Technical Evaluation Report

NATO - RESEARCH AND TECHNOLOGY ORGANISATION
Systems Concepts and Integration (SCI) Panel – 187 Symposium

"*Agility, Resilience and Control in Network Centric Communications*"

Naval Barracks, Amsterdam, The Netherlands,

Tuesday, 27 May, 2008 – Thursday, 29 May, 2008

TER Author[1]: Mr. Terry Vickers

Principal Scientist, NATO C3 Agency, The Hague, NLD

Terence.Vickers@nc3a.nato.int

1. INTRODUCTION

1.1 Theme of the Symposium

The theme of the symposium was to look at three main characteristics of a Network Enabled Capability (NEC) namely, agility[2], resilience and control. These characteristics are influenced by a number of factors such as technology, systems, doctrine & tactics, training and human factors.

1.2 Purpose of Symposium

The symposium's main objective was to enable exchange of information on the theme of the symposium, providing an understanding of the current and emerging methods and technologies in NEC. The information could be used to influence setting of priorities to provide near term and long term capabilities.

1.3 Purpose of this report

This Technical Evaluation Report (TER) is to assess the overall technical situation in the chosen subject, as it emerged from the meeting, to draw conclusions and to make recommendations for further action.

The SCI-Panel's Mission statement is "to further knowledge concerning advanced system concepts, integration, engineering techniques and technologies across the spectrum of platforms and operating environments to assure cost-effective mission area capabilities". The report makes an assessment of contribution the symposium has made towards achievement of the Mission statement.

In addition, an assessment is made of how well the symposium fulfilled its objectives – these were stated as:

"The objective of this symposium is to address the issues in NEC which enable the creation and development of agile and resilient forces and the required command control concepts and procedures. These issues will be discussed from three different perspectives: the Operational perspective, the Systems perspective and the

[1] NOTE: The views contained in this report are the author's personal views, in fulfilling the role of TER author. The views expressed do not represent official NATO or NATO C3 Agency views.

[2] Agility is seen as including robustness, resilience, responsiveness, flexibility, innovation, and adaptation in order to be effective (Alberts and Hayes 2003)

Human perspective. The symposium addressed a number of NATO priorities, including NATO Reaction Force (NRF), Network Enabled Capabilities (NEC) and Defence Against Terrorism (DAT).

1.4 Symposium Outline Programme

The Symposium consisted of 3 Keynote addresses, and 27 presentations arranged in 6 Sessions:

- **Keynote Speakers** provided a high level framework for the rest of the symposium and raised many issues picked up by presentations in the rest of the symposium
- **Session 1 – Command and Control** (C2) looked at a C2 maturity levels, dealing with complexity, effects of mash-ups on C2, the need to be agile and speed up planning processes, self-synchronisation, and Force Planning.
- **Session 2 – Systems and Systems of Systems (SoS)** covered system of system management, middleware software allowing complex systems to be 'self-managed', use of SoS Engineering (architecture and modelling) to improve agility, resilience and control, NATO Human Views and tracing of spontaneous designs.
- **Session 3 – Situation Awareness (SA)** presentations were made on information processing and delivery to the last tactical mile, SA associated with DAT and Homeland defence, SA for semi-autonomous groups and a NATO project to improve a commanders SA.
- **Session 4 – Architectures** looked at security, the other looking at information assurance within NEC, use of hybrid models and influence of cognitive modelling, and a Dutch Architectural Framework
- **Session 5 – Communications and Networking** included briefs on dynamic ad-hoc tactical level networks, interoperable network descriptions, applicability of agent technology; the use of intelligent tactical routers in a heterogeneous communications environment and efficient information management for dismounted soldiers.
- **Session 6 – CD&E and Testing –** provided an overview of CD&E and testing applicable to NEC.

A technical tour of NATO C3 Agency and TNO Defence Security and Safety, in The Hague also took place.

2. EVALUATION

2.1 Chairman's Opening remarks

The SCI-Panel Chairman, Dr. Jim Wickes, welcomed attendees to the symposium. The Chairman explained the role played by NATO and RTO, in particular, in fostering cooperation in scientific and technological Research and Development. The decreasing predictability of military and crisis events, including actions of terrorists (such as those in Afghanistan) requires agility, resilience and control. Developments in these themes will help future work in support to services in the front line.

The Chairman thanked Dr. Hans Keus for putting together a good set of speakers to tackle such a wide ranging subject as NEC.

It was recognised that the SCI-Panel needs to liaise closely with other lines of development, in particular Human Factors and Simulation and Training. Hard core scientists need to work with soft sciences, for example when looking at adaptive decision making, distributed decision making. It was suggested that there is a need to stay within boundaries of a commander's intent.

Given an ever changing/adaptable adversary requires agility but can cause problems for C2. NEC involves 'power to the edge' that is moving decision making to the edge.

Science and Technology needs to be transformed into specific systems, paying particular attention to doctrine, Tactics, Techniques and Procedures (TTPs), and training. There are a number of work areas looking at Concepts, Development and Experimentation. These work areas need to address what kind of systems are needed to support new concepts and developments.

2.2 Keynote Speakers

The Keynote speakers provided high-level perspectives on Network Enabled Capabilities (NEC) from the perspectives of the Netherlands Ministry of Defence (MOD), NATO C2 Centre of Excellence (COE), and NATO Allied Command Transformation (ACT). These speakers touched on many of the issues associated with NEC, some of which were addressed in the symposium by speakers.

2.3 Keynote Address 1 - A Netherlands MOD Perspective Commodore Frank Sijtsma of the Netherlands MOD

Commodore Frank Sijtsma of the Netherlands MOD provided a Netherlands perspective on the NEC. The Netherlands have aligned with NATO views and adopted the term NEC, as it better expresses that a capability that is supported by a network. NEC is an evolutionary process without a strictly defined beginning or end. Doctrines, process, command and control, organisations, personnel and material must develop in a coherent evolutionary way.

NLD has initiated a number of studies, projects, experiments and exercises emphasising that NEC Transformation in The Netherlands is more than just theory.

It is also recognised NEC is the necessary condition for Effects based Operations (EBO) and that EBO requires greater civil military interoperability. Consequently, The Netherlands has undertaken a number of collaborative (CIV-MIL) exercises.

One of the biggest challenges is adapting NEC to the human dimension. Issues to be tackled include the reduction in complexity, information overload, micromanagement and keeping a balance between technological, organisational and cultural changes.

2.4 Keynote Address 2 - Operational Assessment of NATO Response Force (NRF) Col Gerloof Kanis, Director Command and Control Centre of Excellence (CoE)

Col Gerloof Kanis outlined a number of issues associated with the operational assessment of NRF. In doing so, touched on a number of key issues associated with NNEC.

The Netherlands offered to host the C2 CoE, which is to act as a catalyst in the field of C2; this was formally established by an MOU, in June 2007.

It was stated to note that NATO did not have a consistent definition for command and control. Consequently, the C2 CoE, in June 2007, established the following working definition for C2:

"*Command and Control is the exercise of authority and direction by a properly designated commander over assigned forces performed through an arrangement of personnel, equipment, communications, facilities and procedures in the accomplishment of a mission. C2 is the art to use these enablers to accomplish the mission*"

The C2 CoE was tasked to under take an NNEC assessment of NRFs. Doing so required some form of measuring stick, this took the form of the NATO 5 NNEC Maturity levels (NMLs); these range from Standalone (NML1) through to coherent (NML5). This maturity model takes into consideration three factors; firstly the technical network, secondly the cognitive network and finally the social network. It is often

assumed that once the Technology network is up and running all will be well, but is this when the other networks come into play.

The Technical network covers equipment, interoperability and relevance. Feedback from the operational community tends to suggest that there is frustration with all the technology, that there are too many tools, and the tools aren't integrated. It was indicated that often, doctrine was not in place to for exploitation of the tools.

The cognitive network, covers knowledge and information use. The speaker focused on two aspects of the cognitive network – that of training and micro-management.

- Training and Education: People need to train One commander in training stated that '*there is an amazing amount of information but it is difficult to identify that for actionable use*'. A key statement was that training provides the insight in how to exploit opportunities.
- Micro management: The technology network increasingly allows higher levels of command to micro-manage the warfighters. However, the higher commands must trust lower echelons to undertake their mission in line with the commander's intent. Trust is a vital part of the Social network.

Social Network: Culture and Trust are key elements for a well developed social network. Culture refers to an understanding of the 'people' elements, which is vital within NATO. NNEC relies on information sharing and this only occurs if there is trust amongst NNEC components – this includes trust in technology and people and this applies to both military and civil domains. Mutual trust helps reduce 'hiding behind security regulations'. Trust helps attainment of higher levels of NNEC maturity.

2.5 **Keynote Address 3 – NATO Network Enabled Capability, Maj Ukf Boettcher, NATO ACT, NNEC Integrated Capability Team**

Maj Ukf Boettcher iterated a number of issues outlined by the previous key note address – indeed many of the issues were recurrent throughout the symposium. It was indicated that NNEC is not a capability that one can simply buy off the shelf. There is a need to change culture, at all levels. There should be the need to share information as opposed to the 'need to know' principle – this extends across all players in an operation, including non-military organisations. NATO NNEC and EBO - provide a framework, need to build the common funded part of NNEC and the need to federate from different nations.

Standardisation is a good start to gain interoperability, but is not without problems. Within NATO the standardisation process has been seen as a lengthy process. The use of a standard test environment can aid the development and testing process. The NATO project Multi-sensor Aerospace/Ground Joint ISR Interoperability Coalition (MAJIIC) has nine nations working together on an ISR set of standards. Other nations can see that the standards are sufficiently mature to use in theatre.

A warfighter needs check of systems before going into theatre, one such project to do this is the NATO ISAF C4I Enabled Capability (ICECAP project).

NATO is good at developing requirements, but the process is seen as too long. By the time the warfighter in theatre get a set of tools, they have rotated out. Prototyping and spiral development can help alleviate the problem. There is a need to test not just the technology but the social and cultural aspects.

SESSION 1 – Command and Control

This session, consisted of six presentations.

The first paper "**The NATO NEC C2 Maturity Model**" by Professor James Moffat outlined a NEC C2 Maturity model, developed by the NATO RTO SAS Working Group 065. NATO Nations can use the model to assess their level of NEC C2 Maturity. There are five levels ranging from Conflicted C2 to Agile C2 these are similar to the NNEC Maturity Levels[3]. A good example was given of analysis of the change in state of C2 maturity during the Emergency situation generated by Hurricane Katrina, in the USA. The example illustrated that the C2 Maturity varies over time and in general it appeared that there is an increase in maturity levels over time. The maturity model embraces peoples behaviour, for example as trust and situational awareness increases then there is often an upwards move in maturity. It was observed that one can draw a simple analogy with team building; where teams move from storming, norming and performing i.e. de-confliction, establishment of trust and common intent and development of shared situational awareness.

The second paper, "**Using Complex Adaptive Systems Models to increase Agility**" given by Peter Petier outlined adaption[4] as a mechanism for dealing with complexity. The properties of complexity, such as non-linear dynamics, feedback mechanisms and emergent properties were briefly indicated. The consequences of complexity are unpredictability, need for feedback mechanisms, reduced control and change rules. One of the challenges is to design an organisation that recognizes and deals with both large scale and complex encounters. This trade-off is largely determined by mission characteristics (which may change over time). It was suggested that adaptation was seen as a mechanism to adjustment to changes in the mission environment.

The next paper, '**Next Generation C2: Formalising Military Mashups**', was enthusiastically delivered by Dawn Meyerrieks. Defence does not have a unique problem; it should learn from and utilise best commercial practices. The paper highlighted the need to encourage and support dynamic C2 capabilities through tactical collaboration and coordination. Current operations require C2 capabilities that are dynamic, decentralised tactically, centralise strategically, highly mobile, highly connected, optimised for uncertainty, and that innovation should be fostered. To best reconcile the conflicts between operations and acquisition it was proposed the next generation C2 be defined as an innovation platform (a 'framework') that balances the needs of acquisition practice with the ability to innovate operationally. Done correctly, it will provide the field commands the technology, information and process flexibility to affect dynamic C2 through field-generated mashups and widgets built within the C2 framework. The use of mashups can help in the creation of a user defined operational picture (UDOP). It was stated that today's 21-year olds are 'digital natives' and are able to construct 'mash-ups' to solve problems – often in the field. Such mash-ups can solve their problems but sometimes challenged traditional C2. Identification of consumer-metrics is a key identification of the most effective mashups and formalise these.

There is recognition that the planning cycle within most current operations is not agile enough for today's complex operational environment. **Professor Tim Grant**, in his paper "**Agile Planning using concurrent operations to increase resilience in NEC",** looked at the application of concurrent engineering as one approach to increase, by a significant magnitude the planning process. The Dutch military Decision Making Process (DMP) was analysed and in theory it could be significantly speeded up by elimination of a number of steps and making a concurrent a number of steps. The next steps will be to test the theory by the development of a prototype concurrent planner and integrate it into an OODA-based C2 testbed.

---

[3] There is work on the NML to evolve it taking into consideration other maturity models, such as the NEC C2 Maturity Model.

[4] TER Author note: Adaptation is one of the components of Agility. A key aspect for consideration within an NEC context, is the relationship between the ability to adapt and time taken to adapt.

Self-synchronisation is another process that can affect C2 within NEC. The paper **'Self Synchronization: a natural phenomenon or hard work presented by Bart van Bezooijen,** presented the results of a number of experiments to address the question of how much can one rely on natural emergent properties versus training. The main outcomes of the experiments were that teams in networked command chains have to be well trained to cope with extra authorities and possibilities. In addition, it appears that leadership style had a dramatic effect upon the team performance; neurotic leaders having a negative impact, whereas altruistic leaders lead to higher team performances.

The next paper looked at **NATO Network Enabled Capability (NNEC) & Force Planning**, A. Zecca presented a NATO view on NEC and NATO's transformation process. NATO has started a transformation and has the put in place an NNEC process to address the NNEC challenges. The NATO Network-Enabled Capability (NNEC) is the Alliance's cognitive and technical ability to federate the various components of the operational environment from the strategic level (including NATO HQ) down to the tactical level, through a networking and information infrastructure." A number of focus areas for NNEC development of capabilities, were outlined in conjunction with timeframes, out in some cases to 2019. This raised a comment from the audience that suggested these timeframes were too long for the realisation of NNEC capabilities. It was suggested that there need to be more adaption of NEC principles and agile, concurrent thinking and development leading to shorter timeframes. In response it was stated that NATO does have mid-term plans at 5 year points.

SESSION 2 – Systems and Systems of Systems

NEC tends to be realised in part through a System of Systems (SoS). Whether or not a system is a system or a SoS can be a matter of viewpoint. However a commonly accepted definition of SoS is "as a set of arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities (Defense Acquisition Guide Book ch.4)". It is commonly recognised that the term SoS applies to complex systems which may have a number of characteristics: Operational Independence of the Elements, Managerial Independence of the Elements, Evolutionary Development, Emergent Behaviour, Geographic Distribution [see Annex C]. During this session of the symposium four papers were presented concerning SoS.

The first paper "**A model-based Architecture to Manage System-of-Systems", was presented by N. Farcett**. This discussed the importance of SoS management for the success of NEC. To fulfil a given operational objective one 'assembles' a SoS. This must be monitored, reassembled, re-planned and reconfigured in light of changes. After achievement of the SoS objectives the SoS or Subset of the SoS may be disposed of.

SoS management is focused on the inter-system management utilising the existing intra-system management. One can use modelling techniques to produce a meta-model to describe the desired SoS architecture. Based on this meta-model one can produce a SoS architecture and subsequently monitor this architecture. Given the complexity then SoS tool support is required. It was proposed that an exploratory team on SoS management be established on the RTO IST Panel. The TER author, agrees that it appears that work is required to address SoS monitoring and that the RTO is one exploratory route. It is not clear whether this should be under the IST or the SCI Panel. It is suggested that as we need to monitor against the operational objectives, and such factors identifying positive or negative contributions to such an operation are not as yet known it should be addressed by a composite panel, in conjunction with the HF Panel.

The intelligent management of SoS networks was the theme of the second paper ' **NEXUS: Autonomic Middleware for flexible and resilient C2 systems", presented by Alex healing**. A SoS relies on large network of heterogeneous information resources and requires a dynamic network topology. As a system (taken to also refer to a SoS) increases in scale and complexity so does the need for 'self' behaviours, allowing the system to manage itself. The Nexus system is a Peer-to-Peer (P2P) agent-based middleware that creates a fully distributed and highly resilient Service Oriented Architecture (SOA).

SoS engineering must enable expression of the understanding of the operational needs, and produce a resultant Architecture; from which one must spirally develop into the operational community as soon as possible. In the case of SoS modelling, a system consideration of people integrated composite of people, products and processes that provide a capability to satisfy a stated need or objective. The papers entitled '**Impacts of Agility, Resilience and Control in NEC of SoS Architecting, Modelling and System engineering', presented by Jean Luc Garnier and Adaptability of Software Intensive Systems.. presented by H. Bachatene** covered these SoS engineering aspects and introduced the NATO Human Views (NHV). There is a draft of human views linking into Operational activities. The use of NHV can help in traceability of spontaneous design, assess the impact of resultant changes and provide feedback analysis.

It is essential to capture spontaneous use and use this to update architecture models.

SESSION 3 – Situation Awareness

Humans require good situational awareness (SA) to undertake their roles within an NEC environment. There has been much work on SA (individual) and Shared Situational Awareness (SSA). It is the latter which of significance in an NEC environment, especially within a NATO, multinational or multiagency operation. Shared Situational Awareness: is a common understanding of a situation. It is not necessary to have the same 'common picture' [but it helps]. Implicit for SSA is a common understanding of a commander's intent and this aids self-synchronisation. SA and SSA are heavily dependent upon training, experience and of course information feeds. A key point to note is that SA is an individual's mental model, it is not an Operational Picture. The Operational Picture contributes towards SA & SSA.

The 'last tactical mile' is one of the more problematic areas in many ways, especially when it comes to mobile forces often with limited communications connectivity. There is a need for an open systems architecture to offer the opportunity to share information faster and more effectively. **H. Thorpe, presented a paper 'ISR Collection for mobile Forces'** which explored many of the issues associated with the 'last mile' information needs. An outline was given of a SOA prototype called ISR Mobile. This illustrated use of a web services infrastructure that supports ISR data discovery and content exposure across a SOA Enterprise. This architecture developed is open and scalable.

An **Integrated Surveillance Prototypal system** was outlined by **Enrico Storti**. The prototype was developed to address the needs for situation awareness associated with homeland defence, such as harbour protection and base defence. Some aspects of HF were looked at in terms of the desired Human Interface and in terms of visualization of the information.

At the edge, the communications are limited and connectivity can be sporadic. The topic of the next paper covered the creation and use of a local operating picture if the connection to the bigger picture is sporadic. The paper was entitled **Network Enabled Technologies Focused on use by semi-autonomous groups and presented by Professor Motus**. One of the aims of the work was to develop a smart user interface and resulted in an interactive map. This was implemented as a proactive multi-agent, it may operate fully automatically, or in a human assisted mode. In many cases the human assistance is required when verifying the consistency of information. The situational information was updated by information acquired from deployable ad hoc sensor networks and is fused into a local operating picture. An end-user may add additional information on his own situation; this information is only broadcast after by approval of a certifying body.

A concept of sharing of ISR information within NATO was outlined within the presentation '**MAJIIC – Enabling JISR interoperability, presented by Matt Roper**. The aims of Multi-sensor Aerospace/ground Joint ISR Interoperability Coalition programme are to develop a Joint ISR network enabled capability, maximising the use of surveillance and reconnaissance resources. The results of which contributing to the commander's situational awareness. The architecture enables the exchange of information via common formats and the information being used to populate a Coalition Shared Database (CSD). Information within the CSD is meta-tagged and aids information discovery and sharing of information. A recent exercise, TRAIL QUEST helped establish the architecture, processes and standards developed were indeed useful in the real-world. Indeed the architecture has been proposed for use in NATOs International Security Assistance Force (ISAF). Follow-on work will aim to address emerging JISR challenges and to allow collaboration with other programmes.

It was recognised within this presentation and within others in the symposium that a prerequisite to information sharing is trust. For example, the potential of the Coalition Shared Database is only realised when nations have a degree of trust to put in information for sharing. Trust is built up over time and may be facilitated by having in place appropriate security measures. The next session, under the umbrella of Architectures dealt with security measures and architectures.

SESSION 4 – Architectures

The first paper in this session covered '**A security framework for Network-Centric Operations', presented by Dr. Cathrina Candolin**. There is often a view that 'security is there to disappoint users' but as we have heard it is one of the elements contributing to trust. Security is divided into three levels: network security, communication security, and content security. Content Base Information Security (CBIS) is recognised as difficult but taking small steps is one way to tackle the problem. The aim is for a proof of concept within the next 3-5 years. The CBIS concept can be applied to a 'Common Operational Picture' to provide trusted sharing of information.

The next paper in this session, although under the architectures session covered many aspects associated with Situational Awareness, recognising the importance of Human Factors cognitive domains and models. The author of paper '**Rethinking the Networked Adaptive Interactive Hybrid Systems (NAIHS) for NEC, presented by Dr. Kester** looked at a system in its environment and the human and non-human aspects. An outline of a number of models were presented, each of which could be applied to system, human and hybrids. In most cases the humans are a part of the process.
The first model was the Observe Orient Decide Act (OODA) loop – the hybrid 'mind' would be involved in the Orient and Decide aspects. Secondly the Joint Director of Laboratories (JDL) information fusion model. This included the addition of a 5th Level for User refinement, to delineate the human from the machine in the process refinement. And, finally, Mica Endsley's SA model. Subsequently a distributed functional Hybrid System model was proposed taking into consideration aspects of the other cognitive models.

Mr. Stil presented a paper Influence of Architectural Modelling on Agility and Resilience this outlined a number of architectural models, such as DODAF, MODAF, and The Netherlands has developed its own architectural framework called DIVA, to standardise its business process. The information included in architecture models can be used for different types of analyses, and at different moments during the life cycle of the system. The use of such architectural models allow a number of possible analyses, such as static, dynamic analyses, dependency analysis and gap analyses. These allow design for interoperability, resilience and agility. One outstanding issue to be addressed is the releasibility of architectural information from different nations. It is difficult to build a useful NEC architectural model without such information. This again raises the issue of trust.

SESSION 5 – Communications and Networking

Communications and networking are the key underlying enablers to facilitate information dissemination within a NEC environment. NEC clearly operates within a heterogeneous communications environment, and has to have agility and resilience catered for. In some cases at the last tactical mile, connectivity may be sporadic and NEC has to be able to accommodate and make best use of sporadic connectivity.

The first paper in this session covered the utility of sporadic connectivity in the 'last tactical mile'. The paper was entitled '**Joint IP based Rolling Network (JIPR): an alternative network proposition to increase shared situational awareness in Joint Operational Missions", presented by Mr Vos**. The paper put forward the concept of JIPR to enable optimum use of ad hoc, dynamic networks and use of airborne relays for Beyond Line of Sight (BLOS) communications to increase SSA. Simulations showed that there are significant advantages to SSA in having such a JIPR concept. The next steps are to undertake field experimentation.

Being able to describe in a semantic form the composite networks in an NEC environment can aid interoperability and network planning and utilisation. In order to achieve high levels of agility and flexibility it is important that all users and providers have a good overview of the capabilities and possibilities of the network. A Network Description Language (NDL), based on the semantic web, Resource Description Framework (RDF) has been developed in the Netherlands. This was described in the presentation **'Network descriptions and NEC'** by **Ham, Keus and Laat.** NDL offers users and network providers with a common ontology to describe topology information of networks. By listening in on the management traffic a network it is possible to automatically create NDL descriptions of the network. These descriptions can be used to monitor the status of the network, to determine which paths will be used between nodes in the network. This allows the administrators to monitor the network and quickly determine possible bottlenecks.

The next paper, '**Adaptive Autonomy for Agile task coordination', by Martijn Neef and Bob van der Vecht,** explored the role of Agent technology and how autonomy may be achieved. This was primarily theoretically based but could have relevance in NEC. TNO had undertaken research into a model that allows artificial agents to control their own autonomy. In an NEC environment there are many roles (actors) and this can translate directly to agents. Agents have a degree of autonomy, that is, you can determine how much you let external events influence your decision making. Indeed, within the model, agents can decide to reject or select requests. The resilience in NEC will depend on actors doing things on their own even if disconnected from others.

The next two papers looked at the 'last tactical mile'. The first looked at intelligent routing to make best use of all available networks to meet, where possible the desired Quality of Service (QoS).

Within today's current and future NEC tactical environments there are many different transmission media can be used to link the various units and command posts together in the battlespace. Because of the mobility of the units, these transmission means are normally radio based, with different bandwidths and protection abilities, and highly variable availability. The transmission means used in tactical networks have large variations in capabilities making it advantageous to define multiple routing topologies for the different characteristics. These topologies are then used to ensure that data packets are only forwarded on topologies supporting the requirements of the data-flow. A paper presented by **Mr Rossow, entitled 'Multi-Topology Routing in resilient Tactical networks**' outlined an Intelligent Tactical IP Router that had recently been developed and tested in Norway. The objectives of the router are to support prioritization of operation critical traffic and take advantage of parallel paths in the heterogeneous network to efficiently exploit all bandwidth resources. The router should also allow for easy the integration of future radio networks technologies.

The final paper in this session '**Dismounted Soldier System Interoperability Requirements …', presented by Mr. Golonko**, looked at the information needs and communications mechanisms for the dismounted soldier system (DSS). The information needs, recognised multimedia needs and included both data and voice. It was suggested that video streaming should be avoided as it consumes a significant radio bandwidth. A number of interoperability proposals were put forward for data and voice exchange between national DSS in a coalition situation.

SESSION 6 – CD & E and Testing

This final session dealt with Concept Development and Testing (CD&E) within the context of NEC. The CD&E process is a ways of gathering together concepts, assessment for importance and relevance, further development of concepts, experimentation and testing.

The first paper presented by **L. Bordelon**, outlined the results from the **SCI Workshop on V&V of NEC.** This workshop took place in September 2007 and involved 8 participating nations. Although, each nation may have had a slightly different view of NEC, the focus was placed on NNEC. The objectives were to try and develop an approach to V&V and outline a roadmap

Vverification is determining if the NNEC does what it is designed to do, and validation is determining if the NNEC does what it is supposed to do. In this context, V&V must be built into the development of network enabled capabilities in an iterative approach starting with the initial concept of operations. Furthermore, as an NNEC collects, processes, integrates and disseminates information, the V&V of an NNEC in essence feeds the research and development of that NNEC. A Task Group was approved for establishment in May 2008. This Task Group is addressing development of a detailed roadmap or approach to accomplish tasks identified by the workshop.

To ensure effective command and control over NATO forces it is essential that in the future all NATO systems such as weapons, C4I and sensor systems are able to participate in NEC-based coalition operations. To realise this, individual systems and expeditionary forces should become 'net-ready'. The challenge then is to understand how we can determine the net-readiness of NEC 'components'.

The next paper outlined work undertaken for the Royal Netherlands Air Force (RNLAF) leading to the subsequent development of a methodology and test environment as an approach to NECE R&D to address this challenge. The paper entitled '**Agile NEC R&D: A Spiral Approach', was presented by Frank Tempelman**. The methodology and test environment developed is termed Adaptive C4I Test and Interoperability Verification Environment (ACTIVE). ACTIVE is used to test the 'net-readiness' of NATO assets in a controlled environment and to use the test results to incrementally adapt existing assets or to develop new assets leading to continuous improvement of the net-readiness.

Another approach to testing NEC capabilities, a US approach, was presented by **Dan Garnier**, in a presentation entitled '**Testing NEC Capabilities in a Realistic Operational Environment**'. In 2006, a project termed the Joint Test and Evaluation Methodology (JTEM) project was established and led to the development of the Capability Test Methodology (CTM) and underlying analytical framework to determine joint mission effectiveness. CTM is based on a collection of best practices fro designing a test of a systems or SoS in a complex joint environment.

It was suggested that the CTM approach could be extended to a multi-national, NATO and Coalition forces for testing of NEC.

CTM was used in a recent (2007) distributed test event, which involved a notional set of network-enabled air and ground launched weapon systems while employed in a realistic joint mission environment supporting an overall joint fire support task. The results of the test illustrated the value of testing early in the acquisition life-cycle. A key aspect to note was the involvement of live operators, who could interact with the early models to identify shortcomings, areas for improvement and relationship with doctrine, tactics, techniques and procedures (TTPs).

The next paper, '**Combining Experimentation and Multi-Criteria Decision Aid …' presented by JP Pignon**, proposed a system of systems architecturing approach of design, evaluate and redesign. This relies on a step by step spiral refinement of candidate architecture and organisations models.

A methodological approach has been proposed to support this activity. It is based on a multi-level model based approach and a multi-criteria decision analysis scientific technique. SoS architecture evaluation models are built, allowing to aggregate the required multiple points of view characterised by metrics related to both functional and non functional properties. Complementary evaluation techniques based on traditional engineering, collective work, modelling and simulation and experimentation provide Measures of Merit (MoM) values which allow objective assessment, and then comparison, of candidate architectural solutions.

Determination and justification of "best" operational, system and human architectures may be performed at different levels of description on multiple points of view. Results are explicit, as is the evaluation model, which guarantees traceability and transparency of the process, as well as knowledge management of the experts.

The final paper of the session and of the symposium, looked at **'Lessons learnt form Tactical Data Link Integration Flight testing at the Airforce Flight Test Centre',** presented by **John Miljan.** This represented testing specific components of a system of systems, that of Tactical Data Links (TDLs). TDL integration and testing relies on an incremental approach. Such an approach can contribute to a Net Ready certification programme.

2.6 Technical Tour

A technical tour of two Research establishments in The Hague took place in the afternoon of the 2nd Day of the symposium. Visits were made to

- NATO C3 Agency: demonstration of MAJIIC and NATO Integrated Command and Control Software.
- TNO Defence and Security – introduction of the TNO's Advanced CD&E Environment (ACE) facility and presentations on NLD NEC projects.

A large number of positive comments were made to the TER regarding the visit to the R&D establishments.

2.7 Administration & Organisation

The administration and organisation of the Symposium was well thought out and executed. The hosting by The Netherlands was excellent and much appreciated. The facilities provided were ideal, and handling of delegates within the symposium area seemed to go smoothly and the proceedings kept reasonably well to time, overall. On the whole, feedback from delegates, on symposium organisation was overwhelmingly positive.

One area to note is that a number of presenters turned up, just before they were to brief, with their presentation on a USB stick. This caused slight delays in the starting of some of the presentations. It is suggested that there

are measures taken to minimise these effects. Such as strict adherence to time lines for submission, and that all authors who have their presentation on a stick, present themselves to the conference organisers as soon as possible to arrange transfer to the network or computer system being used for the presentations.

2.8 Numbers of attendees

The RTO's aims for Symposia are for greater than 100 participants for a duration of 3-4 days. This objective was not met on this occasion. The total number of participants was 89, of which 54 were SCI-Panel members The TER author is not familiar with the RTOs SCI-Panel's communications/'marketing' strategy and processes but suggests that it could, in light of numbers of participants, was not too successful on this occasion and should be reviewed. It must be recognised that NEC as a subject domain has lost its 'buzz-word status' but within NATO and most nations there is a lot of relevant R&D being undertaken. One would thus have expected a greater audience.

2.9 Views on the Symposium as a Whole

Feedback from those delegates[5] who provided it, is given at Annex A. On the whole the symposium was a worthwhile experience and most of the papers met the objectives of the symposium. The majority of papers were relevant for the theme of the symposium Most delegates were satisfied with the level of the presentations, despite these varying greatly, and most considered the bulk of presentations to have been well organised and presented. Timings were generally felt to be about right.

The paper nominated as "most interesting" was given by H. Thorpe on 'ISR Collection for Mobile Forces'. The TER Author found this paper and one by Dawn Myerrieks, 'Next generation C2: Formalizing mash-ups to be worthy of note.

A number of verbal comments suggested that there was a disconnect between the science R&D and the operational community. Ways to mitigate this should be sought.

3. CONCLUSIONS

NEC is a broad and complex domain covering many subject areas from C2, Human Factors, communications theory and technology, information theory and practice, concept development, experimentation and testing and security. On the whole symposium had a good set of speakers to address these many facets of NEC.

A number of key areas were apparent:

- **Evolutionary pressure – the changing security Environmen**t: The current and future mission-space is one of complexity and uncertainty. NATO and nations will undertake many and varied missions, where effects are very closely coupled with multiple, possibly unintended, consequences. These are some of the drivers for change.
- **Sharing of information**
    - Information sharing is essential.
    - Facilitated by people, organisations and technology it relies on trust.
- **Trust**

[5] Number of attendees at Symposium equalled 89, of which 35 were not Panel Members. There were 19 completed questionnaires.

- Trust is a fundamental requisite to NEC. Without which one can not even begin to 'federate' or work together.
- This is trust between people (in the social/cultural Context) and trust in the underlying technology and systems.
- Levels of trust are built up overtime and can be helped by technology and security, including (IA and CBIS). As levels of trust increases so does NEC maturity.
- Trust is heavily influenced by training, especially within multicultural environments such as NATO. The addition of new members of NATO may introduce some issues that will need to be resolved over time. The establishment of trust between all parties is a prerequisite for any collaborative/ multi-national operation in NEC. Mutual trust must exist at all levels of the participating organisations, to their administrative procedures and to the systems in operation.

- **Agility**
  - There are a number of definitions of agility. One of which, by Alberts & Hayes embraces resilience. It was recognised by a number of speakers that Agility requires flexible ways of executing C2 and in some cases this conflicts with traditional, often hierarchical C2.
  - Knowing when to 'flip' is key to agility is being able to know when to change state. This requires knowledge of what you need to measure, when to (frequency) measure, how to measure and what to do within what time-frame.
- **Emergent properties**
  - Can be both positive and negative and affect the technical, cognitive and social networks. The TER Author believes that an important element in the success of NEC will be the early identification of emergent properties and adaption accordingly. This will require monitoring of the situation. This may be undertaken as part of CD&E and/or the umbrella of SoS management. The critical part of such management is to identify the factors, for a given mission, to be monitored, frequency of monitoring and how the monitoring will take place. It was indicated [D.Meyerrieks] that one should monitor for mission effectiveness (mission/operational indicators) not 'geeky' metrics. If positive emergent properties are identified these should be exploited as soon as possible. Obviously, if negative, mitigating steps should be timely. Emergent properties may result in the need to change TTPs
- **Maturity Models**
  - There are a number of maturity models in existence such as the NATO C2 Maturity, the RTO developed C2 Maturity model and others. These should be harmonised where possible.
- **To the edge & 'Last tactical mile'**
  - One of the most problematic and challenging areas
  - Information – there is a significant amount of work looking at getting information out to and from the edge. This includes best use of existing communications links and ways of utilising fleeting opportunities.
  - Utilisation of information – more work may be required looking at new ways of exploiting information. The generation of mashups by 'young 21 year-olds' may exploit information in ways not currently envisioned. We need to recognise and 'formalise' the best of these. Work under many disciplines, including HF, CD&E, C2 must all contribute to identifying 'doing things better not just faster' and 'doing better things'.

- Power/decision making – recognition that pushing decision making to the edge may decrease the coherence of command. In addition it will require SSA, especially of commander's intent. SSA will increase the possibilities of self-synchronised entities.

- **Human dimension**
  - Although many speakers identified the people aspects as being central to NEC, there was on the whole relatively little work presented on the Human dimension.
  - It should be noted that Shared Situational Awareness does not equal a common operational picture. A COP is an enabler for SSA, but SSA is more to do with the human side of things, training, culture, experience and an awareness of doctrine, TTPs.

- **Meeting of Objectives**
  - The TER felt the symposium met many of its objectives and contributed towards the RTO and SCI-Panels mission statements.

4. RECOMMENDATIONS

The following recommendations are made:

NEC

1. Agreed set of terminology is required for NNEC or at least an understanding of any differences.

Maturity Models

2. Work should be undertaken to address the multitude of 'maturity models' associated with NEC

Metrics

3. In respect to Agility, work on understanding and measuring to identify when a change in NEC state is required (when to 'flip') should be a matter for consideration in a collaborative effort between the RTO Panels, such as SCI and HF, and some of the R&D organisations represented within the symposium.

RTO & SCI Panel

4. RTO/SCI-Panel Communications Strategy and Processes - the RTOs SCI-Panel's communications/'marketing' strategy should be reviewed.
5. Liaison with other Panels: the SCI-Panel needs to liaise closely with other lines of development, in particular Human Factors and Simulation and Training.
6. Technical Tours - Where possible, technical tours to relevant R&D establishments should be encouraged.
7. Completion of the symposium questionnaire should be encouraged
8. Ways to mitigate a suggested disconnect between the science R&D and the operational community should be sought.
9. Funding – greater use of the 'contractor support' funding line should be considered by the SCI-Panel to assist directed work to tackle NEC challenges.

ANNEX A

Symposium Questionnaire Summary Findings

Introduction

The tables below represent a summary of the responses to a questionnaire handed out to participants at the symposium. Firstly, is a breakdown of the attendance at the Symposium, followed by responses to the questions.

Attendees

- How many people attended the SCI-PANEL Meeting 54
- How many people attended the symposium (who were not on the SCI-Panel) **35**
- Total Number of Symposium attendees **89**

Responses to Questions: Total Number of Respondents = **19**

1. Was the Symposium worthwhile?

Very	Sufficiently	Partially	Not at all
12	6	1	

2. The theme of the Symposium was:

Very appealing and topical	Sufficiently appealing and topical	Partially appealing and topical	Not appealing and irrelevant
10	9		

3. Did the papers that were presented meet the objectives of the Symposium?

Most did	About half did	Few did
15	3[6]	

[6] One person could not attend all the papers and did not comment on this or some of the other related questions, hence the figures do not always add up to 19.

4. Were the papers relevant for the theme of the Symposium?

Most were	About half were	Few were
14	4	

5. The general level of the papers that were presented was:

Too deep	**Satisfactory**	Too superficial
	17	1

6. The most interesting paper was:

Number of votes	Paper Number
5	**14 – ISR Collection for Mobile Forces, Mr. H. Thorpe**
2	11 – NEXUS Autonomic Middleware for flexible & resilient C2 Systems, Dr. A. Healing
1	Keynotes
1	Keynote 2 – Operational Assessment of NATO Response Force, Col. G. Kanis
1	5 – Using Complex Adaptive System Models to Improve Agility, Mr. P. Petiet
1	7 – Agile Planning Using Concurrent Engineering to increase, Dr. T.J Grant
1	12 – Impacts of Agility, Resilience and Control in NEC of SoS Architecting, Modelling and System Engineering.
1	17 – The NATO MAJIIC project, M. Roper
1	18 – A Security Architecture Framework for Network Centric Environments, Dr. C. Candolin.
1	22 – Network Descriptions and NEC, J. vd Ham
1	25 – Dismounted Soldier System Interoperability Requirements in Coalition Environment for Various Conflict Scenarios, A. Golonko.

7. The least interesting paper was:

Number of votes	Paper Number
1	5 – Using Complex Adaptive System Models to Improve Agility, P. Petiet
1	9 – NATO NEC & Force Planning, A. Zecca
1	20 – Influence of Architectural Modelling on Agility and Resilience, G. Stil
1	27 – Agile NEC Research and Development: A Spiral Approach, F. Templeman

8. Were the presentations of the speakers well organized and effective?

Most were	About half were	Few were
14	4	

9. The quality of the visual aids (e.g. viewgraphs, slides and video presentations) that were used by the speakers was:

Good	Fair	Poor
15	3	1

10. The time allowed for the speakers was:

Too short	**About right**	Too long
	18	1

11. The time allowed for discussion and exchange of ideas was:

Too short	**About right**	Too long
4	**16**	

12. Was the Symposium effectively organized (location, instructions, duration, audio visual equipment, refreshments, etc.)?

Yes	No – Please provide comments
19	

13. The quality of the translation was: ***Not Appropriate!***

Good	Bad – Please provide comments

14. Your overall assessment of the Symposium:

Excellent	**Very Good**	Good	Fair	Poor
4	**10**	4	1	

15. Please add any other comments you have about the Symposium or this questionnaire:

The following comments were noted:

- **Tactical Level:**
  - "Papers often referred to tactical use in the title – but did not actually address"
- **Administration**
  - "The numbers in the audience was too small (c.20). I would expect c. 100 to come to a symposium to ensure messages get across the whole of NATO & PfP. Why were the SCI-Panel members not attendees at the symposium?" "A slightly earlier lunch would be better"
  - 'All Cell phones 'off' during symposium presentations' [and technical tour]
  - 'More Soft drinks'
  - Slightly earlier lunch would be preferred.
- **Technical Tour**: "It would be nice to include demos in the future. Also, the Tech Tour was very worthwhile.
- **Social Networking & learning**
  - "Opportunity to interface with attendees as valuable as the briefings."
  - "I learned a lot on how defence planning is influenced by research and developments – very useful."

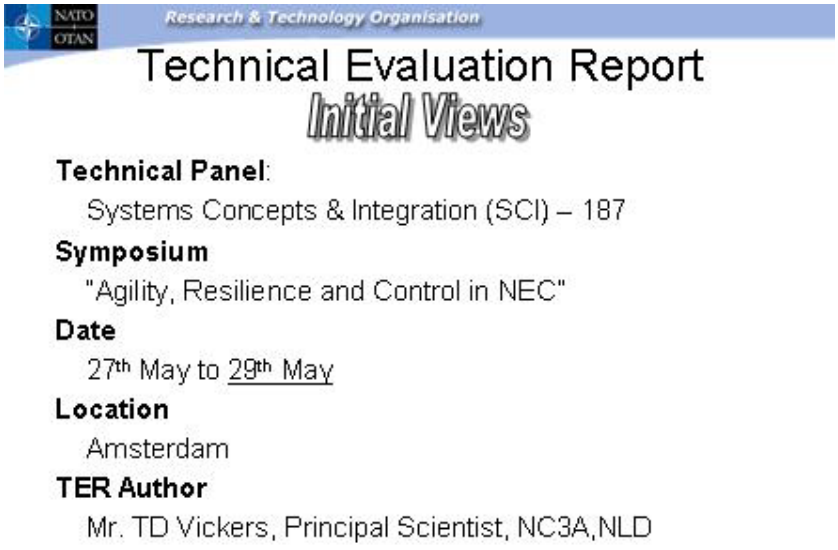
ANNEX B

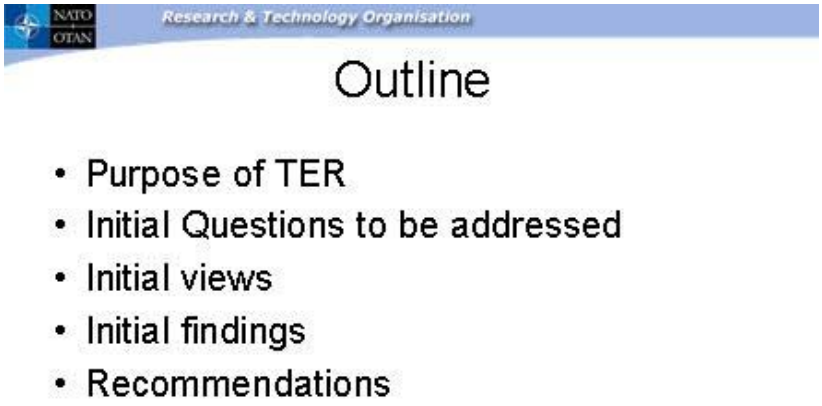
Presentation of Initial Thoughts

Introduction

At the close of the symposium and SCI-Plenary Session the TER author was asked to provide initial feedback on the symposium. The TER author expressed these initial thoughts in a PowerPoint brief.

This has been included in this TER to in the interests of information sharing. It has not been edited and thus is presented 'warts and all'.





Research & Technology Organisation

Purpose of TER

- Present overall technical-scientific situation in the chosen subject
- Comprehensive picture of the meeting presentations as related to their impact on the overall technical-scientific situation
- Set them in relation to each other
- Draw conclusions
- Recommend further actions (work/meetings etc)
- Present the report in a concise, easily digestible form, written in an objective manner
- Submit the report to the appropriate panel or committee as instructed for consideration and forwarding to the RTA Director for approval and potential publication in the proceedings of the meeting.

Research & Technology Organisation

The RTO Mission

To conduct and promote co-operative research and information exchange within NATO and with its "Partners"

Has the symposium contributed towards acheivement of this mission statement?

SCI Mission

" *to further knowledge concerning advanced system concepts, integration, engineering techniques and technologies across the spectrum of platforms and operating environments to assure cost-effective mission-area capabilities"*

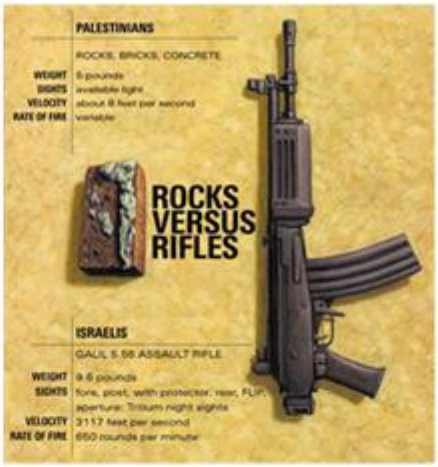
Has the symposium contributed towards acheivement of this mission statement?

•INITIAL VIEWS

Research & Technology Organisation

Drivers for change

- Changing security environment
- Unknown emergent threats
- Legal and political consideration prominent
- Need to cope for above changing environment



Research & Technology Organisation

NEC characteristics

- Agility
- Information Sharing
- Trust
- Technology, cognitive skills
- Decentralised – power to the edge

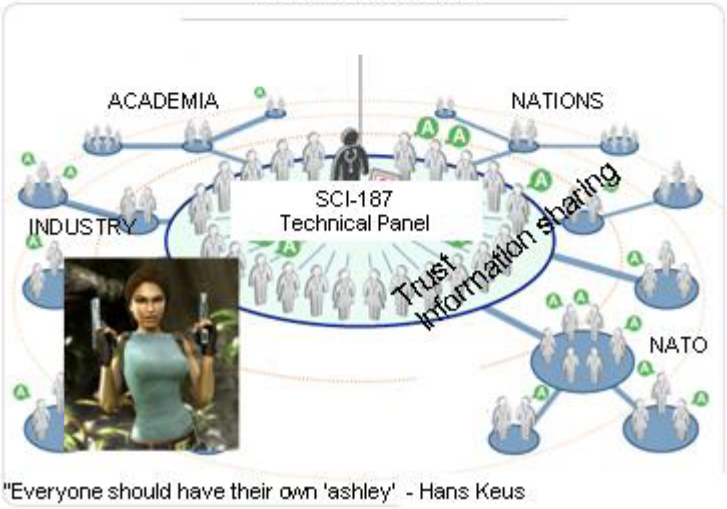
Research & Technology Organisation

NNEC & RTO Similarities

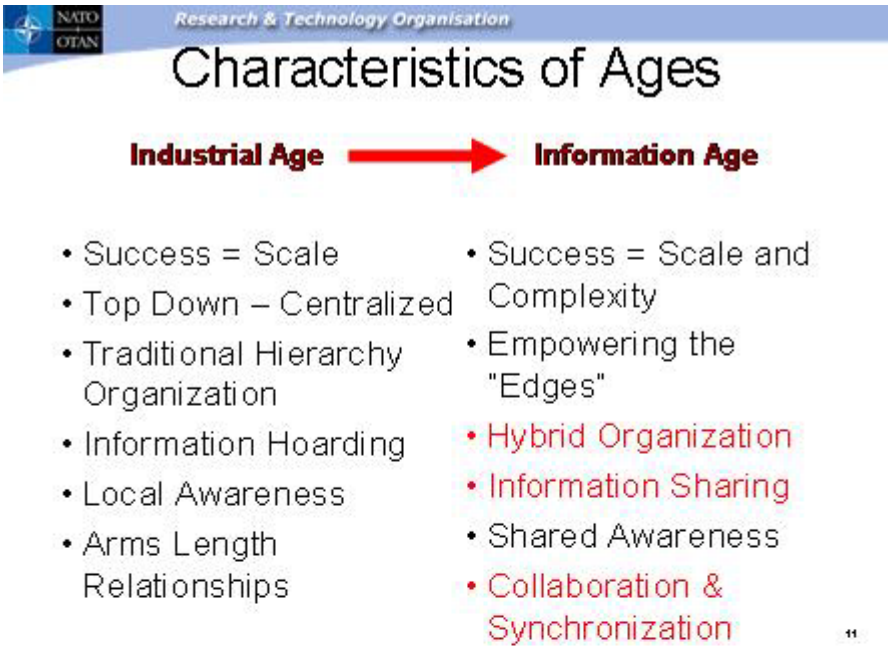
- Set out to achieve a given set of missions & objectives
- Networks
- Encourage information sharing
- Resilient
- Agile

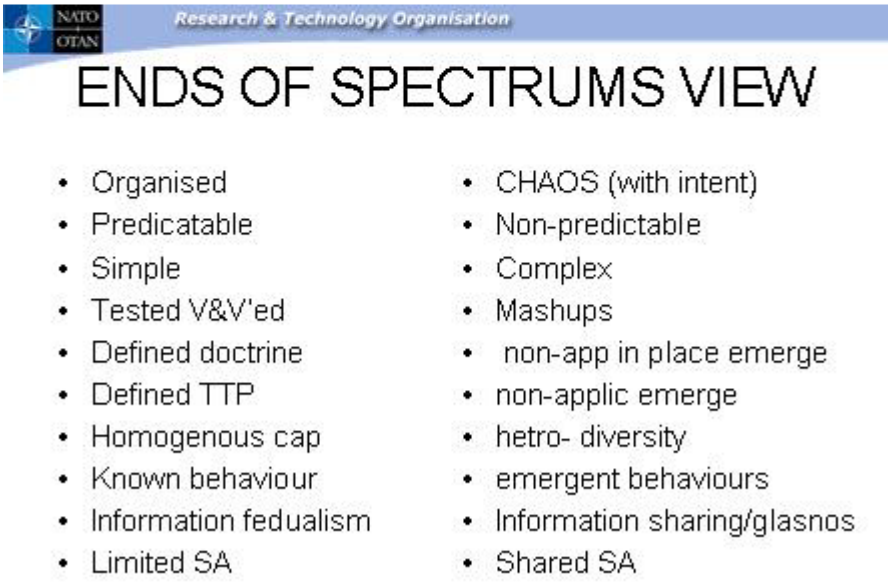
Research & Technology Organisation

RTO – SCI-187 Netcentric?



"Everyone should have their own 'ashley' - Hans Keus


Research & Technology Organisation
Characteristics of Ages
Industrial Age
Information Age
• Success = Scale
• Top Down – Centralized
• Traditional Hierarchy Organization
• Information Hoarding
• Local Awareness
• Arms Length Relationships
• Success = Scale and Complexity
• Empowering the "Edges"
• Hybrid Organization
• Information Sharing
• Shared Awareness
• Collaboration & Synchronization
11

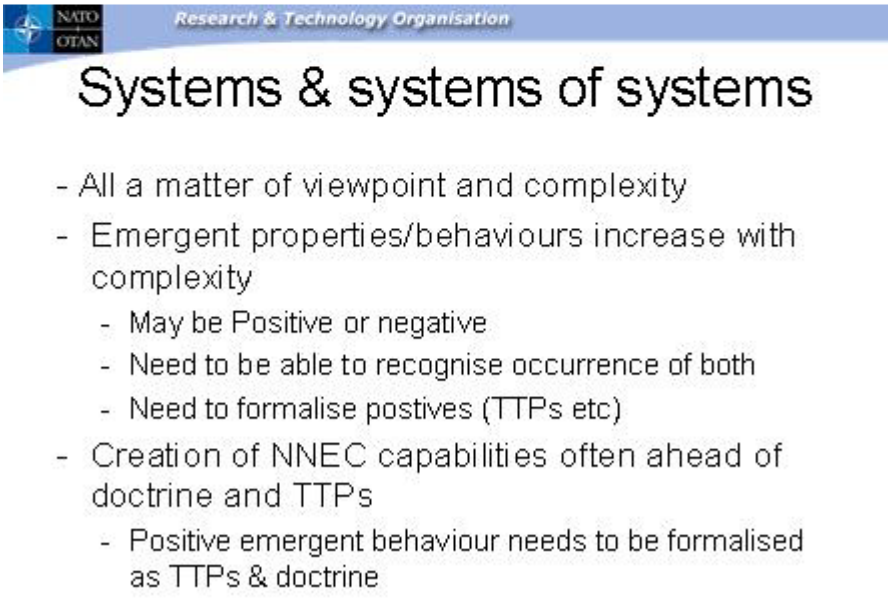

Research & Technology Organisation
ENDS OF SPECTRUMS VIEW
• Organised
• Predicatable
• Simple
• Tested V&V'ed
• Defined doctrine
• Defined TTP
• Homogenous cap
• Known behaviour
• Information fedualism
• Limited SA
• CHAOS (with intent)
• Non-predictable
• Complex
• Mashups
• non-app in place emerge
• non-applic emerge
• hetro- diversity
• emergent behaviours
• Information sharing/glasnos
• Shared SA

•INITIAL FINDINGS

Some Initial Findings

- Excellent set of papers covering some key aspects in NEC – briefed well and Q&A session generating much discussion
- Hosting by Netherlands excellent and appreciated
- Topics covered
  - Command & control
  - Systems & systems of systems
  - Situation Awareness
  - Architectures
  - Communications & networking
  - CD&E and testing


NATO OTAN
Research & Technology Organisation
Command & Control
– initial findings
• NNEC capability maturity model & NNEC C2 Maturity
– Similar to Galliers IS CMM
– Consider rate of transformation, entities/nations at different maturity levels
• Excellent approach to provide scope to audience (researchers to end users)


NATO OTAN
Research & Technology Organisation
Systems & systems of systems
- All a matter of viewpoint and complexity
- Emergent properties/behaviours increase with complexity
- May be Positive or negative
- Need to be able to recognise occurrence of both
- Need to formalise postives (TTPs etc)
- Creation of NNEC capabilities often ahead of doctrine and TTPs
- Positive emergent behaviour needs to be formalised as TTPs & doctrine

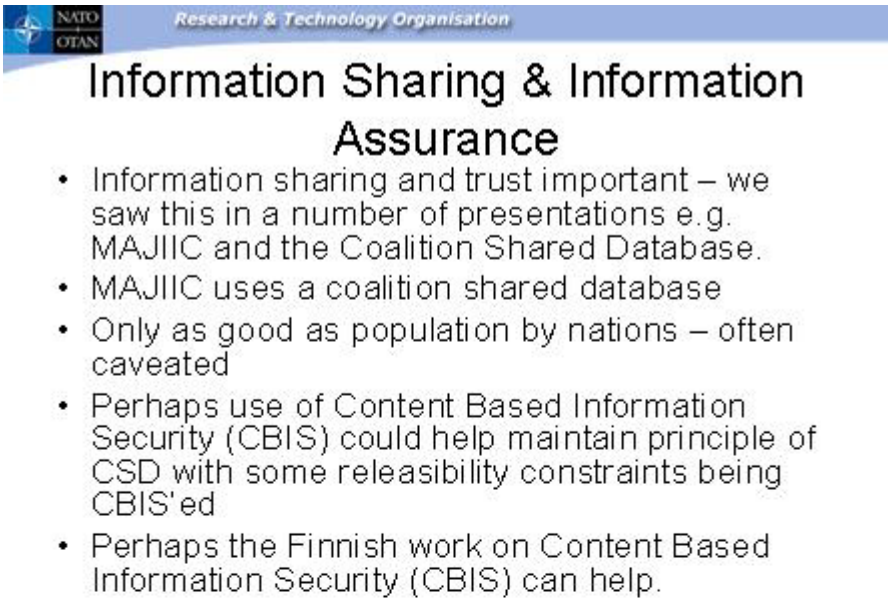
Research & Technology Organisation

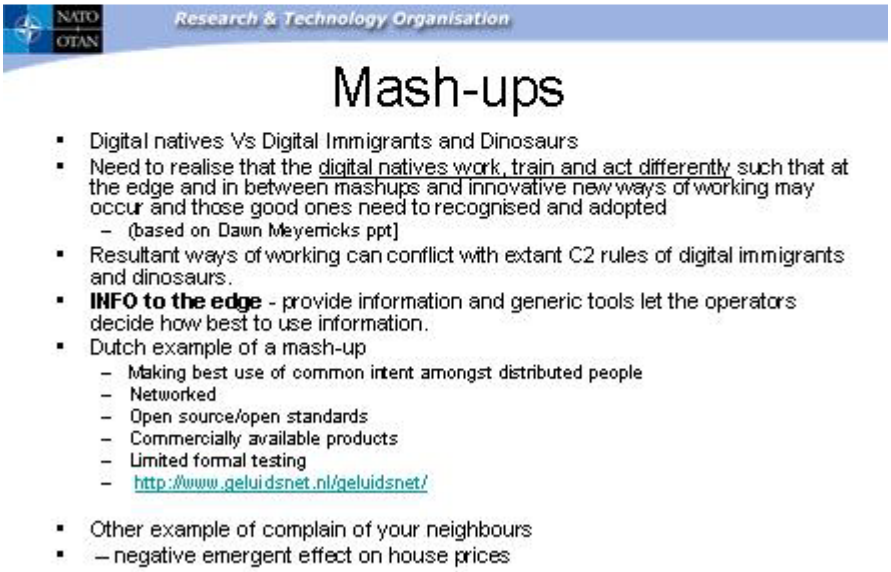
Information focus

- Lots of work on the gathering and dissemination of information at all levels
- May be more work required on looking at new ways of using information, new processes

"doing things better not just faster"
& "doing better things"

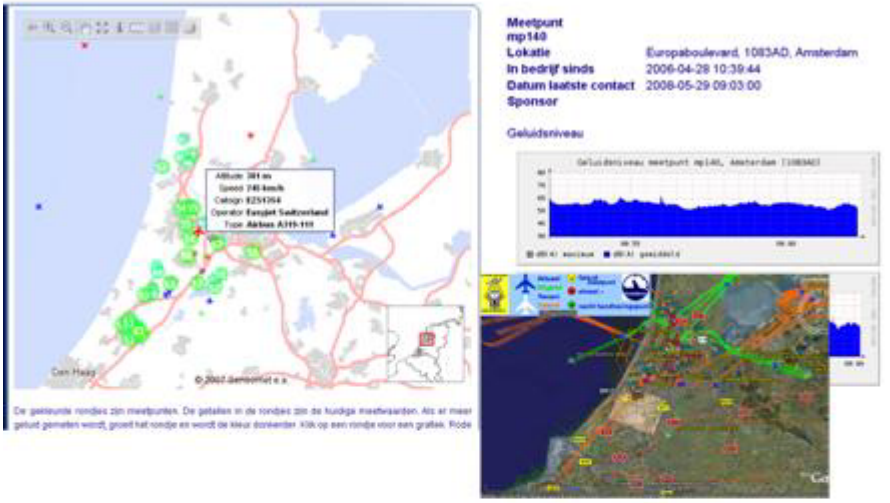
Research & Technology Organisation


NATO OTAN
Research & Technology Organisation
Information Sharing & Information Assurance
• Information sharing and trust important – we saw this in a number of presentations e.g. MAJIIC and the Coalition Shared Database.
• MAJIIC uses a coalition shared database
• Only as good as population by nations – often caveated
• Perhaps use of Content Based Information Security (CBIS) could help maintain principle of CSD with some releasibility constraints being CBIS'ed
• Perhaps the Finnish work on Content Based Information Security (CBIS) can help.


NATO OTAN
Research & Technology Organisation
Mash-ups
▪ Digital natives Vs Digital Immigrants and Dinosaurs
▪ Need to realise that the digital natives work, train and act differently such that at the edge and in between mashups and innovative new ways of working may occur and those good ones need to recognised and adopted
– (based on Dawn Meyerricks ppt]
▪ Resultant ways of working can conflict with extant C2 rules of digital immigrants and dinosaurs.
▪ INFO to the edge - provide information and generic tools let the operators decide how best to use information.
▪ Dutch example of a mash-up
– Making best use of common intent amongst distributed people
– Networked
– Open source/open standards
– Commercially available products
– Limited formal testing
– http://www.geluidsnet.nl/geluidsnet/
▪ Other example of complain of your neighbours
▪ – negative emergent effect on house prices

Research & Technology Organisation

Geluidsnet – mashup



Research & Technology Organisation

People & Human Factors

- People are a key component of NNEC but still emphasis still seems to be on the technical network side
- Human Factors
  - E.g. Situational Awareness is more than just common picture (cf Stat to Tactical TDLs and testing)
  - See work of Mica Endsley (L1 Perception, L2 Comprehension and L3 Projection – cf JDL Fusion Model.
  - May require liaison with HF panel

Research & Technology Organisation

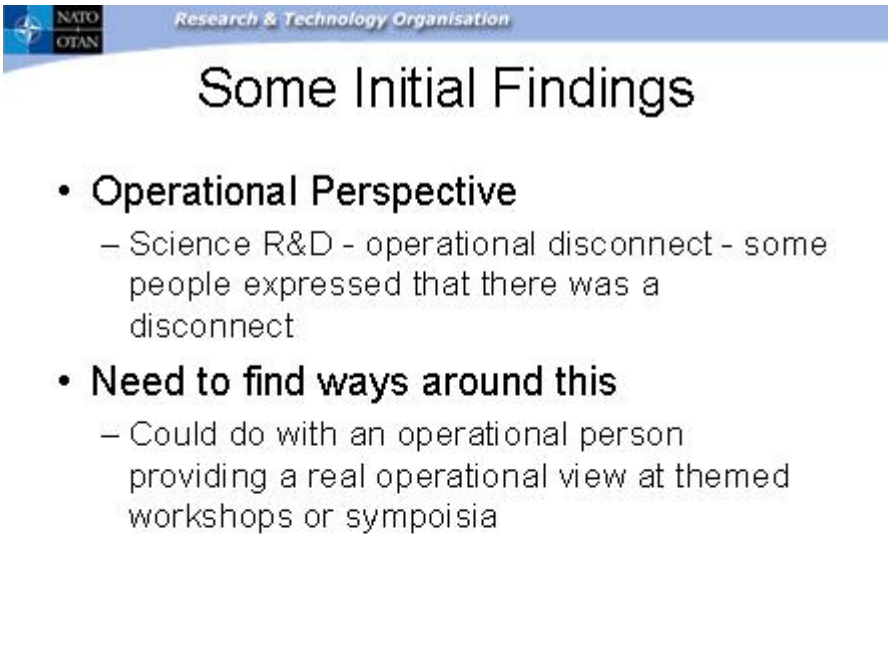
Initial Findings

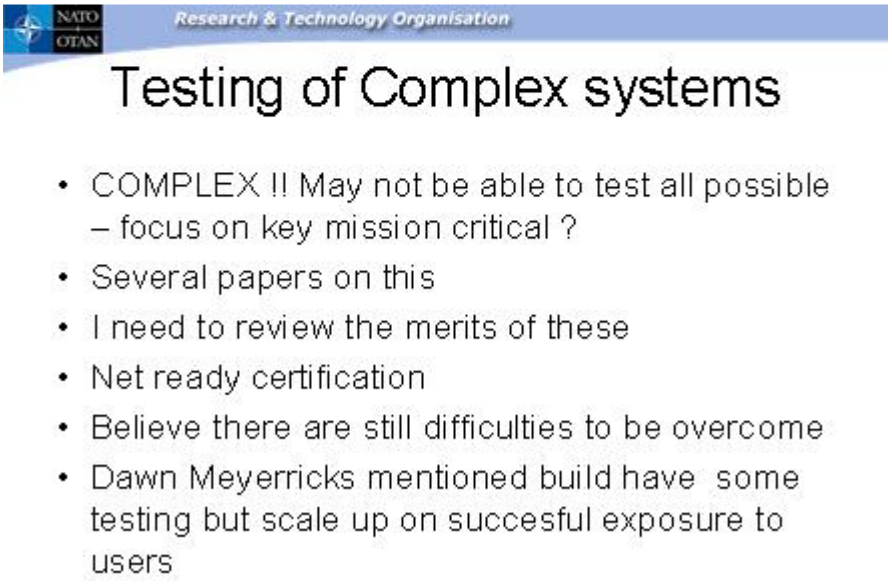
- Last mile – most problematic area in many ways (info to the edge, technical, mashups, lack of TTPs to meet new ways of working as old doctrine TTPs less relevant in new security enviroments
- Lack of persistent connectivity
- SA periodic
- Dynamic environment
- High Pressures for agility

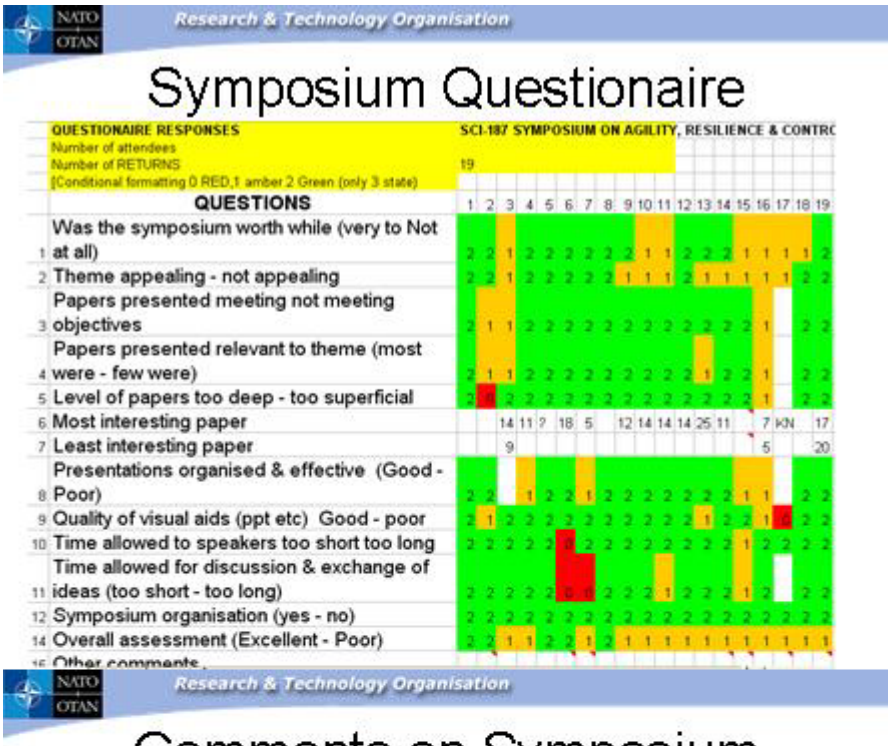
Research & Technology Organisation

AGILITY – Cybernetic Principal

- Agility requires good cybernetic principles, a feedback/monitoring mechanism
  - that is at the right frequency, measuring the right factors to enable a decision maker to make the appropriate decision, and communicate this to the right effectors, in the right timeframe.
- Agility is aided by diversity –
  - Diversification is one mechanism to deal with an unknown future
  - enabling best use of assets of all NATO nations creates diversity aiding agility.


NATO OTAN
Research & Technology Organisation
Some Initial Findings
• Operational Perspective
– Science R&D - operational disconnect - some people expressed that there was a disconnect
• Need to find ways around this
– Could do with an operational person providing a real operational view at themed workshops or sympoisia


NATO OTAN
Research & Technology Organisation
Testing of Complex systems
• COMPLEX !! May not be able to test all possible – focus on key mission critical ?
• Several papers on this
• I need to review the merits of these
• Net ready certification
• Believe there are still difficulties to be overcome
• Dawn Meyerricks mentioned build have some testing but scale up on succesful exposure to users



Comments on Symposium

- "Opportunity to interface with attendees as valuable as the briefings"
- "It would be better to include demos in the future. Also the technical tour was very worthwhile"
- Numbers at symposium to few
- "Why did the SCI panel members not attendees at the symposium"

Comments on Symposium

- "I learnt a lot on how Defence Planning is influenced by R&D – very useful"
- "Papers often referred to tactical use in the title – but did not address"
- Mobile phones should be switched off in the symposia and technical tour
- "Earlier lunch would be preferred"

Some Initial Findings

- human factors, social engineering and cognitive studies are probably one area to be followed up
- dimensions of NEC
  - technological
  - cognitive
  - social
- SoS analogy with pool of services - dynamic use creation of a dynamic SoS
- spectrums -
  - order - disorder
  - system or system of systems matter of abstarction and emergent properties
  - SoS as a service
- Cultural challenges
- CROSS /INTER AGENCY interop - info exchange/sharing
- difference between service and set of services are emergent behaviou and uses.
- OPEN SOURCE and standards required
- Recognising 70% solutions
- Difficulties in V&V on evolving complex systems

- INITIAL
- RECOMMENDATIONS

RTO – Taking the next steps

- Human factors, social engineering and cognitive studies are probably one area to be followed up with HF panel
- Participation
  - Need to encourage participation at symposia how – wider dissemination to Panel reps and beyond
- Taking next steps
  - I need to consider
    - outputs of working sessions
    - Questionaire response
  - Discussion of research areas with ACO
  - Areas for NATO research – feed into ACT cycle

ANNEX C

ABBREVIATIONS/GLOSSARY

ACE	Advanced CD&E Environment
ACT	Allied Command Transformation
ACTIVE	Adaptive C4I test and Interoperability Verification Environment
Adaptability	The ability to change in response to changes in an environment.
Agility	Agility is seen as including robustness, resilience, responsiveness, flexibility, innovation, and adaptation in order to be effective (Alberts and Hayes 2003). Agility is a core ethos of mind, function, equipment and procedure. It will fundamental to future operations and has four attributes, which can be measured: responsiveness, robustness, flexibility and adaptability. [Recommended read - RAF Air Power Review, Vol 6, number 3, Autumn 2003 - http://www.raf.mod.uk/rafcms/mediafiles/497EBDC6_1143_EC82_2E260662250E094B.pdf
Appropriation	"A process in which a technology is explored, evaluated and adopted or rejected by users. As outcomes of the process of appropriation, either the technology is adapted and integrated into the users' everyday lives (appropriation) or users decide not to use it (disappropriation).[Carroll, J. et al "Identity, power and fragmentation in cyberspace; technology appropriation by young people, Working paper 01/IDG/2001, Department of Information Systems,University of Melbourne, 2001.]
C2	"Command and Control is the exercise of authority and direction by a properly designated commander over assigned forces performed through an arrangement of personnel, equipment, communications, facilities and procedures in the accomplishment of a mission. C2 is the art to use these enablers to accomplish the mission" [C2CoE, MOU June 1997]
C4I	Command, Control, Communications, Computers and Intelligence
CD&E	Concept Development & Experimentation
CoE	Centre of Excellence
CTM	Capability Test Methodology
DAT	Defence Against Terrorism
DSS	Dismounted Soldier System
Emergent properties	'Emergent properties' represent one of the most significant challenges for the engineering of complex systems. They can be thought of as unexpected behaviours that stem from interaction between the components of an application and their environment. In some contexts, emergent properties can be beneficial; users adapt products to support tasks that designers never intended. They can also be harmful if they undermine important safety requirements. There is, however, considerable disagreement about the nature of 'emergent properties'. Some include almost any unexpected properties exhibited by a complex system. Others refer to emergent properties when an application exhibits behaviours that cannot be identified through functional decomposition. In other words, the system is more than the sum of its component parts."http://www.dcs.gla.ac.uk/~johnson

ICECAP	ISAF C4I Enabled Capability – NATO program to undertake systems checks before deployment to ISAF.
IP	Internet Protocol
ISR	Intelligence Surveillance and Reconnaissance
JIPR	Joint Internet Protocol based Rolling Network
JTEM	Joint Test and Evaluation Methodology
Mashup	In technology, a mashup is a web application that combines data from more than one source into a single integrated tool; an example is the use of cartographic data from Google Maps to add location information to real-estate data, thereby creating a new and distinct web service that was not originally provided by either source.
MoM	Measures of Merit
MoU	Memorandum of Understanding
NAIHS	Networked Adaptive Interactive Hybrid System
NATO	North Atlantic Treaty Organisation
NDL	Network Description Language
NEC	Network Enabled Capability
NHV	NATO Human Views
NMLs	NNEC Maturity levels. There are 5 levels: • NML 1 – Standalone • NML 2 – De-conflict • NML 3 – Coordinate • NML 4 – Collaborate • NML 5 – Coherent
NNEC	NATO Network Enabled Capability – "*is the Alliance cognitive and technical ability to federate the various components of the operational environment from strategic level (including NATO HQ) down to the tactical level, through a networking and information infrastructure*" [MCM-0032-2006, dated 19 April 2006]
NRF	NATO Response Force
P2P	Peer to Peer
QoS	Quality of Service
R&D	Research and Development
RDF	Resource Description Framework
RNLAF	Royal Netherlands Air Force
SA	Situation Awareness - "*SA is 'knowing what's going on so you can figure out what to do*'. [Barry McGuiness, Sowerby Research Centre] - *SA is "The assimilation of current and historical information to form a mental model of what is going on and what is likely to happen in the future, in order to support timely decision-making***"**

- "*the perception of the elements in the environment within a volume of space and time, the comprehension of their meaning, the projection of their status into the near future, and the prediction of how various actions will affect the fulfilment of one's goals*" [Mica Endsley]

SCI	Systems Concepts and Integration panel
Self-Synchronisation	The seminal work on Network Centric Warfare by Alberts, Garstka and Stein describes the key elements of self-synchronisation as: 'two or more robustly networked entities, shared awareness, a rule set, and a value-adding interaction'. Simply put self-synchronisation is doing the right thing, at the right time, for the right reason without having to be told by someone higher in the chain of command. Some advantages of self-synchronisation are speed of command, speed in exploiting opportunities, adaptability and reduced Planning [Araki, L.M.K., Naval War College, "Self-Synchronisation: What is it, how is it created and is it needed?" 5Feb, 1999 http://handle.dtic.mil/100.2/ADA363229 Self-synchronisation requires - Clear and consistent understanding of command intent; - High quality information and shared situational awareness; - Competence at all levels of the force; and - Trust in the information, subordinates, superiors, peers, and equipment. [Alberts & Hayes – Power to the Edge]
SOA	Service Oriented Architecture
SoS	System of systems is a term used `for a collection of task-oriented or dedicated systems that pool their resources and capabilities together to obtain a new, more complex, 'meta-system' which offers more functionality and performance than simply the sum of the constituent systems'. [Wikkipedia]. **SoS** is defined as a **set of arrangement of systems** that results when **independent** and useful systems are integrated into a larger system that delivers unique **capabilities** (Defense Acquisition Guide Book ch.4, https://akss.dau.mil/dag/). Five principal characteristics are useful in distinguishing very large and complex but monolithic systems from true systems-of-systems. 1. Operational Independence of the Elements: If the system-of-systems is disassembled into its component systems the component systems must be able to usefully operate independently. The system-of-systems is composed of systems which are independent and useful in their own right. 2. Managerial Independence of the Elements: The component systems not only can operate independently, they do operate independently. The component systems are separately acquired and integrated but maintain a continuing operational existence independent of the system-of- systems. 3. Evolutionary Development: The system-of-systems does not appear fully formed. Its development and existence is evolutionary with functions and purposes added, removed, and modified with experience. 4. Emergent Behaviour: The system performs functions and carries out purposes that do not reside in any component system. These behaviours are emergent properties of the

entire system-of-systems and cannot be localized to any component system. The principal purposes of the systems-of-systems are fulfilled by these behaviours.

5. Geographic Distribution: The geographic extent of the component systems is large. Large is a nebulous and relative concept as communication capabilities increase, but at a minimum it means that the components can readily exchange only information and not substantial quantities of mass or energy.
http://www.infoed.com/Open/PAPERS/systems.htm

SSA	Shared Situational Awareness: is a common understanding of a situation. It is not necessary to have the same 'common picture' [but it helps].
System	A system is an integrated composite of people, products capability to satisfy a stated need or objective.[Pignon et al, SCI-187, paper 29]
TDL	Tactical Data Links
TER	Technical Evaluation Report
Trust	There are numerous definitions of trust since the term is used in many different areas like psychology, sociology, and in information science and technology. However, there is no widely accepted definition of trust. Listed below are some examples. ***Trust:*** Strong belief, in the goodness, strength, reliability of something or somebody, responsibility. (The Oxford English Dictionary). ***Trust:*** the assured reliance on the character, ability, strength, or truth of someone or something. (Webster Dictionary). For NEC all these definitions are relevant, the first two on the organisational and personal level, the last taken from computer science, on the system/technical level. The terms trust and assurance are often used interchangeably, but in practice, especially from a systems perspective, these topics are quite different. Trust is a subjective measure that is based on some sort of evidence or beliefs on how the other entity will behave. Security assurance (or assurance) is an objective measurement of how well a device/product does what it is supposed to do supported by evidence resulting from the application of assurance techniques. [Tor Gjertsen, 'Trust', RTO-MP-IST-073].
TTPs	Tactics, Techniques and Procedures
UDOP	User Defined Operational Picture
V&V	Verification and Validation