Command and control in emergency services operations: A social network analysis

ROBERT J. HOUGHTON[1], CHRIS BABER[1], RICHARD McMASTER[1], NEVILLE A. STANTON[2] , PAUL SALMON[2], REBECCA STEWART[3] and GUY WALKER[2]

[1] Human Factors Integration Defence Technology Centre,
Electrical, Electronic and Computer Engineering, The University of Birmingham, UK.

[2] Human Factors Integration Defence Technology Centre,
School of Engineering and Design, Brunel University, UK.

[3] Human Factors Integration Defence Technology Centre,
Department of Human Factors, Cranfield University, UK.

Contact person:
Dr Robert J. Houghton
Electrical, Electronic and Computer Engineering
School of Engineering
The University of Birmingham
Edgbaston
Birmingham, B15 2TT, UK

Phone: +44 0121 4142934
Fax: +44 0121 4144291
Email: R.J.Houghton@bham.ac.uk

There is increasing interest in the use of social network analysis as a tool to study the performance of teams and organisations. In this paper processes of command and control in the emergency services are explored from the perspective of social network theory. We report network analyses based on the observation of six emergency service incidents comprising of three Fire service operations involving the treatment of hazardous chemicals and three Police operations involving immediate response to emergency calls. Finally, the findings are discussed in terms of our attempts to categorise the networks in terms of their structure and the relationship between those structures and the qualities those networks display in the context of the incidents reported. We suggest that social network analysis may have a valuable part to play in the general study of command and control.

Keywords: Emergency response, Command and control, Social networks, Teams

1. Introduction

There is increasing interest in examining organisations and teams in terms of their underlying social networks (e.g., Kilduf and Tsai, 2003). Social networks plot the relationships and/or flow of communications between individuals, groups, computers and other information processing entities as connections (edges) between entities (nodes). The exercise of plotting social networks based upon observations can reveal information about the manner in which work or operations are performed that might not be obvious from the consultation of standard operating procedures and doctrine. Indeed, social network analysis of field studies can be used to assess the divergence of practice from the theory. In the present paper we describe observations of six emergency service incidents (three for Police, three for the Fire service) and on the basis of these observations describe and discuss the form that the social networks took in each of these incidents. We place a particular emphasis on attempting to classify these networks of command and control in terms of archetypes and ask whether these classifications can aid the understanding of what went on in these incidents and ultimately whether a system of command and control network classification can aid in the prediction of team performance.

1.1 Social network analysis

Social network theory is widely used across myriad disciplines; it can be used as a tool to investigate organisations, decision making, the spread of information, the spread of

disease, mental health support systems and so on (see Wasserman and Faust, 1994). In recent years, the discipline of social network analysis has become based very much in empiricism and mathematics; contemporary social network analysis techniques would not exist had Graph Theory not undergone rapid development as a mathematic field in the 1970s. Whilst, at its simplest a social network graph will depict nodes linked by connecting lines giving an immediate (qualitative) overview of the network in question the fact that a network can be represented mathematically as a matrix of values, means that quantitative metrics and algorithms can be applied to the data. These mathematical approaches mean that we can define a network in terms of 'headline' figures. Most recently there has been a great deal of enthusiasm for the using the techniques of social network analysis (SNA) to study the Internet and connections between both web pages and Internet users (e.g., see Adamic, Buyukkoten and Adar, 2003). In terms of studying the architectures encountered in command and control networks (both designed and formed ad hoc) SNA would appear to be the logical choice of analysis tool.

Early social network investigations led to defining specific types of network structure; Leavitt (1951) identified the circle, chain, Y and wheel/star (see Figure 1).

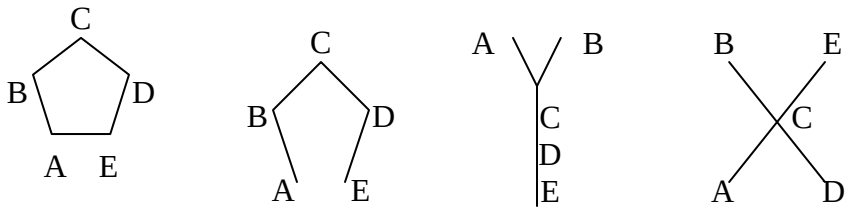

Figure 1: Examples of simple network structures: circle, chain, Y and wheel (star).

In these early studies, Leavitt (1951) demonstrated that group performance, on a simple problem-solving task, was superior under the wheel/star network and worse under the circle network. In this case, collating information via a single source (C in the wheel/star network) would help the group to arrive at the correct answer. However, as the volume of information and the general task complexity increase, so the central figure in the wheel/star network is likely to become overwhelmed with information and performance is more likely to be superior to the decentralised networks, such as the circle (Shaw, 1964). The implication of this early research was that there is unlikely to be a single 'best' structure of network for group performance; rather the structure of the network interacts with the loading on members of the group, the communication channels available to them, the complexity of information and decision-making required of the group, time-pressure and a host of other factors. Having said this, the early work demonstrated that it was possible to systematically study the performance of groups through qualitative analysis of network structure.

1.1.1. Calculating social network metrics. There is a wide range of social network metrics that can be calculated and the selection of approach is dependent primarily on then nature of the data at hand and the aims of analyst (see Wasserman and Faust, 1994). In this paper we restrict ourselves to two relatively simple metrics, namely Sociometric status and Centrality. Sociometric status in essence is a measure of the "connectivity" of a node (the inputs and outputs) relative to the overall size of the number of nodes in the network (see Equation 1; g is the total number of nodes in the network, i and j are individual nodes).

$$Status = \frac{1}{g-1}\sum_{j-1}^{g}\left(x_{ji} + x_{ij}\right)$$ Equation 1.

In practical terms then Sociometric status gives an indication of the relative prominence an individual agent has a communicator with others in the network. Similarly, Centrality is also a metric of the standing a node within a network, but this is in terms of its geodesic distance from all other nodes in the network. That is to say, a 'central' node is one that is relatively close to all other nodes in the network and a message conveyed from that node to an arbitrarily selected other node in the network would, on average, arrive via the least number of relaying hops. We used this Bavelas-Leavitt algorithm to calculate centrality, which is given in Equation 2 (where g is the size of the network and δ_{ji} is the geodesic distance from node i to node j).

$$BLCentrality = \frac{\sum_{i-1;j-1}^{g}\delta_{ij}}{\sum_{j-1}^{g}\left(\delta_{ij} + \delta_{ji}\right)}$$ Equation 2.

It should be clear then that Sociometric status and Centrality indicate slightly different things. In practice the two measures may well, broadly speaking, correlate as centrality may be a product of being highly interconnected (high Sociometric status) and by the same token a high Centrality node may well be used as a hub by other nodes precisely because of its relative to closeness to other nodes. This need not necessarily be the case however: a busy node with many connections (and thus high Sociometric status) may none the less have low Centrality in the event it finds itself on the periphery of the network and its connections limited to other peripheral nodes. The reverse is also true; a node scoring highly in Centrality may achieve this through virtue of its topographical

position within the network rather than because it has particularly many connections (and thus low Sociometric status).

1.1.2. Templates derived from Dekker (2002). One approach to using SNA to assess the structure in emergency service operations is the FINC (Force, Intelligence, Networking and C2) methodology described by Anthony Dekker (Dekker, 2001; 2002). This approach considers the actions of organisations in terms of the deployment of Force, the gathering, fusion and communication of Intelligence, the extent of Networking and the number and role of Command and Control (C2) units. Obviously, because Dekker's work is rooted in the military milieu these terms are phrased in the language of adversarial combat, which belies the fact that they are transferable to the study of other command and control networks in general (like the emergency services): "Our methodology need not of course be restricted to military organizations. For ordinary commercial organizations, 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." (Dekker, 2001, p. 95). Thus for our purposes we can consider 'force assets' to be individuals or agents who act upon an incident (like an attending police officer), 'intelligence assets' to be sources of information prompting action, such as 999 operators and the Police's OASIS command and control system and 'C2 assets' individuals controlling the situation, such as a Operational Command units. Networking is simply the communication links between agents and would, in the case of emergency services, primarily amount to radio or

telephone communications. The ‘sensor to shooter’ paradigm used by Dekker has been translated, therefore, into a ‘detection-to-decision-to-action’ paradigm for our purposes.

Dekker (2002) tested the performance of different social network command structures in playing a simplified and abstracted wargame called Scud Hunt in which players allocate force and intelligence assets within a 4 x 4 board in order to ultimately hunt down and destroy hidden Scud missile launchers. On the basis of intelligence, air strikes can be called in on squares on the board. However, air strikes are not instantaneous with target detection by intelligence assets; intelligence and, in turn, orders to initiate action must be passed up and down the command structure. Thus a command structure that places many intermediary units between force, C2 and intelligence is one that is likely to be quite sluggish in response as there is a time delay encountered each time a message must be relayed. On the other hand, command structures with more intermediary units are usually thus as a result of building in a high level of connectivity. In turn this means that intelligence be pooled and thus the accuracy of that intelligence is ultimately increased.

Within this paradigm, experimental manipulations were also made by Dekker, one to vary the reliability of sensor data (thus varying the importance of fusing intelligence) and the other to vary the speed at which targets changed locations (this therefore acted as an indirect measure of tempo for the Scud Hunters; for example, a slow tempo command structure would get few if any hits against fast moving targets as it would not be able to respond quickly enough). Performance in the game is measured through the number of Scuds destroyed, the number of Scuds missed, and the number of false alarms. Whilst

Scud hunt was originally designed as a game to be played by humans in a laboratory setting, Dekker wrote a piece of software which carried out thousands of automated statistical trials in which different command network configurations repeatedly and automatically 'fought out' a game of Scud hunt. This so-called *Monte Carlo* approach to simulation allows the quantitative assessment of systems that have been represented probabilistically but are too complex (that is, have too many interacting *degrees of freedom*) for analysts to directly assess them otherwise.

1.1.3. Command structures. The following eight basic command structures were evaluated by Dekker (2002) within the Scud Hunt paradigm. These structures are summarised in Figure 2.

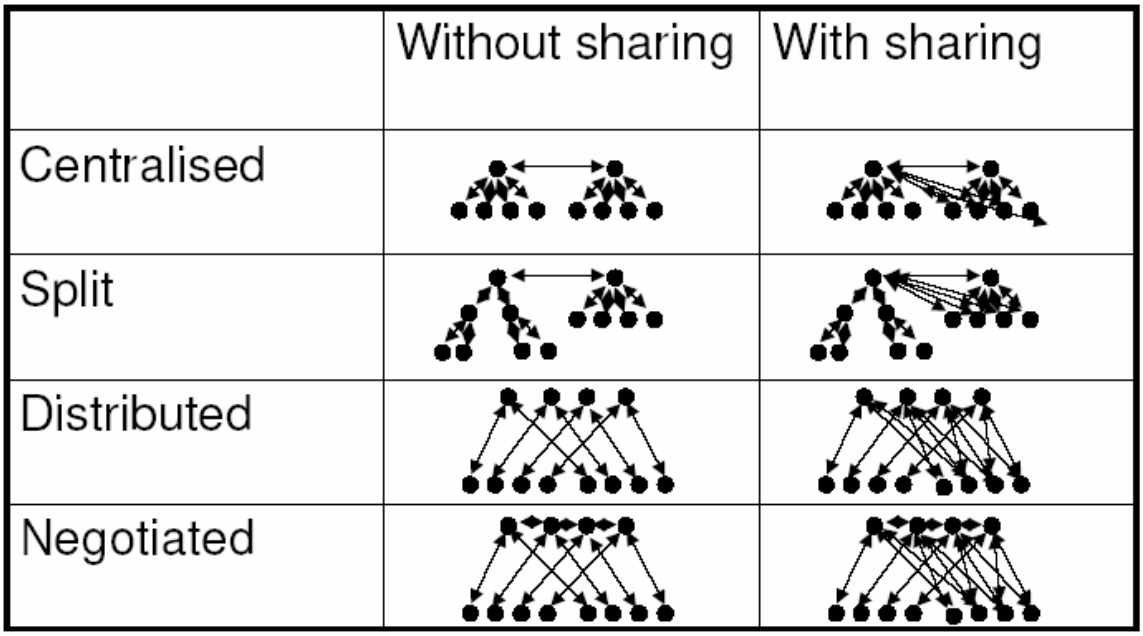

Figure 2. Dekker network architectures

1. Centralised architecture without information sharing.

Within this simple network architecture we see that intelligence data from four intelligence assets is collated by a central Intelligence HQ unit and passed on to a Strike Head Quarters (HQ) unit, which finally directs the attacks of four strike assets. This command structure is associated with the USAF (United States Air Force) who have good communications, good intelligence (from AWACS – Airborne Warning and Control System – aircraft) and can, owing to the inherent speed of jet aircraft, move force assets into position rapidly. It is a fairly hierarchical network in which subordinates answer to superordinates and there are no direct links between strike and intelligence assets; information flows via the chain of command itself.

2. Split architecture without information sharing.

This is very similar to the foregoing centralised architecture, the only modification being the addition of an intermediary layer C2 units (Wing A and Wing B) between Strike HQ and the Force asset squadrons themselves. This architecture is more common in land-based operations where benefit is derived from having local command units owing to issues like the complexity of terrain. As compared with the Centralised architecture there is a clear cost paid for this extra command layer in that it adds an extra delay between orders being issued by the HQ getting to the Force squadrons.

3. Distributed architecture without information sharing.

The distributed architecture contrasts strongly with the centralised and split forms; as can be seen in Figure 4, each Intelligence and Force asset is tied together via a single distributed HQ C2 unit. Thus there are in essence four autonomous self-contained armies

with their own intelligence and strike assets in the field. This architecture is most often found in the context of special operations where decision-making must be done rapidly with regard to small-scale actions. Alternatively, it also describes a ‘cell structure’ used by terrorists and covert intelligence operatives. The self-contained nature of the groupings means that the destruction or infiltration of the unit has its impact restricted to that unit. Clearly one disadvantage of this approach is that information is not shared outside each autonomous grouping.

4. Negotiated architecture without information sharing.

The negotiation architecture is quite similar to the distributed architecture, the only change being that now C2 HQ units can communicate with each other to share information. This ‘peer to peer’ style arrangement is commonly found with regard to emergency services (according to Dekker), as each unit will tend to cover a geographical area and work within that area whilst communicating with peers in other areas.

Architectures 5 to 8 inclusive: “…with information sharing”.

Within his original report Dekker also added four ‘information sharing’ versions of the four command structures already described wherein intelligence is disseminated from intelligence assets to all other C2 HQ units. In the case of centralised and split architectures this does not change the physical layouts of the architectures, just alters their operations by adding an extra degree of delay to processing in the intelligence HQ (in the “…without information sharing” variants it is assumed the intelligence HQ relayed in parallel four packets of intelligence data to the strike HQ; with information

sharing there is an extra time delay whilst the intelligence inputs are fused together). In this case of the distributed and negotiated architectures this means additional connections between intelligence and HQ units. These two variants represent the new paradigm of Network Enabled Capability in which intelligence is shared within a densely interconnected network of sensors and communication links.

2. Observations and analyses

We present now a set of six social networks based on data taken from Fire and Police operations. The Fire incident data was the result of observing training exercises carried out at a Fire Service training facility. The Police incidents are primarily based on observations of force control and the official logs of events held by the Police. In both cases these accounts were supplemented with interviews to ensure accuracy.

2.1. Fire service operations

The Fire Service College, located in Moreton-In-Marsh (Oxfordshire) provides a number of courses to Fire Officers of different ranks as part of the Fire Service IPDS (Integrated Personal Development System) career progression scheme (Fire Service College, 2003). One such course, “Station Managers Managing Incidents” is part of the “Station Management Development Programme”, which is aimed at Officers who have just started or will soon take on the role of Assistant Divisional Officer (ADO) (Fire Service College, 2004). The course features a number of group and individual exercises, known as Tactical Decision Exercises (TDX). These exercises are paper-based simulations of

realistic emergency incidents and are designed to develop the attendee's tactical thinking and decision-making abilities. All of the TDXs involve the participants assuming the role of an ADO who has just been called to proceed to an emergency incident that is already underway (i.e., Fire Service resources have already been despatched); ADOs are called out to emergencies to take charge of the Fire response either when there is a life risk or where the number of Fire units despatched has reached 3 or 4. Thus, the ADO will assume the role of Incident Commander. Three of these exercises have been observed, in order to develop an understanding of how the Fire Service co-ordinate their responses to emergency incidents.

2.1.1. Fire Incident #1: Chemical incident at a remote farm.

Description of the incident. The incident begins with a report of possible hazardous materials on a remote farm, and then added additional information as the incident unfolded, e.g. reports of casualties, problems with labelling on hazardous materials etc. The exercise was designed to encourage experienced fire-fighters to consider risks arising from hazardous materials and the appropriate courses of action they would need to take, e.g. in terms of protective equipment, incident management, information seeking activities etc. Three observers sat in on the exercise and recorded the discussion of the participants. The notes from the discussion were then collated into a combined timeline of the incident. This timeline, and the notes taken during the exercise, then formed the basis for subsequent analysis.

In this incident, the primary goals of the teams were: (i.) locate chemicals, (ii.) determine type of chemicals, (iii.) define appropriate response to chemicals, (iv.) provide appropriate treatment in response to exposure to chemicals. The incident can be said to represent two interlinked activities, which are the responsibility to two separate organisations. The Fire Service will take responsibility for the 'Manage Incident' goal, and will search for, identify and deal with any hazardous chemicals, while the Hospital will deal with the treatment of casualties.

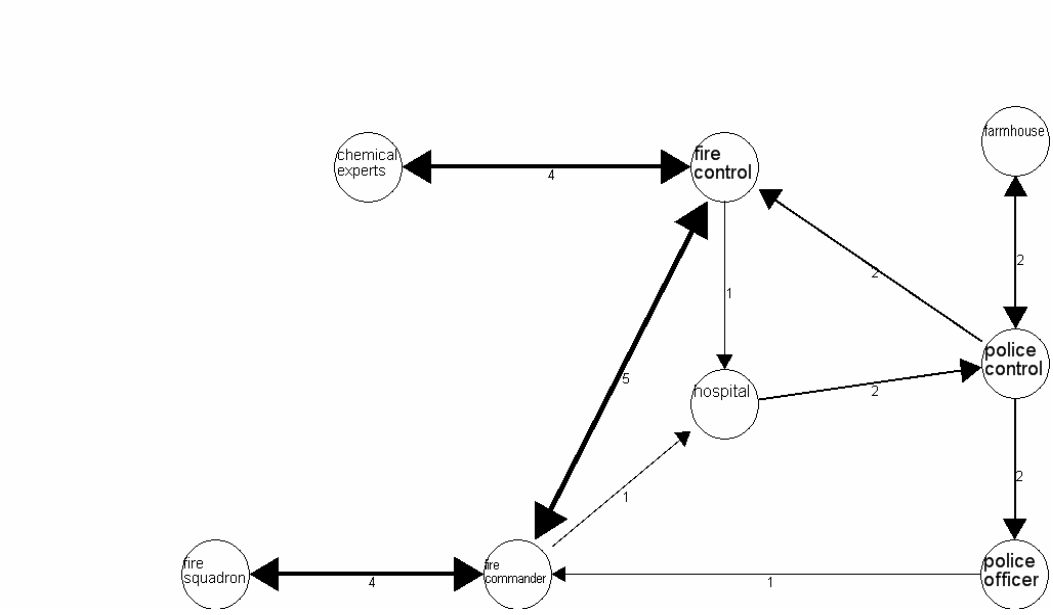

Figure 3. Social network for Fire incident #1.

Analysis. A Social Network Diagram can be created by analysing the patterns of communication between agents within the system (see Figure 3). Comparing this Figure with the template presented earlier suggests that the network represents a Distributed network. A characteristic of this type of network is that the agents tend work as part of small, self-contained units, pursuing their own procedures in order to achieve their own goals. Thus, there is minimal communication across units. Interestingly, one of the ways

in which the incident was presented involved a lag in communication from the hospital to the Fire Crew on site – the hospital did not indicate to the Fire Service that it was treating a patient with specific chemical-related injuries until well into the incident, when it requested an identification of the chemical in order to determine an appropriate course of treatment. In some circumstances, a Distributed network provides an appropriate means of responding in a flexible and adaptive manner, particularly when there is tight coupling between rapid changes in a situation and the need to respond.

Within the network, there are four nodes that appear to have a higher degree of connectivity than the others, i.e., Police Control, Fire Control, Fire Command and Hospital. In order to explore the relative importance of these agents to the network, Sociometric Status and Centrality can be calculated.

Table 1 shows the Sociometric Status for each agent in Fire Incident # 1. From the calculation, a mean status of 0.71 (± 0.38) was found. The value of mean + one standard deviation, i.e., 0.71+0.38 = 1.09, is used to define 'key' agents in this network. From Table 1, it is clear that three agents can be defined as 'key' on this definition, i.e., Police Control, Fire Control and Fire Commander (who can be characterised as the Incident Commander). This would support the previous observation that the network is Distributed, in that it points to three key agents around whom the network operates.

[1] All Social Network Analysis calculations have been performed using the Agna software tool, which can be obtained from http://www.geocities.com/imbenta/agna/

Table 1. Sociometric status of agents in Incident #1.

Agent	Status
police control	1.14
fire control	1.14
fire commander	1.14
hospital	0.86
police officer	0.57
farmhouse	0.29
fire squadron	0.29
chemical experts	0.29

Table 2 shows the Centrality (using Bavelas-Leavitt's index) for the agents in this incident. Again, a notion of 'key' agents can be defined using the mean + 1 standard deviation (i.e., 4.17+0.83 = 5). From this Table, it can be seen that Fire Control is the only agent that exceeds this measure, which indicates that it is the most central agent within this network. However, Police Control, Hospital, Fire Commander and Police Officer also have relatively high centrality scores, i.e., they are, given rounding error, not markedly lower than Fire Control. This again suggests that the network comprises several highly interconnected agents.

Table 2: Centrality in Fire Incident #1

Agent	B-L Centrality
Fire control	5.3
Police control	4.82
Hospital	4.82
Fire commander	4.82
Police officer	4.08
Chemical experts	3.31
Farmhouse	3.12
Fire squadron	3.12

2.1.2. Fire Incident #2: Road traffic accident (RTA) involving chemical tanker

Description of the incident. The incident starts with the ADO receiving a call to attend a road traffic accident involving a tanker and a car in the centre of Chipping Norton at 09:00 on a Monday morning, so there is a lot of traffic congestion of surrounding roads.

Initially the Station Officer requests more information on the emergency: the exact location, tanker details, and the status of the trapped casualty. The ADO reports having difficulty attending the incident scene as there is traffic backed up along the roads into Chipping Norton. The Station Officer (SO) in charge of the scene requests additional Fire and Ambulance resources attend the scene, then their transmission cuts out. Whilst the ADO is still en route to the incident, a report comes through from the SO that 'product' (unknown substance) is leaking from the chemical tanker. The Local Authority mobilizes the HAZMAT officer to attend the scene. Upon arrival at the scene the ADO requests and receives a briefing from the Station Officer regarding their actions to date and the current state of the situation. Some bystanders and the four BA Fire-fighters have developed burns and respiratory problems. The ADO takes charge of the incident and defines an inner cordon, giving instructions that all personnel and bystanders should be withdrawn from this area. A casualty handling area is set up (near the fire pumps and away from the crash scene) where decontamination can begin. An RV point is also set up, for the incoming Emergency Service resources. The ADO gives instructions that the media should be informed - to tell residents to remain indoors; local hospitals are warned to expect self-presenting casualties. Fire fighters trained to use Chemical Protective Clothing (CPC) are instructed to suit up and prepare to attend to the car driver and to investigate the possibility of stopping the tanker leak.

The social network diagram (Figure 4) suggests that this incident has a highly centralised network, i.e., comparable to a wheel/star in described earlier by Leavitt (1951, see Figure 1).

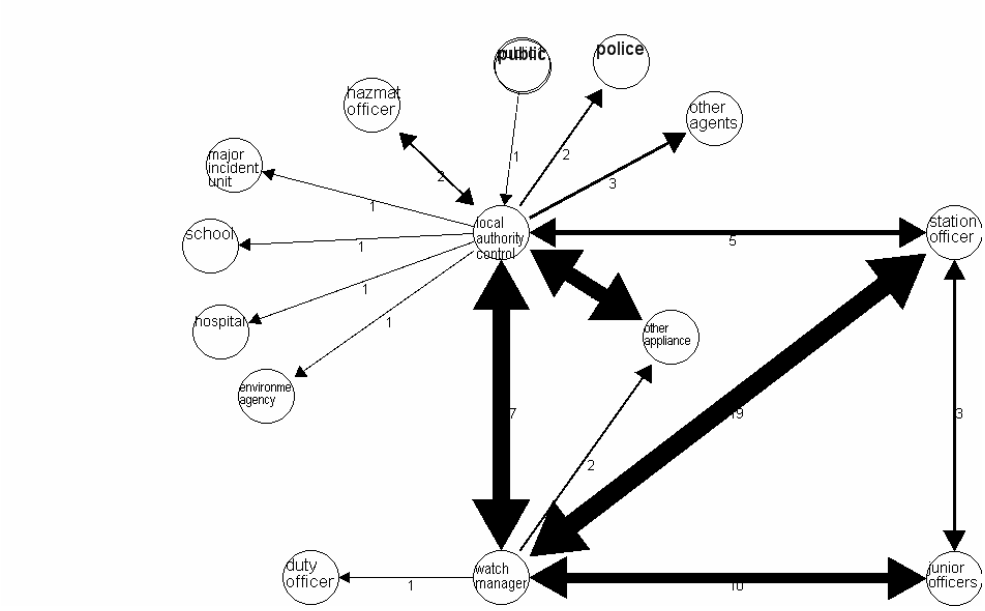

Figure 4. Social network for Fire Incident #2

In terms of Sociometric Status, key agents are defined by mean + 1 standard deviation, i.e., 0.3 + 0.38 = 0.68. Table 3 shows that Fire Control has by far the highest status (1.57), with the Watch Manager (who will assume the role of Incident Commander) being just above the defining score. Interestingly, the status of the Watch Manager increases during the phases of the incident and suggests, at the end, that there are actually two networks – one that focuses on the Fire Control and the other that focuses on the Watch Manager.

Table 3: Sociometric Status for Agents in Fire Incident #2

Agent	**Status**
Fire Control	1.57
watch manager	0.71
station officer	0.43
other appliances	0.28
junior officers	0.29
public1	0.14
police	0.14
other agents	0.14
hazmat officer	0.14
environment agency	0.14
hospital	0.14
school	0.14
major incident unit	0.14
duty officer	0.14
public	0.0

Table 4 shows the centrality scores for agents in Fire Incident #2. Using the mean + 1 standard deviation to define key agents (6.76 + 2.35 = 9.11), suggests that only Fire Control is a high score for centrality. This would suggest that Fire Control lies at the hub of the network. However, it is also very evident that watch manager has also scored highly, supporting the notion that there are two networks present, although this does require our criteria to be slightly relaxed. We feel this is acceptable on the grounds that social network metrics should always be appreciated as descriptive within their context.

Table 4: Centrality for Agents in Fire Incident #2

Agent	**B-L Centrality**
Fire Control	12.1
watch manager	8.66
station officer	7.91
other appliances	7.58
public1	6.74
police	6.74
other agents	6.74
hazmat officer	6.74
environment agency	6.74
hospital	6.74
school	6.74
major incident unit	6.74
junior officers	5.69
duty officer	5.51
public	0.0

In Fire Incident # 2, Fire Control is very clearly the central focus of the network, as it needs to coordinate activities amongst the greatest number of other units; those dealing with the incident and those potentially affected by the incident. It is also the conduit for communication between these actors. In this respect, a defining feature of the network is the traditional ‘wheel’ or ‘star’ network structure, with Fire Control lying at the hub of the majority of communications. This is not to imply that Fire Control fulfils a command role, but that it is the conduit through which agents within the network, particularly cross-agency personnel, will exchange information or communicate requests for information or action.

2.1.3. Fire Incident #3: Factory Fire

Description of incident. The ADO receiving a call to attend a fire at a manufacturing plant. The plant is located in the middle of a densely packed residential area. Three Fire trucks and two specialist units are already in attendance at the incident when the ADO arrives; the Fire Officer in charge has requested an additional 3 units, which are en route. The Officer in charge briefs the ADO on the state of the incident: the fire is in the chemical store at the industrial plant. After the briefing, the ADO takes command of the situation - their priorities are life-risk (including crew safety) and spread of the fire. The ADO orders one unit to assist with the evacuation effort (without entering the inner cordon); a holding area further down the road from the plant is established for evacuees. Attendance by the Police (to assist with the cordon) and Ambulance services (to treat any injured parties) are requested. A second crew is sent to nearby houses to tell residents to remain indoors with doors and windows closed. The ADO then withdraws all units until more information on the types of chemicals can be obtained; another officer is sent to locate the plant Manager. The ADO declares major incident status, so additional resources are despatched to the site by Fire Control. The industrial Fire Team then inform the ADO that there may be liquid Cyanide stored in the burning chemical store, possibly around 20 litres in a single drum. Smoke from the chemical store is rising over the nearby terraces. The ADO orders the withdrawal of units further and requests that a HAZMAT Officer attends the incident. The Police are informed (via Fire Control) to instruct the public to stay indoors with doors and windows shut (Police to manage public from now on). The ADO gives instructions that a decontamination area should be set up and an Officer is appointed to look at possible problems caused by contaminated water.

The fire in the chemical store deteriorates and begins to impinge on the Chemical Processing building; the chemical store itself is not saveable. The plant manager cannot be found, so there is at least one missing person.

Analysis. In Fire Incident #3, the Fire service C2 units (Fire control / Crew Chief) are central, exerting command and control over nearly all parts of the network (see Figure 5). Thus, the structure appears to be similar to that observed in Fire Incident #1. In other words, the network appears to be a Distributed type.

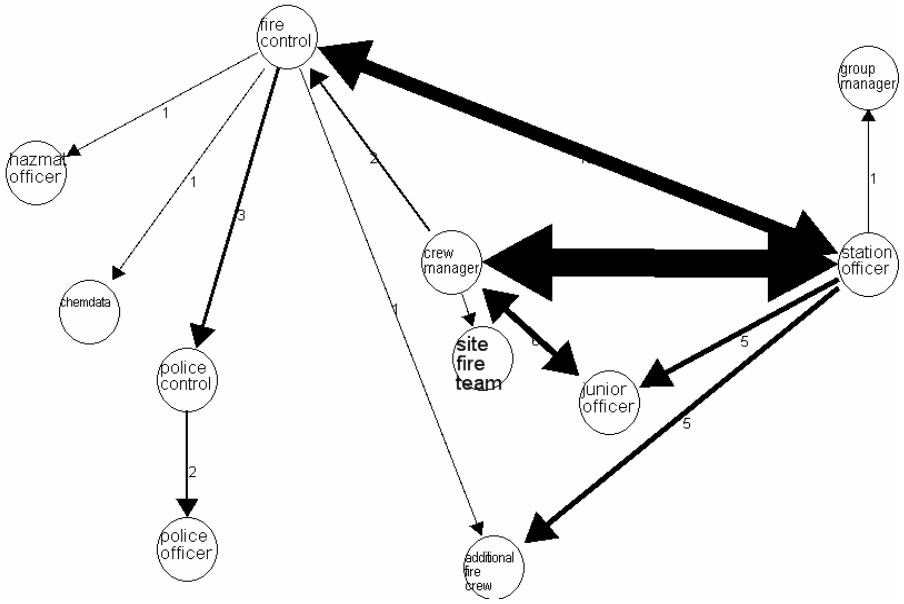

Figure 5: Social network for Fire Incident #3

Table 5 shows the Sociometric status for agents in Fire Incident #3. The Sociometric Status shows key Agents (as defined by mean + 1 standard deviation, i.e., 0.47 + 0.34 = 0.81) to be Fire Control and Station Officer (who can be assumed to take the role of Sector Commander), with the Crew Manager (in the role of Incident Commander) being

close to the defining value. These three agents score much higher than other agents in the network.

Table 5: Sociometric Status for Agents in Fire Incident #3

Agent	**Status**
fire control	1.2
station officer	1.0
crew manager	0.8
junior officer	0.4
police control	0.4
additional fire crew	0.4
site fire team	0.2
police officer	0.2
chemdata	0.2
hazmat officer	0.2
group manager	0.2

In terms of Centrality (Table 6), the key agents (defined by 5.76 + 1.3 = 7.06) to be Fire Control, Station Officer and Crew Manager. In other words, the same agents as were identified through Sociometric Status.

Table 6: Centrality of Agents for Fire Incident #3

Agent	**B-L Centrality**
fire control	8.5
station officer	7.43
crew manager	7.00
additional fire crew	5.95
police control	5.66
junior officer	5.17
chemdata	5.17
hazmat officer	5.17
group manager	4.76
site fire team	4.58
police officer	3.97

2.2. Police operations

Emergency Call Operators prioritise incidents as requiring immediate, early or routine response, according to their urgency. Incidents that are graded as “Immediate Response” are those that require an urgent Police presence, usually because there is a high risk of serious injury or death, or where there is a good chance of an arrest if the response is rapid (i.e. when the crime is still taking place). When an incident is prioritised “Immediate Response”, only the bare minimum of details are taken from the caller by the Emergency Call Operator (i.e. location, nature of emergency and caller’s name), which are then passed on to the Operations Control Unit (OCU) responsible for the area where the call originated. The Operations Centre within the OCU in question will then review the incident priority and allocate resources to respond to it. In the case of “Immediate Response” incidents, West Midlands Police are required to attend the scene within 10 minutes. The OCU may contact the Traffic Section to request the presence of Specialist resources if required. Three ‘Immediate Response’ Incidents have been analysed for this paper.

2.2.1. Police Incident #1: Car Break-in Caught on CCTV

Description of Incident. The night porter of a hotel observes three lads attempting to break into cars in the car park on his Closed Circuit Television (CCTV) monitor. They call 999 and report the crime that is taking place to the Emergency Call Operator, who summarises the information in a new incident log and passes it to the OCU for the incident area. The OCU Operator accepts the log and allocates resources to the incident. The Emergency Call Operator also passes the log to the Traffic Section, who despatch

resources to the incident. The Emergency Call Operator remains on the phone to the Night Porter, who is able to provide further details of the offender's descriptions and actions. One of the Police units arrives at the incident scene, by which time the offenders have fled the scene by car; the Police unit and Night Porter check the CCTV footage for the offender's vehicle. A second Police unit arrives at the scene and begins a search of the surrounding area. The CCTV footage is found to have captured the offenders, but not their car. The Police establish that only one car has been broken into, the owner is located and their ownership of the vehicle verified using the Police National Computer. The owner checks the car and provides a description of the stolen items. The OCU Operator provides a crime reference number, which the Police Officer gives to the owner. The second Police unit finishes the search of the area and all Police units leave the scene. The OCU Operator notes in the log that this incident was a theft from a motor vehicle and adds the approximate time of the crime. They then close the log.

Figure 6 shows the Social Network for Police Incident #1. Comparing this with the models described earlier, there is a striking similarity between this figure and the Split network.

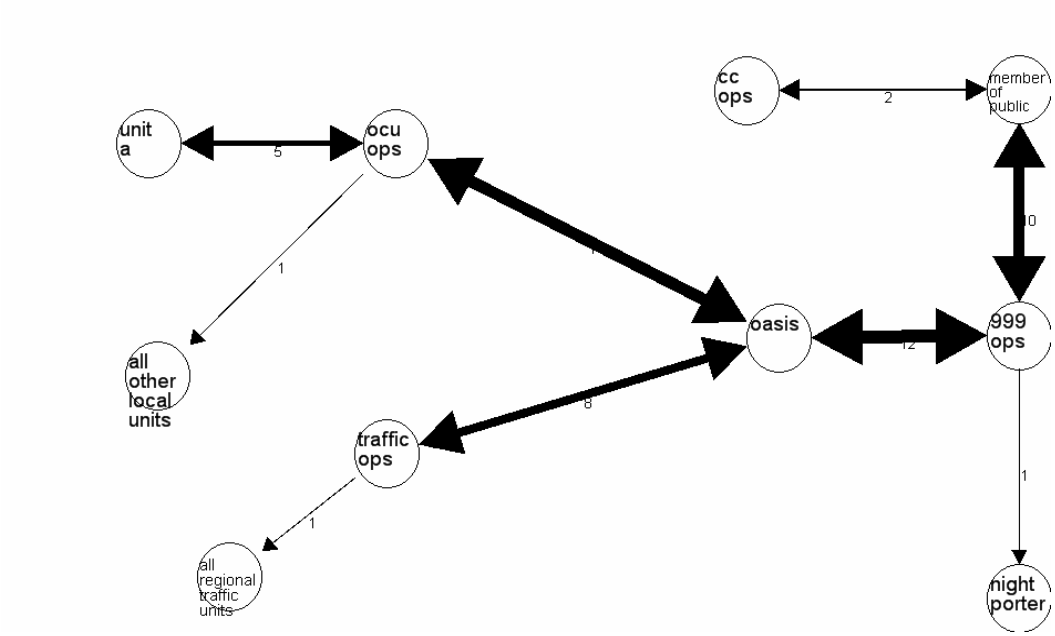

Figure 6: Social network for the Police Incident #1

The Split network has a central node, in this case the OASIS logging system (which generates a log of events for the Police), which leads on to two other nodes, i.e., the OCU and 999 Ops. The Sociometric Status calculations are shown in Table 7. Key agents are defined by the mean + 1 standard deviation (0.4 + 0.2 = 0.6). This analysis further supports the notion of a Split network, in that OASIS, OCUOps and 999Ops all exceed the defined limit for key agents.

Table 7: Sociometric Status calculations for Police Incident #1

Node	***Status***
999 ops	0.66
OASIS	0.66
OCU ops	0.66
member of public	0.44
traffic ops	0.44
CC ops	0.22
night porter	0.22
all regional traffic units	0.22
unit A	0.22

all other local units	0.22

The Centrality calculations are shown in Table 8. Key agents are defined in terms of mean + 1 standard deviation (5.24 + 1.2 = 6.44). In this instance, the most central agent is the OASIS logging system, followed by 999Ops and OCU Ops (although, interestingly, the latter does not meet the criterion for a key agent in terms of centrality).

Table 8: Centrality of Agents in Police Incident #1

Node	***B-L Centrality***
OASIS	7.62
999 ops	6.78
OCU ops	6.10
traffic ops	5.54
member of public	5.08
night porter	4.69
unit A	4.36
all other local units	4.36
all regional traffic units	4.07
CC ops	3.81

2.2.2. Police Incident #2: Suspected car break-in

Description of the Incident. A member of the public calls 999 on their mobile to report that they can see a car being broken into; the Emergency Call Operator summarises this information (in a new incident log) and takes the location from the caller, before handing the log over to the appropriate OCU, as well as the Traffic Section. The caller stays on the phone to the Emergency Call Operator and provides a description of the car and the two suspects; at the same time, the Traffic Section operator broadcasts a request for Traffic units to attend the incident, but does not receive a reply. The caller then reports that the suspects have moved away from the car and gives their direction of travel. The OCU Operator despatches resources to the incident; upon arrival, they check the cars in the street that match the caller's description, but neither vehicle has been tampered with and both have alarms. The OCU Operator notes in the log that this was a false call, but with good intent; the officers leave the incident scene and the OCU Operator closes the log. As with Police Incident #1, this incident is classed as 'Immediate Response' because the crime is still in progress, so there is a chance of capturing the Suspects/offenders at or near the scene, and again there will be a separate task to investigate the Crime. The Unit that arrives at the incident first checks the vehicles in question and finds no damage and concludes that no crime has occurred; the incident is closed.

Analysis. Figure 7 shows the Social Network for Police Incident #2. Once again, it would appear to be a Split network.

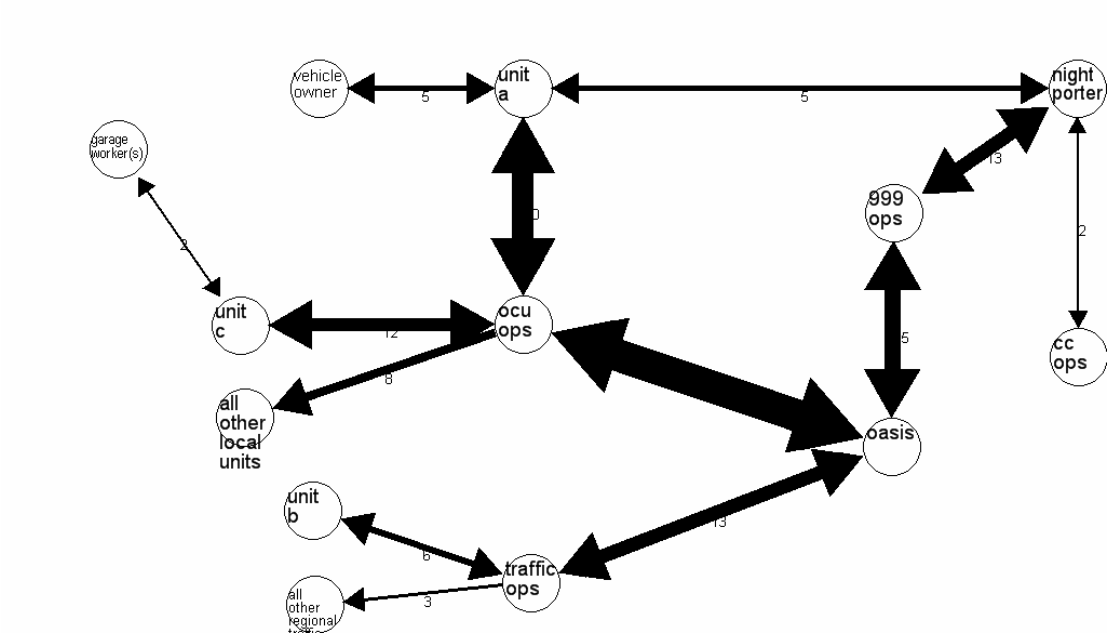

Figure 7: Social network for Police Incident #2

Table 9 shows the Sociometric Status of agents in this incident. The criterion for key agent (mean +1 standard deviation) is Mean 0.4 sd 0.2 = 06. In this incident, OCUOps has the highest status, with the Nightporter, OASIS and Traffic Ops all meeting criterion to be key agents. Presumably this indicates that the source of information (the Nightporter) is playing a continued role, in terms of updating information, with OASIS serving to log the changing information. OCUOps and Traffic Ops both serve to define response in this incident.

Node	***Status***
OCU ops	0.8
night porter	0.6
OASIS	0.6
traffic ops	0.6
999 ops	0.4
unit A	0.4
CC ops	0.2
all other local units	0.2
unit C	0.2
all other regional traffic units	0.2
unit B	0.2

Table 9: Sociometric status in Police incident #2

The Centrality of the agents (see Table 10) show a similar pattern. Key agents must have a score of 6.86 (5.7 +1.16), which indicates that OASIS and OCUOps are the most central agents in this network. Again this indicates an information collation role (OASIS) and a response selection role (OCUOps).

Node	***B-L Centrality***
OASIS	7.83
OCU ops	7.42
999 ops	6.41
traffic ops	6.13
unit A	6.13
night porter	5.87
all other local units	5.04
unit C	5.04
all other regional traffic units	4.41
unit B	4.41
CC ops	4.27

Table 10: Centrality in Police Incident #2

2.2.3. Police Incident #3: Mobile phone robbery

Description of Incident. Incident 3 starts when a girl calls 999 from her mobile to report that her boyfriend has just been attacked and robbed of his mobile phone. The Emergency Call Operator takes down the details of the crime and location (and the direction the offenders headed off in) and passes the log to the OCU covering that area. One OCU Operator despatches a unit to the scene of the incident, whilst a second OCU Operator calls the girl's mobile back for further details of the crime. The girl's mobile is engaged, as she is still talking to the Emergency Call Operator. The caller provides descriptions of the two offenders, as well as the make and model of the stolen mobile phone. The Police unit arrives at the incident scene and begins to search the surrounding area. The girl reports that they are now only two minutes from her house and that her boyfriend has no injuries. The Police unit does not find the offenders during their search and then leaves the area. The OCU Operator notes in the log that this incident was a robbery, enters the approximate time it occurred and closes the log. As with the previous police incidents, Police Incident #3 is classed as 'Immediate Response'. This is because the crime has recently occurred and offenders were 'on foot', so there is a chance of capturing the Suspects/offenders near the scene. There are separate tasks to perform an initial investigation of the Crime, and to treat Injured Parties, as this was an attack. The victim reports that they in fact have no injuries, so no treatment is necessary. A search of the surrounding area is carried out, but the suspects are not found, so the incident is closed (though the long-term investigation would be passed to another police department).

Analysis. The Social Network for Police Incident #3 (see Figure 8) is similar to the other police incidents and shows the characteristic pattern of the Split network.

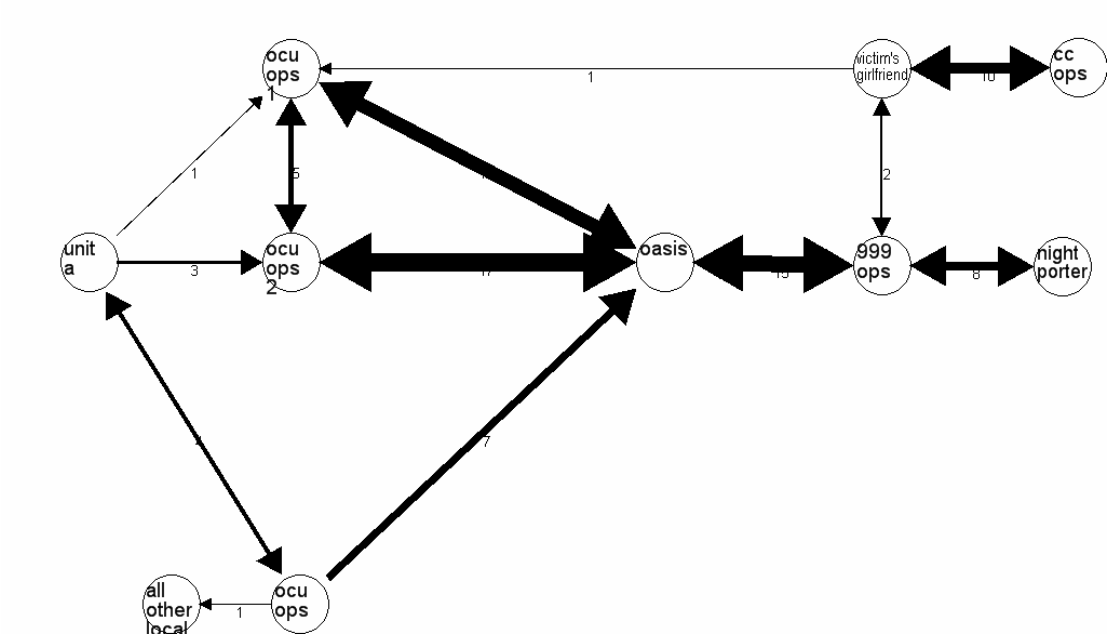

Figure 8: Social network for Police Incident #3

Given the proposal that Police Incident #3 is a Split network, then one would expect Sociometric Status to be high for several key agents. Table 11 shows the results of this analysis. Key agents need to have a score of 0.78 (0.58 + 0.2 = 0.78). From this analysis, key agents can be seen to be OASIS and OCUOps1. This would correspond with previous analyses which have an information collecting agent and a response selection agent.

Table 11: Sociometric Status of Agents in Police Incident #3

Node	**Status**
OASIS	0.89
OCU ops 1	0.89
Victims girlfriend	0.67
999 ops	0.67
OCU ops 2	0.67
OCU ops	0.67
unit A	0.67
CC ops	0.22
all other local units	0.22
night porter	0.22

The results of the Centrality analysis are shown in Table 11. Key agents are defined by 6.17 (5.2 + 0.97 = 6.17). As with the Sociometric Status analysis (Table 12), the results indicate that OASIS and OCUOps are the key agents in terms of being most central in this network.

Table 12: Centrality of agents in Police Incident #3

Node	***B-L Centrality***
OASIS	6.67
OCU ops 1	6.25
999 ops	5.88
Victims girlfriend	5.55
OCU ops 2	5.55
OCU ops	5.26
unit A	5.26
night porter	4.0
CC ops	3.84
all other local units	3.70

3. Discussion

In the present paper we have thus far reported the analysis of six incidents (3 Fire and 3 Police). These analyses are summarised in Table 13.

Table 13. Summary of Fire and Police incidents and analyses.

Number	Incident	Network	Main actors
Fire Incident #1	Hazardous chemicals	Distributed	Police Control Fire Control Fire Commander
Fire Incident #2	Road traffic accident	Hybrid wheel/star and circle (centralised)	Fire Control Watch Manager Station Officer
Fire Incident #3	Chemical fire and evacuation	Distributed	Fire Control Station Officer Crew Manager
Police Incident #1	Car break-in caught on CCTV	Split	OASIS OCU Ops 999 Ops
Police Incident #2	Suspected car break-in	Split	OASIS OCU Ops
Police Incident #3	Mobile phone robbery	Split	OASIS OCU Ops

Any conclusions drawn from the analysis will necessarily reflect the nature of the incidents being studied, the manner in which data were collected and the type of data that could be recorded. With this caveat, it is proposed that the analysis revealed two Distributed networks (Fire Incidents #1 and 3), three Split networks (Police Incidents #1, 2 and 3) and one Centralised (Wheel/Star) network with an additional circle element (Fire Incident #2). Not only were the networks identified graphically, but there results of the Sociometric Status and Centrality analysis of the networks also supported the claims. Dekker (2002) had assumed that emergency services would follow a Negotiated network. Such a network would have a peer-to-peer communication structure. From our analyses it

would now seem that very few emergency service systems follow such a structure. The primary reasons for this could be, in terms of Police operations, the need to maintain a log of the activities performed under the aegis of Police command. In terms of Fire operations there is instead a need to have a central focus for conformation management (this is most evident in Fire Incident #3 which used a heavily centralised structure because of the need to manage a mass of diverse information). In both instances there is, therefore, a need for a central focus within the system. Having said this not all observations demonstrate that the systems are centralised. Indeed, Leavitt (1951) suggested that a centralised (wheel/star) network functions most effectively when operations are based on well-defined procedures and information. Examining the police social networks in terms of Dekker's (2002) set of architectures, it appears the best general match would be with the Split architectures, a design arising from procedures for eliciting well-defined information and clearly defined responses in answer to it. OCUOps tends to act as a C2 asset controlling its respective force and intelligence assets. The Split network architectures are (according to Dekker) used by the USAF (air) and US Army (ground). Dekker's simulations of network architectures using FINC (Dekker, 2002) suggest that Split with information sharing networks are best suited to relatively slow tempo operations where the quality of intelligence is from fair to good. In this case, the role of OASIS would be primarily to ensure that the intelligence can be treated confidently as 'good'. From the point of view of distributed cognition, the OASIS log could be said to be an artefact; a physical manifestation of cognition (e.g., thoughts, plans, memories and so on) that can be shared by collaborating workers (e.g., Hutchins, 1995). OASIS would appear therefore to have multiple roles; as a central record (for audit purposes), as a cognitive artefact which

facilitates collaboration and as a system for allocating responsibility and ownership of incidents in which there is collaboration (we note that ‘ownership’ of the OASIS log is passed between individuals as the incidents unfold). It is also interesting to speculate as to the further sociotechnical impacts OASIS has on police operations; does the terminology used by OASIS (e.g., its nine classifications for incidents) standardise or perhaps constrain the language of policing itself? It is easy to imagine this might be the case if OASIS logs are used for the generation of policing and crime statistics.

It might be argued that the police could alter their current network architecture to something allowing more rapid response. However, examining Dekker’s work we see that this would require either a negotiated sharing network or a distributed network. For the vast majority of police operations these options appear unappealing as they bind small autonomous groups of C2, force and intelligence assets together, a move that poses problems in terms of managing the interaction and synchronisation of such teams if a large enough incident required that they work together (even if OASIS was used as a sociotechnical solution, there would still be difficulties regarding the appropriate hand over and ownership of the log).

A defining feature of a Distributed network is that agents are working independently. In the two Fire Incidents which are proposed to show characteristics of Distributed Networks, the independent working might be a feature of agents addressing different goals, or might arise from dealing with different ‘Sectors’ in the incident. The main reasons for using a Centralised Network would be to either manage information flow or to

coordinate response. Fire Incident #2 can be seen to require both of these activities. The Fire Control serves as the hub for the large network, with many agents contributing to the goal of dealing with the chemical spillage. In this case, rather than necessarily working towards independent goals, the agents could be said to be pursuing subgoals of a shared overall goal. Comparing the prepositional network for Fire Incident #2 with the other Fire Incidents, suggests a higher degree of multiple agents activating knowledge objects, in other words more potential for sharing of information.

The Centralised and Split networks are predominantly functioning to coordinate response, either in terms of 'good' information (in the case of the Police Incidents) or in terms of 'consensual' information (in the case of the Fire Incident). The issue of defining the quality of information is core to the functioning of these networks and indicates the manner in which information is sought and shared. The Distributed networks, on the other hand, are functioning to allow agents to work relatively independently towards separate goals. Thus, the activity is less one of coordination of response, and more one of managing the cooperation of independent agents within a general situation.

The paper shows how network structures can be defined through observation of communication activity. The networks can be presented graphically as network diagrams and can be relatively quickly interpreted with reference to scenarios from which they emerge. The quantitative analysis provided by social network analysis allows the subjective impressions created by the figures to be quantified statistically. It is proposed that social network analysis constitutes a useful method of enquiry in the study of

command and control.

Acknowledgements

This work is supported by a grant from the Human Factors Integration Defence Technology Centre, part-funded by the Human Sciences Domain of the UK Ministry of Defence Scientific Research Programme. The authors would like to thank West Midlands Police and the Fire Service Training College, Moreton-In-Marsh, for granting access to their operations and for their assistance in collecting the data reported here.

References

ADAMIC, L. A., BUYUKKOKTEN, O. and ADAR, E. (2003). A social network caught in the web", First Monday, **8**(6).

DEKKER, A.H. (2001). Applying Social Network Analysis Concepts to Military C4ISR Architectures. Connections, the official journal of the International Network for Social Network Analysis, **24**(3), 93–103.

DEKKER, A.H. (2002). C4ISR Architectures, Social Network Analysis and the FINC Methodology: An Experiment in Military Organisational Structure. DSTO report DSTO-GD-0313.

FIRE SERVICE COLLEGE (2003) IPDS Presentation. Fire Service College, http://www.fireservicecollege.ac.uk/IPDS/IPDS%20presentation%20Marsh%2003.pdf

FIRESERVICE COLLEGE (2004) *Hotline*, **2**. Fire Service College, Moreton-In-Marsh. (http://www.fireservicecollege.ac.uk/hotline/hotline2.pdf).

HUTCHINS, E. (1995). How a cockpit remembers its speeds. *Cognitive Science***, 19**, 265-288.

KILDUFF, M. and TSAI, W. (2003). Social networks and organisations. Sage Publications.

LEAVITT, H. J. (1951). Some effects of certain communication patterns on group performance. *Journal of Abnormal and Social Psychology* **46**, 38-50

SHAW, M. E. (1964). Communication networks. In L. Berkowitz (Ed.), *Advances in Experimental social psychology*, 111-147. New York: Academic Press

WASSERMAN, S. and FAUST, K. (1994). Social network analysis: Methods and Applications. Cambridge University Press, Cambridge.