Paper Submission for:

10th International Command and Control Research and Technology Symposium: The Future of C2

TITLE OF PAPER:

Investigating Alternative Network Structures for Operational Command and Control

TRACK TOPIC:
C4ISR/C2 Architecture

AUTHORS:
Richard McMaster, Chris Baber and Robert Houghton

Point of Contact:
Richard McMaster

Organisation:
Human Factors Integration Defence Technology Centre
The University of Birmingham

Address and Contact Details:
School of Electronic, Electrical and Computer Engineering
Edgbaston
Birmingham
B15 2TT
UK

Tel: (+44) (0)121 414 2934
Fax: (+44) (0)121 414 4291
Email: r.mcmaster@bham.ac.uk

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 for granting access to their operations and for their assistance in collecting the data reported here.

Investigating Alternative Network Structures for Operational Command and Control

R. McMaster, C. Baber and R. Houghton
HFIDTC/The University of Birmingham

Abstract

This paper presents a social network analysis of C2 processes during emergency responses within UK Police operations. Access was given to conduct interviews and observations with Police Officers and Support staff from West Midlands Police C2 facilities and to collect communications data from emergency incidents. This was used to categorise the type of social network in place within West Midlands Police emergency responses; modifications to this data allowed the emulation of interactions that would take place were the police to adopt either more centralised or more distributed networks. The suitability of the new networks for West Midlands Police activity was investigated and the implications for distributed cognitive activities taking place during emergency responses were identified. We propose that such network analysis may be used in the description and comparison of different distributed cognition networks and to enable judgements regarding suitability of network types for certain activities. Finally, it is suggested that this method of network comparison and evaluation may be of use when designing and constructing future C2 networks as part of Network Centric Warfare systems.

1 Introduction

1.1 Network Centric Warfare

Much has been written about what Network Centric Warfare (NCW, known as Network Enabled Capability in the UK) must be able to deliver, in terms of information exploitation and rapid, coordinated activity, for example:

> *"[NEC is] the ability to gather knowledge; to share it in a common and comprehensible form with our partners; to assess and refine it to turn into knowledge; to pass it to the people who need it in an edited, focussed form; and to do it in a timescale necessary to enable relevant decisions to be made in the most economic and efficient manner."*
>
> [Deputy Chief of Defence Staff (Equipment Capability) Cited in: Ministry of Defence, 2004]

However, despite such high-level descriptions of the strategic role of NCW in the future battlespace, it is currently unclear how the C4ISR structures that will realise NCW will function. Concepts which have been applied to NCW such as 'full information accessibility' and a 'resilient information infrastructure'[1] would suggest networks with minimal distance between nodes and a high level of redundancy, but exactly how activity will be coordinated and where command and responsibility will lie within such networks is not clear.

Establishing NEC across a large theatre of operations would create a highly complex, tightly coupled socio-technical system; with information being gathered from multiple sources, combined, analysed and then acted upon within *"...a matter of minutes or even 'in real time'..."* [2], the consequences of errors or omissions at any point within such a network could prove disastrous. Given the costs of implementation and the negative consequences of system failures, it is important that the design and implementation of such C2 networks are carefully managed; analytical techniques which are able to provide practical guidance during system design are required if NCW is to meet the high expectations that have been placed upon it.

1.2 Operations Other than War

Increasingly military operations focus on Operations Other Than War (OOTW). Examples of such activity involve peace-keeping, policing and management of civilian activity. In this paper, we focus on the manner in which a UK Police force conducts a specific type of policing, i.e., emergency response. It is suggested that analogies can be drawn between the manner in which responses are performed and different types of military activity, particularly those under the general heading of OOTW.

1.3 Network Analysis

There is increasing interest in examining organisations and teams in terms of their underlying social networks[3]. 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.
Social network theories are based on the notion that the relationships between individual agents play a determinant role in the performance or action of that social network. Social network theory has been applied across a number of disciplines; it can be used as a tool to investigate organisations, decision-making, the spread of information, epidemiology, mental health support systems, anthropology, child development, etc. Early research[4 5] suggested that there is no single 'best' network structure for group activity; instead, performance is dependant upon how 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 number of other factors. In recent years, the discipline of social network analysis has become based very much in empiricism and mathematics. Whilst, at its simplest a social network graph will depict nodes (actors) linked by connecting lines (termed edges) 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.

One approach to using social network analysis to assess the structure of military organisations is the FINC (Force, Intelligence, Networking and C2) methodology described by Anthony Dekker[6 7]. 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 C2 units. For our purposes we can consider ‘force assets’ to be individuals or agents who act upon an incident (an attending police officer, for example), ‘intelligence assets’ to be sources of information prompting action, such as 999 Operators and the OASIS database and ‘C2 assets’ are individuals controlling the situation, such as Operational Command Units. Networking is simply the communication links between agents and would, in the case of the emergency services, primarily amount to radio, telephone and electronic communications.

1.4 Background to West Midlands Police Operations

Following the reorganisation of local authority boundaries in 1974, seven existing Police forces were merged to form West Midlands Police force (WMP). WMP covers a population of approximately 2.63 million and a geographical area of 348 sq miles, which is divided into 21 Operational Command Units (OCUs). It is the second largest police force in the UK, consisting of 7,966 police officers, 3,373 support staff and 683 special constables. During 2002-2003, WMP dealt with 350,242 crimes and had a budget of £414.7 million[8].

The structure of command and control within WMP is complex, with a large number of control rooms and different communications media in use. Figure 1 provides an illustration of the command centres and main lines of communication used during responses to emergency incidents.
The WMP Force Communications Centre (FCC), situated at Bourneville Lane Police Station, Birmingham, is split into two sections: 999 Operators and Traffic Operators. The 999 Operators handle all emergency calls made to the police in the West Midlands area (approximately 2,000 calls per day), recording the key incident details and passing them to the appropriate control centre.
The FCC Traffic Operators direct the activities of a number of specialist units during responses to emergency incidents. In addition, the FCC Traffic Operators coordinate the police response to an incident with other agencies, including the other emergency services, local authorities and other Police forces.

In the United Kingdom, the primary emergency services (Fire, Police and Ambulance) operate three main levels of incident command. These levels are commonly referred to as Bronze, Silver and Gold[9]. Within WMP, Bronze Command is performed by the local OCUs, which handle the majority of emergency incidents. Silver Command level is the responsibility of the FCC Duty Inspector, who becomes involved in the response when the severity of the emergency requires the planning, coordination and decision-making activities associated with this higher command level[10]. Finally, Gold Command is only brought into the command structure when the decision is made to declare the emergency a major incident[9].

In carrying out their duties, WMP dealt with 679,598 emergency calls over the last year[8]. The following description of WMP emergency incident response process has been produced from interviews and observations of Police Officers and support staff in the WMP FCC and Bourneville Lane OCU, as well as on data collected from archived incident logs on the OASIS command and control system:

999 (emergency) calls that are passed to WMP can cover a wide variety of incidents, ranging from assaults and robberies, to burglaries and road traffic accidents. 999 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. if 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 999 Operator (i.e. location, nature of emergency and caller’s name), which are then passed on to the OCU responsible for the area where the call originated. The Operations Centre (control room) 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, WMP are required to attend the scene within 10 minutes. The 999 Operator may also pass details of the emergency to the Traffic Section, who will send resources to the incident if they are not otherwise engaged.

Communications between the 999 Operator, the Traffic Section and the various OCUs take place primarily via OASIS - Operational and Support Information System - which is used to electronically log and transfer incident details and can be accessed and updated by a number of actors in the command and control network. OCU Control rooms communicate with their local units by UHF radio, whilst the Traffic Section contacts Traffic units via VHF radio.

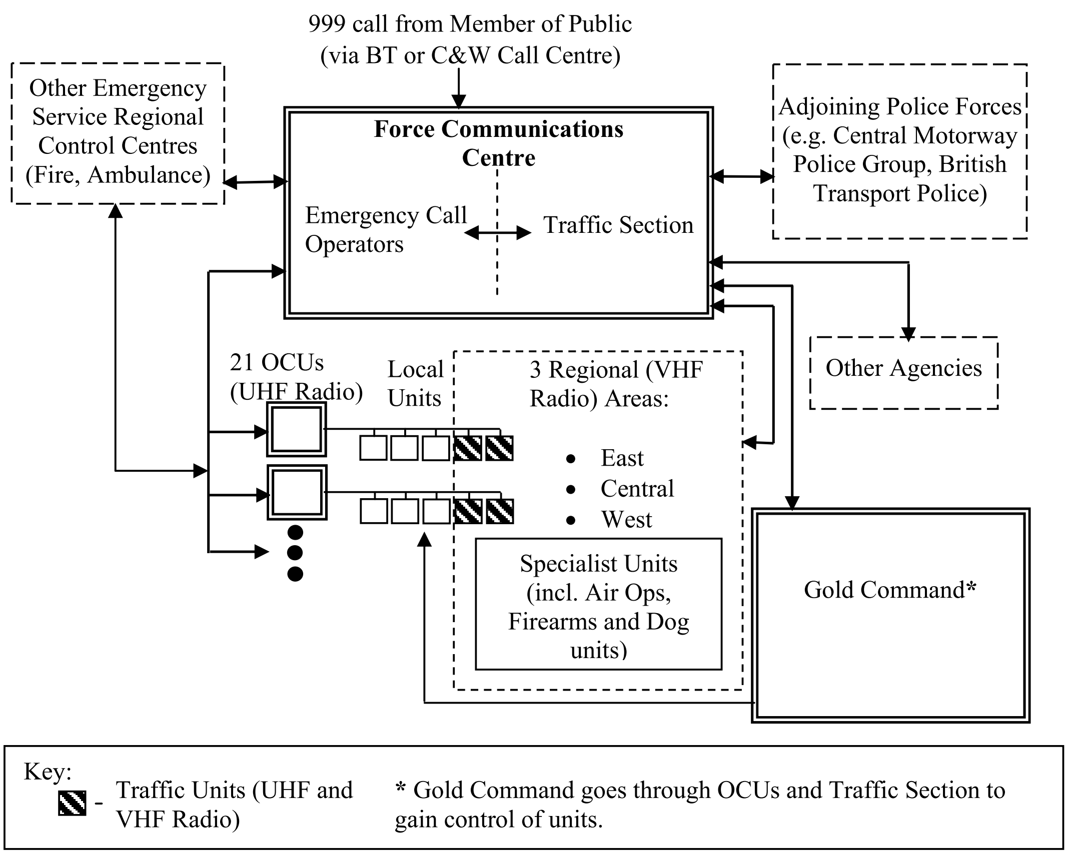

Figure 1: Primary lines of communication used by WMP during responses to Emergency Incidents

2 Analysis of WMP Emergency Response Network

2.1 Emergency Incident Description

In this paper, one emergency incident has been studied using social network analysis, to illustrate the type of network adopted within WMP emergency responses. The incident - a car break-in caught on CCTV - is described below:

> The Night Porter of a hotel observes three youths on his CCTV monitor attempting to break into cars in the car park. The Porter calls 999 and reports the crime that is taking place to the 999 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 999 Operator also passes the log to the Traffic Section, who despatch resources to the incident. The 999 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 tape for footage of the offender's vehicle. A second Police unit arrives at the scene and begins a search of the surrounding area and questioning potential witnesses. 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 (having not located the suspects) 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. There will be a separate task, initiated after this activity, to complete an investigation of the Crime.

This event was a relatively straightforward police emergency, which lasted less than 40 minutes. In spite of this, a number of actors (in this case 8) cooperated in order to rapidly resolve the incident.

2.2 Task Model

A task model for the incident is shown in Figure 2; from this figure it is apparent that the incident can be said to represent two overlapping activities: 'Perform Initial Investigation' and 'Apprehend Suspects'. The Perform Initial Investigation activity was completed during the immediate police response to the incident, however, as details of the suspects' getaway vehicle were not captured, the police were not able to widen their search during the emergency response, so the incident was closed without completing the Apprehend Suspects task (though the long-term investigation would be passed to another police department).

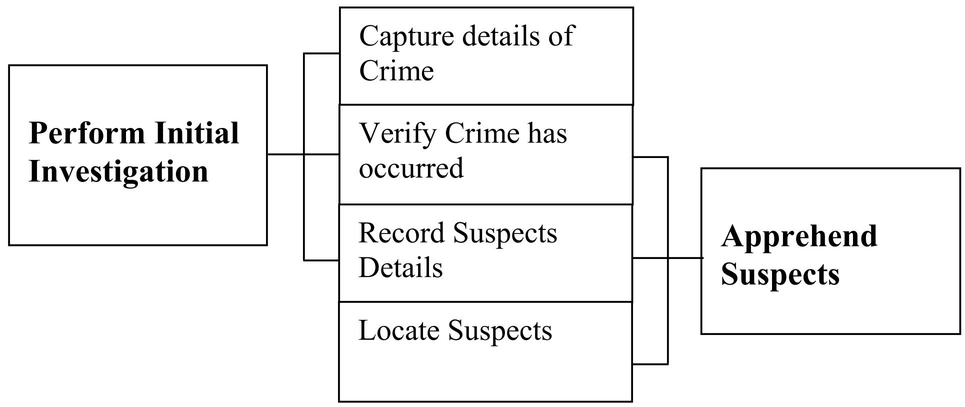

Figure 2: Task Model for Police response to Car break-in

2.3 Distributed Cognition in WMP

Distributed Cognition is the branch of cognitive science which studies systems-level cognitive processes of groups of individuals and artefacts engaged in the performance of a task[11 12]. It is argued that these cognitive processes are emergent properties of the system, and are distributed across it, rather than being contained within a single individual[12]. Distributed cognition is thought to take place in the same way as cognition in the individual, i.e. through the creation, dissemination and transformation of representations of knowledge[11 13 14]. However, unlike individual cognition, where representations are held within the individual's mind, within a distributed cognitive system artefacts (physical objects, language and people) act as representations of task relevant information[11].

It is evident that the social network described above exhibits distributed cognition properties; cognitive activity (i.e. the creation, dissemination and transformations of representations) is spread across the social network, facilitated by OASIS and other technologies: emergency information is collected by one agent (or group of agents, in the case of multiple emergency calls), analysed by another group of agents (the OCU and Traffic Section Operators) and acted upon by a further group (the attending officers). No single person coordinates this activity. This can be demonstrated by examining the question of who the damaged car belongs to in the incident:

> In the emergency incident, the attending Officers discover that a car has been broken into; they then locate the individual who claims ownership of the vehicle. The Officer makes a request to the OCU Operator to check the Police National Computer (PNC) for the vehicle's registration plate; the Operator finds a result for the vehicle registration in the database and relays the description of the vehicle (make, model and colour) and the name of the registered owner to the Officer. The Officer is then able to match the description of the vehicle from the OCU Operator to the car in front of them (establishing that the registered owner of the car listed in the PNC owns the damaged vehicle) and can verify that the name provided by the individual who claims ownership matches the name of the registered owner provided by the OCU Operator.

During this sequence of events no single agent within the network explicitly answers the question of who the car belongs to, nor is the question explicitly asked; rather, the question is raised and answered during the course of several actions by a number of agents within the network. It is the combination, interpretation and re-presentation of information provided by multiple agents within the distributed cognition system that enable it to achieve the goal-state[12 14 15].

2.4 Social Network Analysis

Figure 3 presents the social network diagram for the police incident. Comparing the social network diagram with the models evaluated by Dekker[7], there is a striking similarity between this network and the Split network. The Split network features a central node; for the police incident this appears to be the OASIS incident logging system (which generates a shareable log of events for the Police), which leads on to two other nodes, i.e., the OCU and 999 Ops.

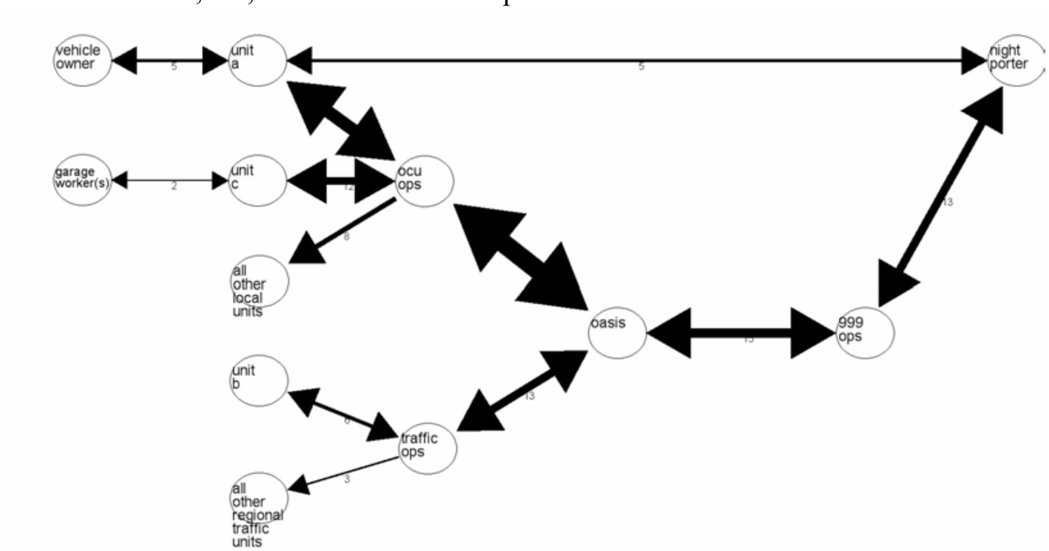

Figure 3: Social network for the Police Incident: Car Break-in caught on CCTV

The social network metrics that are used in this paper are Sociometric status and Centrality. Sociometric status gives an indication of the relative prominence an individual agent has as a communicator with others in the network. Similarly, Centrality is also a metric of the standing of a node within a network, but this is in terms of its geodesic distance from all other nodes in the network. The methods for calculating Sociometric status and Centrality adopted in this paper are covered further by Houghton et al.[16].

Sociometric Status

Given the proposal that WMP emergency response is a Split network, then one would expect Sociometric Status to be high for several key agents. The criterion for key agent status is the mean plus one standard deviation (0.6); in this incident, OCU Ops has the highest status (0.8), with the Night Porter, OASIS and Traffic Ops all meeting the criterion to be key agents (all scoring 0.6). Presumably this indicates that the source of information (the Night Porter) is playing a continued role, in terms of providing new information, with OASIS serving to log and disseminate the changing information. OCU Ops and Traffic Ops both serve to define the response to the incident.

Centrality
The Centrality of the agents show a similar pattern. Again, a notion of 'key' agents can be defined using the mean plus one standard deviation cut-off (6.86), which indicates that OASIS and OCU Ops are the most central agents in this network (with 7.83 and 7.42 respectively). Again this indicates an information collation role (OASIS) and a response selection role (OCU Ops).

Network Description
Examining the police social networks in terms of Dekker's[7] 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. The Split network architectures are (according to Dekker) used by the USAF (air) and US Army (ground). Dekker[7] had thought that emergency services would follow a Negotiated network. Such a network would have a peer-to-peer communication structure. From our analysis it would seem that WMP do not follow such a structure. The primary reason for this could be the need to maintain a log of the activities performed under the aegis of Police command. In addition, Traffic and OCU Ops areas of operations overlap, so the work that they do is not separate (which is assumed according to Dekker's description of a Negotiated network); they are often notified about the same emergency incident and, whilst the incident is usually 'owned' by the OCU, Traffic Section will send resources if they are available and are thought to be necessary, without waiting for a request from the OCU. In fact, some OCU Units (Officers trained in high speed pursuit) are also Traffic Section Units and can monitor both OCU and Traffic communications (shown in Figure 1). Within the social network, Strategic, tactical and operational command levels are not distinguishable; OCU Ops and Traffic Ops independently provide strategic guidance and tactical incident information to the attending officers, as well as more operational commands. Within the social network, OASIS would appear to fulfil multiple roles; acting 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).

2.5 Evaluation of WMP Social Network

In describing the Split network, Dekker[7] commented that it was an architecture used by the US Army for land-based operations. Both US Army doctrine (formed through generations of war fighting experience) and Dekker's experimental results converge on the finding that this social network is best used to support operations where the quality of information is good (that is to say, sensors are reporting accurately and intelligence can be trusted) but speed of response is not so critical as the degree of coordination within that response. However in Police operations, before Units arrive on the scene the sole information source is usually the member of the public who dialled 999 - they are often in a highly agitated state and are prone to making errors or omissions when relating the emergency. One of the first duties of the attending officer is to establish whether there really is an emergency and what the nature of the emergency is.

The Social Network in use in WMP has several nodes (4 steps in the network) between the information source (the caller) and the responding units. Increased intermediate nodes slow down the speed of information transmission across the network, meaning that information can become out of date. This is a problem in fast-paced scenarios, where the nature of the problem can change whilst responding units are still en route. Within the emergency incident analysed in this paper, the suspects had fled the scene only two minutes and ten seconds after the emergency call to the Police was first answered. The Police priority to the call was classified as Immediate Response, as the crime was still in progress; this response priority means that officers will proceed to the incident at speed, which is not without risk to themselves and other road users. In the event, the Police units did not reach the scene before the offenders had left, and they were unable to locate them during their search of the immediate area. Many emergencies are prioritised Immediate Response as there is a high risk of serious injury or death to someone, it is therefore necessary for the Police C2 network to pass details of the emergency to responding units quickly in order to justify the use of high speed driving and to ensure that attending Officers arrive in time to provide an effective response.

A further consequence of the high number of steps required to pass information to responding units is that the information quality may suffer, either from inaccuracies or omissions[6]. In this incident, the description of the emergency was verbally relayed from the Night Porter to the 999 Operator, who summarised it as text in the electronic OASIS log. This log was then passed over WMP intranet to the OCU and Traffic Operators, who verbally recounted it over the radio to the officers proceeding to the scene. Despite the highly trained nature of WMP staff, the conversion of the incident data from verbal to written and back to verbal format allows information to be lost or distorted, especially as the information is not passed verbatim from one agent to the next – each agent summarises the information as concisely as possible, often using police abbreviations and slang.

3 Alternative Network Architectures for WMP Emergency Responses

3.1 Centralised and Distributed Networks

Looking at Dekker's[6] network types, both centralised and distributed networks have small geodesic distances, so the speed of transmission is much faster than in the split network; it might therefore be argued that the police could alter their current network architecture to one of these structures, in order to allow more rapid responses to emergencies. There are features of both types of network, which would suggest that they might be appropriate for the management of WMP emergency responses.

Centralised Network
Dekker[7] associates the Centralised network with the USAF (United States Air Force) who have good communications, good intelligence and can move force assets into position rapidly. Whilst the information received at the start of a police emergency incident often contains inaccuracies and omissions, the hierarchical nature of this type of network may be appropriate for WMP, where the emergency incident is 'owned' by the OCU Controller, who is responsible for coordinating the police response. There is also a need within the police to create a formal record of their actions in response to

emergency incidents. In WMP, this function is carried out by OASIS – the incident log is admissible as evidence in court. The Centralised network may be beneficial to WMP in terms of ensuring that all relevant information is entered into the incident log. Certain Police Operations already follow a more centralised structure, for example in the UK seven of the busiest highways in Europe converge in the Midlands. Due to the tightly-coupled nature of such a heavily used traffic network, it is necessary for police activities to be centrally coordinated, this is done by the Central Motorway Police Group (CMPG), who control all police Motorway activity in the Midlands and some neighbouring counties.

Distributed Network

Dekker[7] suggests Distributed social networks were found in, for example, the Special Forces, wherein different sub-groups have somewhat different agendas and roles to fulfill. In terms of Dekker's experimental paradigm, he found such social networks performed best in situations in which a fast tempo of response was required but sensor quality itself was not necessarily optimal. This results in "Intelligence Superiority" wherein the best possible use is made of limited intelligence and steps are taken to rapidly uncover as much information as possible (breadth is emphasised over depth). As we have discussed earlier, police operations often require a rapid response and the information that is passed to the attending officers can be patchy or inaccurate.

Another defining feature of a Distributed network is that agents are working independently. Looking at the activities of the responding units in the police emergency described above, it can be seen that the units are engaged in tasks relating to different goals: one unit reviews CCTV footage, interviews the witness, inspects the damaged car and records details of stolen items (part of the 'Perform Initial Investigation' goal in Figure 2); the other unit uses details of the suspect's descriptions during interviews with nearby members of the public and patrols the immediate area (part of the 'Apprehend Suspects' goal in Figure 2).

Rather than merely hypothesising as to whether one of these network types may be more appropriate for WMP activity, by modifying the data gathered for the emergency incident described earlier and repeating the Social Network Analysis, it is possible to simulate police C2 activity within these two network types.

3.2 SNA for Centralised Network

Figure 4 shows the social network for the emergency incident described earlier, with the data modified to represent a more centralised network. In reality, moving all of the OCU Control centres from their local stations into the same control room as the Traffic Section would make the change to a centralised network. This is simulated in the Centralised network shown here by merging OCU Ops and Traffic Ops into a single control role. The new controller role now manages the response of all attending units, both local OCU resources and regional Traffic units, passing incident details from OASIS. The merging of Traffic Ops and OCU Ops into a single node in this network is justified, because they perform a similar role and had similar Sociometric status and centrality values in the original network.

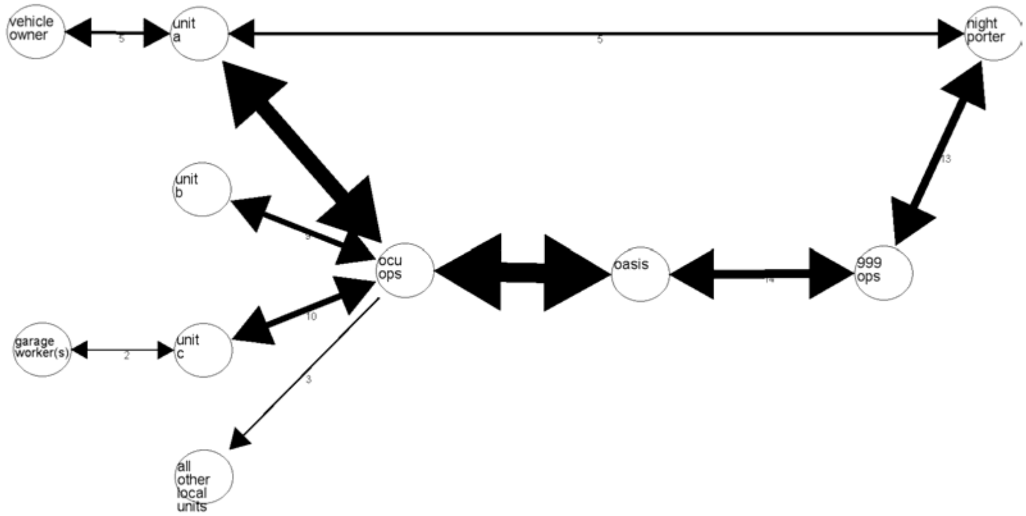

Figure 4: Modified Social network for the Police Incident – Centralised Network

Sociometric Status

The criterion for key agent status identifies only one agent - OCU Ops – as having key status (scoring 17.33, criterion = 10.25). This is to be expected for such a centralised network: OCU Ops filters all incident information from OASIS before passing it to the responding units; OCU Ops also acts as the single command role in the network, directing and coordinating the activity of the attending Officers.

Centrality

Analysis of the Centrality of the network agents identified two key agents: OCU Ops and Unit A (with 7.77 and 6.31 respectively, criterion = 6.29). Within this network we would expect OCU Ops to have key status, as the central command and information dissemination node. Unit A's key status is likely due to it being slightly better connected within the network relative to other agents (having 3 connections, compared to 1 or 2 for all other nodes bar OCU Ops), due to the fact that Unit A converses with both the Night Porter and the vehicle owner during the incident.

Network Description

The Centralised network is a hierarchical structure in which subordinates answer to commanders, with information being passed via the chain of command itself. As with the original Split network, strategic, tactical and operational command are not distinct, though they are now being fulfilled by a single agent – the controller (OCU Ops). As the responding units are being directed from a central command point, there will need to be a relatively high level of operational direction (e.g. "Unit A – interview witness", "Unit B – search for suspects") to ensure that all aspects of the emergency response are coordinated, i.e. so that all three responding agents do not try to interview the Night Porter, or all ignore the Night Porter and the CCTV footage and instead conduct searches for the suspects.

3.3 Evaluation of Centralised Network

In the centralised network structure there is now only one Agent in the C2 role, which should lead to a more efficient response; with two separate control rooms sending agents off to the same emergency, there is a danger of actions being duplicated.
Beyond this, there is little to recommend the centralised network for this type of activity. The new network has not shortened the distance across the network between the information source and the responding units, so there is no advantage in terms of shortened response times or reduction in information errors. The network still features a delay in passing information to the police units, as the controller reviews the information from OASIS before deciding whether to pass it onto the attending officers. There is also the danger that an overly controlling command structure may remove Officers' freedom to apply their knowledge and experience in a timely manner, preventing them from taking the initiative in dynamic situations.

3.4 SNA for Distributed Network

Figure 5 shows the social network for the emergency incident described earlier, with the data modified to represent a distributed network. In this network, emergency incident information is sent from OASIS directly to all attending Officers (e.g. via wirelessly networked PDAs), who then coordinate their activities by sharing communications amongst themselves. As with the Centralised Network, the roles of OCU Ops and Traffic Ops have been combined into a single supervisory position.
In addition, the communications data has been altered, so that the C2 agents and responding units communicate with each other about the same amount. We are attempting to level out communications, which is justified because in such a network everyone has an equal probability of talking to each other.

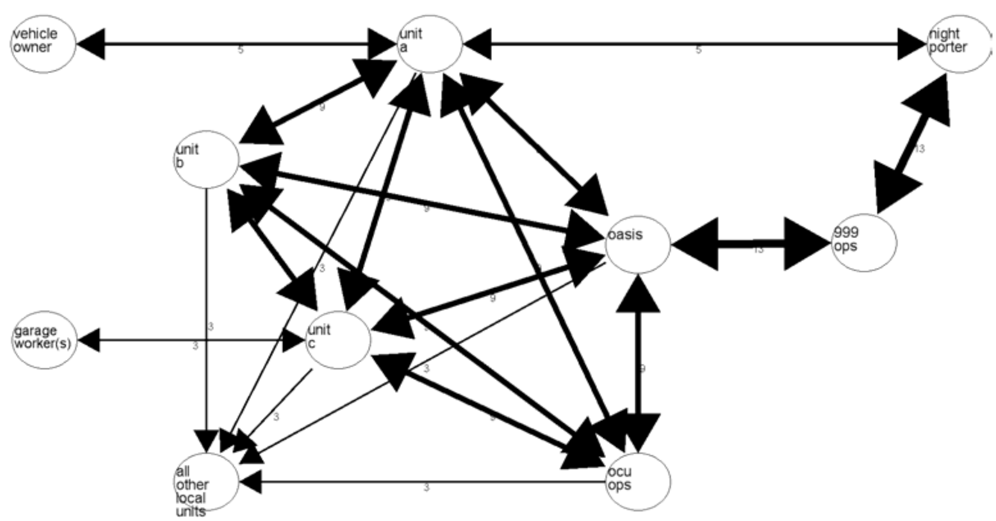

Figure 5: Modified Social network for the Police Incident – Distributed Network

Network Description

The distributed architecture is most often found in the context of special operations where decision-making must be done rapidly with regard to small-scale actions[7]. The distributed network shown here features a clearer distinction between levels of command than the split or centralised networks: strategic command is provided by the OCU Ops role, who defines the type of police response and is responsible for 'owning' the incident log; OCU Ops also provides some tactical command, in terms of meeting resource requirements for the incident; tactical information on the state of the incident is provided directly to attending Officers by OASIS; the detailed operational decisions are now made by the responding units themselves, as they coordinate their activities with each other.

Sociometric Status

The criterion for key agent status gives only two key agents, OASIS and Unit A (11.56 and 10.89 respectively, criterion = 10.17), probably because they are the most highly involved agents in the scenario, with OASIS logging all communications between agents involved in the response and Unit A still handling interactions with the Night Porter and the vehicle owner, as well as communicating with the other attending Officers. Looking at the other responding units (Units B and C), both have much higher status scores than in the original network (8.67 and 9.33 respectively, compared to 0.2 for both in the Split network); so there are several nodes with high Sociometric status, supporting the claim that this is a distributed network.

Centrality

For a distributed network, we would expect that centrality would be similar across all agents. An analysis of centrality for the network showed that only Unit A qualifies as a key agent (6.73, criterion = 6.26); however, it was also found that five of the other agents have centrality scores just short of the key status criterion: OASIS, Unit C, OCU Ops, Unit B and All other local units (scoring between 5.69 and 6.16), suggesting that the network does comprise several highly interconnected agents.

3.5 Evaluation of Distributed Network

The high level of communication across the distributed network supports the rapid acquisition, analysis and dissemination of information, which is a priority during the time-critical early stages of an emergency incident when it's nature is still being defined. Providing the responding units with direct access to OASIS further reduces the distance across the network that information has to travel, which could speed up police responses and reduce errors and omissions in incident information due to repeated transformations. The self-organising nature of the activity of the attending officers means that they are able to effectively coordinate their actions, whilst at the same time retaining their autonomy, because the role of the controller is now more of a strategic/tactical command level.

3.6 Conclusions of Network Simulations

From our evaluations of the three networks described in this paper, it would appear that the distributed network may offer certain advantages to WMP over the current Split architecture; as information certainty reduces, it might make more sense to move to a distributed network, which is better suited to operating in conditions of high uncertainty or information unreliability where greater flexibility is necessary. Distributed network may also complement the high levels of operational autonomy of Attending Officers, whilst at the same time allowing for a more coordinated response from all resources. Rather than creating formal distributed architectures, it may be possible for WMP to make use of geographic location information and Officer's availability status to form ad hoc distributed networks to respond to emergency incidents. Officers are already called to attend to an emergency based on their location relative to the incident scene and their level of commitment to other duties; it should be possible to form a networked working group of attending officers, who are then able to rapidly coordinate their activities.

An illustration of when moving from the Split network to a more distributed structure would be beneficial for WMP is provided by looking at a summary of another emergency incident involving thefts from cars:

> In this incident a member of public called 999 at night to report that a group of youths were breaking into cars. The 999 Operator passed the incident log to the local OCU and the Traffic Section; the OCU despatched resources to the scene, though the suspects fled from the police on foot through the gardens of near-by residential properties. Additional resources were then deployed to the scene and proceeded to cordon the area (using vehicles on main roads) and search for the suspects (on foot). WMP helicopter was despatched to the scene by the Traffic Section, to use a thermal imaging camera to search for the suspects. The Officer in the helicopter identified people hiding in the gardens; the locations of the individuals were relayed to the Officers on the ground (via Traffic Section and the OCU Operator) who then found and apprehended them. The Officers on the ground then completed the tasks of investigating the thefts from the motor vehicles and placing the suspects into custody, whilst the helicopter was despatched to another incident.

In this incident, in order for the Officer in the helicopter to pass directions to the Officers on the ground, the message would have been radioed to the Traffic Section Operator, who would enter it into the OASIS log; the new information in the log would have been seen by the OCU Operator, who would have then radioed it to the attending Officers. The reason for this is that the helicopter (a specialist unit) and OCU Units operate on different radio systems (Figure 1). The centralised nature of the system architecture has created a bottleneck; ideally, the Officer in the helicopter would be able to communicate directly with the Officers on the ground below them, allowing for a faster response to their directions.

WMP are in the process of introducing Airwave, a new digital radio communications system across the force. It has a number of new features, such as text and colour picture messaging and direct access for Police Officers in the field to the Police National Computer[17]. The new system will resolve the current radio compatibility problems and allow communication between officers anywhere across the West Midlands. Airwave also allows the creation of working groups of officers who are dealing with the same incident. Not only does such technology make the types of ad hoc distributed social network discussed here possible, the adoption of this digital system may require it. WMP currently have no plans to alter the existing C2 structure when Airwave is implemented. However, the new capabilities of the Airwave system, such as the ability for attending Officers to communicate directly, without needing to go through their control room[18], may compromise the C2 network if no modifications are made to the structure, for example by affecting lines of communication, reducing feedback to control centres and compromising the role of OASIS as a comprehensive up to date record of emergency incident details.

4 Discussion

4.1 Sense-Making

Burnett et al.[19] have identified two forms of collaborative networks that support sense-making; namely the Community of Practice (CoP) and the Exploration Network (EN). The CoP is *"...centered on a well-defined domain of knowledge and expertise...The goal of the community is to create, maintain and share its knowledge within a well-defined domain."* [19] This would appear to fit well the way in which the Split network description of WMP operations implies that a limited amount of knowledge can be defined and then heavily shared amongst agents. Within the concept of the CoP there is also the notion that the community consists of experts who communicate with each other using specific terminology: from a sociotechnical perspective this is possibly an effect that the shared language of the OASIS system has upon its users. By contrast, the Distributed network described in this paper could reflect the alternate form of sense-making network in operation, that of the Exploration Network. Where the CoP produces a depth of knowledge, the EN instead emphasises breadth: *"Memberships to these communities is loosely defined, with members having similar or very different patterns of interpretation, assumptions and beliefs."*[19] In terms of the Distributed Network, this EN pattern could be manifest as wide ranging discovery of a variety of knowledge by individuals. Thus, the CoP network would most likely be found in situations in which well-defined procedures could be applied to clearly understood problems, and the EN network would be applied to situations in which uncertainty was relatively high.

4.2 Distributed Cognition and Alternative WMP Networks

Socially distributed cognition systems feature several human agents exchanging representations whilst engaged in goal-directed behaviour[20]. It is the coordination and communication of human agents – mediated by artefacts – that enables the system to achieve its goals:

> *"By bringing representations in the system into co-ordination with each other, information can be propagated through the larger cognitive system, being continually modified and processed by a number of individuals and artefacts, until the desired result is reached."*
>
> [Perry, M.J. and Macredie, R.D. (n.d.), p3]

In order to effect this coordination, individual agents within the system need to have an understanding of ‘who knows what’ within the system, which includes knowing who within the network possesses information; agents must know where to go to obtain information. Additionally, agents must have an understanding of the division of labour, i.e. how activities are organised across the system[21]; agents possessing information need to know who to pass it to. In terms of the Centralised network discussed earlier, understanding ‘who knows what’ and how activity is organised is a relatively straightforward matter; there is a single point of contact for most of the agents (OCU Ops), who directs the activities of the ‘strike’ units and who they report back to. There is a central repository of incident data (OASIS) and roles and responsibilities within the system are also clearly defined (within standard operating procedures). However, within the Distributed network it becomes more difficult for agents to know who to go to for information or who to pass new information to; there are now many points of contact for all agents and a large number of potential information sources; roles within the network may be less well defined, especially if social networks are created and disbanded on an ad hoc basis. There is the danger that, if agents are not able to pass information through the system effectively, information processing at a systems-level (i.e. resolution of the emergency incident) could break down entirely. One solution may be to give everyone access to an information repository which maintains a comprehensive record of the emergency incident (such as OASIS), so that agents always know where information can be found and should be passed to.

5 Conclusions

We have demonstrated that it is possible to use network communications data to create credible simulations of new network structures undertaking the same tasks. Not only were the different network types identifiable from their diagrams, but the measures of Sociometric status and Centrality also supported these classifications. These network simulations have allowed us to explore different configurations of a C2 system and identify their potential strengths and weaknesses. For WMP this analysis may prove beneficial ahead of their transition to a new communications network.

SNA provides a quantitative means of studying the flow of information and the division of labour within a network – which are fundamental to developing an accurate understanding of it as a distributed cognition system[21]. The graphical and statistical outputs from SNA, along with the ability to identify network types means that comparisons can be made between different distributed cognition systems and recommendations can be made as to how C2 structures can be improved to enhance system performance. However, such network analysis can only be fully understood by examining the context of the network in question; without a thorough qualitative analysis of the social network, i.e. a study of the goals and constraints acting upon the system; examination of the roles of actors and artefacts in achieving these goals; identification of representations and how they are utilised by the system[21], it is impossible to make judgements on the suitability of the network architecture or to predict how changes to the structure of the system will affect systems-level cognitive activities, such as perception, representation, decision-making and action.

Despite the small-scale nature of the incident discussed in this paper, the problems of how to structure social networks are the same for larger C2 systems, such as those that will be required for NCW. Issues regarding trade-offs between speed of response and accuracy of information and whether to opt for centralised control structures or more autonomous strike units will need to be identified and addressed before NCW structures can be designed and implemented. In this paper, we have presented a method for describing, comparing and evaluating social networks within the context of the activity being performed, which may be able to offer practical benefits to NCW development in terms of identifying how the associated social networks may actually operate.

References

1. Ministry of Defence (2004). *Network Enabled Capability.* Retrieved March 2005 from http://www.mod.uk/issues/Network_Enabled_Capability/

2. Secretary of State for Defence (2002) *The Strategic Defence Review: A New Chapter*. TSO (The Stationery Office). Retrieved August 2004 from http://www.mod.uk/issues/sdr/newchapter.htm

3. Kilduff, M. and Tsai, W. (2003). *Social networks and organisations*. Sage Publications.

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

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

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.

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

8. West Midlands Police (n.d.) *About Us*. Accessed August 2004 (http://www.west-midlands.police.uk/about_us/index.shtml).

9. Cabinet Office Civil Contingencies Secretariat (2003) *Dealing With Disaster – Revised Third Edition*. Brodie Publishing Limited, Liverpool. Retrieved August 2004 from http://www.ukresilience.info/contingencies/dwd/dwdrevised.pdf

10. HM Inspectorate of Constabulary (1999) *Keeping the Peace: Policing Disorder*. HMIC, London. Retrieved August 2004 from http://www.homeoffice.gov.uk/docs/poldis.html

11. Flor, N. V. and Hutchins, E. L. (1991). Analyzing Distributed Cognition in Software Teams: A Case Study of Team Programming during Perfective Software Maintenance. In J. Koenemann-Belliveau, T. G. Moher and S. P. Robertson (Eds.) *Empirical Studies of Programmers: Fourth Workshop*. 36-64. Norwood, New Jersey: Ablex Publishing Corporation.

12. Artman, H.; Garbis, C. (1998) Situation Awareness as Distributed Cognition. In T.R.G. Green, L. Bannon, C.P. Warren and J. Buckley. (Eds) *ECCE 9: Proceedings of the Ninth European Conference on Cognitive Ergonomics*, 151-156. European Association of Cognitive Ergonomics (EACE), Le Chesnay, France.

13. Perry, M. (2003). Distributed Cognition. In J. M. Carroll (Ed.) *HCI Models, Theories and Frameworks. Towards a Multidisciplinary Science*. London: Morgan Kaufmann.

14. Hutchins, E. (1995). How a Cockpit Remembers Its Speeds. *Cognitive Science*, 19 (3), 265-288.

15. Norman, D. A. (1993). *Things that Make Us Smart*. Menlo Park, California: Addison-Wesley.

16. Houghton, R.J., Baber, C., McMaster, R., Stanton, N.A., Salmon, P., Stewart, R. and Walker, G. (2005, in preparation). Command and control in emergency services operations: A social network analysis.

17. O_2 Airwave Service Website (n.d.) *About O_2 Airwave*. Accessed March 2005 (http://www.airwaveservice.co.uk/airwave5.asp)

18. Home Office Communications Directorate (2004) *Police Briefing, January 2004*, Just Customer Communication. Retrieved August 2004 from http://www.policereform.gov.uk/docs/policebriefingjan5.html

19. Burnett, M., Wooding, P., & Prekop, P. (2004). Sense Making - Underpinning Concepts and Relation to Military Decision-making. *9th International Command and Control Research and Technology Symposium* Copenhagen, Denmark, 14-16 September. CCRP, Washington, DC.

20. Perry, M (1999) The Application of individually and socially distributed cognition in workplace studies: two peas in a pod? *Proceedings of the European Conference on Cognitive Science, 1999*; Siena, Italy, p87-92.

21. Perry, M.J. and MACREDIE, R.D. (n.d.) Distributed cognition: investigating collaboration in large and highly complex organisational systems. Retrieved March 2005 from http://www.brunel.ac.uk/~cssrmjp/homefiles/papers/MP_RM.pdf