19th International Command & Control Research & Technology Symposium

"C2 Agility: Lessons Learned from Research and Operations"

Reconciling Hierarchical and Edge Organizations: 9-11 revisited

Paper ID 114

Topic(s)
Primary:

Topic 2. Organizational Concepts and Approaches

Alternate:

Topic 1: Concepts, Theory, and Policy

Topic 5: Modelling and Simulation

Names of Authors
Tim Grant & Erik de Waard

Point of Contact
Tim Grant

Retired But Active Researcher (R-BAR)

Koningin Wilhelminastraat 13, 3405 XP Benschop, The Netherlands

Tel: +31 (0)638 193 749

tim.grant.work@gmail.com

Abstract:

A recurring theme in the C2 literature is the organizational structure of military forces. Research homes in on the hierarchical and edge organizational forms. The contrast between them has become well understood, aided by the C2 approach space and the wide-spread use of the ELICIT platform. Simulation shows that edge organization is better suited to network-centric operations. However, few military forces have discarded the hierarchical structure, despite claiming to be networked. Hence, our research asks whether these two archetypal forms can be reconciled with one another.

By revisiting a case study of the events of September 11th, 2001, reported on in the 11th ICCRTS, we show that this apparent paradox can be resolved by distinguishing organizational structure from the

communication patterns that flow over that structure. The communication pattern can be easily changed by changing the rules for who to inform when something happens. This is consistent with representing organizations as layered networks, with units linking the layers and layers corresponding to the domains in the NCW value chain. The paper reviews the knowledge on hierarchical and edge organizations, outlines key ideas from network science and agent-based modelling, revisits the 9-11 thought experiment, and draws conclusions and makes recommendations.

1. INTRODUCTION

A recurring issue in the Command & Control (C2) literature is the organizational form best suited to network-centric operations. Drawing on Mintzberg's (1979) work on organizational archetypes, five classic organizational forms have been identified: the *simple structure*, the *machine bureaucracy*, the *professional bureaucracy*, the *divisionalized* form, and the *adhocracy*. The traditional military organizational form, namely the *hierarchy*, corresponds to the machine bureaucracy. Alberts & Hayes (2003) added a sixth form, the *edge organization*, characterized by a prominent operating core, emergent leadership, and the absence of technostructure and support staff.

In the C2 literature, the debate invariably focuses on the hierarchical and edge forms. While hierarchical organizations are suited to industrial-age C2, information-age C2 requires the agility offered by the edge organization. Crucially, as Table 1 shows, these two organizational forms differ in terms of the variables that Mintzberg (1979) uses to specify the different archetypes. Alberts & Nissen (2009) conclude that hierarchical and edge organizations are contrasting alternatives.

Table 1. Variables for hierarchy and edge (adapted from Alberts & Nissen, 2009, Tables 1 & 2).

Variable	Meaning	Hierarchy	Edge
Centralization	Breadth of decision rights	High	Low
Vertical specialization	Limitedness of job control	High	Low
Horizontal specialisation	Narrowness of job breadth	High	Low
Formalization	Formalization of work processes	High	Low
Liaison devices	Means of horizontal interaction	Few	Many
Planning & control	Management of output	Action planning	Performance control

Despite all the advantages claimed for network-centric operations over the past 15 years, military organizations cling stubbornly to the hierarchical form. How can military organizations claim to be network-centric or network-enabled without having adopted the edge organization? This would surely seem to be a clear case of "having your cake and eating it".

This paper offers a possible explanation. Drawing on ideas from network science, the paper argues that hierarchical and edge organizations can be reconciled by representing an organization as a layered network, with organizational units appearing as nodes in each network. The layers correspond to the domains in the NCW value chain. More specifically, the organizational structure defined by superior-subordinate relationships between units takes the form of a hierarchy[1]. These superior-subordinate relationships are in the socio-organizational domain. By contrast, organizational behaviour is expressed by a network of information passing over this organizational structure. Information-passing occurs in the information domain. When information runs predominantly vertically up and down the structure, then the organization behaves hierarchically. When information runs largely horizontally, then the organization exhibits edge behaviour. The computing and communications infrastructure – a third network, in the physical domain – must provide the connectivity to support the desired information passing pattern. To illustrate this explanation, the paper revisits the first author's 9-11 thought experiment from the 11th ICCRTS (Grant, 2006).

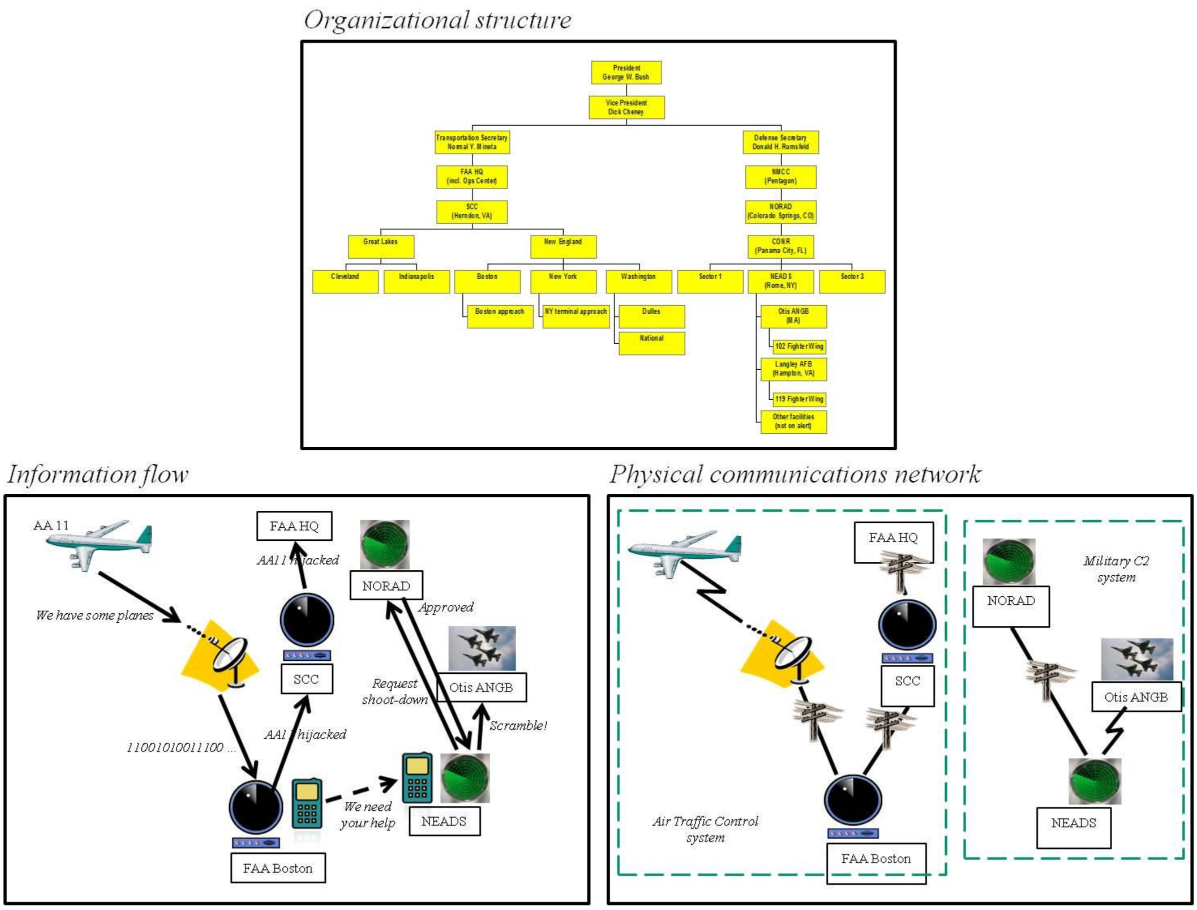

Figure 1. Organizational, information, and physical networks.

Taking our clue from 9-11, the organizational, information, and physical networks can be illustrated as shown in Figure 1. The organizational structure at the top of the figure shows the two

[1] Note that a hierarchy is a specialized form of network in which each unit has just one superior and superiors have one or more subordinates.

organizations involved: the Federal Aviation Authority (FAA) to the left and the US Department of Defense (DoD) to the right. Both have a hierarchical form, with the FAA being headed by the Transportation Secretary and the DoD by the Secretary of Defense. In essence, the FAA and US DoD represent a (civil-military) coalition. At a higher level, the two organizations report to the US President and Vice President.

Information flow is depicted to the left in Figure 1. The flow of information forms a chronological sequence of hops, shown as arrows. In network science terms, this is an example of a *directed* network or *digraph*. The flow of information starts when the hijacker of American Airlines flight 11 (AA11) broadcasts "We have some planes" on the FAA's radio frequencies. This is picked up by a radio mast and transmitted (possibly digitally, as shown here) to FAA's Boston centre, where a controller correctly interprets this as a sign that AA11 is hijacked. Following Standard Operating Procedures (SOPs), he/she informs the FAA's System Command Center (SCC). Detecting that the hijack involves violence, he/she also phones a friend in DoD's North Eastern Air Defense Sector (NEADS), asking for military help. In other words, the sequence branches at this point. The call to NEADS eventually results in an order to Otis ANGB to scramble its fighter jets. Note that the information passes through several of the units also shown in the organizational structure: FAA Boston, SCC, FAA HQ, NEADS, NORAD, and Otis ANGB.

The physical communications network is shown to the right in Figure 1. The communications network was partly wired (shown by the "telephone poles") and partly wireless (shown as "lightning flashes"). On September 11, 2001, the FAA's Air Traffic Control (ATC) system and the US DoD's military C2 system were separate from one another. It was not possible to exchange data between them. In network science terms, the physical communication network consisted of two *components* that were *unreachable* from one another. Note how the physical network enables (or, in this case, disables) certain patterns of information flow. It was the lack of interoperability between the ATC and C2 systems that meant that the two organizations had to exchange information by other means, namely mobile phone, telephone, and video-conferencing. As in the information network, the physical communications network includes several of the units shown in the organizational structure.

As well as drawing on ideas from network science, the paper elaborates these ideas taking concepts from agent-based modelling. Instead of regarding organizational units just as atomic nodes in a network, each node/unit is considered to have internal functionality for sensing, decision making, and acting (including communicating with other nodes/units). In short, each node/unit is considered to be an *agent*. How the node/unit/agent behaves is constrained by *norms*, which can be thought of as decision rules of the form IF <situation> THEN <action>. In particular, we consider *structural* and *dialogical* norms, i.e. those defining the organizational structure and those constraining how one agent communicates with others.

The purpose of this paper is to show how hierarchical and edge organizational forms may be reconciled using ideas drawn from network science and agent-based modelling. Organizations are represented as layered networks of units, with units' agent functionality being constrained by norms. Only structural and dialogical norms are discussed here.

There are five sections in this paper. Following this introductory section, section 2 reviews the relevant knowledge on hierarchy and edge organizations in organization and management theory

(OMT). Section 3 draws on the network science and agent-based modelling literature to reconcile the hierarchical and edge organizational forms. Section 4 illustrates these ideas by revisiting Grant's (2006) 9-11 thought experiment. Section 5 draws conclusions and makes recommendations for further work.

2. RELEVANT OMT: HIERARCHY VS. EDGE ORGANIZATION

Advocates of the edge organization argue that traditional, military hierarchical structures are best suited to take on symmetrical adversaries on a linear battlefield (Alberts & Hayes, 2003). Yet, the modern-day challenge of dealing with asymmetrical threats such as terrorists and insurgencies and operating in a nonlinear battlespace are said to be problematic for this type of organizational design. The ruling assumption within this research community is that the machine-like response patterns of traditional hierarchies do not support the speed, responsiveness, and creativity that is needed to cope with the uncertainties and unfamiliar situations of contemporary military operations. The key solution is found in a fundamental change in the C2 process. To be more precise, a three-dimensional shift has to take place in the key variables of the C2 process (Alberts & Nissen, 2009). First, regarding the allocation of decision rights (ADR) the focus has to shift from a single actor to a collective network approach. Second, regarding the patterns of interaction (PoI) a shift has to take place from constrained – highly formalized and tightly managed- to unconstrained. Third, the distribution of information (DoI) needs to develop from a tightly controlled information flow to a situation of widespread information sharing. It is believed that this three-dimensional shift makes military organizations more agile. First, because available information can be combined in new ways, tailored responses are stimulated. Second, because decision making authority is decentralized and less formalized, the speed of reaction increases.

Based on these assumptions, the C2 community has developed a toolkit, known as ELICIT, to empirically test the foundations of the new C2 process. In an ELICIT experiment, Thunholm et al. (2009) compare differences in decision speed, decision accuracy, and the level of shared correct situation awareness between a traditional hierarchy, an edge organization, and a hybrid form. Their main conclusion is that centralization versus decentralization is not an either/or question. Although, decentralization is an important attribute of networked operations, a certain level of centralized coordination remains important for the overall coordination of today's complex, multi-dimensional task setting. The experiment they conducted namely showed that the hybrid organization and the traditional hierarchy performed equally well on decision accuracy and situation awareness. The hybrid form only outperformed the hierarchy on speed of decision making.

Despite this interesting conclusion, the study only partly explains the importance of reconciling a centralized and decentralized organizational structure. Above all, this has to do with the fact that the focal point of the experiment is on the composition of decision making groups. Regarding the practical relevance of the experiment, Thunholm et al. (2009, p.9) state the following: "*Putting the game in real-world context, the organization can be seen as an intelligence organization that has to analyze incoming data and inform its client (or government) about the assessment*". Of course, these types of organizations generally play an important role within military operations. Staff elements at different organizational levels, supporting a commander in his decision making process, come to mind first. Yet, there is more to military task force performance than the C2 approach of staff elements.

Going back to the assumption that the key challenge of modern-day military deployment is dealing with unfamiliar and uncertain situations, it could be argued that, to learn more about the reconciliation of the hierarchical and edge organizational forms, the starting point of an academic discussion should not only be the composition of decision making groups but also the overarching design principles of a military formation. Organization theorist Galbraith (1973) explains that an organization confronted with a high level of uncertainty should ideally react in two ways. First, it should try to increase its information-processing capacity. Second, it should try to reduce its need for information processing. So far, the former path has received most attention within today's C2 community. The latter has remained rather underexposed. Regarding this latter path, Galbraith argues that creating self-contained organizational elements is an effective way of reducing an organization's need to process information.

Studying the evolutionary process of C2 from the Stone Age up to the Vietnam war, Van Creveld (1985) has embraced Galbraith's (1973) theory, concluding that dealing with uncertainty has been the essence of warfare throughout the ages. In an attempt to generalize from his historical analysis, he stresses that responsive military organizations will need to make low-decision thresholds possible by creating semi-autonomous units at a fairly low organizational level. He does not abandon the hierarchical structure as a whole. Instead, he supports the idea of merging a clear hierarchical chain of command with an inherent level of freedom for the frontline echelons. Van Creveld, first of all, refers to the successful blitzkrieg doctrine, which was strongly based on the operational autonomy of the German *pantzer* divisions, to make his point. Second, he explains that the self-controlling capacity of the three division-sized task forces, each consisting of three independent brigades, was the main reason for the clear Israeli victory in 1967.

Apart from these historical cases, more recent military experiences also support Galbraith's (1973) theory. For example, De Waard, Volberda and Soeters (2013) explain that the Netherlands Army of today follows a deployment strategy of fine-grained modularization. This is a strategy that basically goes against Galbraith's advice. Despite the fact that a brigade can be seen as the smallest military building block that has a sufficient combination of functional elements – the principle of combined arms – to conduct military operations autonomously for a lengthy period of time, the Netherlands Army has decided to abandon the brigade structure as its main unit of action. Experiences show that the new approach of mixing and matching all sorts of smaller functional organizational elements into customized task forces has had a negative impact on the ability of these customized formations to cope independently. First, unit cohesion suffers, because people and organizational elements have to work closely together without actually knowing each other. Second, additional staff elements have to be deployed to take on the task of coordinating the mixture of unfamiliar functional units. Third, a series of training programs are needed to lift the tailor-made structures to sufficient level of military professionalism.

All in all, this decision of fine-grained functional grouping has pushed the ability to cope from the frontline echelon to the operational commander and his staff. A central integrating role has become essential to overcome the internal organizational complexity that has been created. If the Netherlands' situation is projected to a higher order reality of multinational and multi-service military cooperation then one can well imagine that organizational complexity increases. Therefore, the existence of large-scale staff structures within most multinational military operations is no surprise. Yet, the risk involved is that these staff elements become preoccupied with the internal functioning of the composite military formation. Using Mintzberg's (1983) words, the staff then turns into a sort of technostructure that coordinates and standardizes work processes for the whole organization. However, when the staff starts to think and decide for frontline units then the organization strongly starts to resemble a centralized machine bureaucracy.

In this respect, the emergency response to the hurricane Katrina offers some useful additional insights. Majchrzak, Jarvenpaa, and Hollingshead (2007) explain that in the immediate aftermath of this disaster the formal response system failed, which had dramatic consequences. Referring to a government report they state: "*Despite the existence of these formal plans, extensive training, and bureaucratic structures, when the authority structure breaks down, as occurred during Katrina, so do the formal plans*". At the same time, they hail the US Coast Guard, as one of the few government agencies, for its responsiveness. The ability of the Coast Guard operational commanders to act relatively autonomously is seen as the main reason for their success in the field.

Implicitly, the Katrina study makes clear that a centralized complex network of interdependent organizations and organizational parts is vulnerable, since coordinating the activities of the different network members depends on a formal C2 hierarchy. If somewhere in this hierarchical line nodes are missing, unavailable, unanticipated, or in conflict - typical conditions for an unpredictable crisis situation - the decision-making process can become seriously jeopardized. If, on the contrary, a network consists of largely independent organizational building blocks, decision-making can be decentralized, which makes the network as a whole more resilient. It leads to a situation in which central command and its different network partners only discuss and decide on issues that concern the network as a whole. The vast majority of lower level decisions and coordination activities can be kept in the hands of the decentralized organizational parts, closest to where it all happens. This is, basically, how the Coast Guard operated in the emergency network after Katrina had struck. Its relative independence offered the Coast Guard commanders the possibility to make their own decisions and to improvise. For example, they accepted help from civilian boat operators to rescue people from the waterways. This had never been standard protocol in any emergency exercise, but turned out to be a very effective and efficient way of covering the vast crisis area.

Taking a step back from these practical experiences and re-focusing on the challenge of reconciling the hierarchical and edge organization, the key solution seems to lie in smartly combining hierarchical supervision with lower level organizational autonomy. In this respect, Weick (2004, p. 43) argues that contemporary organizational design is about embracing "the charm of the skeleton". With this skeleton metaphor Weick emphasises that a major pitfall in organizational design is over-specification. As a result, structures become too narrowly defined, inherently lacking the resilience to cope with uncertainties. Since flexibility, adaptability, and agility are words that can be read in almost every DoD policy report, less organizational specification seems to be the way to go for the military. More concrete, this points in the direction of a skeleton hierarchy, that smartly distributes power to the front line echelons, without losing overall control.

3. RECONCILING HIERARCHICAL AND EDGE ORGANIZATION

The approach that we propose for reconciling the hierarchical and edge organizational forms draws on ideas from network science and from agent-based modelling.

3.1 Layered Networks

Monsuur, Grant & Janssen (2011) introduced the idea of *layered networks*, in which some nodes may simultaneously belong to multiple networks. For example, consider military units. In the physical domain, commanders are interested in the units' locations and their possible routes to other locations. This can be modelled as a network, with units and locations as nodes and routes as arcs. Technically, the physical network is a *bipartite graph*, because there are two types of node (Newman, 2003). Moreover, the arcs may be *directed* if routes are one-way. In the information domain, commanders are interested in information, how it is distributed across units, and how information can be transmitted from one unit to another. This can be modelled as a network in which units and pieces of information are nodes and telecommunication links as arcs. This information network is again a bipartite graph, and the arcs may be directed. In addition, arcs may be weighted according to their bandwidth and typed to show what level of secrecy they can provide to the information carried. In the socio-organizational domain, commanders are interested the formal and informal relationships between units. The units are nodes and the relationships are arcs in a social network. These arcs may have several types, e.g. to show whether they are formal or informal. If the relationship is formal, then the arc representing it may be directed to show which node represents the superior.

The key point is that military units appear as nodes in several networks. This implies that the networks are interleaved. Monsuur et al (2011) provide the mathematics for modelling the influences from one network to another. On the basis of the NEC literature, Grant (2014) argues that networks form a series of layers, with the geographical layer at the bottom, the physical, information, and cognitive layers in turn above, and the socio-organizational layer at the top.

3.2 Agent-Based Organization

Agent-based modelling brings in the idea of *agency*, namely that entities are capable of sensing their environment, taking decisions based on sensed information, and acting autonomously. Moreover, agents can communicate with one another. Applied to networks, this allows nodes and arcs to be more than atomic entities, perhaps with attributes (e.g. a type, a weighting, a direction, etc.) More specifically, nodes and arcs can have internal structure. This addresses one of the key criticisms of network science, whereby networks only model the structure of a real-world phenomenon, but not its functionality.

In artificial intelligence, the agents (i.e. nodes) are often structured internally according to the Beliefs, Desires, and Intentions (BDI) model of agency (Georgeff, Pell, Pollack, Tambe, & Wooldridge, 1999). In C2 applications, the agents represent organizational units. Moreover, an obvious candidate for structuring agents internally is Boyd's (1996) Observe-Orient-Decide-Act (OODA) loop or similar C2 functionality (Grant & Kooter, 2005) (Brehmer, 2005) (Jensen, 2014). BDI and OODA can be regarded as being duals of one another. Grant (2011) proposed a corresponding internal process model for communication arcs in network-enabled C2 systems.

3.3 Organizational Norms

Several researchers have applied agent-based modelling to represent organizations (Ferber, Gutknecht, Jonker, Müller & Treur, 2000) (Dignum, 2004) (Horling & Lesser, 2005). Very simple organizations may consist of a handful of people, but most organizations are sub-divided into a variety of groups, such as departments, divisions, regions, business units, teams, and the like. There may also be several levels of sub-division, generally known as *echelons* in military terminology. We will use the generic term “unit” for an organizational group, whatever its size or level in the organization. Usually, several lower-level units report to a single unit at the next higher level, resulting in an organizational hierarchy. However, variants that are not strictly hierarchical are possible, as in matrix organizations. One of these is the edge organization, which can be regarded as a “flat” hierarchy, i.e. one with no more than two levels.

In agent-based models of organizations, each unit is usually represented as an agent. Since this brings with it the standard internal structure and functionality of agents, the resulting organization is inherently modular. Standard information exchange representations and communication protocols ensure that the units can communicate with and understand one another. The agents’ behaviour and interactions must be constrained in some way. One way is to provide them with a common set of goals, because this distinguishes an organization from an arbitrary collection of agents. To supplement this, each unit has associated with it a set of norms and/or values, effectively representing the unit’s “organizational culture”. An agent joining the group is expected to comply with these norms and values. In certain situations, agents that fail to comply may be punished or even expelled from the group. Researchers have modelled all of these mechanisms, together with how a group’s set of norms and values may evolve over time and how an agent resolves conflicts between norms and values when it is a member of multiple groups simultaneously.

In the agent-based modelling literature, norms are often represented as IF-THEN rules. Researchers have distinguished several categories of norm. Coutinho et al (2005) distinguishes structural, functional, deontic, and dialogical norms. *Structural norms* define the agents’ relations through the notions of roles, groups, and links. *Functional norms* describe how a multi-agent system decomposes its global goals (as *plans*) and passes the decomposed goals to the agents (as *missions* or *tasks*). *Deontic norms* describe how the agent is permitted to, obliged to, or prohibited from behaving. *Dialogical norms* define the valid illocutions that agents may exchange (i.e. they respect a common ontology, knowledge representation language, and communication language), the protocols used to exchange them, and with which other agents these illocutions may be exchanged. Norms have an obvious C2 application in representing doctrine, rules of engagement, and the like. In this paper, we will focus on structural and dialogical norms, i.e. how organizations are structured into units, and how the communication between these organizational units is constrained.

4. 9-11 REVISITED

4.1 Thought Experiment

In the 11th ICCRTS, the first author presented the results of a thought experiment in NCW based on the events of September 11, 2001 (Grant, 2006). The objective of the thought experiment was to validate the NCW value chain. In retrospect, this thought experiment can also serve to show how organizations can be regarded as agent-based, layered networks, enabling the hierarchical and edge organisational forms to be reconciled with one another.

The thought experiment focused on the events from the viewpoint of the cooperation between civil air traffic control (ATC), as embodied in the Federal Aviation Authority (FAA), and military air defence (AD), as embodied in the North American Aerospace Defense Command (NORAD). Source material was drawn from the final report of the National Commission on Terrorist Attacks upon the United States (9/11 Commission, 2004) and the declassified timeline for September 11, 2001 (9/11 Commission, 2005). Additional material in a series of articles from Aviation Week & Space Technology provided insights into events within the FAA (AWST, 2001) and NORAD (AWST, 2002a/b) and from the fighter pilots' viewpoint (AWST, 2002c).

The 9/11 Commission report (2004, p.17-18) describes the protocols for the FAA to obtain military assistance from NORAD, as they existed on September 11, 2001. These protocols assumed that the aircraft pilot would notify the FAA controller of a hijacking by radio or by "squawking" a Secondary Surveillance Radar (SSR) transponder code of "7500". Controllers would notify their supervisors, who would in turn inform management all the way up to FAA Headquarters in Washington DC. FAA Headquarters had a hijack coordinator, who would contact the Pentagon's National Military Command Center (NMCC) to ask for a military aircraft to follow the flight, to report anything unusual, and to aid search and rescue in the event of an emergency. The NMCC would seek approval from the Office of the Secretary of Defense to provide military assistance. If approval was given, the orders would be transmitted down NORAD's chain of command. The protocols did not contemplate an intercept, assuming that the fighter escort would take up a position five miles directly behind the hijacked aircraft from where it could monitor the aircraft's flight path. Based on this description, Grant (2006) depicted the organizational structure and reporting chain, as it should have happened, as shown in Figure 2.

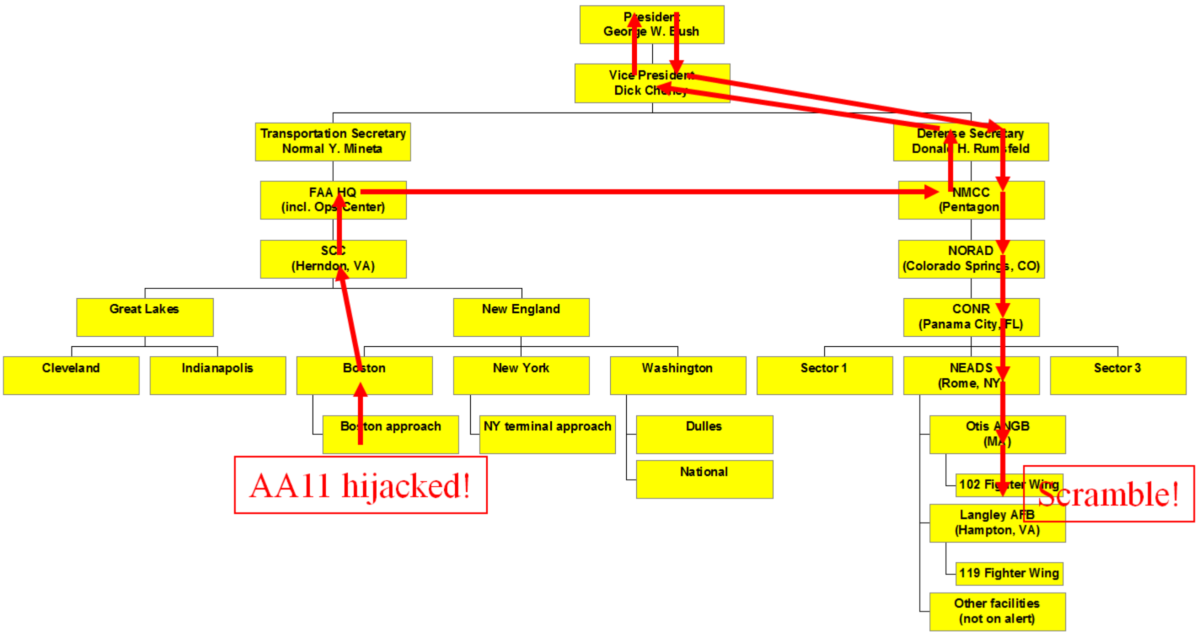

Figure 2. 9-11 reporting chain, as it should have happened (Grant, 2006, figure 3).

Figure 2 depicts as organisational hierarchies the units involved in the events of September 11, 2001, from the FAA and the Defense Department (including the Pentagon and NORAD), plus the US President and Vice President. The yellow rectangles show the units, linked together by superior-subordinate relationships (grey lines). The superior unit is higher up in the figure. For example, the FAA's System Command Center (SCC) is shown as being subordinate to FAA HQ, and with the FAA Great Lakes and New England regions as its subordinates. Likewise, on the military side of the figure, Otis Air National Guard Base (ANGB) and Langley Air Force Base (AFB) are subordinate to the North Eastern Air Defense Sector (NEADS).

The reporting chain, shown as a series of red arrows, is overlain on the organizational hierarchies. With the exception of the FAA hijack coordinator in the FAA HQ, all reports in Figure 2 go up the hierarchy, following the superior-subordinate relationships. Orders go down the hierarchy, again following the superior-subordinate relationships. The arc from the FAA hijack coordinator to the NMCC is neither a report nor an order, but a request (for assistance) going from one organizational hierarchy to another. With the exception of this request, the reporting chain mirrors the organizational structure.

As the 9/11 Commission report states, the pre-existing protocols (2004, p.18) "*presumed that:*

- *The hijacked aircraft would be readily identifiable and would not attempt to disappear;*
- *There would be time to address the problem through the appropriate FAA and NORAD chains of command; and*
- *The hijacking would take the traditional form: that is, it would not be a suicide hijacking designed to convert the aircraft into a guided missile.*

On the morning of 9/11, the existing protocol was unsuited in every respect for what was about to happen."

Figure 3 shows what actually happened following the hijacking of American Airlines 11 (AA11), again taken from the 9/11 Commission report. The report states (9/11 Commission, 2004, p.18, bold emphasis added) that "*Boston Center did not follow the protocol in seeking military assistance through the prescribed chain of command.* ***In addition to notifications within the FAA****, Boston Center took the initiative, at 8:34, to contact the military ... . At 8:37:52, Boston Center reached NEADS. This was the first notification received by the military – at any level that American 11 had been hijacked*". The additional notification from Boston Center to NEADS is shown as a red arrow running horizontally across to NEADS. The detailed description in (AWST, 2002a) shows that this was a report, not a request for assistance. Moreover, a similar across-organization report was generated by a controller in Boston Approach to a friend at Otis ANGB, also shown in Figure 3. In both cases, the Boston controllers used their mobile telephones, rather than the FAA's communications infrastructure. By contrast, the request that should have gone from the FAA hijack coordinator to the NMCC did not happen, as the 9/11 Commission report notes (ibid., p.19) but without giving an explanation[2].

---

[2] The first author understands that the hijack coordinator was on vacation, and his deputy had not yet been trained in requesting assistance from the NMCC.

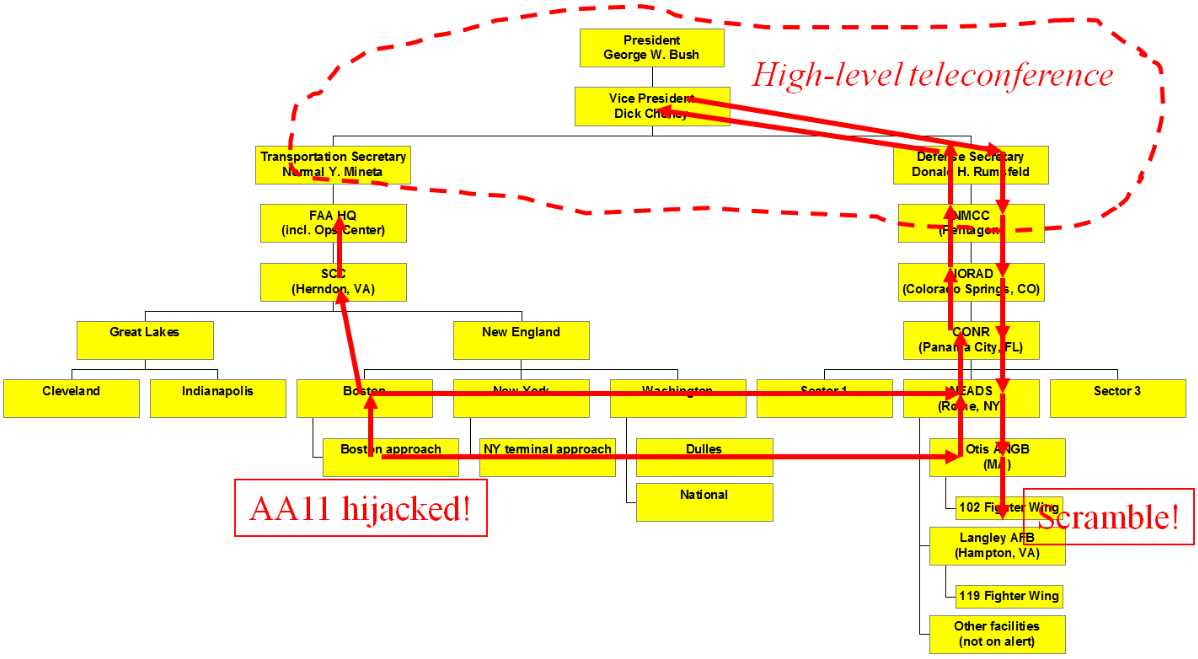

Figure 3. 9-11 reporting chain, as it actually happened (Grant, 2006, figure 4).

What is difficult to depict in Figure 3 is that the Battle Commander in NEADS telephoned his superior in NORAD seeking authorization to scramble the Otis fighters. His superior instructed the NEADS Battle Commander to "*go ahead and scramble them, and we'll get authorities later*" (9/11 Commission, 2004, p.20). In short, the scramble orders from NORAD progressed down the hierarchy to the 102 Fighter Wing at Otis *in parallel with* the reporting upward from NORAD to the President. Only after a protracted high-level teleconference did the formal authorization come down the hierarchy to back up what the NORAD commander had done on his own initiative. By the time that this happened, all four hijacked aircraft had already crashed. Analysis of the corresponding timeline showed that the NORAD commander's use of his own initiative, together with the across-organization reporting from the FAA to NEADS, had saved around 70 minutes.

Inspection of Figure 3 shows that, in addition to following the protocol, FAA's Boston Center and Boston Approach had effectively performed self-synchronization by informing their friends in NEADS and Otis. What actually happened, then, was both hierarchical and edge in nature. Indeed, it was most fortunate that self-synchronization happened. If the two Boston controllers had not informed their military contacts, then the reporting chain would have been interrupted when it reached the FAA hijack coordinator, delaying the US response for an indeterminate length of time. Moreover, the controllers' actions created the opportunity for the NORAD commander to use his initiative.

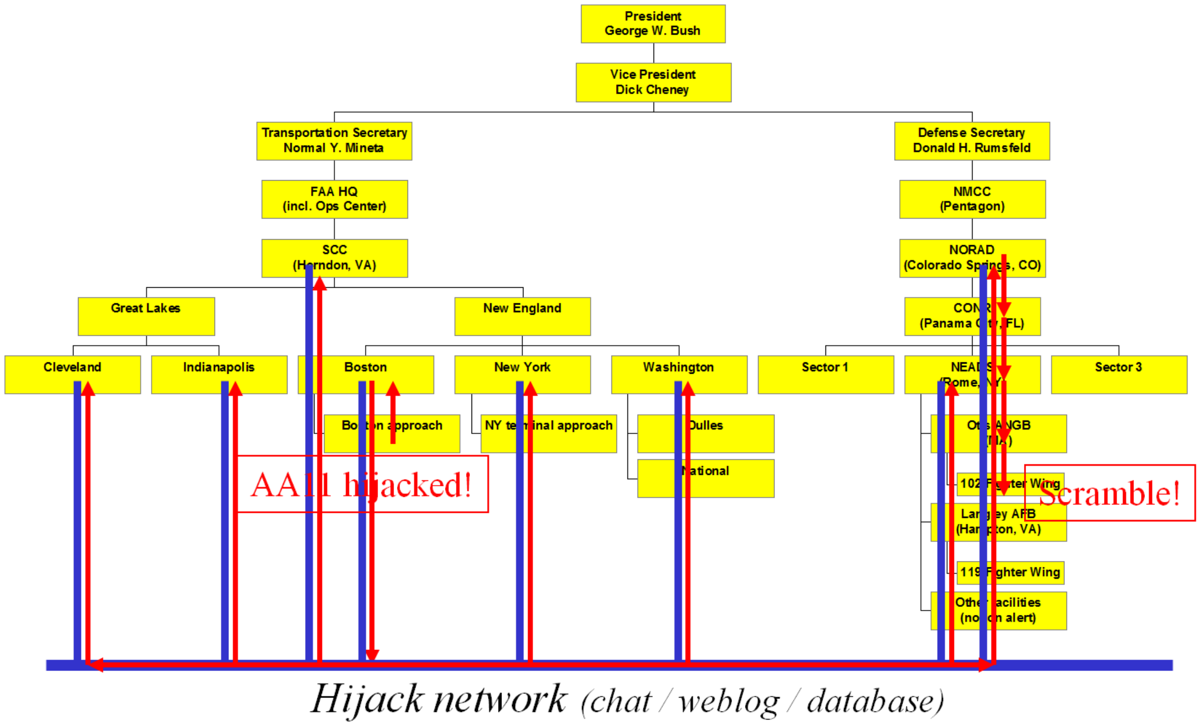

Figure 4. 9-11 reporting chain, as it could have happened (fully networked) (Grant, 2006, figure 5).

In his thought experiment, Grant (2006) extended this line of thinking by identifying a third – hypothetical – case, in which all those involved in responding to the hijackings on September 11, 2001, were fully networked. With suitable technology, anyone suspecting that an aircraft had been hijacked could notify this to all units via a hijack network, shown in blue in Figure 4. Immediately, all hijack network users would be made aware of the situation, without having to wait until the report had made its way step-by-step up the FAA organization and across to the NMCC. Timeline analysis (Grant, 2006) showed a further saving of 12 minutes, assuming that the NORAD commander would have again used his initiative.

4.2 Analysis

For the purposes of this paper, we note that Figure 2 and Figure 3 show two networks overlaid on one another, exactly as Monsuur et al (2011) assumed. The structural hierarchy, defined in terms of the superior-subordinate relationships between organizational units, is shown as yellow rectangles joined by grey lines. Overlaid on the structural hierarchy is a network of messages passing information from one unit to another. A third network appears in Figure 4, representing the physical computing and communications infrastructure used to transmit these messages.

Looking at these Figures, it can be seen that the structural hierarchy remains identical in all three cases. The structure does not need to change in going from the (almost) fully hierarchical case that the pre-existing protocol called for, through the combined hierarchical and edge case that actually happened, to the (hypothetical) fully-networked case. What changes from one case to the next is the shape of the information-passing network. The physical network is merely enabling; it must not preclude or restrict the desired pattern of information passing. For example, if the two Boston controllers had been restricted to using the FAA's communications infrastructure, then they would have been unable to contact their friends in the military. Fortunately, they possessed – and were allowed to use – mobile telephones[3] that supported communication with anyone whose number they knew.

Using (dialogical) norms, it would be easy to change the way in which information is passed between agents. This can be done for each of the three cases, as follows:

- *Should have happened*. The pre-9/11 protocol for FAA controllers could be expressed as the following rule:

IF you receive information that an aircraft has been hijacked **THEN** pass the information to your superior.

The FAA hijack coordinator would also have had an additional rule stating that:

IF you receive information that an aircraft has been hijacked **AND** violence has been used **THEN** pass the information to the NMCC **AND** request military assistance from them.

- *Actually happened*. In the actual event, the FAA Boston controllers acted as if they were obeying the following two rules, both of which matched the situation:

IF you receive information that an aircraft has been hijacked **THEN** pass the information to your superior.

IF you receive information that an aircraft has been hijacked **AND** violence has been used **AND** you have a friend in the military **THEN** pass the information to your friend.

- *Could have happened*. The fully-networked case could be expressed as the rule:

IF you receive information that an aircraft has been hijacked **AND** the information is not already on the hijack network **THEN** post the information on the hijack network.

In summary, the 9-11 thought experiment has shown that it is possible to alter the behaviour of an organization without changing its structure by giving the organizational units different sets of norms. The underlying computing and communications infrastructure must permit this pattern of behaviour. More specifically, given the appropriate dialogical norms, network-centric behaviour typical of edge organizations can be expressed by an organizational hierarchy supported by communications infrastructure with a networked connectivity. Moreover, norms can be readily changed, making the organization flexible, adaptable, and agile.

5. CONCLUSIONS AND FURTHER WORK

The hierarchical and edge organizational forms have been contrasted in the C2 literature. While the hierarchical organization is suited to industrial-age C2, information-age C2 requires the agility

[3] Other technologies, such as the public switched telephone network (i.e. landlines), email, or social media, could also have made this possible, assuming the parties at both ends had access to and were allowed to use them.

offered by the edge organization. Despite all the advantages claimed for network-centric operations over the past 15 years, military organizations are still structured as hierarchies, yet claim to be network-centric. This would seem to be paradoxical.

This paper offers a possible explanation, by showing how hierarchical and edge organizational forms may be reconciled using ideas drawn from network science and agent-based modelling. Organizations may be regarded as consisting of layered networks, with these networks in different C2 domains. The superior-subordinate relationships between units defines a structural hierarchy in the socio-organizational domain. The pattern of information passing defines a network in the information domain. Computing and communications infrastructure is networked in the physical domain. Units are more than just atomic nodes, but possess functionality for sensing their environment, decision making, and acting (including communicating with other units), i.e. they can be regarded as agents. Their structure and behaviour can be constrained using norms, which are readily changed to smartly suit the prevailing situation, so implementing Weick's (2004) "skeleton" hierarchy. Moreover, the units link the networks. Monsuur et al (2011) provides the appropriate mathematics for modelling such linked, layered networks.

These ideas are illustrated by revisiting a case study of the events of September 11, 2001, used as a thought experiment in the 11th ICCRTS (Grant, 2006). Based on the 9/11 Commission Report (9/11 Commission, 2004) and declassified timeline (9/11 Commission, 2005), this case study analyses the communication within and between the FAA and NORAD resulting from the hijacking of American Airlines 11, both as this should have happened according to the pre-existing protocols and as this actually happened on the day. A third, hypothetical case analyses what could have happened if the FAA and NORAD had been fully networked on September 11, 2001. The case study shows that different communication patterns can play over the same (hierarchical) organizational structure. Finally, the analysis shows how the different communication patterns can readily be altered by changing the rules defining each unit's communication behaviour (a.k.a. dialogical norms).

The main contribution of this paper is that it has decoupled organizational structure from the pattern of communications running over this structure. This allows the hierarchical structure to remain unchanged while the organizational behaviour varies from hierarchical to edge/networked in response to changes in the dialogical norms given to the organizational units. The limitations are that the ideas have only been tested against a single case study.

Further work is needed to elaborate and validate the ideas presented in this paper. An obvious step would be to implement an agent-based simulation with the agents' structure and behaviour being constrained by IF-THEN rules representing norms. This should be used to reproduce the three cases in the 9-11 thought experiment. When this has been achieved, the simulation could then be applied to a variety of other scenarios.

References

9/11 Commission. (2004). *The 9/11 Commission Report: Final report of the national commission on terrorist attacks on the United States*. Washington DC: US Government Printing Office.

9/11 Commission. (2005). *Staff Monograph on the "Four Flights and Civil Aviation Security"*. Posted on US Government National Archives website, 12 September 2005. Retrieved 4 November 2005 from http://www.archives.gov/research/9-11-commission/.

Alberts, D.S. & Hayes, R.E. (1999). *Network Centric Warfare: Developing and leveraging information superiority*. 2nd edition, Washington DC: US DoD Command & Control Research Program.

Alberts, D.S. & Hayes, R.E. (2003). *Power to the Edge: Command Control in the information age*. Washington DC: US DoD Command & Control Research Program.

Alberts, D.S. & Hayes, R.E. (2006). *Understanding Command and Control*. Washington DC: US DoD Command & Control Research Program.

Alberts, D.S. & Hayes, R.E. (2007). *Planning: Complex endeavors*. Washington DC: US DoD Command & Control Research Program.

Alberts, D.S., & Nissen, H.E. (2009). Toward Harmonizing Command and Control with Organization and Management Theory. *International C2 Journal*, 3(2), 1-59.

AWST. (2001). *Crisis at Herndon: 11 Airplanes Astray*. Aviation Week & Space Technology, 155, 25, pp. 96-99, 17 December 2001.

AWST (2002a). *Exercise Jump-starts Response to Attacks*. Aviation Week & Space Technology, 156, 22, pp. 48-52, 3 June 2002.

AWST (2002b). *NORAD and FAA Sharpen View Inside Borders*. Aviation Week & Space Technology, 156, 23, pp. 50-52, 10 June 2002.

AWST (2002c). *F-16 Pilots Considered Ramming Flight 93*. Aviation Week & Space Technology, 157, 11, pp. 71-74, 9 September 2002.

Boyd, J.R. (1996). *The Essence of Winning and Losing*. Unpublished lecture notes, Maxwell Air Force Base, AL.

Brehmer, B. (2005). The Dynamic OODA Loop: Amalgamating Boyd's OODA loop and the cybernetic approach to Command and Control. In Alberts, D.S. (Ed.), Proceedings, 10th International Command & Control Research & Technology Symposium, Washington DC: US DoD Command & Control Research Program.

Coutinho, L.R., Sichman, J.S., & Boissier, O. (2005). Modeling Organization in Multi-Agent Systems: A comparison of models. Proceedings, SEAS 2005.

De Waard, E. J., Volberda, H. W., & Soeters, J. (2013). Drivers of Organizational Responsiveness: Experiences of a military crisis response organization. *Journal of Organization Design*, 2(2), 1-13.

Dignum, V. (2004). A Model for Organizational Interaction: Based on agents, founded in logic. Unpublished PhD thesis, University of Utrecht, The Netherlands.

Ferber, J., Gutknecht, O., & Jonker, C.M., Müller, J-P., & Treur, J. (2000). Organization Models and Behavioral Requirements Specification for Multi-Agent Systems. In International Conference on Multi-Agent Systems (pp. 0387-0387). IEEE Computer Society.

Galbraith, J.R. (1973). *Designing Complex Organizations*. Reading, Massachusetts: Addison-Wesley.

Georgeff, M., Pell, B., Pollack, M., Tambe, M., & Wooldridge, M. (1999). The Belief-Desire-Intention Model of Agency. In *Intelligent Agents V: Agents Theories, Architectures, and Languages* (pp. 1-10). Berlin Heidelberg: Springer.

Grant, T.J., & Kooter, B.M. (2005). Comparing OODA and Other Models as Operational View Architecture. In Alberts, D.S. (Ed.), Proceedings, 10th International Command & Control Research & Technology Symposium (paper 196), Washington DC: US DoD Command & Control Research Program.

Grant, T.J. (2006). Measuring the Potential Benefits of NCW: 9/11 as case study. In Alberts, D.S. (Ed.), Proceedings, 11th International Command & Control Research & Technology Symposium (paper 103), Washington DC: US DoD Command & Control Research Program.

Grant, T.J. (2011). Combining Information Sharing and Seeking in Networked Coalitions. In Santos, M.A., Dugdale, J., & Medonça, D. (Eds.), Proceedings, 8th international conference in Information Systems for Crisis Response And Management (paper 253), Lisbon, Portugal: ISCRAM.

Grant, T.J. (2014). Formalized Ontology for Representing C2 Systems as Layered Networks. In Grant, T.J., Janssen, R.H.P., & Monsuur, H. (Eds.). *Network Topology in Command and Control: Organization, operation, and evolution*. Hearshey, PA: IGI Global, chapter 5.

Horling, B., & Lesser, V. (2005). A Survey of Multi-Agent Organizational Paradigms. *Knowledge Engineering Review*, 19 (4), 281-316.

Jensen, E. (2014). Modelling Command and Control in Networks. In Grant, T.J., Janssen, R.H.P., & Monsuur, H. (Eds.). *Network Topology in Command and Control: Organization, operation, and evolution*. Hearshey, PA: IGI Global, chapter 4.

Lewis, T.G. (2009). *Network Science: Theory and applications*. Hoboken, NJ: John Wiley & Sons.

Majchrzak, A., Jarvenpaa, S.L., & Hollingshead, A.B. (2007). Coordinating Expertise Among Emergent Groups Responding to Disasters. *Organization Science*, 18(1), 147-161.

Mintzberg, H. (1979). *The Structuring of Organizations: A synthesis of the research*. Englewood Cliffs, NJ: Prentice-Hall.

Mintzberg, H. (1983). *Structure in Fives: Designing effective organizations*. Englewood Cliffs, N.J.: Prentice-Hall.

Monsuur, H., Grant, T.J. & Janssen, R.H.P. (2011). Network Topology of Military Command & Control Systems: Where axioms and action meet. In Bauer, J.P. (Ed.), *Computer Science, Technology, and Applications, vol 3* (pp.1-27). Hauppauge, NY: Nova Science Publishers, Inc.

Thunholm, P., Chong, N.E., Cheah, M., Kin Yong, T., Chua, N., & Ching Lian, C. (2009). Exploring Alternative Edge versus Hierarchy C2 Organizations using the ELICIT Platform with Configurable Chat System. *International C2 Journal*, 3(2), 1-52.

Van Creveld, M. (1985). *Command in War*. Cambridge: Harvard University Press.

Weick, K. E. (2004). Rethinking Organizational Design. In R. J. Boland & F. Collopy (Eds.), *Managing as Designing* (pp. 36-53). Stanford: Stanford University Press.