# Military Operations Research and Situation Awareness in Networks

*René Janssen & Herman Monsuur*

## Introduction

*Operations Research*

What is the best we can do when we only have limited time to decide? Who must act? When? Where? How? As we live in a world where change is both far reaching and fundamental, we are probably facing such questions. It is good then to know that Operations Research (OR) can help you to take the right decision. This scientific discipline emerged from a process of solving optimization problems with strategic, operational, technical and tactical aspects. With the analytical and computer, and also conceptual, based approach, OR provides people and organizations with a rational basis for decision-making.

OR plays an important role, both in the public and private sectors. Whether one thinks about transportation, inventory planning, communication network design, risk management, health care, reverse logistics (reuse or disposal of products and material) or e-business. OR is a powerful tool in the hands of everyone involved in management. When OR is applied to the military domain, we speak of Military Operations Research (MOR). This special branch of OR focuses on subjects like search and detection, combat modelling, multi-criteria analysis, planning and logistics of military operations, inspection strategies for counter-drugs operations, measures of effectiveness for new weapon systems, game theoretic models for conflict, network theories, homeland security, value and effect of battlefield information, deployment of UAV's, decision analysis, war on terror, detection and mitigation of threats, bio-attacks, terrorists' networks, etc. Like many fields of scientific research, Military Operations Research has become a highly multi-disciplinary endeavour.

The MOR section of the NLDA has its 'home base' at the Royal Netherlands Naval College in Den Helder. This section concentrates on search and detection, combat modelling, homeland security and Network Enabled Capabilities (NEC). The most used scientific methods are statistical analysis, simulations, network theories, game theory, decision analysis, etc.

*(Military) Network Science*

'Information dominance and superiority' and 'network centric warfare' are terms that have become part of the lexicon associated with the transformation of the military force in the 21st century. Also well-known are the four tenets of network centric warfare: 1. A robustly networked force improves information sharing and collaboration; 2. Such sharing and collaboration enhance the quality of information and shared situational awareness; 3. This enhancement, in turn, enables further self-synchronization and improves the sustainability and speed of command; 4. This combination dramatically increases mission effectiveness. The concept of NEC involves the use of complex systems, consisting of many components that are heterogeneous in functionality and capability with both non-local and non-linear interactions and effects. The network aspect of this all captures the essence of transformation and is also a central element in improving combat effectiveness. Studying social, cognitive, physical and information networks is therefore of paramount interest. But, in spite of this dependence on networks, in military sciences, little is known about, for example, the relationship between architecture and functioning of a network: given some task, will a hierarchical network be outperformed by certain other network configurations that are more flexible? What about information propagation through a network? What are the mechanisms that explain why and how networks change over time? Or, with respect to security, which networks are prone to deliberate attacks on their nodes? What about the modelling of networks characterised by noisy and incomplete data? The answer to these questions contributes to the desired situation awareness at higher command levels and thus to the decision-making process.

In this contribution, we focus on the relation between the network's architecture and situation awareness, which forms the basis for decision-making.

*Networks and network value*

The concept of a network has become a basic and central notion in several scientific disciplines. In sociology and economics, many issues, like the interaction between individual entities, are formulated in terms of networks. In literature one may find several illustrations of this network approach; for comprehensive introductions see, for example, [Barabási, 2003], [Watts, 1999], [Dutta, 2003] or [Wasserman and Faust, 1994]. In military sciences, the concept of network centric operation has also attained considerable attention. The issue here is how operations are affected by the topology (the structure of links and nodes) of information networks, physical networks and social networks. See [Cares, 2004], [Darilek et al., 2001], [Monsuur, 2007b] or [Perry et al., 2002, 2004] for more information. Fig. 1 represents an example of a topology for a generic network.

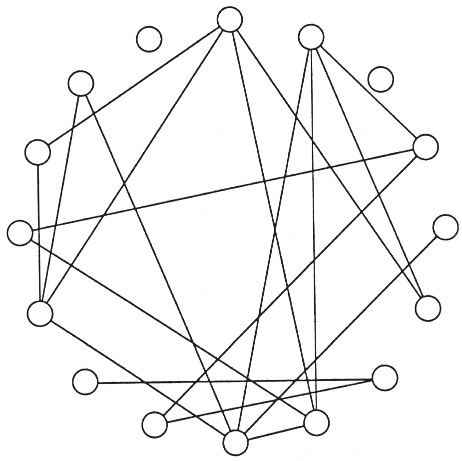


*Figure 1. Illustration of a network*

We assume that the network generates value for itself as a whole, but also for the individual nodes that are connected through links of the network. In a social network for example, the network value of a particular node may be something like status or prestige that a node derives from characteristics of its local network structure. For example, if a node is in a brokery position, meaning that the network becomes disconnected if it removes links, its status may be high. An important characteristic of a social network is that if a node somehow succeeds in gaining extra status, this also adds to the status of neighbouring nodes. So, network value is transferable and the extent of transferability depends on the strength of the tie between the two nodes. For a military network, where nodes exchange information they have gathered and processed, the network value may be situation awareness. The level of situation awareness is a result of the functioning of the information exchange network. Transferability depends on usability of information: is the information that is relayed to a particular node relevant, timely, concise, and is it highly regarded in terms of source and content? For an arbitrary network, this network value may also depend on exogenous (network independent) or unique characteristics, such as abilities and resources. In the case of military networks, these exogenous characteristics of the individual units may be their decision making facilities. For an overview, see the following table taken from [Monsuur, 2008].

*Table 1. Network value, transferability and exogenous value*

| *Type of network* | *Network value* | *Transferability depends on* | *Exogenous value* |
|---|---|---|---|
| *social network* | *status or prestige* | *strength of tie* | *abilities and resources* |
| *alliance network* | *monetary gains/ competitiveness* | *corresponding standards* | *internal organization* |
| *military information network* | *situation awareness* | *usability of information* | *information fusion capabilities* |

Networks consist of a number of distinct entities that may be similar or dissimilar (components, people, military formations). These entities interact in such a way that new properties or behaviours emerge that are beyond the capabilities of any of the entities acting alone. In general, networks may be considered from three perspectives: *Network structure* (links, nodes, connection rules), *Network evolution* (behaviour of network: deterministic or stochastic and its adaptation to the environment) and *Network dynamics* (mechanisms for networked effects). We will elaborate on these perspectives showing that (abstract) network theories are useful for studying emergent behaviour and emergent properties (shared situation awareness, agility, robustness) in the NEC domain.

*Network structure*

Consider the ancient Chinese game of 'GO' in which players capture stones and occupy territory. The board on the left of Fig. 2 shows a traditional grid; the board on the right shows a grid designed for a complex network. There are large hubs, clusters and long distance connections. It is clear that in order to win this game, new strategies will have to be developed. For example, on the left, a traditional strategy creates advantage from a great number of adjacent stones, while new strategies have to take into consideration hubs and long distance connections between cleverly placed clusters. An appealing property of these 'battles of networks' (also from a military point of view) is that complex networks prevent competitors from guessing the specifics of their strategies.

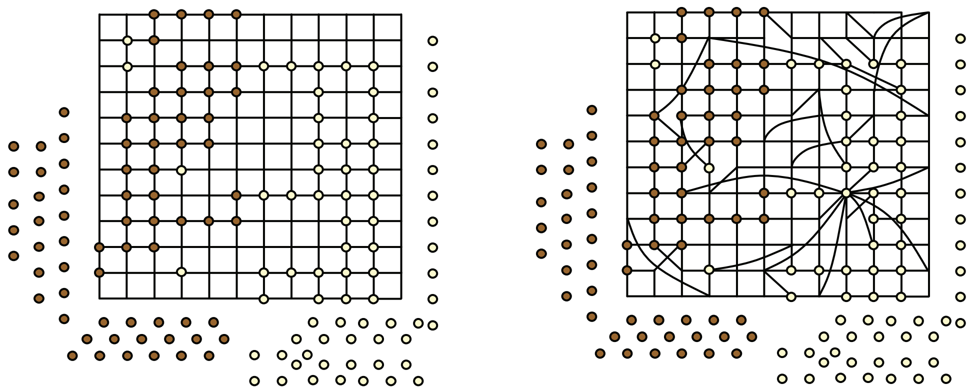


*Figure 2. The game of GO on a regular and complex network structure (Modification of a figure from Harvard Business Review 2006: Battle of the Networks, [Cares, 2006])*

It is clear that network structure matters, also for NEC. For another illustration we refer to [Grant, 2006], where the chaos that resulted from the 9-11 attack is analysed using a more flexible and agile network, instead of a fixed hierarchical network.

*Network evolution*

Suppose that a military commander has suggested the following network, in order to control a certain area of operation, see Fig. 3. Nodes represent decision facilities, information fusion centres, combat units, ground based air defence, etc. The nodes relay information they gather and process in order to increase situation awareness for the whole network (or just for the military commander).

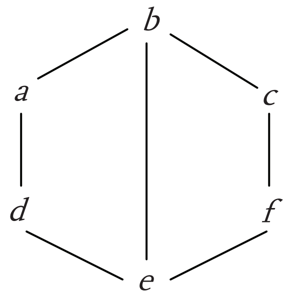



*Figure 3. The planned information network*

After a few hours of successful, autonomous functioning of the network, the commander considers his job done. The next day, he is informed that the network has rearranged itself. The nodes *a* and *c* now directly exchange information; moreover, nodes *b* and *e* were planning to finish their direct link. How can the actions of these individual, autonomous nodes be explained? A possible explanation might be that in the original network node *a* is covered by node *e*. This means that all of its connections that provide information (from *b* and *d*), also provide information to node *e* and, in addition, node *e* also receives information from node *f*. Something similar holds for node *c*. Note that, if nodes *a* and *c* decide to connect, they become uncovered. So, covered nodes, suffering a structurally visible position, will have an incentive to rearrange the network, either by adding or by severing links. As is proved in [Monsuur, 2007a], only a few network topologies can emerge from this process of actions of the individual nodes: complete networks, star networks and simple cycles.

In the literature one may find many models that try to explain how certain network topologies do emerge. A well-known example is *preferential attachment*. This mechanism assumes that a new node connects to nodes of the existing network with probability proportional to the number of connections these nodes already have. The result is that the 'rich-get-richer': a small number of very well-connected nodes (hubs), a medium number of moderately connected nodes and a large number of sparsely connected nodes. This resembles the structure of the internet. Fig. 4 is an artist impression of the internet (www.andreae.com/images/Pictures_and_Logos/Internet-map.gif ), showing a few large hubs that are connected to an extreme number of other nodes.

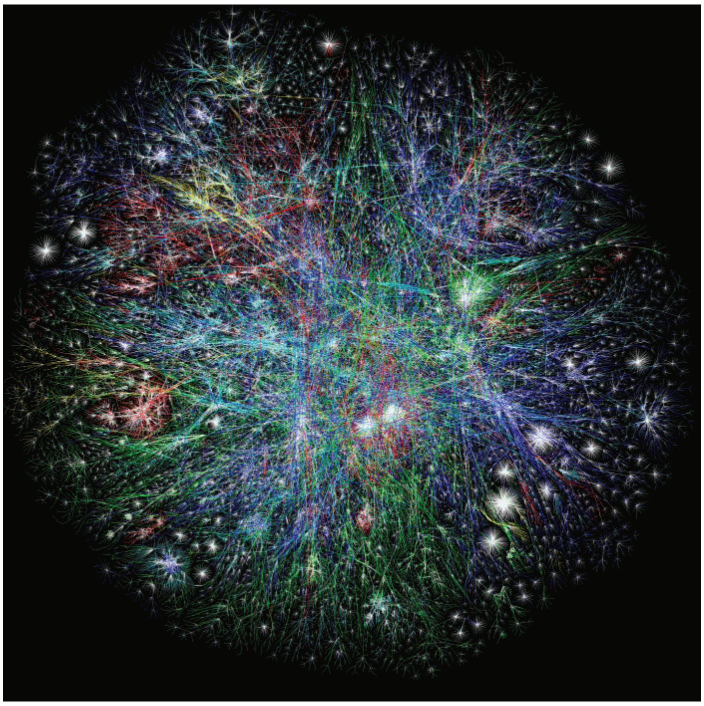


*Figure 4. The internet as a scale-free network*

*Network dynamics*

Because of the many ways in which forces could network efficiently, there is an interest in modelling and experimentation, and therefore there is a corresponding interest in metrics for network centricity. These metrics may shed light on the interplay between network topology and dynamics, where the role of the network's topology is to serve as a skeleton on which dynamic processes, such as the transfer of information, takes place. In the literature on NEC, one may find several metrics for the network effects, such as self-synchronisation and situational awareness, see Table 2, taken from [Fewell and Hazen, 2003].

For example, *speed of command* is the time required to complete one full cycle of the observe-orient-decide-act loop; *force agility and massing of effect* has to do with the ability to achieve a massed effect at some critical point in the battle space, and then to reorganise quickly to amass effects elsewhere as the situation develops; *self-synchronisation* means that the units' efforts are such that they are mutually supportive in the accomplishment of the overall goal, without the need for detailed centralised control.

*Table 2. Characteristics of network-centric military systems*

| | | |
|---|---|---|
| *Top level – force level characteristics:* | | |
| • *speed of command*<br>• *self-synchronisation*<br>• *effect-based operations*<br>• *information superiority* | • *force agility and massing of effects*<br>• *shared situational awareness*<br>• *reachback*<br>• *interoperability* | |
| *Second level – characteristics of decisions* | | |
| • *speed* | • *soundness* | |
| *Third level – characteristics of information* | | |
| • *relevance, clarity*<br>• *accuracy*<br>• *comprehensibility*<br>• *value* | • *timeliness*<br>• *consistency*<br>• *secrecy*<br>• *deg. of interoperability* | • *age, currency*<br>• *completeness*<br>• *authenticity* |
| *Fourth level – general characteristics of networks* | | |
| • *availability*<br>• *reliability* | • *concurrency*<br>• *survivability* | • *coverage*<br>• *security* |
| *Base level – physical properties* | | |
| • *bandwidth, network topology, server speed etc* | | |

Many studies attempt to measure the effect of networks on (military) operations. Some studies compare the effects of centralization and decentralization [Dekker, 2002, 2005], other studies try to measure the effect of information for the army or navy [Perry et al., 2002, 2004]. Other studies investigate network statistics such as link to node ratio, connectivity and cluster coefficients. These statistics are investigated to find suitable metrics for networked effects described in the table above, for example see [Cares, 2004].

*Situation awareness*

Underlying the concepts of Network Enabled Capabilities or Network Centric Warfare is the belief that a decision-maker – for example a military unit – can take better decisions if more or better information is presented to him. To be more precise, better information yields better situation awareness of a decision-maker, which in turn enables him to take better decisions. Usually more or better information can be obtained by sharing information with others. The concept of situation awareness is generally understood as ‘knowing what is going on’, implying the possession of knowledge and understanding to achieve a certain goal. It is the *perception* of the elements in the environment, the *comprehension* of their meaning and the *projection* of their status in the near future [Endsley, 1995]. Nodes represent decision facilities, information fusion centers, combat units and so on. There are several factors that influence this awareness of the situation that is presented to a decision-maker, or more generally, a node in the network. Among these factors is, firstly, the quality of the information available at individual nodes. Quality of information has several aspects, for example: completeness, correctness and currency [Perry et al., 2004]. Combined, they add to the situation awareness of a node. Secondly, as networks provide an opportunity for cooperating entities to share information, situation awareness of a particular node also depends on its positioning within the network and the network topology. Thirdly, it depends on characteristics of the individual decision-makers themselves, such as experience and training, quality of information fusion facilities, the rate at which information can be processed, the location within the area of operation, the psycho-social environment, organization, prior knowledge, etc.

In the process of transformation towards networked operations, military organisations face high demands regarding their flexibility and coherent integration of sensor, weapon and decision-making capacities. To be successful and to achieve the desired result, it is important to improve coordination of operations through sharing situational information. In this contribution, we focus on the second factor mentioned above, which is an important research area: *the situation awareness of networked elements* [National Research Council, 2005, 2007]. Our results can be used to gain insight into the role of the configuration of the network regarding the improvement and exchange of situation awareness. It also makes possible the comparison of alternative investment into C4I.

*Our approach and results*

In our model, we distinguish two independent aspects of situation awareness of a node in a network. First of all, we distinguish the exogenously (network independent) given attributes and characteristics of the individual nodes. Examples are its decision-making and information fusion facilities, its training and its positioning within the area of operation. Secondly, we study the importance of a node with respect to the distribution of information. This follows from its local network surroundings and the network topology. We combine these two influences to assess situation awareness.

In the base model, the vector of situation awareness $v$, is determined using the following mathematical (recurrent) relation:

$$v = \alpha A v + b,$$

where $b > 0$ is a vector of given characteristics regarding situation awareness. The matrix $A$ represents the network structure and contains all the relevant features of the network, its nodes, links and transferability of information. In general, $b$ and $A$ can be determined using techniques from multiple-criteria decision analysis that aggregate various characteristics into a single scalar, see [Monsuur, 2007b]. The parameter $\alpha$ may be interpreted as the relative importance of $Av$ with respect to $b$. So, the vector $v$ representing situation awareness is the weighted sum of two components: the vector $b$, (the 'stand-alone' situation awareness) and secondly, the improvement that results form transferred situation awareness, $Av$, of this final vector $v$ itself.

It is important to realize that the mathematical relation formulated above may also be interpreted as follows: The situation awareness of the set of nodes, as represented by the vector $v$, is 'confirmed' by the network structure (links and transferability of information) and exogenously given characteristics or private information of each node, as represented by the vector $b$. We will show that the process of updating situational information using links of the network is equivalent to solving our functional relation between $v$, $A$ and $b$.

We also present stochastic variations on this model to include uncertain willingness or possibility of individual nodes to transfer information to adjacent nodes (as may be experienced in practice). We introduce a network performance metric that can be used to compare different network configurations and which takes into account stochastic behaviour of the nodes. It also can be used to compare investments in the (C4I) structure of the network. We illustrate our results by simulation. This shows that:

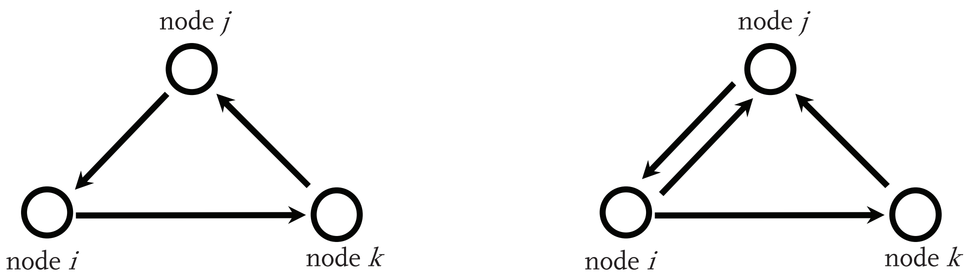
- Updating information using the network topology (information flowing along links) yields new quality characteristics of the nodes (new situation awareness);
- The network performance metric can be used to compare various alternative network configurations.

For other (social) network analysis methods used to analyze military architectures, we refer to [Dekker, 2002, 2005], [Ling et al., 2005], [Perry and Moffat, 2004] or [Cares, 2004]. For example, in [Dekker, 2002], a methodology is introduced that combines social network analysis techniques with military thinking about organizational structure. Metrics are calculated, such as number of links, degree of nodes and distances in networks, to conduct delay analysis, centrality analysis and intelligence analysis.

**The calculation of situation awareness in a network of (partially) cooperating nodes**

As stated previously, cooperating nodes in a network get better situation awareness by sharing information. This process of updating information within the network only depends on given deterministic characteristics of the nodes themselves and the joint network structure. So individual nodes are always in a position to receive information from adjacent nodes or hand over information to others if possible *and* they are always prepared to do so. This assumption states that the nodes behave fully deterministically. However, this will later on be relaxed by allowing uncertain behaviour of the nodes.

A network is a structure made of nodes (i.e. military units) that are tied by links. Each link is assumed to be a *one-way link*, i.e. the information flow along a link will always be in *one direction only*. From the viewpoint of an information receiving node *i*, node *j* is an adjacent node of this node *i* if there is a link from node *j* to node *i*. In return, node *i* is an adjacent node for node *j* if a link exists from node *i* to node *j*, see Fig. 5.




Node *j* is an adjacent node of node *i* but not the other way round. Node *j* can only receive information from node *i* via node *k*.

Node *i* and node *j* are adjacent nodes of each other.

*Figure 5. Adjacent nodes*

We assume that the nodes are labelled from 1 to $n$. With each node $i$ we associate a real nonnegative number, $b_i$, which is called the 'stand-alone' situation awareness of this particular node. In general each $b_i$ can be determined using techniques from multiple-criteria decision analysis which aggregate various characteristics of a node into a single scalar. The vector $b$ contains all the individual values $b_i$.

If there is a link from node $j$ to node $i$, we associate a real nonnegative number, $a_{ij}$, with this link which represents the usability of the information flowing from node $j$ to node $i$ from the point of view of the receiving node $i$, see Fig. 6. These numbers $a_{ij}$ can also be determined using techniques from multiple-criteria decision analysis. If there is no link from node $j$ to node $i$, we put $a_{ij} = 0$. The $n \times n$ matrix $A$ with the entries $a_{ij}$ is called the adjacency matrix.

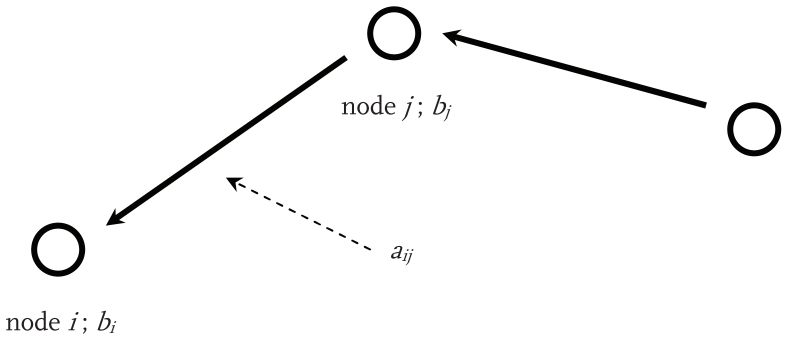



*Figure 6. Usability of information*

Next we introduce a discount factor $\alpha$, $0 < \alpha < 1$, which brings in the fact that the usability of information which is flowing along links will decay over time, i.e. information will lose its usability if it is getting older. Before sharing information the situation awareness of the nodes is given by the vector $b = (b_1,\ldots,b_n)^T$. After each node has received information *only* from its adjacent nodes, the new situation awareness of the nodes is given by $b + \alpha Ab$. By iteration information can be updated through the network, so that nodes also receive information from nodes which are not adjacent nodes, but are two, three, or more steps away. Updating information in $M$-steps yields the situation awareness, $v_M$, which for $M \geq 1$ is defined recursively as follows:

$$v_0 = b;\ v_1 = b + \alpha A v_0;\ \ldots\ldots;\ v_M = b + \alpha A v_{M-1}.$$

Taking the limit of $M$ tending to infinity, we get the following result:

$$v = \lim_{M\to\infty} v_M = \lim_{M\to\infty} \sum_{k=0}^{M} \alpha^k A^k b = (I - \alpha A)^{-1} b.$$

We call $v$ the (definite) situation awareness of the nodes after sharing information. This vector $v$ satisfies the equation

$$v = \alpha A v + b.$$

In this sense we can say that $v$ is 'confirmed' by the network structure and the 'stand-alone' situation awareness of the nodes, $b$.

<u>Example:</u> Consider the network of Fig. 7, with nodes Joint Strike Fighter, Ground Based Air Defence, etc. Assume that we take

$$b = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix} = \begin{pmatrix} 1.00 \\ 0.50 \\ 0.85 \\ 1.00 \\ 0.30 \end{pmatrix}, \qquad A = \begin{pmatrix} 0 & 0.5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.5 & 0 \\ 0 & 0.5 & 0 & 0 & 0.5 \\ 0.5 & 0 & 0.5 & 0 & 0 \\ 0.5 & 0 & 0 & 0.5 & 0 \end{pmatrix}, \qquad \alpha = 0.25.$$

Solving the equation $v = \alpha A v + b$ yields the following situation awareness:

$$v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{pmatrix} = \begin{pmatrix} 1.09 \\ 0.67 \\ 1.01 \\ 1.26 \\ 0.59 \end{pmatrix}.$$

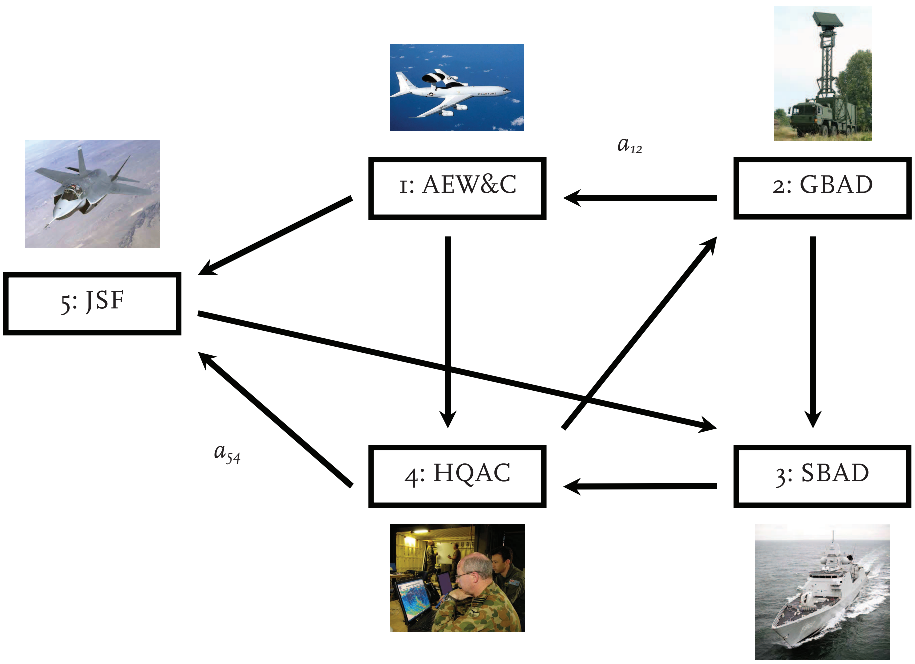



*Figure 7. A communication network*

So we can conclude that each node has more situation awareness. For example the situation awareness of node 5 was 0.30 and has become 0.59, so it has almost doubled.

Next we introduce a network performance metric which combines given characteristics of the nodes with the Network Topology in order to compare different network configurations. As stated before, updating information in $M$-steps yields situation awareness, $v_M$. For $M \geq 1$ we define the network performance metric $NTb_M$ by

$$NTb_M = \frac{e^T v_M}{e^T b} = \frac{e^T \sum_{k=0}^{M} \alpha^k A^k b}{e^T b} = \sum_{k=0}^{M} \alpha^k \frac{e^T A^k b}{e^T b},$$

where $e$ is a vector of 1's. Taking the limit of $M$ tending to infinity, we get the following result:

$$NTb = \lim_{M \to \infty} NTb_M = \frac{e^T v}{e^T b} = \frac{e^T (I - \alpha A)^{-1} b}{e^T b}.$$

Example (continued):

$$NTb = \frac{\sum_{i=1}^{5} v_i}{\sum_{i=1}^{5} b_i} = \frac{1.09 + 0.67 + 1.01 + 1.26 + 0.59}{1.00 + 0.50 + 0.85 + 1.00 + 0.30} = 1.27$$

We can calculate this number also for other network structures in order to compare the different networks. Notice that instead of the fixed value $\alpha = 0.25$, we can plot $NTb$ as a function of the variable $\alpha$. This yields Fig. 8.

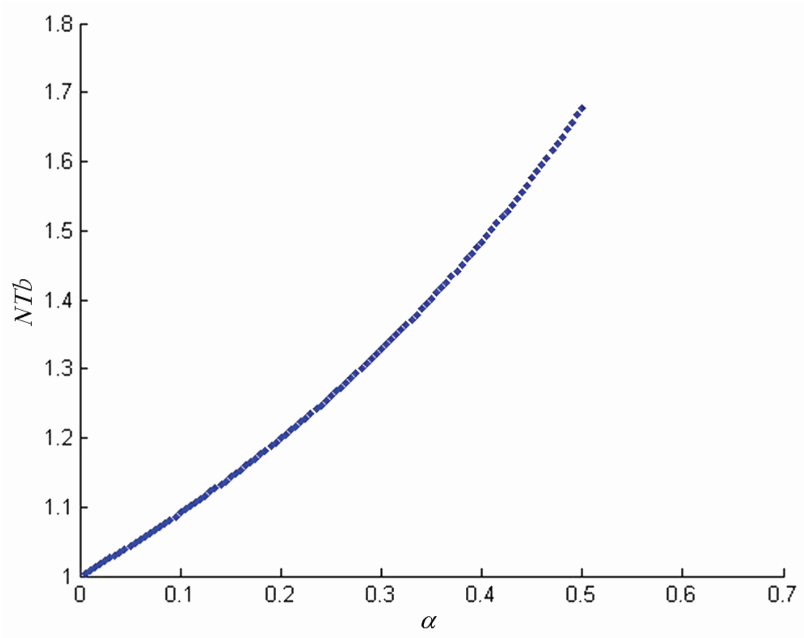



*Figure 8. NTb as function of α*

Up to now we assumed that individual nodes are always in a position to receive information from adjacent nodes or hand over information to other nodes if possible *and* they are always prepared to do so. However as may be experienced in practice, the process of updating information not only depends on given deterministic characteristics of the nodes itself and the joint network structure. It also depends on the *uncertain* willingness or possibility of individual nodes to receive and transfer information. We will now take into account this uncertainty.

At each stage $k$, $k \geq 1$, of the process of updating information within the network, the uncertain behaviour of the nodes is modelled by a collection of independent and identically distributed random variables $Y_{k,ij}: \Omega \to \{0,1\}$, $1 \leq i,j \leq n$, such that

$Y_{k,ij} = 1$ if an information flow between node $j$ and node $i$ is possible;
$Y_{k,ij} = 0$ if an information flow between node $j$ and node $i$ is not possible.

For a fixed outcome $\omega$ in the sample space $\Omega$ the process of updating information in $M$-steps yields the situation awareness, $V_M(\omega)$, which for $M \geq 1$ is defined as follows:

$$\begin{aligned}
V_0(\omega) &= b \\
V_1(\omega) &= b + \alpha A_1(\omega) V_0(\omega) = b + \alpha A_1(\omega) b \\
&\vdots \\
V_M(\omega) &= b + \alpha A_M(\omega) V_{M-1}(\omega) \\
&= \ldots = b + \alpha A_1(\omega) b + \alpha^2 A_2(\omega) A_1(\omega) b + \ldots + \alpha^M A_M(\omega) \cdots A_1(\omega) b \\
&= b + \sum_{k=1}^{M} \alpha^k \left( \prod_{s=0}^{k-1} A_{k-s}(\omega) \right) b
\end{aligned}$$

where the matrices $A_k(\omega)$ have the entries $a_{ij} Y_{k,ij}$. Note that we obtain the former, deterministic expression for the situation awareness $v_M$, if all the matrices $A_k(\omega)$ are equal to $A$. The network performance metric that combines the given characteristics of the nodes with the Network Topology is defined by

$$NTb_M = \frac{E\left(e^T V_M\right)}{e^T b} = 1 + \sum_{k=1}^{M} \alpha^k \frac{E\left(e^T \left(\prod_{s=0}^{k-1} A_{k-s}\right) b\right)}{e^T b},$$

where $E(.)$ denotes the expectation and $e$ is a vector of 1's. Most of all we are interested in the case when $M$ tends to infinity. So let $\{D_1,\ldots,D_N\}$ be the collection consisting of all outcomes of $A_1(\omega)$. Notice that this collection is always finite, because $N \leq 2^n$.

Suppose $\alpha \leq \left( \max_j \left( \sum_{i=1}^{n} a_{ij} \right) \right)^{-1}$. Then the network performance metric that combines the given characteristics of the nodes with the Network Topology is defined by

$$NTb = \frac{\int e^T x \, d\mu(x)}{e^T b}.$$

Here $\mu$ is the unique probability measure which satisfies the equation

$$\mu = \sum_{m=1}^{N} P(A_1 = D_m) \, \mu \circ f_m^{-1},$$

where each $f_m$ is the affine mapping $f_m : x \mapsto b + \alpha D_m x$. The existence and uniqueness of this probability measure follows from the fact that $\{f_1,\ldots,f_N; P(A_1 = D_1),\ldots, P(A_1 = D_N)\}$ is an iterated function system with probabilities. The integral $\int e^T x \, d\mu(x)$ in the expression of $NTb$ can be determined by applying Elton's theorem [Elton, 1987], i.e. fix a sequence of matrices $\{A_k(\omega)\}_{k\geq 1}$ for some outcome $\omega$ in the sample space $\Omega$. Let the orbit $\{x_n\}_{n=0}^{\infty}$ be defined by $x_0 = b$ and $x_{n+1} = b + \alpha A_{n+1}(\omega)\, x_n$. Then with probability one

$$\lim_{n\to\infty} \frac{1}{n+1} \sum_{k=0}^{n} e^T x_k = \int e^T x \, d\mu(x) \ .$$

So in order to determine *NTb*, we use the fact that *NTb* equals the expression

$$\lim_{n\to\infty} \frac{1}{n+1} \left( 1 + \sum_{k=1}^{n} \frac{e^T x_k}{e^T b} \right) .$$

Example (continued):
Assume that $p$ is the probability that an information flow between node $j$ and node $i$ is possible, independently of the choice of $i$ and $j$. Then for $p = 1$ we get of course the former (deterministic) result: *NTb* = 1.27. For $p = 0$ the nodes don't share information, so we get: *NTb* = 1. For values of $p$ between 0 and 1, the graph of the function *NTb* as a function of $p$ is as in Fig. 9.

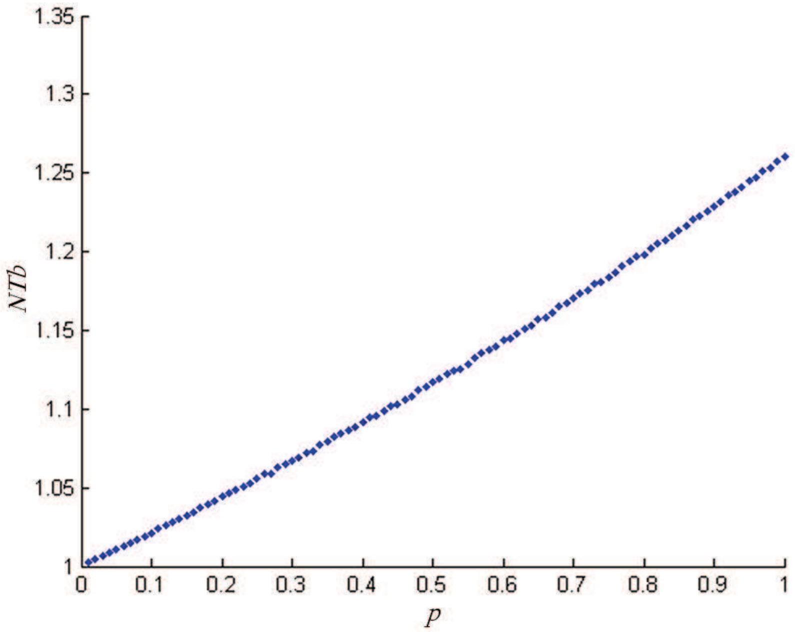



*Figure 9. Graph of NTb as function of p*

**Conclusion**

*'The achievement of military effect will, in the future, be significantly enhanced through the networking of existing and future military capabilities, under the banner of Network Enabled Capabilities (NEC)'* [Ministry of Defence UK, 2005]. NEC has three overlapping and mutually dependent dimensions: Networks, Information and People. At the heart of NEC is a network that is used to distribute information. It enables Defence forces to acquire, generate, distribute, manipulate and utilize information. Information is gathered from a variety of sources, enters the network and is then disseminated through the network to improve situation awareness. It can be exploited, leading to decisions to achieve a desired outcome. Decision-makers must identify what information is required and available to

make the right decision. Therefore, effective information management will grow in importance, especially in a networked environment. People will need to learn how to share and find information from a variety of sources and then use that information to optimise their decisions.

Our results and approach can contribute to a better understanding of the interaction between these three dimensions of NEC. We give two examples.

*Network and information*
We are able to calculate the impact of the specific configuration of the network on the improvement and exchange of situational information. This enables the comparison of alternative investments into C4I.

*Network and people*
Another spin-off of our approach and results is the possibility to investigate the interaction between the various types of networks and the various types of agents' behaviour, when they have the task to solve complex problems. For example, given a fixed network topology, and a complex problem that has to be solved, one may investigate the effects of changing the behaviour and decision-making qualities of agents or people. Or, consider a given set of agents, each having some fixed decision-making qualities. Then one may investigate the influence of changing the network topology (for example by deleting the hierarchical structure and moving towards a more flexible network structure) on how these agents (or people) take advantage of new technology. Results of the kind we presented can also be used if one wants to validate new technologies or concepts in a military environment.

Generally speaking, findings of this kind of research can be used to support the modelling of warfare, decisions on force structures, trade-offs among the platforms' weapons and C4ISR systems. Last but not least, it may significantly contribute to changes in doctrine and tactics, techniques and procedures.

**References**


Barabási A-L. (2003) *Linked*. A Plume Book.

Cares, J. (2004) *An information age combat model*. Alidade Incorporated. Produced for the Director, Net Assessment, Office of the Secretary of Defense (under contract TPD-01-C-0023).

Cares, J. (2006) Battle of the Networks. (The HBR List of Breakthrough Ideas for 2006). *Harvard Business Review*, 40-41.

Clark, T., Moon, T. (2002) Assessing the Military Worth of C4ISR Information. *Proceedings 7-th International Command and Control Research and Technology Symposium*.

Darilek, R., Perry, W., Bracken, J., Gordon, J. and Nichiporuk, B. (2001) *Measures of Effectiveness for the Information-Age Army*. RAND, Santa Monica.

Dekker, A.H. (2002) Applying Social Network Analysis Concepts to Military C4ISR Architectures. *Connections* 24(3): 93-103.

Dekker, A.H. (2005) Network Topology and Military Performance. In: Zerger A. and Argent R.M. (eds.) *Modsim* 2005 International Congress on Modelling and Simulation. Modelling and Simulation Society of Australia and New Zealand, December 2005, pp 2174-2180.

Dutta, B. and Jackson, MO (Eds.) (2003) *Networks and Groups, Models of Strategic Formation,* Springer.

Elton, J.H. (1987) *An Ergodic Theorem for Iterated Maps*, Ergodic Theory and Dynamical Systems, volume 7, pp 481-488.

Endsley, M.R. (1995) Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors* 37(1): 32-64.

Fewell, M.P., Hazen, M.G. (2003) *Network-Centric Warfare; Its Nature and Modelling.* Report DSTO-RR-0262.

Forman, E.H., Gass, S.I. (2001) The Analytic Hierarchy Process – An Exposition. *Operations Research* 49: 469-486.

Grant, T.J. (2006) *Measuring the Potential Benefits of NCW: 9/11 as a case study.* Proceedings 11th ICCRTS Conference.

Ling, M.F. (2005) Nonlocality, Nonlinearity and Complexity: on the Mathematics of Modelling NCW and EBO. *Proceedings 22nd International Symposium on Military Operational Research.*

Ling, M.F., Moon, T., Kruzins, E. (2005) Proposed Network Centric Warfare Metrics: from Connectivity to the OODA Cycle. *Military Operations Research Society Journal* 10: 5-13.

Ministry of Defence UK (2005) *Network Enabled Capabilities.* JSP 777.

Monsuur, H. (2007a) Stable and emergent network topologies: a structural approach. *European Journal of Operational Research,* 183 (1), 432-441.

Monsuur, H. (2007b) Assessing Situation Awareness in Networks of Cooperating Entities: A Mathematical Approach, *Military Operations Research,* volume 12 number 3, pp 5-15.

Monsuur, H. (2008) Network induced powerbase: the appreciation of contributing to the value of other nodes. To appear in: *Social Networks, Development, Evaluation and Influence.*

National Research Council (2005) *Network science.* The National Academies Press.

National Research Council (2007) *Strategy for an Army Center for Network Science, Technology, and Experimentation.* The National Academies Press.

Perry, W., Button, R.W., Bracken, J., Sullivan, T., Mitchell, J. (2002) *Measures of effectiveness for the information-age navy. The effects of network-centric operations on combat outcomes.* National Defense Research Institute, RAND.

Perry, W., Moffat, J. (2004) *Information sharing among military headquarters: the effects on decisionmaking.* RAND Monograph 2004.

Perry, W., Signori, D., Boon, J. (2004) *Exploring information superiority: A methodology for measuring the quality of information and its impact on shared awareness.* National Defense Research Institute, RAND.

Watts, D.J. (1999) *Small Worlds, The dynamics of networks between order and randomness,* Princeton Studies in Complexity, Princeton University Press.

Wasserman, S., Faust, K. (1994) *Social network analysis: methods and applications.* Cambridge University Press, Cambridge.