COMMERCIAL INFORMATION TECHNOLOGY FOR MILITARY OPERATIONS: INFORMATION SHARING AND COMMUNICATION SECURITY IN AD-HOC COALITIONS

Velizar SHALAMANOV, Goran JOHNSON, and Georgi KIROV

Abstract: The article presents the main results from the CITMO'2004 conference held in Sofia, Bulgaria. The purpose of this publication is to clarify the basic principles of Commercial Information Technologies for Military Operations (CITMO) and to develop a listing of the more important recommendations for information sharing and communication security in ad-hoc coalitions. For the purpose of the conference, the applications of commercial information technologies for military operations are discussed in four broad categories: information sharing / intelligence dissemination in ad-hoc coalitions, COTS for increased network-based interoperability, encryption and translation services in network systems, and telemedicine in natural and manmade disasters.

Introduction

This article discusses the use of Commercial Information Technology for Military Operations (CITMO). It considers the problem of information sharing and communication security in ad-hoc coalitions. The basic concept behind this subject is that the commercial information technology is the cornerstone for military transformation and network-centric operations. That has provided the NATO military capabilities demonstrated in many countries, but it raises four sets of related issues for the future which CITMO'2004 sought to address:

- Information Sharing / Intelligence Dissemination in Ad-Hoc Coalitions;
- COTS for Increased Network Based Interoperability;
- Encryption and Translation Services in Network Systems;
- Telemedicine in Natural and Manmade Disasters.

.

These issues are very important due to their relevance to future military operations such as network-centric warfare, asymmetric threats (terrorism and transnational criminality), and next generation information systems.

Information Sharing / Intelligence Dissemination in Ad-Hoc Coalitions

The first issue is sharing information technology with the allies and intelligence dissemination in ad-hoc coalitions. If we are to fight together with allies and coalition partners in the future, we will need to be able to share information technologies with them, and to gain from their own experiences with network-based operations. One approach would be to develop intelligence information-sharing systems using commercial off-the-shelf software and hardware systems to disseminate uniquely national information to all coalition partners. The integration of such information technologies into military operations should allow for improvements in capability and afford a greater opportunity to realize the future network-centric operational concepts.

It is important to note that identifying appropriate technologies, capable of fulfilling needs, requires defining that the natural environment for military operations during the next 10 years will be ad-hoc coalitions. This will necessitate policy, legal and doctrinal changes in NATO, other international organizations, nations, NGO and the UN in large. From the conceptual point of view, the most important factors for information sharing / intelligence dissemination in ad-hoc coalitions can be defined as follows:

- C4 architecture framework for coalition operations focused on flexible interoperability;
- There is a need for strong leadership for the process and coordination body;
- Global Coalition C2 System is between Internet and GCCS;
- Lead nation concept to be implemented in the area of C4.

The experts in the field of information sharing / intelligence dissemination in ad-hoc coalitions recommend:

- Wider dissemination of NATO standards and larger use of civilian standards;
- Provide common architecture-based approach for life cycle management of C4 systems for ad-hoc coalition operations;
- Develop model for context-driven multilevel trust between participants;
- Provide easy transition from military to civilian C4/CIS infrastructure; and
- Integration of legacy systems.

COTS for Increased Network Based Interoperability

Integration and incorporation of COTS components into legacy and emerging systems has never been more attractive in the information industry. This interest in COTS products is premised on a number of factors, not least of which is the spiraling cost of software. Given the current state of shrinking budgets and growing need, it is obvious to almost any observer that appropriate use of commercially available products is one of the remedies that might enable the governments to acquire needed capabilities in a cost-effective manner. In systems where the use of existing commercial components is both possible and feasible, it is no longer acceptable for the government to specify, build, and maintain a large array of comparable proprietary products.

Three dimensions of COTS are crucial to successful applications:

- *Technical*: degree of integration and interoperability achieved within the larger systems;
- *Managerial*: infrastructure for the certification of COTS in given applications;
- *Resource*: library of certified components.

For the purposes of the CITMO'2004 conference, in order to illustrate the technical role of the COTS, the following issues were discussed:

- Communications security and security infrastructure at large;
- Correlation and data fusion;
- Mediation and translation services;
- Representation, data/info models and controlled access;
- Standards and protocols;
- Information exchange models (portals for push-pull integration);
- Testing and certification for interoperability (including on-line);
- Robustness, survivability;
- Degradation architecture.

The benefits of the COTS use for increased network-based interoperability are pointed out in these directions: reduced design, reduced programming, reduced cost, reduced risk, and increased interoperability.

It is important to distinguish environments in which COTS can operate – some environments are easy, others are hard. There is a limited interoperability even when the "easy" environment interacts with the larger system:

- Certain data can be imported and exported;

- Certain objects like documents and drawings can also be imported and exported;
- Program objects (e.g., equations from a math or statistics program) cannot be imported into a spreadsheet program.

As a result of the discussion the following recommendations were suggested:

- Legal regulation of declassification of information for sharing in near real time;
- Data exchange to achieve COP;
- Core set of interoperability services / set a minimum standard of interoperability and perform C4 review studies periodically;
- Support ACT for CDE/ATD in C4 Interoperability through center of testing and certification, including training;
- Coordinated R&D to include larger number of partners and international organizations.

Telemedicine in Natural and Man-made Disasters

According to the definition of the CITMO experts, telemedicine provides:

- Access to the medical services and databases via Internet – for identification of the problem or new development;
- Teleconsultation and tele-education – for health-care professionals and public health programs;
- Vital signs monitoring – communication of patient data to distant doctors using simple devices for recording ECG, pulse rate, oximetry, blood pressure and respiratory parameters;
- Image transfer and videoconferencing – for distance conferencing, consultation with local and international specialists.

Telemedicine involves communication and sharing of resources, which can be of various kinds, including data, expertise, and processing.

The first kind concerns multimedia patient data (e.g., not only descriptive, textual information but also diagnostic images, audio and other one-dimensional measurements, 3D data sets, etc.). This is the basic resource exchanged in telemedicine, being the basis for almost every activity.

In respect to the expertise, every time an opinion is requested, exchange of specific expertise occurs. This is an untouchable but extremely valuable resource, and, in telemedicine, regards mostly diagnosis, prognosis and therapy. As an example, remote expert consultation is strictly related to the delivery of expertise.

The third resource—specific data processing—is sometimes possible only at some sites, mainly because it needs either particular expertise or particular hardware/software configurations, not available everywhere. Processing activities exploited by telemedical tools are image processing (e.g. 3D reconstructions, quantitative evaluations, etc.) and statistical data analysis.

As a result from the CITMO'2005 discussions, the main problems of telemedicine in natural and man-made disasters can be summarized as follows:

- Networks have to be built in a fast way after disaster;
- Hardware and software configurations not available everywhere;
- Complex topology of communication networks – networks consist of many elements;
- High dimension of optimization tasks – a lot of patient parameters have to be estimated;
- Great dynamics of input conditions and uncertainty of parameters.

In addition, the Common Operational Picture (COP) in coalition operations may be enhanced through incorporation of sensor information on the status of individual soldiers.

The working group scenario was emergency response to an injured person from one nation, awaiting transportation to a medical facility, while a medic from another nation provides assessment and first aid. Telemedical support to that individual was the focus of discussion.

Telemedicine Communication Networks

Different methods were discussed as an attempt to resolve the above mentioned communication problems:

- A method for network configuration based on the combination of Soft Computing Technologies, e.g. fuzzy logic, with Software Agents (SA);
- Distributed Software Agent approach;
- Mobile TETRA System.

Soft Computing Technologies (SCT) are defined as Intelligent Technologies (IT), using methods tolerant to uncertainty and complexity of real world phenomena. SCT's representatives are: fuzzy logic, neural networks, and genetic algorithms, which can be enriched with another group of probabilistic reasoning, evidence theory, rough sets theory, taboo search, etc.

According to the FIPA (Federation of Intelligent Physical Agents) definition, an agent is an active software entity that is embedded in an environment, which it senses and acts upon.

The working group suggested the following recommendations:

- Use of Open-Source Software;
- Use of IP-based communications;
- Use of high level of security.

Architectural Issues in Developing Medical Support for Coalition Operations

The challenges of joint medical support may be described systematically along the three architectural views:

- The operational architecture view is a description of tasks and activities, operational elements, connectivity and information flows required to accomplish or support military operations. The operational view of the architecture outlines the following challenges:
    - Forces from different countries use different procedures (differences in medical practice);
    - Difficulties in defining—and agreeing on—Responsibility;
    - Medical support architecture is a part of the overall coalition C2 architecture (the definition of which is a significant challenge by itself).
- The system view is a description of systems and interconnections providing, or supporting, warfighting functions. The following issues were addressed during the discussion:
    - Interface issues (GUI, HMI) are not critical given the open system concept is applied throughout;
    - Many unique databases exist. It seems important to have a “middleware”/”proxy server” or “metadata engine” to provide for use of variety of databases, including legacy databases;
    - Satellite communications are becoming a standard for exchange of information in telemedicine, in particular for communications between a field hospital and a stationary (or “reference”) hospital. A throughput of 2 Mbps is both desirable and practical in this case;

  - The use of satellite communications will be increasing for other exchanges in the architecture;
  - One important application is the creation of standard medical thesaurus.

- The technical architecture view is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The following issues were considered:
  - Currently, each country applies unique own approach to smart cards for personal medical records;
  - Processes of standardizing medical records/data are underway in Europe, the USA, etc. One common standard would facilitate coalition medical support;
  - Efforts are underway to standardize first aid reports, e.g. the NATO field card;
  - In coalition telemedicine, the use of IP-based communications is a must. It shall allow much easier integration of COTS technologies;
  - Commercial/civilian telemedicine technology forecast is essential.

Considering the recommendations, it is critical to develop a full architectural description of the coalition medical support if we want a predictable and manageable development. This will require interdisciplinary and multinational effort.

Sensors and Data

Scenario

This subgroup focused on the emergency response scenario and asked what data should be collected. Desired patient data to be transmitted to the staff at the telemedical facility is: Blood Pressure, Respiration, O2, ECG, Temperature and Picture. Medical records would not be needed for transmission to the field due to the fact that in the scenario of a patient awaiting transportation field technicians would not have time to use them. Positive patient identification is desired so that medical records could be transmitted to the medical facility to which the patient is going to be transported. Devices should also be available to maintain an accurate timeline of patient treatment and response. Many subgroup members believed that adequate sensors were already available commercially and that the principle challenge was agreement on standard in a coalition such as NATO.

Conclusions and Recommendations

1. Legal regulation of declassification of information for sharing in near real-time applies to ad-hoc networks. The analog in telemedicine is regulation of accessibility to personal medical data, in particular releaseability of non-readily measurable data (e.g. allergies, vaccinations, treatment related to operations in NBC environment) in emergency situations.
2. Data exchange to achieve COP applies to ad-hoc networks. This may not be applicable in the same sense in telemedicine. COP implies a many-to-many relationship whereas telemedicine is presumed to have a one-to-one or one-to-many relationship. It is possible, though, to exchange real-time information on the medical/ physical status of soldiers that would contribute to COP.
3. Core set of interoperability services / Set minimum standards of interoperability and perform C4 review studies periodically is a concern of ad-hoc networks. The conclusion of the delegates is that telemedicine will use existing C4 networks. A core set of applications, including for example Medical Thesaurus, would provide valuable contribution to medical support in coalition operations.
4. Support ACT for CDE/ATD in C4 Interoperability through Center of testing and certification, including training for ad hoc networks. This is also applicable to telemedicine data and applications.
5. Coordinated R&D to include larger number of partners and international organizations for both telemedicine and ad-hoc networks.
6. Wider dissemination of NATO standards and larger use of civilian standards for ad-hoc networks. For telemedicine in particular, the emphasis is on civilian standards. There was a consensus among the delegates that medicine is medicine and that for the most part, distinction between civilian and military is not necessary or desired.
7. Provide common architecture-based approach for life cycle management of C4 and telemedicine systems for ad-hoc coalitions operations.
8. Develop model for context-driven multilevel trust for information sharing between participants in ad hoc networks. Barriers to information sharing can, in reality, be expected to hinder life-saving efforts. In telemedicine, the trust issue is much more physical. For example, has this patient been exposed to biological agents and/or can this patient be expected to have been inoculated against them.
9. Provide easy transition from military to civilian C4 / CIS infrastructure. The conclusion of the delegates is that telemedicine will use existing C4 networks and that no further work appears to be necessary.

10. Integration of legacy C4 and telemedicine systems is necessary.
11. Improve PIMS concept and platform for operations.
12. Strengthen sharing of lessons learnt in the area of C4 and telemedicine.
13. Mobility and security is to be considered as critical criteria in C4 COTS equipment selection and future R&D. In telemedicine, the emphasis is on mobility; security of medical information is again a valid consideration.
14. C4 Virtual and physical identification capabilities have to be improved. In telemedicine, positive identification of an individual and association with that individual's medical data is critical.

Conclusions

This article reported on the CITMO'2004 conference discussions in the field of information sharing and communication security in ad-hoc coalitions. It considered commercial information technologies as approaches to the challenge of developing, deploying, and sustaining complex software system products or services in the military operations. The paper presented the work and recommendations of the four working groups.