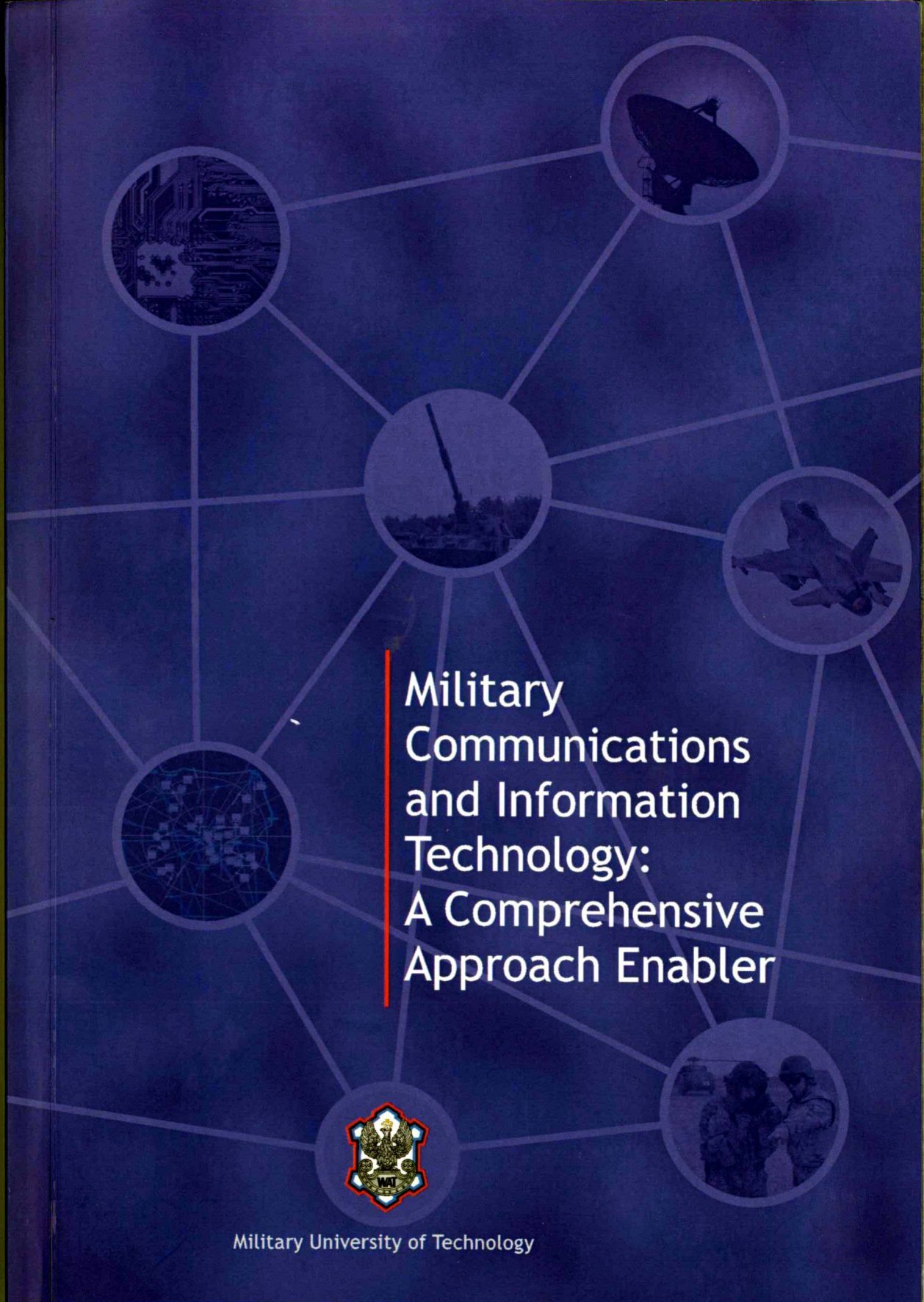

Military Communications and Information Technology: A Comprehensive Approach Enabler

Military University of Technology

Reviewers:
Prof. Jürgen Grosche, Fraunhofer Institute for Communications, Information Processing and Ergonomics (FKIE), Germany
Prof. Ryszard Antkiewicz, Military University of Technology, Poland

Editor:
Marek Amanowicz

Co-editors:
Peter Lenk
Andrzej Najgebauer

ISBN 978-83-62954-20-9

Publication qualified for printing without editorial alterations made by the MUT Publishing House.

DTP: *Martyna Janus*
Cover design: *Barbara Chruszczyk, Joanna Kulhawik*

Publisher: Military University of Technology

Press: Druk: P.P.H. Remigraf Sp. z o.o., ul. Ratuszowa 11, 03-450 Warszawa

Warsaw 2011

Contents

Foreword

The NATO nations are in the process of evolving their traditional mode of combat to a paradigm of Network Centric Operations that are conducted in a dynamic environment usually with unanticipated partners and irregular adversaries. The success of this process strongly relies on the progress in achieving of the Alliance's ability to integrate the various components of the operational environment and reaching the state in which better-informed decisions are made and implemented faster than an adversary can react. Lessons learnt from recent operations clearly show that the military can no longer act alone in modern warfare, but must interact and rely on support from non-military governmental and non-governmental organizations. To enable this, NATO adopted a "Comprehensive Approach" that is interpreted as: "a commonly understood principles and collaborative processes that enhance the likelihood of favourable and enduring outcomes within a particular situation".

Knowledge management and, as a consequence, information exchange amongst all parties involved in the actions are the most important tenets of such an approach. Progress in information exchange leads to improvement of the situational awareness and provides accurate and real-time information of friendly, enemy, neutral, and noncombatant locations, scaled to a specific level of interest and the special needs of all participating bodies. In the consequence, human operators are able to perceive and uniformly interpret the real situation in the battlespace.

However, growth in information sharing requires understanding of cultural differences and greater trust as well as an acceptance of the greater risks involved. It is evident that these issues cannot be solved in traditional ways and require advanced technology support to provide modularity, flexibility and security in connecting heterogeneous systems of cooperating parties. Many research efforts aimed at elaboration and implementation of innovative communications and information technologies in military systems enabling this comprehensive approach have been undertaken world-wide. Selected results of such activities are presented in this book.

The book contains the papers originally submitted to the 13th Military Communications and Information Systems Conference (MCC) held on 17-18 October 2011 in Amsterdam, The Netherlands. This annual event brings together experts from world-wide research establishments, industry and academia, as well as representa-

tives of the military Communications and Information Systems (CIS) community. The conference provides a useful forum for exchanging ideas on the development and implementation of new technologies and services into military systems. It also creates a unique opportunity to discuss these issues from different points of view and share experiences amongst European and NATO CIS professionals.

The papers included in this book are divided into seven sections that correspond to the conference topics, and reflect the technology advances supporting both Network Enabled Capabilities and the Comprehensive Approach, i.e.: Communications and Information Technology for Civil-Military Collaboration, Information and Knowledge Management, SOA Challenges for Real-time and Disadvantaged Grids, Information Assurance and Cyber Defence, Wireless Communications, Tactical Communications, Cognitive Radio and Spectrum Management Techniques.

The guest editors would like to take this opportunity to express their thanks to the authors and reviewers for their efforts in the preparation of this book. We believe that the book will contribute to a better understanding of the needs for information exchange in modern operations, identify some of the technical challenges that co-working with military and non-military organizations can bring. The readers will find here some of the extant and evolving solutions that reflect the thrust of current research as the CIS military community strives to enable the comprehensive approach and to facilitate the achievement of decision superiority.

Marek Amanowicz
Peter Lenk
Andrzej Najgebauer

Command and Control Portal as a Unified Way of Collaboration of Different Staff Cells in Army Headquarters on Operational Level as well as Cooperation with External Civil Organisations

K. Muchewicz, H. Kruszyński, M. Piotrowski, R. Pałka, T.Z. Kosowski

TELDAT, Cicha street 19-27, 85-640 Bydgoszcz, Poland

Abstract: Civil-Military Co-operation is commander's tool allowing achieving aims of the non- military operations, which are often carried out in parallel with those of warfare, in order to coordinate these two lines of action and to highlight priority for military purposes. Military commanders, during day to day operations, face with various difficulties at the same time trying to prevent from decrease in unit's efficiency and its capability to complete mission tasks. Although they are well trained to perform assigned duties they cannot deal without specially designed tools and modern technology. Instant collection and dissemination of information, efficient collaboration and common situational awareness are factors needed in order to secure effective cooperation with both military and civilian organisations. This can be achieved only by study of NATO doctrines and concepts, such as NNEC [1-3], EU NEC [20] or CIMIC [6], and newest technology capabilities.

Based on that study, a specially designed web based information system can be introduced that is scalable, flexible, interoperable and extendable. Headquarters Management Systems Web Portal is a solution for army requirements which highly increases commander's effectiveness on operational level where cooperation with civilian organisations is essential in time of war and peace. Described solutions, in the article, can be used as a support of NATO expeditionary operations or EU Battlegroups, which are mainly involved in civil-miltary operations such as Crisis Response.

Keywords: Command and Control Information Systems, C3IS, HMS C3IS JASMINE, NNEC, CIMIC, EXPEDITIONARY OPERATIONS, Web Portal, Web Services, operational level

1. Introduction

Civil-Military Co-operation is commander's tool allowing achieving aims of the non-military operations, which are often carried out in parallel with those of warfare, in order to coordinate these two lines of action and to highlight priority for military purposes.

Nowadays, both military and civil headquarters need modern technology for efficient and effective collaboration of entities and organisations, in order to fulfil required tasks and goals. Moreover, Civil-Military Co-operation [6] is essential

for a commander who links army units and civilian agencies active in a theatre of military operations.

For a staff commander, who is responsible for carrying out a military mission consisting of constant adapting to current battlefield requirements, it is very difficult to achieve proper and reliable coordination of subordinate soldiers without a help of specialized tools.

On the operational level of command reliable means of communication can be used to provide wideband digital radio or satellite connections between different command posts on the battlefield. As a result, an amount of data that can be interchanged between high level command posts of cooperating organizations is not an issue. Therefore, with use of properly designed information systems, commanders can focus on their tasks, make faster decisions and increase speed and effectiveness of command.

It is highly demanded that all modern projects are created and modified in accordance with NATO Network Enabled Capability (*NNEC [1][2][3]*) and European Union NEC (EU *NEC [20]*) concept which is about people, processes and technology. It ensures compatibility between various solutions. People need to share information for better situational awareness and faster decision making. That is where a technology becomes very useful for effective data collection, process and dissemination to the right users at the right time.

2. Collaboration of staff cells at operational level in headquarters

HQ (*headquarters*) is usually divided into groups [4] – staff cells having a clearly defined role (*function*), and responsibilities. Their work is coordinated to ensure that the commander is provided with the necessary data to make decisions.

Staff is responsible for ensuring the advice and assistance to the commander and provide support to subordinate commanders. It performs many different tasks that require good organization of work and accomplishment of many goals.

The organizational structure of commands in most of the land armies NATO, which is similar to the ones defined in ATP-Pub 3.2 [5], is presented in Figure 1.

Figure 1. Headquarters structure (developed based on [4])

Groups shown in this figure have strictly designated areas of responsibility and create leadership structure, while the main group, and a group of specialist liaison officers make up the staff – an essential part of leadership structure.

Commander group consists of officers and organizational units, which work directly with the commander.

Main group consists of (*depending on the level of command*) branches, departments and sections (*holders*).

Specialty staff group includes organizational units responsible mainly for the use of different types of forces.

Liaison group function is to ensure the efficient exchange of information between the home and cooperating headquarters.

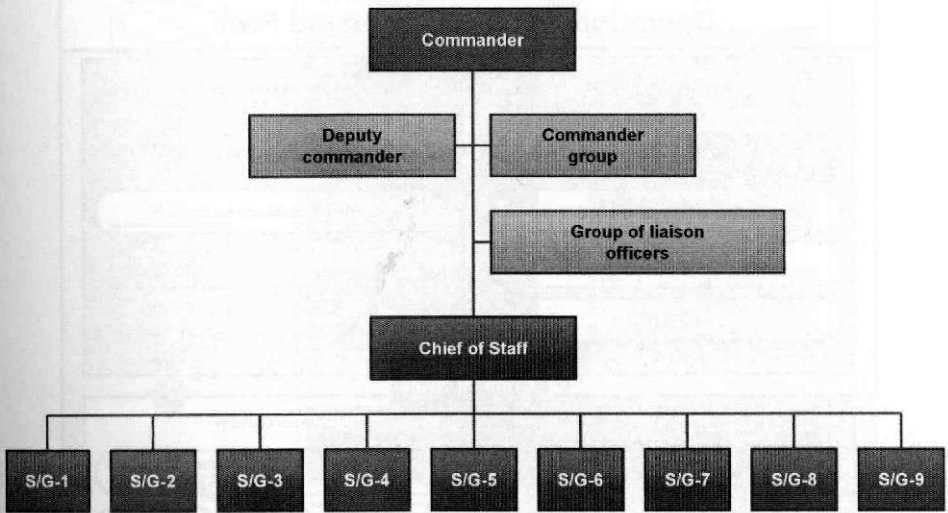

Figure 2. Staff organization (developed based on [4])

The organizational and functional structure is based on the recommendations of the publication of ATP – 3.2. Land Operations. The proposed organization [5] of the main headquarters groups is as follows:

G/S-1 cell of Human Resources and Administration;
G/S-2 cell for reconnaissance and electronic warfare;
G/S-3 cell for operational issues;
G/S-4 cell for logistic support and medical care;
G/S-5 planning cell;
G/S-6 cell for communication and information transmission;
G/S-7 cell for doctrines and training;
G/S-8 resources and finances;
G/S-9 cell for civil-military cooperation (CIMIC [6]).

Positions and command posts

Positions and command posts are managing operations centres. They allow commanders command in any kind of action. They ensure the realisation of leadership and are essential place of work for commanders.

In accordance with accepted principles in the military command posts are organized into three parts [4]:

- operational part (*the body of command post*),
- communications node (*telecommunications hub, and the centre for battlefield mail*),
- security group.

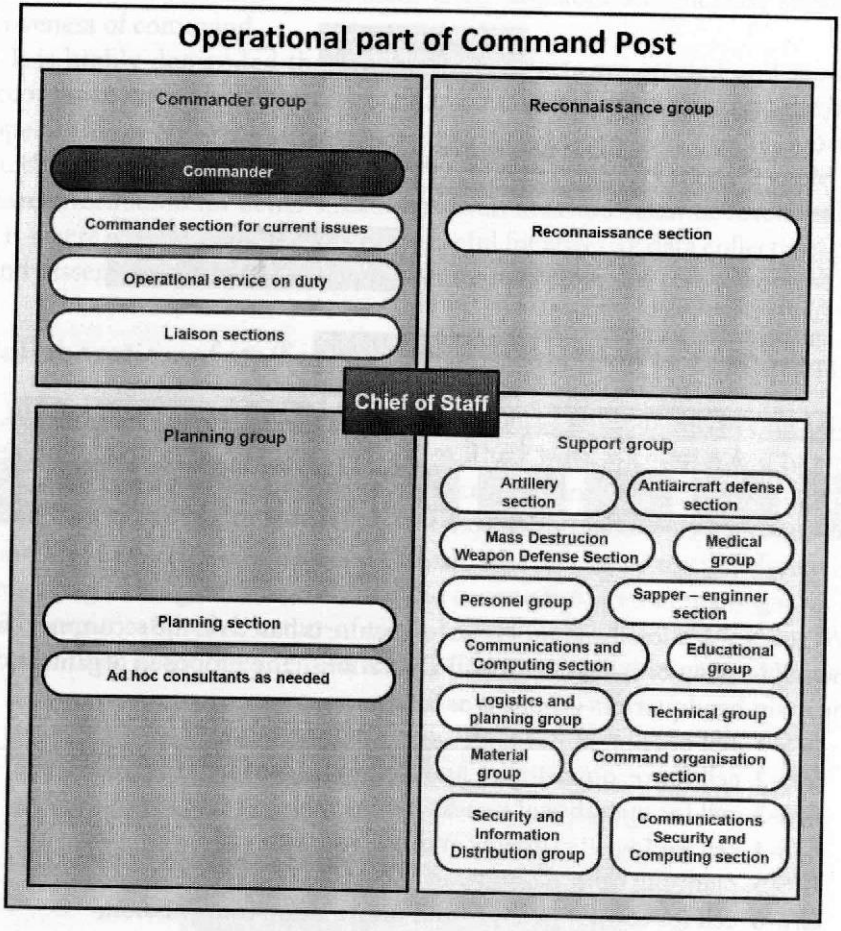

Figure 3. Operational part of command post (developed based on [4])

Depending on the **level and destination of a command post**, its internal structure is formed from functional components separated from one or more

organization cells, combined in the appropriate centres, teams, groups, sections, as essential components of the operational part of command post. There are always responsible (partially) for the planning and current activities and they include functional cells:

- Command,
- Planning,
- Diagnosis,
- Support.

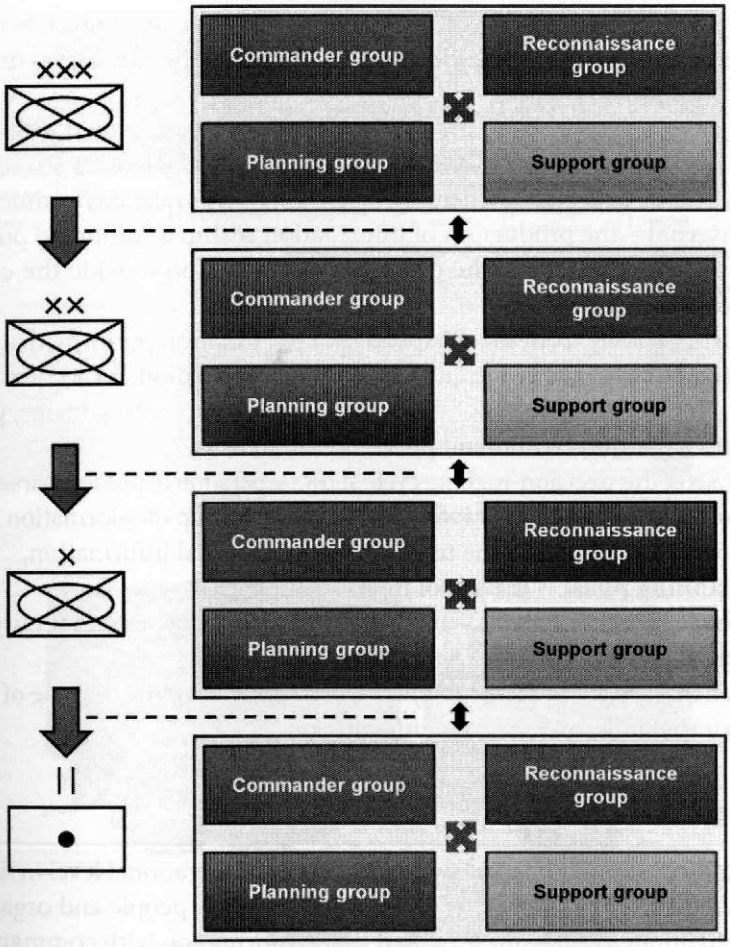

Figure 4. Types and flow of information (developed based on [4])

Information relations in the command system

Circulation of documents in the command system requires that there exist ways of exchanging information through an organizational structure and level of command – Figure 4.

Using the criterion of **organizational structure in information system**, there are two types of informational links [4]:

- orderly (*hierarchical*) – associated with subordination (*sending 'down' orders, sending 'up' reports*),
- cooperation (*functional coordination*) – related to the exchange of information between functional people inside the headquarters or the exchange of information within the specialty at the same level or between different levels.

Using the criterion of the **direction of the flow of command post** – the environment one can distinguish three types of informational links:

- **inbound external** – collecting information from the environment,
- **internal** – the production of information within a command post,
- **outgoing external** – the transfer of information outside the command post.

Leadership issue from the perspective of the function performed is a cyclical process of collecting, processing and exchanging information. To accomplish these tasks are organized at all levels of command the various centres, teams, groups or sections of a functional command post.

Analysis of this **decision-making cycle** allows separation of phases characterized by different intensity of exchange of information in each group of information links [4]:

- **positioning phase** – the use of inbound external information,
- **planning phase** – the use of internal links,
- **phase of putting tasks** – the use of external information of outgoing external links,
- **control phase** (*targeting troops in the course of action*) – the use of outgoing external links and external information.

3. Concept of realization

Described ways of collaboration of staff cells at operational level in headquarters impose directed implementation of solution. Many people and organisations need to collaborate at the same level and share information with commanders and superior commanders.

The main goal of **HMS JASMINE** system is to improve work of officers within Headquarters Command at the brigade or battalion level of command. It is accomplished by a dedicated web portal existing in a local telecommunication network of a command post.

Command Staff Portal provides functionality dedicated to the different sections and groups. The basis of its activity is a server that allows individual users to have a direct access to shared data and documents generated as files (*reports, plans, orders, notifications, alerts etc*).

Furthermore, it is assumed that already existing and fielded software components of **JASMINE** [7][8][9] system will be used, on both the server and individual workstations, to extend capabilities and functionalities of the Web Portal.

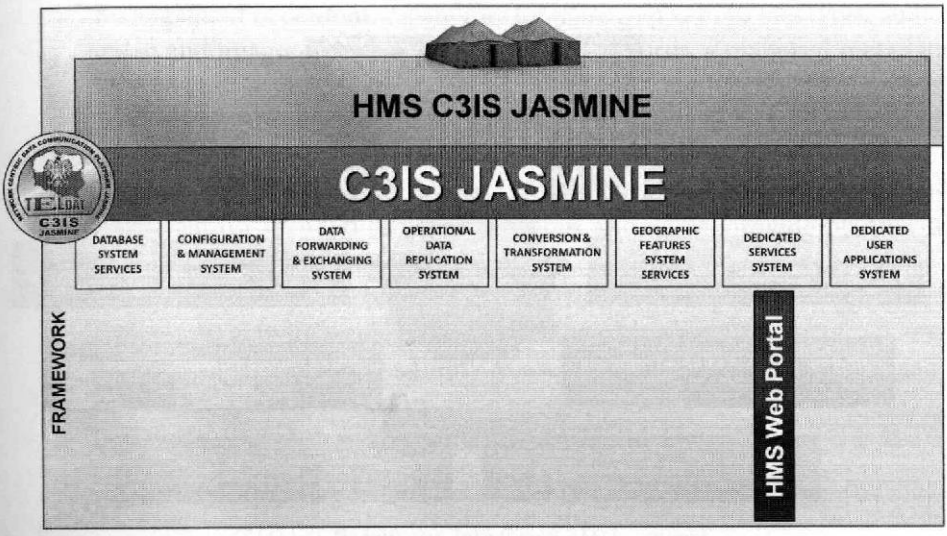

Figure 5. HMS C3IS JASMINE structure (© *TELDAT*)

Figure 6. HMS JASMINE – shelter and portable version (© *TELDAT*)

Local data communications network will be implemented by hardware components of the JASMINE system in shelter or portable version. However, the software supporting the work of Staff will be developed in a dedicated version of the operational level Command Support System – **HMS C3IS JASMINE**.

Implementation should be transparent from business point of view and be flexible to future expansion. It should contain many independent modules responsible for different tasks and jobs in defined communities of interests. Shared information should be exchanged with established and acceptable workflow.

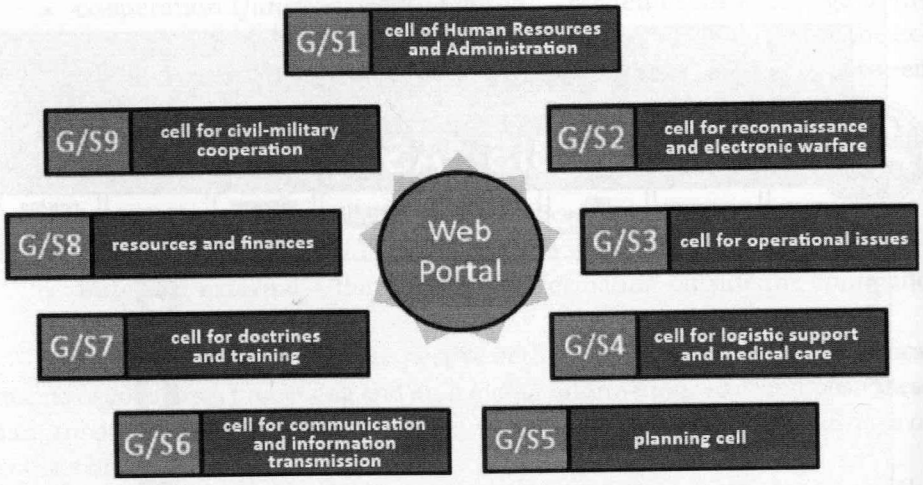

Figure 7. HMS Web Portal structure (© *TELDAT*)

Moreover it should be able to connect to many sources and gain various data from different interfaces. This data should be managed accordingly, with relation to files in operational system and other digital assets. User will also need strong social collaboration and search functions. Taking all these conditions for consideration we have decided to use **Service Oriented Architecture** in the design and production stage.

Service Oriented Architecture is concept promoted by **NATO Network Enabled Capability** [2] and EU NEC [20] pointed as right one for military command systems. Its main assumption is modularization of business functions for greater flexibility and reusability. Software systems are built from components with defined interfaces, which interior is "black box". Every component represents service with defined scope of action.

The more granular the components (*the more pieces*), the more they can be reused. When functions in a system are made into stand-alone services that can be accessed separately, they are beneficial to several parties. The architecture also provides a way for consumers of services, such as web-based applications, which are the most common and known example of using SOA, to be aware of available SOA-based services. Referring to all mentioned assumptions we have analysed

available Web Based solution which can be used as a base for creation our product and we have selected **Microsoft SharePoint in 2010 version** [10].

Microsoft SharePoint is a family of software products developed by Microsoft for collaboration, digital assets sharing and web publishing. It is a Web based server that can be used to build portals and content management sites for collaboration. It is very versatile in a number of features and supports various enterprise and Web scenarios and, what is the most important, can be used as a building platform to build systems atop its framework. Main features include:

- **management of content:** capabilities for managing various files types, audio, video and images, support for terms and keywords, a managed metadata service and tagging features, content organizer, ability to define content types and re-use them across site collections, or even farms,
- **application integration:** possibility to connect SharePoint, business applications and other external data, this includes information that may reside within Web 2.0 services like blogs and wikis, provide read/write capability,
- **social computing:** like blogs and wikis, rich member profiles, tagging and comments, activity feeds, people search, workspaces,
- **business intelligence:** possibility to use scorecards, dashboards and self-service analysis functionality,
- **enterprise search:** including related searches, wild cards, spell check.

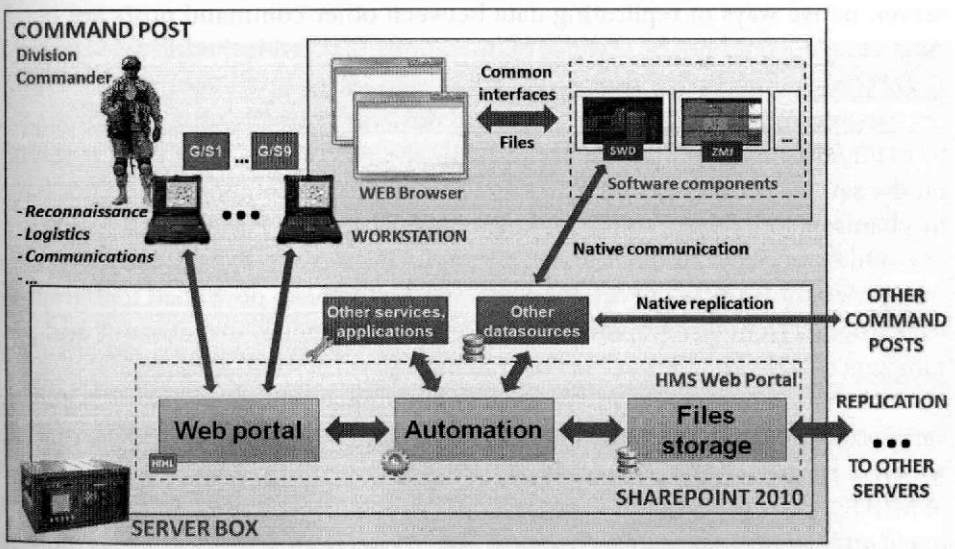

Figure 8. HMS C3IS JASMINE architecture (© *TELDAT*)

Command Staff consists of a group of officers performing a specific task for a commander. From the viewpoint of user Web portal is an element integrat-

ing the functions of the whole system in HQ. It is embedded on the Server Box JASMINE server [11] with HMS Web Portal installed.

Users use the workstations that run Web browsers and additional software components that allow them to take advantage of the functionality offered by the JASMINE system.

Officers of specified section log into the system and utilize the specified function modules for which they have permissions. They gain access to their allocated resources and system functionality that allows them to carry out their duties in an efficient way. There is also access to the so-called basic data which is public and requires no logging into the system.

Web Portal consists of different components responsible for data presentation, database storage and services that automate user work as well as other components of the system.

HMS Web Portal is a platform designed for collaboration and files group working which allows concurrently working on documents and their exchange between servers. The system includes a set of services that leverages the power of the engine and integrates them with the JASMINE system. Thus creates a platform on which the command staff can work regardless of number of functional groups it is currently consisting of.

On workstations software components have an ability of connecting directly to system native data sources and provide user with functions capable of data presentation and manipulation. Moreover, in the context of other data sources on the server, native ways of replicating data between other command posts are used. An example would be the transfer of operational data with the BRM (*Battlefield Replication Mechanism*) [12] protocol of C3IS JASMINE system.

In addition, software components, which work directly on files allow users to manipulate them on workstations, while the outcome of their work is stored on the server. Thus, despite the fact that some software components do not have mechanisms for collaboration, it is ensured by HMS Web Portal functionalities.

Other services and applications residing on the server may be used by automating services of HMS Web Portal. An example would be to download topographic backgrounds from Geographic Services servers or provide current status and parameters of individual services of command support system C3IS JASMINE.

The automation services are capable of automatic transfer of data between various data sources. As an example, officers prepare an order, as a Word document, which is submitted to command support system C3IS JASMINE and recreated in MIP JC3IEDM (*Multilateral Interoperability Program – Joint Consultation, Command and Control Information Exchange Data Model [13]*) database model. Another example would be to download information from the JASMINE TBD (*TELDAT Battlefield Directory*) database storing information about human resources and transfer them to C3IS JASMINE system database.

Automation services are also responsible for synchronization of constantly changing data between various data sources. It is assumed that the user will be able to make a decision about automatic data transferring between different sources as well as predefined patterns of behaviour.

The user has capability of searching and creating reports from all available resources (*files and data sources*) to which has permit. Such functionality is implemented by automation service and is associated with the generation of reports from different data sources.

It should be stressed that the security and confidentiality of data exchange in each of command headquarters can be secured by IEG JASMINE that is an implementation of NATO Information Exchange Gateway concept [14]. Flow of information between different security and system domains is controlled in reference to basic services (*ex. electronic mail, instant messaging, web browsing*) and functional protocols (*ex. MIP Data Exchange Mechanism Baseline 3 replication* [15], *NATO Friendly Force Information* [16])

4. System functionalities

HMS Web Portal is a portal with many subpages connecting with various services. This is the basement for work of command post and staff users. We can distinguish user modules specialized in user-friendly service of organizational and individual cells – which are part of the functional structure of headquarters.

Figure 9. HMS Web Portal – main page (© *TELDAT*)

Specialized modules

System supports headquarters organisational structure recommended by NATO alliance, the ATP-3.2 as a newer form (*G/S1-G/S9*), which is accepted as binding by most NATO armies:

- **G/S1, a module for human resources**: possibility to edit ORBAT and TASKORG, adding and removing users, military record and army quantity, human resources record (*friendly and enemy – captives*), reports, providing with personal forms,
- **G/S2, a module for reconnaissance and electronic warfare**: support for reconnaissance centres in analysis from many sources and situation monitoring, support for operational reconnaissance section in managing information needs and exchange, reconnaissance planning and putting tasks, gathering information from reconnaissance, summary and reports, support for developing ways to counteract electronic threats, keeping and managing documents from interrogation of prisoners, direction of the reconnaissance teams, collecting information about their records,
- **G/S3, operational module**: supports the process of coordinating the work of all of the organizational staff, preparation of documents related to the provision of permanent combat readiness, collecting and studying data about the situation and preparation the operational-tactical calculations, development of combat orders and regulations, organizing positions and command posts, the change of operational data – planning, reporting on the current situation, plans of attack and surprising opponents, hydrological and weather data collection and reporting, contamination and infection data collection and reporting, writing verbal orders commander, provision of maps and other topographic documents, the daily combat operations diary, situation map,
- **G/S4, a module for the logistics and medical care**: logistics support (*transportation, supplies, repairs*), medical support, support of the host country – coordination of logistical support by the host country,
- **G/S5, a module for planning**: supports the planning and forecasting campaigns, operations, tactical actions, variant planning, operational analysis,
- **G/S6, a module for communication and information transmission**: management of communications and IT systems, radio frequencies management, cryptography,
- **G/S7, a module for the doctrines and training**: doctrines, exercises and training planning,
- **G/S8, a module for the resources and finances**: supports the activities of the civil secretariat, management of civilian personnel, financial planning and budget, support for organisation and execution of contracts,

- **G/S9, a module for the civil-military cooperation**: data collection and preparation of documents relating to the host country's resources, negotiations on the arrangements and agreements on co-ordination and support, coordination of civil-military cooperation, coordination with other government bodies of the emergency response sections in the event of public emergency.

All modules should allow to work with the formalized documents that are created based on predefined patterns. Each module will have a typical set of the documents templates characteristic for its job. It enables to work through a web browser with the following types of MS Office documents: MS Word, MS Excel, MS PowerPoint.

Information sharing and dissemination

Portal functionality, beyond the storage of files, provides an implementation of the documents relevant access policy, archiving, sharing management information, business processes and publishing content. Web Portal allows to enter the documents in paper form, which, after scanning the user's request may be subject to a process of automatic recognition (*OCR*). The system also allows voice input information. Portal fully integrates with the operating system. Documents can be easily managed from a file manager built into the operating system (*Explorer*). Documents in the portal can also be viewed directly from the operating system.

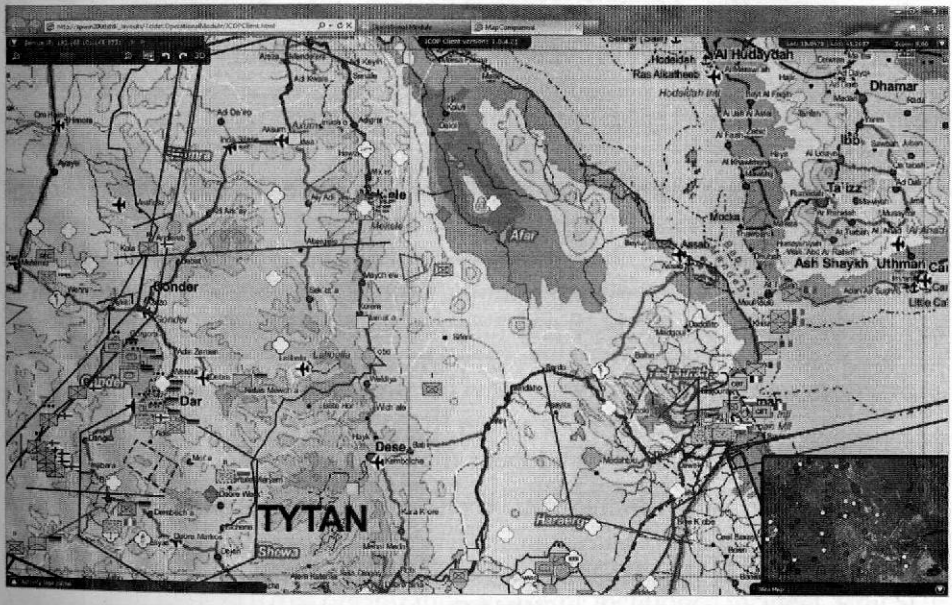

Figure 10. HMS Web Portal – JCOP Client page (© *TELDAT*)

HMS Web Portal system allows sharing of information between multiple types of databases, files or other formats and connect to various sources of data. The basic sources include: IHS JANE's database (*the database that stores various information regarding geographical situation, the weather, a description of the armoured vehicle in a piecemeal manner [17]*), MAJIIC (*Multisensor Aerospace-ground Joint ISR Interoperability Coalition [18]*), TBD – (*TELDAT Battlefield Directory – provides directory services, a logical and precise way to describe all human resources and hardware*), JC3IEDM and C2IEDM [19] (*older and newer versions of MIP database models*), IMS (*Information Management System* – a database system that stores information about the battlefield), files, photos, voice and video recording.

Automation process

Through the process of automation some of the data is imported and delivered automatically through indicated in the previous sections data sources. Some data, however, will require manual entry by the user. Regardless of where and how to enter data, further proceedings against them will be automated according to a defined pattern of information flow.

For the data directly related to SharePoint, the flow of information stored and associated cycles are defined within its native mechanisms. For the remaining elements the definitions of flows is encoded during creation of modules. One of the primary automation process, which can be distinguished, is the process of creating and editing plans and orders. The flow of plans and instructions is strictly defined in the server. Additionally, the system is able to automatically analyze the collected information, and, if necessary, to make the conversion. The operator introduces the plan in the form of a text document (*this may be a Microsoft Word document*), which is then accepted by the immediate supervisor. Such a document goes to the server and according to the flow of documents is further transmitted.

Each server operates independently, but between each of them data is replicated from both the HMS JASMINE system and the data stored and related to SharePoint. However it does not mean, that all servers are obligated to keep all the data. There may be specialized servers that are running a limited number of modules, such as only for the logistics purposes. Everything depends on the software configuration prepared on a particular server and user permissions.

Communication among users

HMS system allows communication between officers working in the staff of command, or the officers in different command levels and specialties. Methods of communication are different for various purposes and depend on demand. They include:

- **Instant text messaging (*JCHAT*)** – communication via text messaging available via the Internet or via a web browser application.

- **E-mail** – communication using e-mail.
- **Voice** – using voice communication between officers in the command staff, functional groups or between the staffs of command.
- **Video** – communication using video image coupled with the transmission of voice (*videoconference*). As for voice chat would be possible with one or more people
- **Forums** – communication using forum / newsgroup.

5. Practical implementation and cooperation with other systems

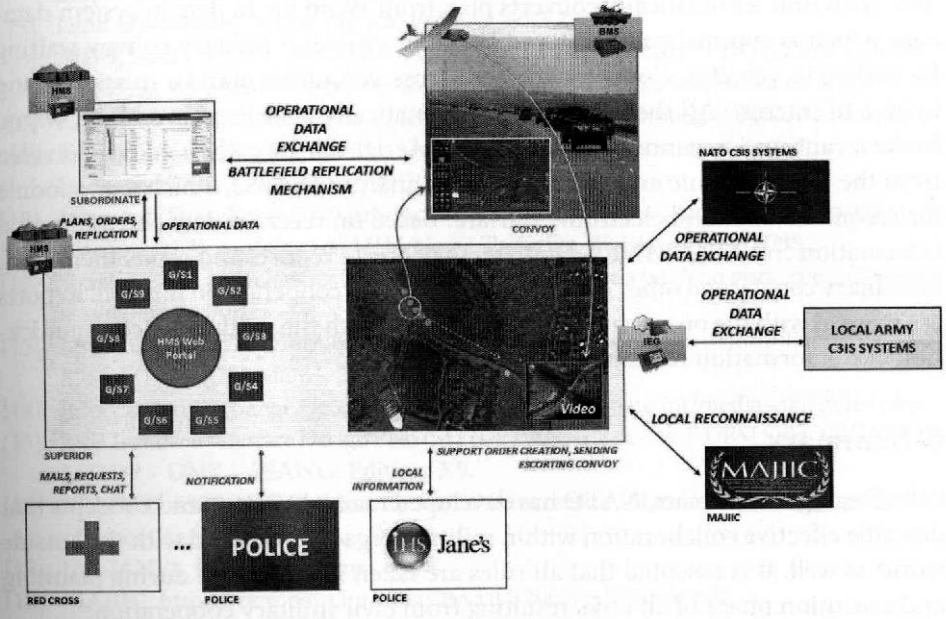

Figure 11. Example – imaginary situation presenting cooperation of entities with Web Portal (© *TELDAT*)

In current paragraph there will be described imaginary example of HMS Web Portal practical implementation (*see* ***Figure 11***). At first, it has to be assumed that there exist two military units: superior (*SUP*), and subordinate (*SUB*). Each unit has standalone server which are connected with using native replication mechanism. From NATO C3IS SYSTEM unit SUP receives, via one of the standardized protocols, military data regarding some incident in particular area. All data is being presented in JCOP Client application directly from Web Portal, users can see military symbols defining what and when happened. From LOCAL ARMY C3IS SYSTEM, using some other standardized military protocol, unit SUP receives help request from the Red Cross organization regarding mentioned incident. Unit SUP, section G/S9, using module for the civil-military cooperation creates and exchanges

mails with the Red Cross organization about possibility of sending military convoy protecting Red Cross volunteers during expedition to incident area. Red Cross organization sends information about people taking part in action with multimedia files which are being saved in HMS Web Portal storage. All data about human resources is being saved in hierarchical manner in section G/S1 with module for human resources. Automatic flow is started which notifies sections G/S5 (*which uses module for planning*), G/S4 (*module for the logistics and medical care*) and GS/3 (*operational module*) about need of creating plan for a mission. Sections cooperate with each other using emails, instant messaging and portal web pages, creating plan as Word document. Plan is replicated, based on automatic workflow, to SUB unit. SUB unit automatically converts plan from Word file to data in system database which is automatically sent and becomes visible to military convoy waiting for orders in vehicles. Convoy with Red Cross volunteers starts a mission going to area of interest. All their moves are automatically visualised in web browsers. In the meantime Unmanned Reconnaissance Aerial Vehicle gathers audio and video from the planned route and sends to further analysis to G/S2, which uses module for reconnaissance and electronic warfare. Based on received data and additional information from IHS JANE's database, they create reports and sends them back to military convoy and other interested nation which cooperates in mission. Reports are merged with the ones written by section G/S6 with the module for communication and information transmission.

6. Summary

During recent years, NATO has developed many doctrines and concepts that describe effective collaboration within military organisations and with the outside world as well. It is essential that all rules are taken into account during planning and execution phase of all tasks resulting from civil-military cooperation.

Considering all aspect presented in the article, a specialized Web portal (***HMS Web Portal***) for commanders who want to improve efficiency, information quality and collaboration is a must. Furthermore, it is manifest that technologies such as Service Oriented Architecture, Web Services, Web Portals and SharePoint are crucial to ensure system scalability, flexibility, interoperability and future development.

HMS C3IS JASMINE is a web based information system that meets all essential requirements of high level commanders. Furthermore it is a right tool for right people to secure collaboration of unit's sections and groups as well as cooperation with civilian organisations.

Described in the article solution can be used as a support of NATO expeditionary operations or EU Battlegroups, which are mainly involved in civil-military operations such as Crisis Response.

REFERENCES

[1] ISSC NATO Open Systems Working Group, Allied Data Publication 34 (ADatP-34) NATO.
[2] Maj. Yavuz Fildis, J. Troy Turner, NATO Network Enabled Capability (NNEC) Data Strategy, 2005.
[3] Copeland P., Winkler M., Technical note 1197 Analysis of Nato Communications standards for the NNEC, 2006.
[4] Research and development work, *Teleinformatyczny System Wspomagania Dowodzenia na Poziomie Taktycznym*, under scientific guidance of Prof. Jozefa Michniaka, Ph. D., Eng., National Defence Academy, Warsaw, 2009.
[5] Land Operations, Allied Tactical Publication 3.2.
[6] AJP-9, NATO CIVIL-MILITARY CO-OPERATION (CIMIC) DOCTRINE, 2003.
[7] Zawadzki W., *JASMIN wkracza do armii*, Nowa Technika Wojskowa nr 5/2007.
[8] Kruszynski H., *Zastosowanie systemu Jasmin*, Nowa Technika Wojskowa nr 9/2006.
[9] Kruszynski H., Apiecionek L., Dziamski M., *JASMIN w warsztatach,* Combined Endeavor 2008, RAPORT nr 06/2008.
[10] Microsoft SharePoint 2010 product official portal, http://sharepoint.microsoft.com
[11] Wachowski T., *Mobilny JASMIN*, Nowa Technika Wojskowa nr 1/2008.
[12] Sierakowski L., Muchewicz K., *Wymiana danych operacyjnych na poziomie taktycznym w systemie Jasmin.*
[13] Multilateral Interoperability Programme, The Joint C3 Information Exchange Data Model (JC3IEDM Main), 2007.
[14] Information Exchange Gateway (IEG) http://tide.act.nato.int/mediawiki/index.php/
[15] MIP Technical Interface Design Plan (MTIDP), ANNEX A – MIP DEM SPECIFICATION, MTIDP – DNK – SEAWG, Edition: 3.5.
[16] STANAG 5527 NATO Friendly Force Information Standard for Interoperability of Force Tracking Systems.
[17] IHS JANES, http://www.janes.com/
[18] MAJIIC, http://www.nato.int/docu/update/2007/pdf/majic.pdf
[19] Multilateral Interoperability Programme, The C2 Information Exchange Data Model (C2IEDM Main), 2005.
[20] EXTRACT FROM THE NEC VISION EU NEC VISION REPORT, www.eda.europa.eu/WebUtils/downloadfile.aspx?FileID=1152

Reliable and Effective Management of Hardware and Software in Battlefield Environment

Krzysztof Muchewicz, Henryk Kruszyński, Marek Piotrowski, Tomasz Kosowski, Marcin Woźniak

TELDAT Sp. J., Cicha street 19-27, 85-650 Bydgoszcz, Poland

Abstract: The current military and civilian information and communication structures are very complex systems. These structures provide many useful services running on the network, mostly an IP one Open System Interconnection model which was developed by the International Organization for Standardization lets integrate services from different suppliers of equipment in easy way.
However, it is required to adapt infrastructure to rapid cooperation between various civil services with the army. Crisis situations, such as earth quakes, floods or terrorist attacks, entail a need for effective adaptation for the new conditions to exchange information. Civil emergency service may need valuable information from the military headquarters. This requires possibility to define interfaces and run services on IT infrastructure in safe and easy way. That is why IT systems should have the tools to achieve rapid results in terms of configuration, reconfiguration and resources management. This article explains the necessity of utilizing such tools, as well as possible solutions supporting configuration for the Civil-Military Co-operation.
Solutions described in this article are suggested and possible to be implemented as an IT support for EU Battlegroups and battle groups for expeditionary NATO operations, that participate, among others, civil-military operations. The estimated wide civil-military collaboration extent of such groups brings a necessity to equip them with effective tools, that provide a possibility of fast multiple network connection configuration, especially for networks based on IP protocol.
Keywords: hardware management, software management, battlefield environment, CiMiC, expeditionary operations

1. Introduction

The rapid development of information and communication technologies where the time of configuration and preparation is critical, makes the manual way of managing hardware and software inefficient and insufficient for the requirements of military institutions. As a result, there is a need for creation of fully automated and flexible management subsystem in accordance with current standards in this area.

Configuration and network devices management is one of the most important features of military communication and transmission systems. An extensive network, as well as smaller sub-networks, provide infrastructure which consist of a lot of networking devices based on IP protocol. The accuracy and speed of configuring

those devices will increase performance of the managed network. Besides network devices configuration, services setup is a necessity. Some services provide basic functionality, such as user authentication and time synchronization. However, the most important are those providing user tools that he directly uses in his work, such as battlefield common operational picture, or the location of ambulances for the emergency management station.

An important aspect of prepared infrastructure is time needed for fast implementation. The importance of rapid network device configuration increases at in combat [7]. With a battlefield situation change, the infrastructure adaptation need occurs. Military mission success depends on the reconfiguration time.

Nowadays military network do not work alone. They must be connected often to different kinds of civilian networks for improving cooperation between military and civilians. This cooperation allows to realize more complex missions and is crucial to the success of operation [1]. There must be some kind of activity coordination with national and non-governmental organizations and agencies. Such cooperation affects on relationship with the inhabitants of that territory, where the mission is lead. Often the exchange of information during military assistance is required during emergencies. All these activities require speed in action and generate the need for reliable network infrastructure, which increases the efficiency of cooperation between various organizations, including such issues like sharing or allocation of responsibility for certain actions.

2. Battlefield infrastructure management scenarios

Administrators requirements and configuration processes.

As, in most cases, devices of IT infrastructure are configured directly on the battlefield, the configuration scenario differs from that used in civilian environment. The specificity of military actions assumes that all knowledge of how to set up working environment should be possessed by a single entity or group of soldiers, The administrator help should be limited to a minimum. We can also observe the process of specialization: individual soldiers are responsible for configuration of limited group of elements. Some soldiers are responsible for managing physical devices, others for preparing network addressing and others for setting up services or battlefield management systems.

In classic management and configuration model, the process of configuration strictly follows the OSI model of network infrastructure [2]. This means that it is divided in particular phases that corresponds to each network layer. This implies the following task sequence:

- deployment of physical devices on battlefield,
- setup of physical connections between devices,

- device configuration (*i.e. addressing scheme*),
- dedicated services installation (*including battlefield management systems*).

In battlefield environment described sequence is often reversed. Soldiers start configuration from setting up the logical connections between different tactical and command levels. They are also deciding what type of data and services are involved in communication process. Then they think about equipment – what kind and how many resources they need. After that they prepare architectural scheme of device connections. This let them prepare equipment and physical connections.

Lot of equipment in changing environment

Additional aspect of managing battlefield environment is plurality of the means of communication. In addition to Ethernet copper networks, fiber-optic and radio connections are also present. Most of these connections are characterized by limited bandwidth, which forces the use of other ways providing configuration and performing device management rather than over network. So there is a need for different way of setting up equipment configuration. It must be a system for a soldier with little knowledge about IP networks and services configuration. This system should be able to prepare IT network configuration in quick and easy way.

On military battlefield background there is also another issue – changing conditions. Typically, digital battalion consists of about 60 mobile battle and command vehicles, with additional approximately 70 support vehicles (*including transport, repair, medic*). This often results in more than hundred objects equipped with mobile IT network components. Each command vehicle has from 1 to 5 workstations with the variety of systems, that need to be configured. Each vehicle also has a variety of devices for communication, such as VHF, HF or wideband radio, satellite terminals or personal radio for communications with a single soldier. A single soldier has its hardware equipment and software which also needs to be configured. Moreover, there is often need to change the structure of whole system – the command vehicles could change their roles, ORBAT and data exchange points.

All of this entails the reconfiguration of military and civil IT infrastructure for exchanging information purposes. Sometimes, some changes in communication equipments settings must be made. Otherwise some systems must be switched to work in new conditions. The changes may determine requirements for changing the IP addresses of the devices. Such frequent changes in working conditions imply the necessity of doing pretty hard work to adapt the IT infrastructure. Therefore, sometimes some configuration variants are prepared before needed. Such prepared configurations could be implemented quick for example where there is a need to join the system to crisis staff in case of flooding.

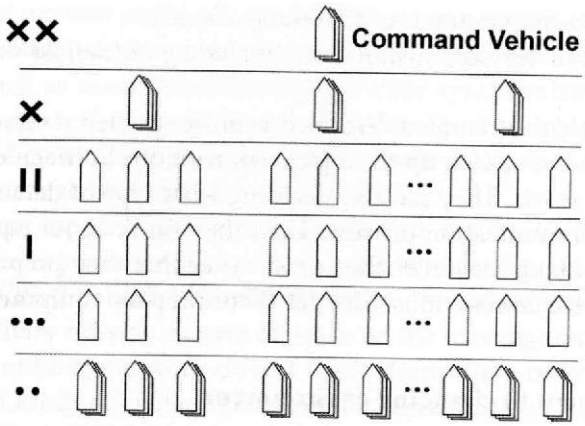

Figure 1. Digital battalion example (© *TELDAT*)

To solve mentioned problems different approaches have been taken. Among them is the JASMINE Module Management (*JMM*) application which will be presented in next paragraphs.

3. Management tool that serves its purpose

Among the solutions dedicated to the configuration of IT infrastructure there is a software JASMINE Management Modules, which offers a new perspective on the problem of configuration on the battlefield environment. It takes into account the specific conditions of the battlefield:

- lack of people with the expertise knowledge,
- problems with the transmission of large amounts of data to the device configuration,
- the need for IT infrastructure to adapt quickly to changing conditions,
- the need to combine independent and autonomous systems for civil-military co-operation in a possibly short time.

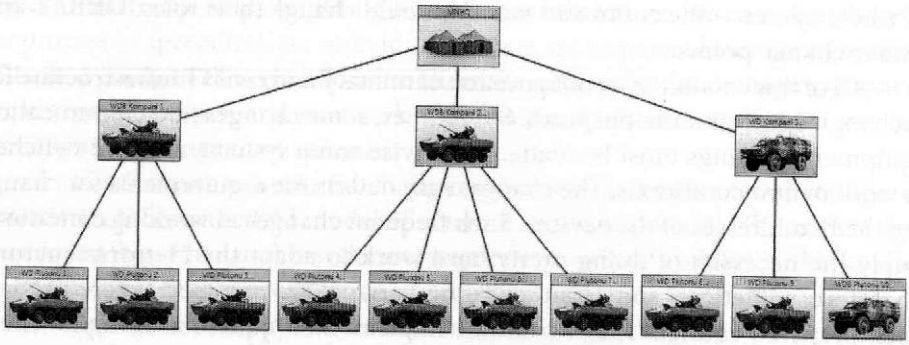

Figure 2. Digital battalion on JMM (© *TELDAT*)

JMM proposes a graphical model to make the setup process. A single configuration is represented as a collection of interconnected nodes symbolizing its individual elements. This is illustrated by Figures 2 and 3.

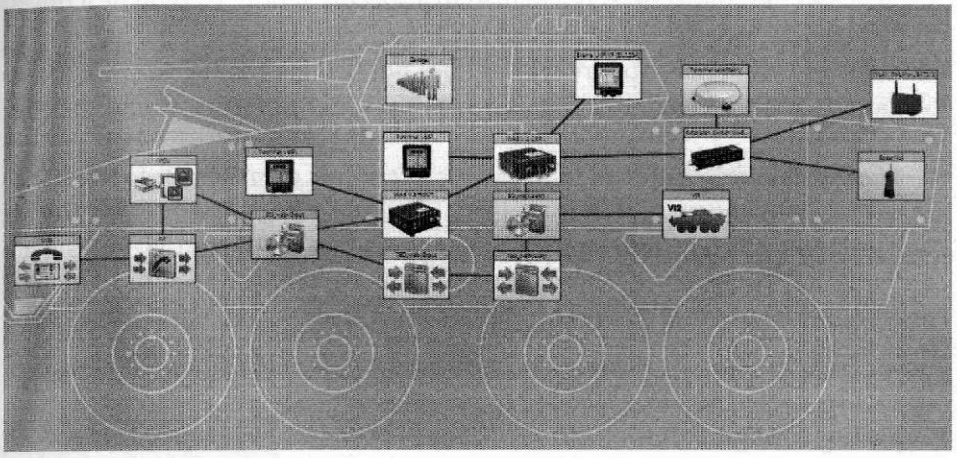

Figure 3. Command vehicle and his equipment: hardware and software (© *TELDAT*)

There are following part of the configuration:

- A physical device – which represents an actual device, that is the configuration subject,
- Services – which represent a service that is installed on a particular device.

Please note that today the construction of the network does not end with the IP network configuration. The network is configured to run the services, recommended by North Atlantic Treaty Organization [6][7], such as:

- emails,
- file sharing
- web browsing,
- VoIP telephony,
- data directories,
- user authorization services,
- network time synchronization services which are very important in case of system security,
- common operation picture systems with information exchanging in particular protocols.

Each of these services require determining user authorization, along with their privileges. Only services, provided by the network, make IT infrastructure effective and give an advantage on the battlefield.

Developing IT infrastructure

As the consequence of treating configuration as a graph, it is possible to define the various connections between the elements.

Each of the connections is assigned to a specific action. It could be a physical connection between elements and the logical element relationship. Starting positions of command support system does not bring anything to work for, as long as this position will not cooperate with the other to form a whole complex logical system.

Graphical presentation of IT infrastructure allows many people to work with a single schema configuration. Each of them is able to create their own "view" on the configuration, which includes only those elements that are interesting for user according to his competence. This allows user to solve problems on the battlefield condition when user has different and partial knowledge about whole system that needs be built.

Preparing configuration

The process of preparing the configuration can be divided into several stages:

- The network administrator defines the physical devices used to build the network and design the physical connections between them.
- Exercises commander defines addressing scheme for the network and basic services required to be implemented i.e. emails, www.
- Commanders of the different levels of command configure the command support systems for use by their subordinates.

Configuration process could be completely reversed. Commanders at all levels can choose what services are needed for their work, what information and how should be exchanged. Following this definition, another user can put the physical devices into JMM. It is remarkable, that this software provides an automated check whether a service is compliant to run on a particular instance of the device. This avoids trying to start services where they have no chance to work (*or even run*) correctly.

After determining the type and number of physical devices needed, the administrator can apply the IP address scheme for the network, or this scheme could be generated automatically. This approach does not require the user, who works with battlefield common operational pictures systems, having knowledge about hardware, its configuration and capabilities.

4. Management tool at changeable environment

JMM is a tool, which does not require administrator with lot of knowledge about deploying and configuring IT infrastructure. Lots of technical experience

knowledge is inside the core of this application. JMM provides solution for quick and easy way of reconfiguration for changing environments. It is a tool which increases the speed of connecting different networks. Configuration could be prepared and modified in many differents ways. Hardware and software could be reconfigured manually or automatically. It is also a simple interface for connecting different system devices and services for managing in one place.

Administrators requirements

The general way for preparing configuration on JMM is illustrated on Figure 4.

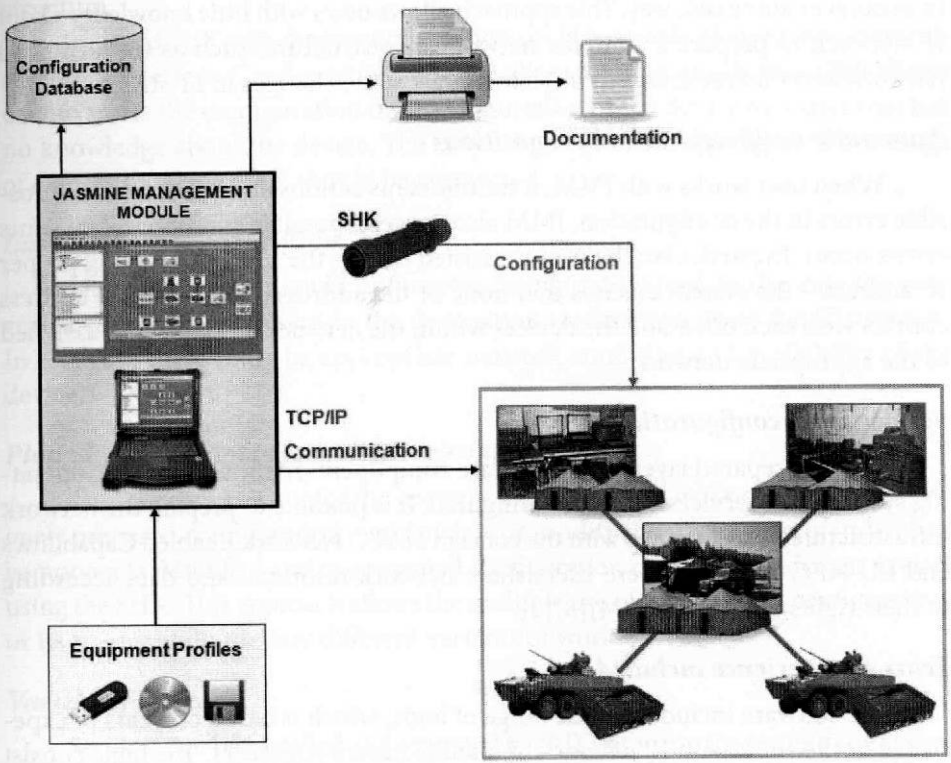

Figure 4. Generation configuration process (© *TELDAT*)

Network layer configuration

The starting point for building a network is gathering information on the actual hardware and equipment, which will be used to built IT infrastructure. Using this knowledge and the logic of network construction and configuration services, JMM software provides user features enabling them to customize the configuration. With JMM, using simple Drag & Drop mechanisms, and lot of wizards, users define connections between devices and services. It is possible to define physical

network connections using wide range of media: from Ethernet through WAN connection and digital voice trunk. The software also provides capability of radio frequency planning and preparing configuration for the radios supplied by different manufacturers.

For use in the forthcoming schedule of radio communications (*broadband radios, personal radios*), it is possible to check the radio network range, or allocate adequate frequency.

Default settings

When there is prepared physical hardware layer, some additional settings for individual devices could be configured. IP addresses scheme could be changed in manual or automatic way. This approach allows users with little knowledge about IP network to prepare a complex network infrastructure, such as for advanced network administrator, and to implement fast some changes in IT structure.

Automatic notifications and propositions

When user works with JMM, it monitors his actions and informs about possible errors in the configuration, JMM also suggests possible solutions when some errors occur. In particular, the user is assisted during the process of giving proper IP address – the system ensures that none of the addresses will generate address conflict with each other and the devices within the network device will be assigned to the appropriate network.

Service layer configuration

On the prepared layer with hardware components, defined software, operating systems and services could be configured. It is possible to prepare the network infrastructure in accordance with the concept NATO Network Enabled Capabilities and EU NEC concept, where users share network resources and data according to their rights and needs [3][4][8][9].

Years of experience included

The software includes a wide range of logic, which is based on years of experience in the work with IP network of manufacturers engineers. The logic consist of defined several algorithms. There is a device validation algorithm, which includes restrictions imposed by the device or service against their own setup or configuration of other components.

Some services and equipment to work properly require the presence of other devices configured in special way. The JMM tool automatically checks for their presence and retrieves relevant parameters. So there is no requirement for the administrator of the IT infrastructure to have wide range of knowledge in the subject of setting network configuration and services.

Configuration processes

An algorithm for the physical configuration of the equipment or services define how previously created configuration by the user of the program has to be delivered to the device.

Manual configuration

After completion the stage of preparation configuration of hardware and software, the prepared configuration has to be generated. The final result of this process could be passed directly to the Self-Programming Hardware Key (*SHK*), or may be stored locally for a future reuse and then propagated over the network infrastructure.

Prepared SHK with device configuration could be simply plugged into appropriate device interface. Configuration process will start automatically then. This allows user to make the configuration or reconfiguration of the device by a user that has no knowledge about the device. The only scope of knowledge required is a range of devices to which SHK should be connected.

Easy Remote configuration

Alternatively, user could use remote configuration tool. In this case the generated configuration is sent to the destination workstation using the IP network. In this case there must be appropriate network condition and availability of the device.

Plan ahead variants of possible (re)configuration

Another convenience for the operator is possibility to make changes to a previously prepared configuration – add, delete or modify the parameters of individual components. Modified and re-generated configuration can be embedded on devices using the SHK. This approach allows the multiple use of the prepared configuration, or its fragment, to prepare different variants of work.

Variety of services

Services can be installed and operated by SHK, or using the remote configuration, reconfiguration and deployment service. Using appropriate communication medium, with enough bandwidth, services could be changed remotely, or some additional services could be installed. This allows the administrator of the Command Support System C3IS JASMINE to be reconfigured or even update the system without physically visiting each command vehicle on which the system is working.

The setup process is fast and simple. JMM user can prepare their configuration in a way, which decreases the time which IT infrastructure needs to adapt to changing conditions of his work.

Lot of equipment in changing environment

Equipment management

The devices are stored and grouped in storage elements. This element allows users to define subsets of devices depending on their needs such as belonging to the organization, individual staff. These criteria are defined arbitrarily. The devices can be used repeatedly in different configuration which could be divided into sub configuration. This approach allows user to easily manage large amounts of equipment.

Extendable profiles of devices and services

In cooperation with the civil, military is necessary to combine different systems, which work with devices from different vendors. JMM application is modular software which adapts to increasing amount of equipment and services subjected to the configuration process, of connecting to different systems, i.e. emergency staff.

The core application is responsible for interaction with the user via graphical interface, generating reports and alerts to the user. Knowledge about how to configure individual devices and services is contained in the modules attached to the application. The purpose of each is to provide a profile for each device and service which describes them.

This profiles include the following elements:

- Metadata describing the specific device or service:
  - Name,
  - Graphical representation,
  - Description with installation process.
- Functionality provided by service or device and its exact characteristics:
  - In the case of a device -information to determine its class: routing device, gateway, switch, etc.
  - In the case of services – information to determine the required operating system, communication protocol, etc.

Providing appropriate profile allows JMM to configure a new service. This modular approach allows user to easily expand the range of configurable services, such as a service in specific subsystem. Where the system is combined with the civilian system, for example, emergency staff, adding the appropriate module allows to build configuration of the civil service in the military network, and vice versa.

Civil-Military Co-operation

As one can observe, the hardware and device management infrastructure described in the article conforms not only to battlefield applications. It can be used in scenarios with wider use context, including cooperation with non-military

organizations. Such cooperation is the mostly non predictable situation because is widely used especially in case of some disasters.

The common example of such scenario is crisis situation in which there are two or more autonomic systems (*one or more of them are civilian*) that need to share information. This implies the reconfiguration of current infrastructure on both sides and should be part of well-known procedures. In this case it is only necessary to provide profiles for devices and services belonging to other – civilian – system.

5. Conclusion

A prerequisite for conducting effective operations on the modern battlefield is to ensure reliable operation of ICT infrastructure. Work environment preparation has to be done in the shortest possible time and with the involvement of a minimum number of people, and especially non-expertise.

In addition, it is necessary to provide solutions in a very short time to replace or supplement the infrastructure incapable of further action, such as damaged as a result of combat operations, or lost to the enemy. Such tasks must be performed quickly and efficiently. Equally important is the flexibility to adapt to the changing conditions encountered on the battlefield.

Therefore, it is necessary to use a configuration management system that meets the requirements of these tasks. In an emergency, there might be required to cooperate with the civilian services in rapid way, which entails the need to interconnect the systems. Possibility of fast reconfiguration of the network connection by defining the interfaces and the rules of sharing services and data will be a key factor during humanitarian missions, where the cooperation of local authorities with the military is necessary. In such cases, the second often defines the success of the mission. JMM is a system, that fulfills these requirements.

Solutions described in this article are suggested and possible to be implemented as an IT support for EU Battlegroups and battle groups for expeditionary NATO operations, that participate, among others, civil-military operations. The estimated wide civil-military collaboration extent of such groups brings a necessity to equip them with effective tools, that provide a possibility of fast multiple network connection configuration, especially for networks based on IP protocol. JMM application has been successfully tested inter alia with an unit that belongs to UE Battlegroup, which confirmed its usefulness.

REFERENCES

[1] AJP-9, NATO CIVIL-MILITARY CO-OPERATION (CIMIC) DOCTRINE, NORTH ATLANTIC TREATY ORGANIZATION NATO STANDARDIZATION AGENCY, LETTER OF PROMULGATION, 2003.
[2] International Organization for Standardization, ISO-IEC 7498-1:1994(E) Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, 1996.
[3] Yavuz Fildis Maj., Turner J.T., *NATO Network Enabled Capability (NNEC)*, Data Strategy, 2005.
[4] ISSC NATO OPEN Systems Working Group, NATO C3 Technical Architecture, Architectural Descriptions and Models, Allied Data Publication 34 (ADatP-34), Volume 3, 2005.
[5] Copeland P., Winkler M., *Technical note 1197 Analysis of Nato Communications standards for the NNEC*, 2006.
[6] ISSC NATO OPEN Systems Working Group, NATO C3 Technical Architecture, NC3 Common standards profile (NCSP), Allied Data Publication 34 (ADatP-34), Volume 4, 2005.
[7] ISSC NATO OPEN Systems Working Group, NATO C3 Technical Architecture, Base Standards and Profiles, Allied Data Publication 34 (ADatP-34), Volume 3, 2005.
[8] EXTRACT FROM THE NEC VISION EU NEC VISION REPORT, www.eda.europa.eu/WebUtils/downloadfile.aspx?FileID=1152.
[9] „NATO C3 INTEROPERABILITY HANDBOOK FOR EXPEDITIONARY OPERATIONS" – AC/322-N(2009)0037 8 April 2009 NATO CONSULTATION, COMMAND AND CONTROL BOARD (NC3B).