

# Modelling Network-Enabled C2 using Multiple Agents and Social Networks

Tim Grant<sup>12</sup>

**Abstract.** This paper describes work in progress in developing an architecture for Command & Control systems based on an empirical model of the military commander's thinking processes. It shows how social network constructs could be added to a multi-agent system to model network-enabled capabilities in a complex, real-world domain, using the events of September 11, 2001, as a case study. Areas for further research are identified.

## 1 INTRODUCTION

Military operations have changed dramatically in nature since the end of the Cold War in 1989. Nowadays, coalitions are formed from the forces of many nations ("combined operations") and multiple services ("joint operations"), allied with civilian organizations such as commercial suppliers, government departments, international and non-governmental organizations, and the media ("civil-military cooperation"). Instead of all-out warfare, operations may take the form of defence, diplomacy, and development (the "three D's"), often simultaneously.



**Figure 1. RNLA's Battlefield Management System.**

In military organizations, monitoring and control of operations is known as Command & Control (C2), defined as: "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission" [1]. C2 functions include "planning, directing, coordinating, and controlling forces and operations", and a C2 system consists of "an arrangement of

personnel, equipment, communications, facilities, and procedures".

The dramatic changes in the nature of military operations, coupled with developments in Information and Communication Technologies (ICT), have required equally dramatic changes in military C2. Twenty years ago, communications in-theatre were by voice or morse code over VHF/UHF radio, with the positions of own and enemy forces being plotted on paper maps using pencils. Long distance communications were by telex or by voice over HF radio. Today, military vehicles are fitted with GPS receivers, and broadcast their position periodically by data messages over Combat Net Radio to the superior commander and to other vehicles from the same unit. A in-vehicle display (see Figure 1) shows the position of all vehicles in the unit, automatically plotted in real time on a map or satellite photograph of the area. The same display can be copied by satellite links to headquarters, possibly thousands of kilometres away, or by data links to friendly ships and aircraft. The same system can be used to disseminate operational orders from the commander to all vehicles in the unit, as well as providing email and chat functionality. The key benefit is increased C2 tempo and agility.

These changes have less visible organizational consequences. Linking all units, vehicles, ships, aircraft, and individual soldiers, sailors, and airmen to headquarters means that the entire military organization will soon be networked together. Instead of emphasizing the flow of formal communications (situation reports and operations orders) up and down the organizational hierarchy, peer-to-peer communications and collaborative processes are becoming increasingly important. Trials and small-scale operational applications have shown that there are several pitfalls, including information overload and the temptation for high-ranking officers to micro-manage operations. Military doctrine must change accordingly. The NATO term for the desired future state is Network-Enabled Capabilities (NEC)<sup>3</sup>, defined as "the Alliance's cognitive and technical ability to federate the various components of the operational environment, from the strategic level (including NATO headquarters) down to the tactical levels, through a networking and information infrastructure (NII)" [2].

Modern C2 system architectures must reflect these changing needs. As the NATO definition shows, a NEC-era C2 system is seen as a federation of units networked to one another, lending itself to agent-based architectures. In 2005, the Netherlands Defence Academy initiated a Network-Enabled C2 Systems research project entitled "Beyond Situation Awareness" aimed at addressing the research question: "Is it feasible and advantageous in terms of operational agility to construct NEC-

<sup>1</sup> Faculty of Military Sciences, Netherlands Defence Academy, P.O. Box 90.002, Breda, Netherlands. Email: [t.j.grant@nlda.nl](mailto:t.j.grant@nlda.nl).

<sup>2</sup> Also visiting Professor, Department of Computer Science, University of Pretoria, South Africa. Email: [tgrant@cs.up.ac.za](mailto:tgrant@cs.up.ac.za).

<sup>3</sup> Known in the USA as Network-Centric Operations.

era C2 system architectures based on the human users' needs, functions, and thinking processes?"

The starting point for the project was US Air Force Colonel John Boyd's [3] Observe-Orient-Decide-Act (OODA) model of the military commander's decision-making process. Although it is an empirical – rather than scientific – process model, OODA is taught widely in military academies throughout NATO. It is the *de facto* standard way of modelling the military C2 process, in effect having been extensively peer-reviewed.

The first step in the project was to benchmark OODA against similar process models in the psychological and cybernetics literatures. This disclosed shortcomings [4] that were addressed by rationally reconstructing OODA [5]. Two Masters students from the University of Liverpool (UK) developed an initial test-bed based on the rationally reconstructed OODA (OODA-RR) model, demonstrating it using the domain of a computer intruder ("hacker") versus a system administrator [6] [7] [8].

As the HackSim domain lacks any organizational features<sup>4</sup>, the next step is to apply the test-bed to a larger, more representative domain, such as the US civil-military Air Traffic Control (ATC) / air defence (AD) organization that attempted (unsuccessfully) to shoot down Al Qaeda's hijacked airliners on September 11, 2001. Analysis [9] shows that this domain includes examples of communication up, down, across, and between hierarchies. Moreover, the communication flow differs according to whether events unfolded as *should have* happened given the Standard Operating Procedures (SOPs) then in force, as they *actually did* happen, and as they *could have* happened if the ATC / AD organization had been linked using NEC. Hence, the 9/11 domain is a worthy test for social network techniques.

The purpose of this paper is to show how social network constructs could be added to an OODA-RR-based multi-agent system to model network-enabled capabilities in military Command & Control. Coming from the multi-agent systems community, this paper addresses the first SNAMAS'09 research question: how to use social network analysis results for developing multi-agent systems. The key contribution is as a demonstration of how a complex, real-world domain (namely military C2) can be translated into theoretical constructs in the social network field. A major limitation is that the paper describes work in progress that has not yet been tested by implementing and evaluating it.

The paper consists of seven sections. Section 2 outlines the organizational aspects of present-day military Command & Control (C2). Section 3 summarizes the transformation to Network-Enabled Capabilities (NEC). Section 4 describes the rationally reconstructed OODA (OODA-RR) model and the HackSim test-bed. Section 5 illustrates the issues using the events of September 11, 2001, as a case study. Section 6 shows how social network constructs could be added to OODA-RR to model NEC. Section 7 draws conclusions and identifies directions for future work.

## 2 MILITARY COMMAND & CONTROL

Organizational structure allows authority, responsibilities, and processes to be allocated to organizational entities such as

individuals, work groups, (project) teams, departments, sites, branches, organizations, consortia, and coalitions. The predominant relationship that defines organizational structure is one of power: a superior has power to give instructions and assign tasks to his/her subordinates. Power is often expressed in terms of resources. These resources may be measured in terms of money, manpower, or equipment. For example, the military commander who is assigned a squadron of 12 fighter aircraft has more power than one who has a flight of four fighters.

There is a variety of organizational structures. An organization may have a charismatic, bureaucratic, cooperative, functional, matrix, flat, network, or virtual structure. Present-day military organizations are mature, complex, and large-scale and are invariably hierarchical. Since military forces have become highly specialized, they often exhibit strongly bureaucratic traits. Because military commanders may have to order their subordinates to put their lives at risk, there are strong legal requirements attached to the superior-subordinate relationship. Operational communication in a military organization is highly formalized, with subordinates transmitting situation reports ("sitreps") up the hierarchy to their superior, and superiors disseminating operation orders ("op-orders") down the hierarchy to their subordinates. The path that sitreps and op-orders follow up and down the organizational hierarchy is known as the "reporting chain". The formats for sitreps and op-orders, the terminology to be used, and the circumstances in which they should be created is strictly prescribed by doctrine.

The fundamental functionality that C2 systems provide is one of communication between elements of a military force. Since modern military forces are highly mobile and may be widely spread over the operational area, the primary communications gap that a C2 system must bridge is one of geographical separation. The communications infrastructure in-theatre must be wire-less, with wired infrastructures only being feasible in fixed locations such as (air)bases, harbours, and headquarters. At the same time, C2 systems must bridge communications gaps between levels in the organizational hierarchy, between specializations, and between different services (i.e. army, navy, and air force).

Superimposed on top of the communications functionality, C2 systems must support the decision-making process at each level in the organizational hierarchy. Decision making involves aggregating, interpreting, and combining the sitreps a commander receives from his/her subordinates into an overall picture of the operational situation. Psychological research in the field of situation awareness shows that building up accurate and timely awareness of the prevailing situation is necessary (but not sufficient) for the commander to make good decisions [10]. The operational picture is a key input for the sitrep that the commander must make to his/her own superior. More importantly, the operational picture forms the basis for selecting responses to the situation, for generating courses of action that will bring about the selected response, and for developing the operations orders that incisively describe the commander's intentions.

Boyd's OODA loop is the canonical model for describing the military decision-making process. As Boyd drew it (see Figure 2), OODA is a cyclic model of four processes. By implication, the OODA processes are possessed by an agent that interacts competitively with other such agents in the environment. Boyd emphasized the Orient process both graphically and in text. He

---

<sup>4</sup> Other than the adversarial relationship between the intruder and the system administrator.

described the Orient process in the following terms [11, underlining in original]: “Orientation is an interactive process of many-sided implicit cross-referencing projections, empathies, correlations, and rejections that is shaped by and shapes the interplay of genetic heritage, cultural tradition, previous experience, and unfolding circumstances. ... Orientation is the schwerpunkt. It shapes the way ... we observe, the way we decide, the way we act.” By contrast, he did not detail the three other processes. We interpret these three processes as follows:

- Observe is the process of acquiring information about the environment by interacting with it, by sensing it, or receiving messages about it.
- Decide is the process of making a choice among hypotheses about the environmental situation and among the possible responses to that situation.
- Act is the process of testing the chosen hypothesis by interacting with the environment and of generating expectations about the environmental response for subsequent Orientation purposes.

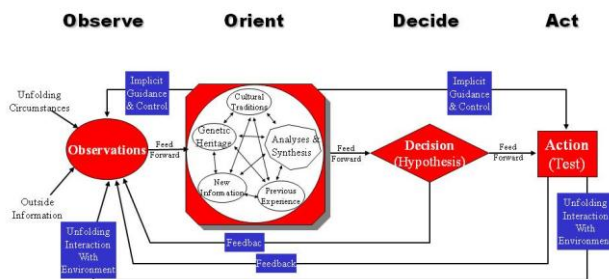


Figure 2. Boyd's OODA loop.

A unique feature of the OODA model is Boyd’s emphasis on tempo, i.e. the decision cycle time. Boyd expressed this as follows [11]: “in order to win, we should operate at a faster tempo or rhythm than our adversaries or, better yet, get inside the adversary’s Observation-Orientation-Decision-Act loop.”

Several authors have pointed out that Boyd’s OODA loop is purely reactive. Despite off-line, deliberative planning occupying a prominent place in military C2 doctrine and training, Boyd’s OODA loop does not include a separate Plan process. Some authors attribute planning to the Orient process, others to the Decide process, and still others add a fifth Plan process to Boyd’s original OODA loop.

### 3 NETWORK-ENABLED CAPABILITIES

In joint and combined operations, the flow of communications across the organizational hierarchy becomes essential to organizational performance. In coalitions and civil-military partnerships, communications must also flow between hierarchies. The pattern of communications flow adopts the form of a graph or network. In the 1990s, commercial organizations introduced flatter organizational structures supported by Internet technologies to exploit the power of informal communication

flows (termed “eCommerce”). The US Department of Defense started to investigate analogous developments under the title of “Network-Centric Warfare” (NCW) towards the end of the 1990s. More recently, the term Network-Centric Operations (NCO) has gained currency in the USA, while NATO has adopted the term Network-Enabled Capabilities. The aim is the same: to increase combat power afforded by more robust and effective computer and communications networking.

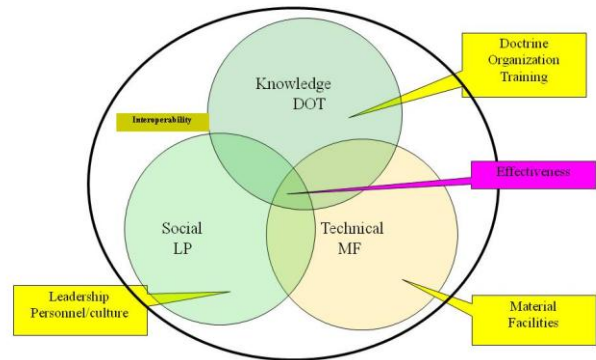


Figure 3. Technical, cognitive, & social viewpoints.

The original driver for NCW / NCO / NEC was technological. However, the community has accepted that, to be effective, any change in technology (“materiel”) must be accompanied by simultaneous changes in doctrine, organization, training, materiel, leadership, personnel, and facilities: the “DOTMLPF factors”. Moreover, networking can be seen from technical, cognitive (knowledge), and social viewpoints (see Figure 3).

There are four NEC tenets [12], often depicted as a value chain mapped onto the physical, information, cognitive, and social domains:

- A robustly networked force improves information sharing.
- Information sharing and collaboration enhance the quality of information and shared situation awareness.
- Shared situation awareness enables self-synchronization.
- These in turn increase mission effectiveness.

Organizational structure has been an important element of NEC research. Alberts and Hayes [12] argue that decision authority must be delegated from the centre of military hierarchies down to the edge of the organization. The US Naval Postgraduate School has studied such “edge” organizations extensively using computational experimentation techniques to bridge the gap between laboratory and field study [13]. Orr and Nissen [14] compare the Edge Organization against Mintzberg’s [15] five archetypical organizational configurations: Simple Structure, Machine Bureaucracy, Professional Bureaucracy, Divisionalized Form, and Adhocracy. The Machine Bureaucracy corresponds to the traditional military organizational hierarchy. Orr and Nissen’s results confirm that no single configuration is best for all circumstances. They elucidate seven specific performance measures that provide multi-dimensional insight into different aspects of organizational performance. The Edge Organization exhibits considerable agility, resisting performance degradation even under challenging conditions. They conclude that the military commander should vary the organizational

structure according to the prevailing situation. One limitation of their research is that the communications flow pattern is dependent on the organizational structure.

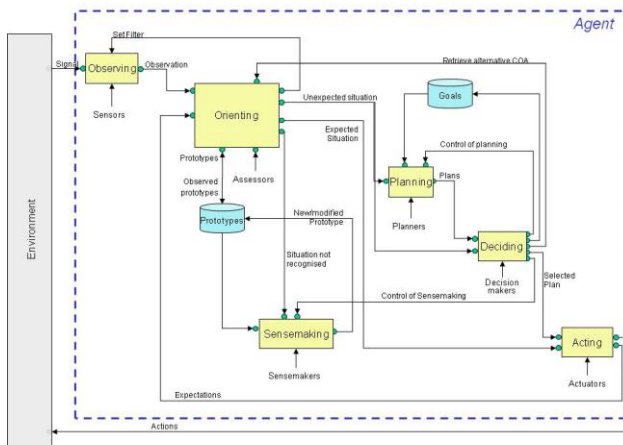
Nissen [16] compares the communication structure of the hierarchical (Machine Bureaucracy) and edge organizations:

| Hierarchy                      | Edge                      |
|--------------------------------|---------------------------|
| Vertical channels (stovepipes) | Horizontal network        |
| “Wheel” structure              | “Circle” structure        |
| Few links                      | Many links                |
| Low information exchange       | High information exchange |
| Push                           | Post & smart pull         |
| Meetings                       | Person-to-person          |

**Table 1. Communication structure.**

#### 4 OODA-RR TEST-BED

The rationally reconstructed OODA (OODA-RR) model was formalised using the SADT / IDEF0 notation and validated using a systematically generated set of use-cases. Boyd’s original 4 processes were retained, with their names ending in “ing” to emphasize that they are continuous, concurrent processes. Two processes (Planning and Sensemaking) and two data structures (Goals and Prototypes) were added. Planning generates one or more new plans in real time for responding to each unexpected situation identified by Orienting. Deciding selects which plan will be enacted. Sensemaking is a Weickian [17] real-time learning process that creates new or modifies existing Prototypes from the experience gained in coping with novel situations. The agent boundaries and the environment through which agents interact were explicitly represented. More details on the rational reconstruction and on the resulting OODA-RR model (see Figure 4) can be found in [5].



**Figure 4. OODA-RR model.**

To test the feasibility of the OODA-RR model, two Masters students designed and implemented the HackSim test-bed. To keep the work involved within the constraints of a Masters project, the Planning and Sensemaking processes were not implemented, and the user-interface and performance requirements were relaxed. The test-bed was designed in UML, with each OODA-RR process becoming an object-class in UML.

Auxiliary object-classes were added. The test-bed was implemented in Java. Two instances of an OODA-RR agent were created, one representing the computer intruder and the other representing the system administrator. The intruder’s target computer network was implemented as a set of instances of the Environment object-class. An initial pair of rule-sets representing the intruder’s and system administrator’s respective “doctrines” were generated by hand from one of the possible intruder-system administrator interaction scenarios [6]. The Masters students then iteratively extended the rule-sets. Their thesis [7] [8] include traces of several interaction scenarios.

The limitations of the implemented HackSim test-bed are:

- The Planning and Sensemaking processes have not yet been designed, implemented, and integrated with the object-classes representing the other OODA-RR processes.
- There is no explicit representation of organizational or other relationships between instances of the OODA-RR agent. The adversarial interaction between the intruder and system administrator instances was implicit in their respective rule-sets.

Finally, there is no representation in OODA-RR of collaborative processes, equivalent to the team-focused behaviours and outcomes in [18].

#### 5 9/11 CASE STUDY

On September 11, 2001, the Federal Aviation Authority (FAA) was responsible for civil air traffic over the Continent US, and the North American Aerospace Defense Command (NORAD) was responsible for military air defence. The FAA’s primary concerns were maintaining separation between aircraft and the nation-wide effects of severe weather or airport congestion. Operationally, the FAA was organized into 22 Air Route Traffic Control Centers, with an overall System Command Center (SCC) located in Herndon, Virginia. In the FAA headquarters, the Operations Center received notifications of incidents, including accidents and hijackings. NORAD’s mission was to defend the airspace of Northern America from external attack by ballistic and cruise missiles or bombers. Such attacks were expected to come over the Atlantic or over the North Pole. NORAD was divided into three sectors, of which only one – the Northeast Air Defense Sector (NEADS) – was involved in the events that day. NEADS could call on two alert sites, each with one pair of ready fighters: two F-15s at Otis Air National Guard Base (ANGB) and two F-16s at Langley Air Force Base (AFB).

Prior to September 11, 2001, the FAA and NORAD had developed procedures for working together in the event of a hijacking. Military assistance would normally take the form of providing a fighter aircraft to escort the hijacked airliner, to report anything unusual, and to aid search and rescue in an emergency. Because the FAA and NORAD C2 systems were not interoperable, the relevant FAA control centre would relay tracking information to NORAD to vector the fighter to a position some 5 miles behind the hijacked airliner. Every attempt would be made to have the hijacked airliner switch to the hijack-in-progress transponder code so that it would become visible to NORAD. In short, the procedures assumed that:

- The airliner crew would continue to fly the airliner, albeit following the hijackers’ directions.
- The hijacked airliner would be readily identifiable and would not attempt to disappear from radar.



class would also have to be given an attribute representing peer agents to be informed in the case of a hijacking.

In effect, two networks are superposed in the 9/11 case study: one representing the vertical, superior-subordinate reporting chains, and the other representing the horizontal peer-to-peer links. In all three cases (*should-have*, *actually-did*, and *could-have*) the FAA hijack coordinator would have had the Pentagon as a peer agent to be informed in the case of a hijacking. In the *actually-did* case, the agents representing the Boston approach and air route traffic control centres would also have had their Otis ANGB and NORAD acquaintances as peer agents to be informed in the case of a hijacking. In the *could-have* case, each of the FAA SCC, all FAA Air Route Traffic Control Centers, NORAD, NEADS, Otis ANGB, and Langley AFB would have had all the other control centres as peer agents.

In terms of social network constructs, the formal reporting chains running vertically in an organizational hierarchy could be represented as regular graphs or lattices [25]. The informal horizontal peer-to-peer links could be represented as small-world or scale-free networks.

## 7 CONCLUSIONS & FURTHER WORK

This paper describes work in progress in developing a C2 systems architecture based on the OODA-RR model of the military commander's thinking processes. It outlines some organizational aspects of present-day military C2, summarizes the transformation to NEC, and describes the HackSim test-bed implementing the OODA-RR agent model. The complex, real-world events on September 11, 2001, are used as a case study to show how social network constructs are needed to supplement a multi-agent system model.

Areas for further work include:

- Designing, implementing, and integrating OODA-RR's Planning and Sensemaking processes into the HackSim test-bed.
- Extending OODA-RR to include collaboration processes, and designing, implementing, and integrating this functionality into the HackSim test-bed.
- Implementing in the HackSim test-bed those attributes needed to represent agents' formal and informal social networks.
- Modelling the 9/11 case study in the HackSim so as to reproduce the *should-have*, the *actually-did*, and the *could-have* cases.

## REFERENCES

- [1] US Department of Defense. Dictionary of Military and Associated Terms. Joint Publication 1-02, 12 April 2001, as amended through 12 July 2007 (2007).
- [2] NATO. NATO Network-Enabled Capabilities Feasibility Study. Version 2.0, MCM-0032-2006 dated 19 April 2006 (2006).
- [3] J.R. Boyd. The Essence of Winning and Losing. Unpublished lecture notes (1996).
- [4] T.J. Grant & B.M. Kooter. Comparing OODA and Other Models as Operational-View C2 Architecture. Procs. 10<sup>th</sup> ICCRTS, Washington DC, USA. US DoD Command & Control Research Program, Washington DC, USA (2005).
- [5] T.J. Grant. Unifying Planning and Control using an OODA-Based Architecture. Procs. SAICSIT 2005, White River, South Africa. University of Pretoria, South Africa (2005).
- [6] T.J. Grant, H.S. Venter, and J.H.P. Eloff. Simulating Adversarial Interactions between Intruders and System Administrators using OODA-RR. Procs. SAICSIT 2007, Fish River Sun, South Africa. Nelson Mandela Metropolitan University, South Africa (2007).
- [7] Maarten Dollenkamp. Examining OODA as an Architectural Basis for Intrusion Detection Systems. MSc thesis, University of Liverpool, UK, 25 December 2007 (2007).
- [8] Michiel Dollenkamp. Research in the Feasibility of OODA as an Architectural Basis for Intrusion Detection Systems. MSc thesis, University of Liverpool, UK, 24 December 2007 (2007).
- [9] T.J. Grant. Measuring the Potential Benefits of Network-Centric Warfare: 9/11 as case study. Procs. 11<sup>th</sup> ICCRTS, Cambridge, UK. US DoD Command & Control Research Program, Washington DC, USA (2006).
- [10] M.R. Endsley. Theoretical Underpinnings of Situation Awareness. In: *Situation Awareness Analysis and Measurement*. M.R. Endsley and D.J. Garland (Eds.). LEA, Mahwah, NJ, USA (2000).
- [11] J.R. Boyd. Organic Design for C2. Unpublished lecture notes (1987).
- [12] D.S. Alberts and R.E. Hayes. *Power to the Edge: Command ... Control ... in the Information Age*. US DoD Command & Control Research Program, Washington DC, USA (2003).
- [13] M.E. Nissen and R.R. Buettner. Computational Experimentation with the Virtual Design Team: Bridging the chasm between laboratory and field research in C2. Procs. 9<sup>th</sup> ICCRTS, Copenhagen, Denmark. US DoD Command & Control Research Program, Washington DC, USA (2004).
- [14] R.J. Orr and M.E. Nissen. Hypothesis Testing of Edge Organizations: Simulating performance under industrial era and 21<sup>st</sup> century conditions. Procs. 11<sup>th</sup> ICCRTS, Cambridge, UK. US DoD Command & Control Research Program, Washington DC, USA (2006).
- [15] H. Mintzberg. Structure in 5's: A synthesis of the research on organization design. *Management Science*, 26: 322-341 (1980).
- [16] M.E. Nissen. Hypothesis Testing of Edge Organizations: Specifying computational C2 models for experimentation. Procs. 10<sup>th</sup> ICCRTS, Washington DC, USA. US DoD Command & Control Research Program, Washington DC, USA (2005).
- [17] K.E. Weick. *Sensemaking in Organizations*. Sage, Thousand Oaks, CA, USA (1995).
- [18] P. Essens, A. Vogelaar, J. Mylle, C. Blendell, C. Paris, S. Halpin, and J. Baranski. *Military Command Team Effectiveness: Model and instrument for assessment and improvement*. NATO RTO Technical Report AC/323(HFM-087)TP/59, April 2005 (2005).
- [19] 9/11 Commission. The 9/11 Commission Report: Final report of the national commission on terrorist attacks on the United States. US Government Printing Office, Washington DC, USA (2004).
- [20] 9/11 Commission. Staff monograph on the "Four Flights and Civil Aviation Security". US Government National Archives website, posted 12 September 2005, accessed 4 November 2005 (2005).
- [21] Aviation Week & Space Technology. *Crisis at Herndon: 11 airplanes astray*. AWST, 155 (25): 96-99 (2001).
- [22] Aviation Week & Space Technology. *Exercise Jump-starts Response to Attacks*. AWST, 156 (22): 48-52, 3 June 2002 (2002).
- [23] Aviation Week & Space Technology. *NORAD and FAA Sharpen View Inside Borders*. AWST, 156 (23): 50-52, 10 June 2002 (2002).
- [24] Aviation Week & Space Technology. *F-16 Pilots Considered Ramming Flight 93*. AWST, 157 (11): 71-74 (2002).
- [25] M.E. Gaston and M. desJardins. Social Network Structures and their Impact on Multi-Agent System Dynamics. Procs. 18<sup>th</sup> FLAIRS, Clearwater, FL, USA (2005).