wasserman, S. and K. Faust. 1994. *Social Network Analysis: Methods and Applications*. Cambridge University Press.