On Information Superiority Achievement

Darko Galinec
Ministry of Defence of The Republic of Croatia
Bauerova 31/2, Zagreb
darko.galinec@morh.hr

Ljerka Luić
B4b Zagreb
Ulica grada Vukovara 271, Zagreb
ljerka.luic@b4b.hr

Željko Katalenić
Ministry of Defence of The Republic of Croatia
Bauerova 31/2, Zagreb
zeljko.katalenic@morh.hr

Abstract. *In presence of rapid development of information and communications technology (ICT) able to increase data processing, much more data can be stored, used and/or mediated and disseminated. Technology for extracting and assembling data into valuable information set has become of huge importance nowadays. Information and knowledge become a resource of strategic importance in complex systems, both business and military. On the other hand the question of credibility of the collected data arises: complex systems have to deal with an increasing access to information with less knowledge about their origins and their quality. Due to this lack of information on information, contemporary organizations suffer from organizational indifference: There is a constant presence of the risk that multitude of voices in an organization's environment turns into an unintelligible cacophony or even white noise [16].*
In this paper the ways and means for achieving information superiority in complex systems are examined, with special emphasis to military systems. As a result, two approaches within the military domain are presented: Network Enabled Capability (NEC) and Multilateral Interoperability Programme (MIP). Firstly, if implemented correctly those enable technical, semantic and process interoperability. Secondly, consistent appliance of proposed approaches leads to possible achievement of information superiority.

Keywords. command and control information system, information superiority, network enabled capability.

1 Introduction

By following the hypotheses of Peter F. Drucker and Dirk Baecker we can observe the dawn of the so called *next society*. The crucial driving force of the corresponding change is the evolution of computer communication as new media of dissemination: Much more data than ever before can be saved, activated and disseminated. In addition, bits and bytes can't be read like books because they have to be mediated and reproduced by resource consuming software and hardware. Finally computer communication manifests and presses ahead the detemporization, virtualization, and poly-contextuality of information, and is therefore said to be the major driver for an unmanageable complexity of communication [16].

In the military most decision situations possess a degree of ambiguity and uncertainty and are not easily captured in a static or stochastic model. This has led to an increased use of "fuzzy sets" in analyzing decisions, not in an attempt to quantify the unquantifiable, but as a way to formalize our way of dealing with the unquantifiable and imprecise [1], [5]. The concept of fuzziness is related to the idea of the "fog of war" introduced by Carl von Clausewitz. In his discourse *On War*, Clausewitz presents two concepts leading to difficulties in conflict, friction and fog. Friction is the effect of numerous minor incidents which reduce the level of performance so the intended goal is not reached [2]. There are physical and psychological aspects of friction. Friction due to a hostile physical environment is usually more obvious; it is caused by darkness; bad weather or terrain, physical exertion; degraded command and control, logistics, maintenance, or weapon systems; or merely chance bad luck; or psychological factors, such as stress produced by the interaction of combatants and the environment of war. Another source of friction is the "fog of war." Fog is the uncertainty of war, caused by factors such as inaccurate, incomplete or contradictory information, deviations in weapon system efficacy, actions of the enemy, and the enemy's nebulous capabilities and intentions [4]. Operational decision-maker usually faces decisions under conditions of uncertainty-intrinsically imprecise decisions under adverse conditions would normally be faced in military operations.

2 Information superiority

Information superiority is that degree of dominance in the information domain which permits the conduct of operations without effective opposition [17].

Sound thinking and decision making are more than mere loose ends of network-centric warfare.

Moreover, success in competition on the military cognitive plane will not necessarily follow success on the technological plane. Therefore, what is needed is a coherent strategy to build battle-wise forces.

2.1 Decision superiority

Decision superiority-"the process of making decisions better and faster than an Adversary"-is essential to executing a strategy based on speed and flexibility. Decision superiority requires new ways of thinking about acquiring, integrating, using and sharing information. It necessitates new ideas for developing architectures for command, control, communications and computers (C4) as well as the intelligence, surveillance and reconnaissance assets that provide knowledge of adversaries. Decision superiority requires precise information of enemy and friendly dispositions, capabilities, and activities, as well as other data relevant to successful campaigns.

Battle space awareness, combined with responsive command and control systems, supports dynamic decision making and turns information superiority into a competitive advantage adversaries cannot match. Persistent surveillance, ISR management, collaborative analysis and on-demand dissemination facilitate battle space awareness. Developing the intelligence products to support this level of awareness requires collection systems and assured access to air, land, sea and space-based sensors.

Decisions to apply force in multiple, widely dispersed locations require highly flexible and adaptive joint command and control processes. Commanders must communicate decisions to subordinates, rapidly develop alternative courses of action, generate required effects, assess results and conduct appropriate follow-on operations. A decision superior joint force must employ decision making processes that allow commanders to attack time-sensitive and time-critical targets. Dynamic decision making brings together organizations, planning processes, technical systems and commensurate authorities that support informed decisions. Such decisions require networked command and control capabilities and a tailored common operating picture of the battle space [18].

Awareness of the growing operational and strategic importance of decision superiority must exist, which has some but not all of the elements of the superiority in cognitive capacity and performance that we call battle-wisdom. It also tells us that responsive command and control systems, collaborative analysis, and on-demand dissemination of information are important to decision superiority. This is encouraging. However, this official explanation of what is required for decision superiority fails to stress human cognition-how people think and how well they decide. It is as if battle-wisdom-the capacity to integrate reliable intuition and rapid reasoning and the abilities to anticipate, decide quickly, seize opportunities, and learn in action-is assumed, needing only better intelligence sensors, information networks, and processes to succeed. It calls for commanders to communicate their decisions to subordinates, without recognizing that the subordinates may well be better informed than their superiors to decide what to do. The networking is not that it enables commanders to promulgate orders but that it informs those "on the edge" and permits them to collaborate, accept responsibility, and take initiative. The key to decision superiority lies not in the information network but in the human [9].

2.2 Decentralized Decision making

The value of self-directed learning can be undermined if individuals lack the trust and confidence of their superiors and are not granted the authority to make decisions. Many strong businesses are distributing decision making authority to those on the front lines, a practice that not only enables an organization to act with greater agility and speed but also imparts confidence to those who make the decisions. Businesses in the 1980s and 1990s were swamped with new management theories-to name a few: total quality management, continuous improvement, right-sizing, core competence, process engineering, strategic alliances, competitive strategies, learning organizations, empowerment, flattening of hierarchies, cross-boundary teaming etc. None of these theories alone induced sustainable organizational change without the mutual commitment of leadership and rank-and-file employees. For reform to be sustainable, an organization must put into practice certain values and principles concerning information, people, and trust: transparency; open information-sharing; cross-boundary communication and collaboration; an understood mission and values; a culture that rewards taking responsibility; a commitment to learning; and a willingness to give talent room and to give people the confidence and authority to make decisions. Many companies, large and small, have achieved success by applying these principles and practices. Although focused on decentralized decision making, other ways of enhancing and harnessing information, people, and trust also can contribute to the overall success of an organization.

As predicted by theories of complex adaptive systems, corporate decentralization seems to be a rewarding way to function in a dynamic marketplace. Problems are too complex and markets too urgent for the one or the few to understand, decide, and act. Organizations that need to wait for bureaucratic procedures, chain-of-command review, or decisions from on high before acting on an opportunity may not be able to survive in fluid and unfamiliar situations [9].

3 Situation Awareness

Situation Awareness (SA) has several dimensions and is closely related to Decision Support Systems.

SA is the perception of environmental elements within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. It is also concerned with perception of the environment critical to decision-makers in complex, dynamic areas from aviation, air traffic control, power plant operations, military command and control (C2). SA involves being aware of what is happening to understand how information, events, and actions will impact goals and objectives, both now and in the near future. It directly depends on Information Superiority and Common Operational Picture (COP). COP is a single identical display of relevant (operational) information (e.g. position of own troops and enemy troops, position and status of important infrastructure such as bridges, roads, etc.) shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situation awareness [17].

Situation awareness may be expressed and presented as follows:
SA = f (IS, COP).

3.1 Role of the Defence Chief Information Officer

Within defence organizations, situation awareness is generally divided into two categories - real-time battlefield situation awareness (e.g., US Blue Force Tracking) and a broader, less real-time capability often associated with either a balanced scorecard or "dashboard" for senior leadership:

- Battlefield SA - one of the biggest problems the US system has faced is the exponential growth in both usage and data feeds (data from various sensors). The system was not initially designed to support this environment and was developed in a very "stovepipe" fashion. The future of this and similar systems is their ability to adapt quickly to changes in mission, environment, and data streams. The primary role of the Chief Information Officer (CIO) in this environment should be to define and enforce data interoperability standards to enable the system to be agile - see the attached research on architecting the emergent enterprise. Functional proponents and functional oriented developers will seldom see the value or long-term impact of developing to an enterprise vision. This is the prime function a Defence Chief Information Officer (DCIO) can bring to the battlefield systems. However, as further discussed below, linkage of the value of an enterprise ICT approach to mission accomplishment is critical. In the case of battlefield SA, that value is likely best expressed in terms of agility to changing mission situations and interoperability with current and future coalition partners.
- Enterprise SA - in addition to the standards work mentioned above, the DCIO has several additional functions that should be performed in support of this broader Situation Awareness requirement. The most basic function is to work with the mission leads to develop an Information technology (IT) Strategy [7]. Also, key pieces of the IT Strategy are the Enterprise Architecture [15] and the Enterprise Sourcing Strategy [6]. One of the keys to CIO success in transitioning from an infrastructure services operator to a full mission partner is developing a mission performance mindset. Mission performance metrics and how ICT impacts those mission performance metrics is one of the more challenging aspects of CIO life for most defence CIOs, but is also the area that is most powerful in linking ICT capabilities to mission capabilities. Attached is a sample CIO dashboard for defence organizations that reflects the concepts of performance management of both the mission capabilities and ICT operations. The suggestion would be to expand upon the Mission Performance section as an Enterprise dashboard for the senior non-IT leadership within the organization.

3.2 Typical challenges

Two main challenges for DCIO exist:

- Credibility - many warfighters and mission leaders have had poor experiences with the stability and responsiveness of central ICT organizations and, therefore, the CIO lacks credibility to "sit at the table". Linking IT performance to Mission Performance metrics is a critical 1st step in establishing that credibility.
- Knowledge - many DCIOs lack the mission understanding to communicate the value of ICT capabilities to the mission in terms the non-ICT leadership understands. There are several ways to overcome this, either by bringing more mission personnel into the ICT organization or detailing a senior ICT manager to work with and even deploy with combat unit to fully understand the mission challenges and vocabulary.

Based on the results of business process analysis, CIO as a leader of ICT function in a complex system can and should initiate process change, streamline the processes or suggest introduction of the new processes if necessary, in order to improve overall business process [8].

Military organizations have been, and will continue to be, challenged to improve the tactics, techniques, and procedures (TTPs) associated with executing their mission. ICT has played a major role in the evolution of TTPs over the past 15 years and that IT role is increasing with the adoption of Net-Enabled Warfare

concepts. However, leaving the application of ICT to support business process improvement in the hands of the knowledgeable functional proponent has resulted in numerous marginal systems and an extensive array of stove-piped applications. Too often, an emerging technology or the latest "gadget" that is purported to solve all their problems overly influences the well-meaning functional lead. Functional proponents, who are paid to be functional experts and not ICT experts, are even more prone to fall into the trap of "peak of inflated expectations". DCIOs have an opportunity and an obligation to take a leading role in the effective and efficient application of ICT to mission process improvement across all functional areas [14].

4 Consultation, command and control architecture framework

NATO consultation, command and control architecture framework (NAF) version 3 with its views and the reports generated from the NATO meta model (NMM) based repository defines a common language for architecture representation, and it provides the means to help achieve better communication between architects as well as between architects and stakeholders.

The United Kingdom Ministry of Defence Architectural Framework (MODAF) defines a standardized way of conducting Enterprise Architecture and provides a means to model, understand, analyze and specify Capabilities, Systems, Systems of Systems, and Business Processes. The purpose of MODAF is to provide a rigorous system of systems definition when procuring and integrating defence systems. MODAF was originally based on the United States Department of Defense Architectural Framework (DoDAF), extending it by two additional viewpoints - strategic and acquisition. The first version of the development DoDAF was developed in the 1990s and was called Command, Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework. Revision 3 of the NAF is identical to MODAF at its core, but extends the framework by adding views for bandwidth analysis, Service Oriented Architecture (SOA) and standard configurations.

The seven views are:
- NATO All View (NAV)
- NATO Capability View (NCV)
- NATO Operational View (NOV)
- NATO Service-Oriented View (NSOV)
- NATO Systems View (NSV)
- NATO Technical View (NTV)
- NATO Programme View (NPV)

Each view has a set of subviews.

The use of standardized views serves as a lingua franca as it provides a unified way of describing complex real world objects. It is important both to architects and stakeholders that those involved in an architecture process are aware of this fact and use it to their common interest. This common language will also help to establish a common arena for discussing architectures and consequences across Communities of Interest (CoIs) in NATO as well as across Nations and organizations [13].

4.1 Interoperability policy and interoperability directive

The aim of the NATO Interoperability Policy (NIP) is to achieve and maintain the Alliance's consultation and military operational effectiveness by implementing interoperable and affordable C3 systems providing the right information to the right user at the right time. The policy describes roles and responsibilities necessary to support the implementation of the policy as well as the documentation and products needed to achieve interoperable and affordable C3 systems to meet the needs of the Alliance. The NATO Interoperability Directive (NID) provides binding directives for the application of the NATO C3 interoperability process and the use of key enablers throughout the life-cycle of NATO C3 projects, hereby the NAF. The NAF document provides the rules, guidance, and views for developing and presenting architectures to ensure a common denominator for understanding, comparing, and integrating architectures.

The NID describes:
- mandatory architecture types
- minimum set of architecture views and sub-views (previously called templates)
- architecture roles and responsibilities [13].

4.1.2 Strategic vision

Decision superiority necessitates a force that is organized, trained and equipped to operate in a collaborative, globally integrated common operational network. This network must link military forces, government and non-government agencies, and others in a seamless planning, assessment and execution environment. The provision of enabling technology to provide for the seamless exchange of information is critical. Interoperability and interconnectivity will be key enablers to achieving decision superiority.

Network-enabled capability is critical to the rapid delivery of military effects and will allow powerful new combinations of combat power. The realization of the strategic vision will be the transformation of NATO and National capabilities into a NATO Network enabled Capability (NNEC) environment. The strategic vision transforms the way operational and business processes are considered to a more

holistic view of required capabilities and away from a system oriented paradigm. This holistic approach requires a framework to guide development of the capabilities in a consistent and Network enabled manner [13].

4.1.3 Network enabled capability

Network enabled capabilities are critical to the rapid delivery of military effects. It provides an ability to deliver precise and decisive military effects with unparalleled speed and accuracy through the linking of sensors, decision makers and weapon systems. When implemented, NNEC will allow commanders to conduct operations across the spectrum with greater awareness, confidence and control. It relies upon the ability to collect, fuse and analyze relevant information in near real time so as to allow rapid decision making and the rapid delivery of the most desired effect.

Information flow problems are especially critical when adding coalition forces outside of NATO allies. The NATO approach to network enabled capabilities is based upon the realization of the Networking and Information Infrastructure (NII), concatenation of NATO and National information infrastructures and communications infrastructures necessary to achieve NNEC. Network enablement, which underlies NNEC, compels a shift from point-to-point exchanges between heterogeneous systems to a many-to-many exchange of information trough tagging and posting of information in an enterprise-wide shared space.

NNEC intends to make information visible, accessible, understandable and useful to authorized users on a mission-wide or enterprise-wide network in order to support effects-based planning and operations in a network enabled environment. In this network enabled environment, the degree of interface control needs to be minimized. Key interfaces are only controlled when tightly engineered interfaces are required. NNEC requires a framework and family of services for uniform, effective and efficient security. Security core services provide a common, reliable and benign operational environment. Security related services provide Information Assurance (IA) capabilities that are commonly required across the enterprise. The actual NATO portion of any NNEC, including Networking and Information Infrastructure (NII), defined as the federated network of NATO and national information infrastructures and communications infrastructures necessary to achieve NNEC, will be dwarfed by the collective sum of the NATO Nation's forces and infrastructure. However, NATO provides the framework for the political consultation process and also plays a crucial role in the development of the architectures and effective interoperability standards, and by arranging testing and exercise venues that ensure that all Nations forces can interoperate.

At the planning level, the NNEC updated Overarching Architecture (OA) defines the structure of NII systems and components, their relationships, and the principles and guidelines governing their design, operation and evolution over time. The OA is used to determine interoperability and capability requirements, advance the use of commercial standards, accommodate accessibility and usability requirements, and implement security requirements both within NATO and between federated systems.

The NNEC Strategic Framework will provide the Vision, Concept, Architecture, Business Case, Road Map, Programme plan and resource requirements necessary to take NNEC forward to implementation. An important driver of NNEC is the fact that NNEC will be a federation of systems as opposed to a system of systems. A second driver is the need to consider a service oriented approach to the provision of capabilities. The descriptions and drivers highlight the complexity of architecting, designing, and managing the implementation of NNEC. To handle this complexity requires a common framework that ensures consistency and clearly defined relationships among the elements of the NNEC architecture.

Because architecture is an essential part of the NNEC strategic Framework, the NAF v3 will support and help NATO authorities and Nations to develop and implement the NNEC vision.

Benefits of network enabled capability include:

- Creating a faster and seamless flow of information between different levels of command, allowing a higher operational tempo.
- More effective use of a geographically dispersed force, and the facilitation of reach-back. As the ranges of sensors and weapons increase and the ability to move information rapidly improves, geographic implications are minimized. A network-enabled force can mass effects without the necessity to mass forces. This in turn reduces risk by avoiding the presentation of attractive, high-value targets to the enemy.
- Permitting Nations to offer specialist capabilities and exploit synergies and economies of scale by exploiting interoperability in a plug & play environment. Above all, this offers the Alliance the ability to deliver more for less.
- The creation of agile, flexible, and responsive Command and Force structures. NATO Architecture Framework (NAF) supports and can help NATO and Nations to develop and implement the NNEC vision [13].

4.2 Multilateral interoperability programme

It is necessary to describe Multilateral Interoperability Programme strategy to achieve interoperability of cooperating national Command and Control

Information Systems (C2IS) at all levels of command, in support of multinational, combined and joint operations in order to provide a focus for the MIP Programme of work [12].

4.2.1 The description of MIP

MIP is an interoperability organization established by national C2IS system developers with a requirement to share relevant C2 information in a multinational/coalition environment. As a result of collaboration within the programme, MIP produces a set of specifications which, when implemented by the nations, provide the required interoperability capability.

MIP provides a venue for system level interoperability testing of national MIP implementations as well as providing a forum for exchanging information relevant to national implementation and fielding plans to enable synchronization. MIP is NOT empowered to direct how nations develop their own C2IS.

Key points:

- MIP focuses on interoperability of command and control (C2) systems, which includes the Land view of Joint operations, but encourages contributions from Air, Maritime and other CoIs.
- MIP specifications are based on operational requirements developed into a fieldable interoperability solution.
- MIP assures the quality of the specification through operational and technical testing of national implementations.

A conceptual illustration of how the current MIP interoperability solution works is illustrated below (Figure 1).

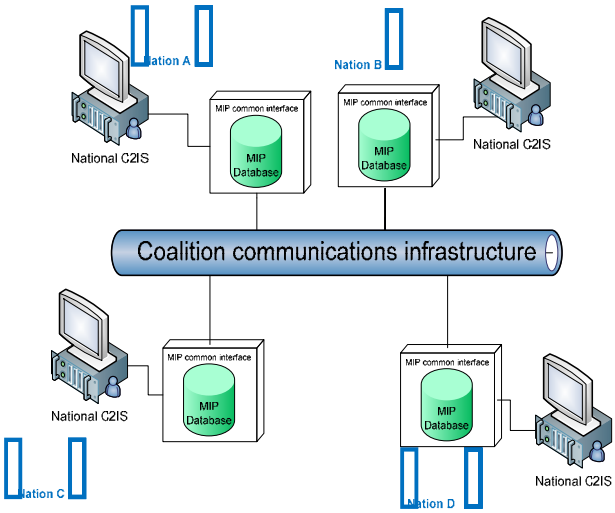

Figure 1: Different coalition C2IS connecting via the current MIP solution

The MIP solution refers to two or more national C2IS exchanging information by employing their respective implementations based upon the agreed MIP technical specifications[1] and supporting procedural and operational documentation.

The vision for the Multilateral Interoperability Programme (MIP) is to become the principal operator-led multinational forum to promote ***international interoperability*** *of Command and Control Information Systems (C2IS)* ***at all levels*** *of command.*

The MIP scope is to deliver a command and control interoperability solution in net centric environment focused on the Land operational user in a Joint environment including the requirements of Maritime and Air communities.
The MIP scope is derived from considering the constraints and limitations of the MIP solution [12].

4.2.2 Constraints, limitations and mission

Constraints:

- Resources:
  - Time available to work on the MIP specification.
  - Availability of operational and technical human resources.
  - Lack of centralized funding.
- Governance based on consensus.

Limitations:

- A focus on Land interoperability requirements for two reasons:
  - Historical interoperability capability gap in the Land environment.
  - Current operational focus on Land operations.

Mission:

MIP is to further develop and improve interface specifications in order to reduce the interoperability gap between different C2IS.

4.2.3 Tasks, main products and documents

- Support fielded MIP solutions.
- Further improve the MIP solution by adopting modern development approaches and standards[2].
- Harmonize with NATO and leverage other appropriate concepts, profiles and standards[3].
- Improve flexibility in using the MIP solution in ad-hoc coalitions.

[1] The technical specification includes a common data model and agreed exchange mechanisms.
[2] Examples of approaches and standards include the NATO Architectural Framework (NAF), Model Driven Development, Service Orientation and common standards (XML, UML, RDF, etc.).
[3] Examples include NNEC, APP-11, APP-6, etc.

- Extend the scope of MIP interoperability.
- Engage Maritime, Air and other CoIs to cooperate with MIP.
- Examine better ways of structuring the MIP programme.

The main products from the programme are:
The Joint Consultation, Command & Control Information Exchange Data Model (JC3IEDM) promulgated by NATO as STANAG 5525[4].
Documents:

- Operational documents:
  - Instructions on how to use the MIP solution.
  - Record of incorporated Information Exchange Requirements.
- The programme's Exchange Mechanism specifications and associated procedures.
- Technical documents: Guidance for nations and CoIs on how to implement the MIP specification within the context of their national C2IS.
- Supporting documents: Procedures for testing the MIP specification.

The programme does not include the following aspects of C2IS development:

- National C2IS hardware and software.
- National C2IS software designed to implement and process the MIP specification. However, MIP provides test events to enable nations to evaluate their own systems against MIP specifications.
- Any responsibility for manning and operating national C2IS [12].

4.2.4 Components

MIP should be understood in the context of its 3 integrated components:

- **Organization –** An international military data interoperability organization that meets to define common information exchange requirements (IERs), which can be exchanged between different national C2IS.
- **Specifications –** Delivering an assured capability for interoperability of information. MIP facilitates interoperability through defining/developing common technical standards and associated documentation. MIP intends to further develop and improve interoperability standards in order to support understanding in a common working environment.
- **Materiel development**
  - A forum for national implementers to synchronize their MIP C2IS material fielding plans.
  - An organization that assists in testing national C2IS in accordance with MIP specifications, which is focused on fielded solutions and iterative development [12].

[4] STANAGs are NATO standardized agreements. STANAG 5525 establishes a common data model that NATO nations individually ratify and implement in their own C2IS.

5 Conclusion

In this paper information superiority as one of the arguments of the situation awareness function is analyzed (besides the common operational picture as another function's argument). In this connection some main characteristics of information superiority, common operational picture and situation awareness are elaborated, explained and presented.

Interoperability of information is essential and an assured capability for this is vital. The successful execution of fast moving operations needs an accelerated decision-action cycle, increased tempo of operations, and the ability to conduct operations simultaneously within combined/multinational formations. Commanders require timely and accurate information. Also, supporting command and control (C2) systems need to pass information within and across national and language boundaries. Additionally, forces must interact with non-governmental bodies, and international and national aid organizations. IT must act as a force multiplier to enhance operational effectiveness at each level of command by enabling the sending, receiving, filtering, fusing, and processing of ever-increasing amount of digital information [11].

Due to complexity of the interoperability solution: process (operational), semantic (systems and data) and technical (computers and networks) author seeks appropriate model for C2IS integration. The role of the DCIO along with the challenges he meets in his endeavor to deploy systems which could lead to information superiority is described as well.

In effort to examine the possibilities of information superiority achievement, place and role of MIP are investigated, contributing though to the understanding and knowledge about the interoperability approaches to process and semantic interoperability in the military. In this connection MIP's approach focused on semantic interoperability of C2ISs, aimed at advancement of Network-Centric Warfare (NCW) which is based on NNEC is presented and shortly described. According to The Institute for Defense & Government Advancement (IDGA) [10], [11] MIP was successful in establishing multinational joint C2 common core data standards that can enable and accelerate achieving transformational data strategies for international and national information sharing. MIP's C2 data sharing standard was adopted in 2007 by NATO, as STANAG 5525.

According to the author's best knowledge MIP is world's unique approach to interoperability in information superiority achievement and military

international cooperation. MIP's approach and solution presents world's military "state of the art" interoperability solution and aims to become the model for information superiority achievement, interconnecting different coalition C2ISs at all levels of command in net centric environment.

References

[1] Binaghi E., Rampini A.: **Fuzzy decision making in the classification of multisource remote sensing data**, Optical Engineering, Vol. 32 No. 6, pp. 1193-1204, Atlanta, USA, 1993.

[2] Clausewitz C. von: **On War**, translated by Michael Howard and Peter Paret, Princeton University Press, Princeton, USA, 1989.

[3] Clements S. M.: **The One with the Most Information Wins? The Quest for Information Superiority,** Graduate School of Logistics and Acquisition Management, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA, 1997.

[4] Department of the Air Force (DAF): **Basic Aerospace Doctrine of the United States Air Force**, Volume II. AFM 1-1. Essay C: Human Factors in War; pp. 17-23, Washington, USA, 1992.

[5] Dockery J. T.: **The Use of Fuzzy Sets in the Analysis of Military Command**, in *Decision Information*. Ed. Chris P. Tsokos and Robert M. Thrall, Academic Press, New York, USA, 1990.

[6] Dreyfuss C., Maurer W., Cohen L.: **Business Value of Services in Sourcing Initiatives**, Gartner, Inc. 2008.

[7] Gartner Executive Program: **IT Strategy: A CIO Success Kit** , Gartner, Inc., USA 2009.

[8] Galinec D., Ferek-Jambrek B. (2008): **Process Transformation for Reaching Agility: Chief Information Officer Role**, Conference Proceedings, CECIIS 19th International Conference 2008, Faculty of Organization and Informatics, Varaždin, pp. 317-324.

[9] Gompert D. C., Lachow I., Perkins J.: **Battle-Wise: Seeking Time-Information Superiority in Networked Warfare**, Center for Technology and National Security Policy National Defense University, Washington D.C., USA, 2006.

[10] The Institute for Defense & Government Advancement (IDGA): **About IDGA**, available at http://www.idga.org/, Accessed: 29th June 2009.

[11] Multilateral Interoperability Programme (MIP): **Interoperability**, available at http://www.mip-site.org/, Accessed: 30th June 2009.

[12] Multilateral Interoperability Programme (MIP): **MIP Vision & SCOPE (MV&S)**, PMG Edition 6.3, Montebello, Canada, 2009.

[13] North Atlantic Treaty Organization: **NATO C3 System Architecture Framework (NAF) Version 3**, NATO C3 Board (AC/322), Brussels, Belgium, 2007.

[14] Ringdahl B.: **Improving Business Processes Executive Summary for Defense Sector - May 2009 EXP Report,** Gartner, Inc., USA 2009.

[15] Robertson B.: **Enterprise Architecture Research Index: Integrating EA with Business Strategy**, Gartner, Inc. 2009.

[16] Swiss Sociological Association: **"Identity and organization" Workshop**, available at http://www.inderscience.com/mapper.php?id=116, Accessed: 29th June 2009.

[17] US Department of Defense: **DOD Dictionary of Military and Associated Terms,** Joint Chiefs of Staff (JCS), Washington D.C., USA, 2009.

[18] US Department of Defense: **National Military Strategy of the United States**, Joint Chiefs of Staff (JCS), Washington D.C., USA, 2004.