Kerner Menyhért

MILITARY ADAPTATION OF PROTECTED INFORMATION SYSTEMS

Abstract / Absztrakt

Special defense needs, characteristic for this field only, are being formulated for the protected information systems used in the defense sphere. National and military defense operations ask for different information systems; therefore development projects for various systems have been started. The common goal is to establish the information based army. Many standards, tools and developments have been adopted from the civil sphere. The NATO transformation objectives support the formation of the information based army as well. The flawless communication between the different military information systems is of crucial importance, interoperability between systems has to be supported for an effective task management. The complex military information systems face an increasing number of threat types, therefore many national and NATO regulations have been introduced for the protection of information.

A védelmi szféra által használt védett informatikai rendszerekkel szemben speciális, csak erre a területre jellemző védelmi követelmények jelentkeznek. A nemzeti és haderőnemi védelmi feladatok eltérései miatt eltérő informatikai rendszerek kifejlesztésére indultak programok. A közös cél az információ alapú haderő megteremtése. A fejlesztésekhez a civil szféra szabványait, eszközeit és szolgáltatásait is felhasználják. A NATO transzformáció célkitűzései is támogatják az információ alapú haderő kialakítását. Az eltérő katonai informatikai rendszerek közötti kommunikáció alapvető fontosságú, a rendszerek közötti interoperábilitást biztosítani kell a hatékony feladatvégzéshez. A komplex katonai informatikai rendszerek egyre több fajta fenyegetéssel néznek szembe, melyek kiküszöbölésére nemzeti és NATO információvédelmi előírások születtek.

Keywords / Kulcsszavak: *military informatics, protected military information systems, NATO Stanags, interoperability ~ katonai informatika, védett katonai informatikai rendszerek, NATO szabványok, interoperábilitás*

INTRODUCTION

Communication has always been a key issue for military forces. The underlying causes are obvious: the joint control of military forces and weaponry needs fast communication; exact circumstance evaluation and gathering as much information as possible is needed in order to make the right decisions. These needs are present in other fields (commerce, for example) as well but with lesser importance. The applied technical devices were firstly used only for transferring (telegraph, radio), protecting (code books and systems) or gathering information (listening-posts), but the expansion in the field of electronic development has made it possible to develop such military information systems that allow complex military operations. The information

provided and processed by these systems is of great importance in the right and fast decision-making of army commanders.
Providing the troops involved in the operation with the adequate information (circumstance evaluation), the information exchange between the cooperating units increases the effectiveness of the operation. The increasing informatization of the various weapon systems allows the increasing integration of military systems, resulting in a smaller number of forces needed to complete the tasks. Lesser specific devices, capable for different tasks with the help of operational software, decrease development costs, and can be used more flexibly, and for more than one task. It can be demonstrated that the Internet and the relying technologies have changed military forces just as much as the business sphere for example.

The digital precision network based army is the military force of the future that provides superior advantage over traditional armies. Besides this the group of possible threats has been expanding as well. These represent entirely different vulnerabilities for military information systems than before. Such are the unauthorized access, malware, database modifying and destruction, the increasing danger of electronic reconnaissance and attack. All together the authenticity, confidentiality, availability of information handled by military information systems as well as the flawless operations of such systems has to be increasingly protected.

The informatics innovations principally feed the needs of the civil sphere, which represents the main market for informatics products. With the end of the Cold War most of the countries have reduced their military expenses, so these have to be used more effectively. On order to achieve this, military information systems rely on standards, tools and programs already existing in the civil sphere. Special military information systems, devices and applications can be built upon existing IT technologies. Despite this fact, the adaptation of different national armies to information based military forces generally takes long time and needs substantial costs.

The developed NATO countries (USA, Great Britain, France, Germany, Canada) are contributing the most to the development of the information based military forces. The obvious causes for this can be found in the significant development costs. The United States, as the leading power in the informatization of military forces, has the clear objective to fully integrate all military systems, beginning with the battlefield sensors, through the individual soldier, ending with the army command. About 200 billion USD will be spent on the development of softwares and components for the Global Information Grid (GID) program in the next two decades [1]. Besides that, many other projects are being developed separately or synchronized in the different army services. These developments will then be integrated to the GIG system, one such project is the Win-T tactical internet for instance. Outside the US, the French MOE SIC Terre, BOA and Comm@nder, the British DII and Bowmen, the German FAUST, HEROS and BIGSTAF systems represent the changes in the military forces.

Besides the national military information developments, joint NATO programs have been created for the enhancement of the common forces. The NATO transformation program is meant to transform the alliance to meet the expectations of the 21st century, the creation of the information based military force being one of its major objectives.

Information exchange is especially important, as each NATO task is being handled collectively by soldiers of different nations. These soldiers of different countries may differ in their languages, equipment and information systems. For the improved effectiveness of the joint

operations it is necessary to develop programs that enable the communication between different systems through NATO conform procedures and data models, and enhance the interoperability skills. The NATO interoperability issues have to be taken in consideration when developing national systems.

SPECIAL MILITARY NEEDS FOR PROTECTED INFORMATION SYSTEMS

The information systems of the defense sphere have to be extremely reliable; information security is a key issue. The amount of information that has to be processed for an effective operation is constantly increasing (sensors, reconnaissance and background information), this information (sound, pictures, data) needs to be transmitted, requiring a high bandwidth and great processing capacity from the system. In case of the mobile devices of tactical information systems the available (radio-) bandwidth can be a restricting factor. It is necessary to level out the communicational speed for the individual units, mostly because the execution of tasks depends not only on the quantity of information, but requires the possibly fastest disposability as well.

The military systems can strongly differ in terms of architecture, development level and system philosophy from country to country, and from military service to service as well. These systems can be integrated with the help of interfaces. Via these interfaces, the individual, special protocols are converted to common-standard protocols. New developments should not be platform dependent, and should need a very low amount of resources for the adaptation tasks. Additionally, there is a strong need for the ability of connecting older systems and devices. Military operations can be extremely multi-faceted. For instance, a fighting unit's tactical network differs in large amount from the information system of a providing unit situated in the home territory; e.g. no radio broadcast is needed, the system can be built up from common information components. Despite this heterogeneity the interconnection of different systems is required for an effective job.

The military information systems have been developed to meet the various requirements of the customers; therefore completely different systems have been developed or are under development in the various countries or services. The causes of the differences can also be found in the various information technological possibilities regarding the running of the programs and in the available development funds. In order to support the operations of the information based army, a reliable, fast and safe way of communication between individual systems is needed for the network integration and the information exchange between the systems. In our days this should be handled even more widely, since the information exchange between coalitional and allied forces is an elementary requirement.

The effective communication that is independent from all circumstances has a key importance in the success of military operations. It is important therefore for the enemy to jam, disturb, block the communication, or to transmit disinformation. The joint security of communication lies in the cryptography, the communication channel, and the transmission protection [2].

Some components of the military information systems work under special environmental conditions. Field devices have to endure extreme temperatures or humidity, mechanical impacts, they are used under different light conditions, and their overall usage differs from the civilian

application. Additionally radio transmittance is widely used, which requires the obscuration and encryption of communication.

The operation, maintenance and development of the increasingly complex systems, as well as the maintenance of the proper safety level, constitute an increasing challenge to the operating organizations. The possible number of threats is growing together with the size and complexity of these systems. Besides the technical challenges an increasing number of organizational, legal and other non-technical problems need to be solved [3].

DEVELOPMENT DIRECTIONS OF PROTECTED MILITARY INFORMATION SYSTEMS

With the end of the Cold War the possibility of global conflicts has decreased. The roles of a nuclear weapons arsenal have changed, and the role of information has been revaluated in the military thought. The fast technical development and the wide spreading of the Internet technology has made it possible to build an information-focused, precision-driven network-based army. Network-based armies need complex, high-capacity and protected military information networks. Many programs all over the world have been started to achieve this goal. The largest development programs have been started in the developed NATO countries; the leading position is occupied by the large-scale programs of the United States.

The GIG (Global Information Grid) is the large military network of the US Department of Defense, offering complex solutions for the military challenges of the future [4]. The system provides information superiority to all services, and supports joint coalition tasks as well [5]. According to the developers, the presently available information systems are not suited to fulfill the various needs and objectives. Information security and the reliability of systems need to be brought to a higher level, and the services of the system should be available from anywhere in the world. The protected system contains own and rented communication and information systems and services. Apart from the systems of the Department of Defense, it comprises the national security and intelligence systems which share information within the system. Interfaces are being established towards coalitional and allied forces, enabling the effective execution of joint operations. The system is not finalized; it underlies a constant development based on experiences to meet further customer needs [6]. During the developments, besides the security issues, important development objectives are the interoperability with the pre-existing systems and with the systems which are to be connected, as well as the backwards compatibility. In order to connect to the uniform GIG interface, the uniform usage of standard tools and different media, and the unification of the digital environment in use is required. Thus, less development is needed and the system becomes more transparent. The usage of the IP, which constitutes the base of the Internet, was an obvious choice to be the common GIG communication platform. This way the various systems that make up the GIG can differ from each other in terms of architecture, but they can commonly access it through the interfaces.

The WIN-T (Warfighter Information Network-Tactical) is the tactical intranet of the US military forces. It is the network of the future, which will dispose of all other communication systems. The system supports wired and wireless sound, video and data transfer. It uses available commercial channels and technologies for transfer as well. Via this system all information from unclassified to secret/SCI information can be transferred [7]. The WIN-T tactical network as a

whole can be divided into sub-networks like the WAN (Wide Area Network) dynamic network (supporting the communication of tactical operation HQs); the tactical internet network (basically with protected mobile radio connection, for data transfer only); military radio network (with mobile and portable radios); a network connecting the tactical operation HQs (for data transfer only); global transmitter service (high-speed data transfer via satellites). The network requires a high bandwidth, for which the bandwidth of commercial satellites can be used [8]. The system is under development, the security protocols especially need further development [9]. Furthermore it has a constant connection to the global information grid (GIG-BE) and the TSAT satellite communication network [10].

The JTRS (Joint Tactical Radio System) project, providing a uniform radio system for the network, is closely related to the WIN-T. [11] The currently used SINCGARS radio system is out of date by now and its bandwidth is not suitable for the transmission of larger amounts of data. [12] The level of informatization is indicated by the fact that the multi-channeled, multi-mode, high-data speed radio system already uses the software radio concept. According to this only the most necessary elements (mechanical and RF carrier frequency elements, high performance data signal processor) are hardware elements, the ciphering and signal processing (and even the demodulation) is performed by programs. This leads to the advantage of increasing the potential and speed of system-modifying, because only the processing program must be uploaded with the new version. Moreover, the running application provides an adaptive signal processing which adapts to the actual task, e.g. it can decrease the effects of radio jamming without the active intervention of the users. Due to the multipurpose use of radios the size of the radio set can be decreased as well.

The sooner started FCS (BS) (Future Combat Systems (Battle Command software)) system was called upon life by the recognition that in the military operations of the future an enormous advantage is ensured by the informatization of the operations. The system is organized into 5 layers, namely: standards (network-centric standards, constituting the base of the network), transport (providing protected, reliable, broadband communication), services (providing services which serve the operations), applications (applications which are being used during the design and execution of operations) and sensor-platform layers. [13] The standards layer provides the ability of interoperability with the protected national systems of other coalition forces. The development calls forth the evolving of a collective system of individual soldiers, unmanned vehicles, mobile units and the accompanying sensors. [14]

The British Defence Information Infrastructure (DII) is being operated by the Department of Defence, with an ability to reach the land, naval and air forces through this system. Moreover, it reaches the ships and air bases situated on the sea, with exception of the airplanes in air. [15] The system is Windows-based and this VPN can be accessed through a Web browser. The system is based on the concept that on the computers of the end-users no protected information is being stored: it is automatically deleted after use. After logging in, the user can only access the authorized data. Not only data, but pictures, videos and sounds can also be transferred, the applications in the system are supporting for example the VOIP (Voice Over Internet Protocol) sound transfer protocol.

The controversial Bowmen [16] is the tactical communication system of the British army which provides protected sound and data communication. [17] The system is designed in a way that all

the main mobile units, helicopters, marine objects are able to use it. The sound and data transfer is encrypted, complying with the COMSEC regulations.

The big advantage of the French MOE SIC Terre program (Maitrice d'Oeuvre d'Ensemble des SIC Terre) is that it integrates the pre-existing systems with a frame based on the Internet protocol. This way one can avoid the development and the introducing of the expensive new tools. The system will have the ability to unite the C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) systems and to cooperate with the BOA. [18] It uses a common core (e.g. containing a tactical intranet), therefore during the future developments it is sufficient enough to add the new applications to it. Moreover, for the "plug-and-play" applications there is no need to change the inner core, or only a minimal change is necessary.

The French BOA (Bulle Operationnelle Aeroterrestre) program, demonstrating network centric warfare, is only under development currently, but its objective is to create the technical background of the digital network-centric army. [19] It provides help in the presentation and the testing of the opportunities provided by the new technologies supporting the operations. The simulations are used in the analysis of land operations. Based upon the results, their planning and modeling is also possible. By using the results it is possible to determine the development trends of the future French land forces.

The Comm@nder C4I (Computerised Command, Control, Communications and Intelligence) system, accessible worldwide for the defense and security users, is being developed with the cooperation of Thales and Microsoft. The system ensures not only the availability of common tools, but it also satisfies the local needs worldwide. [20]

The german HEROS (Heeresführungsinformationssystem für die rechnergestützte Operationsführung in Stäben) program is a combat level command and control information system. FAUST (Führungsausstattung taktisch) is a combat internet system with management and communication functions, providing positional information as well. The system has already proved to be useful in practice. [21] The BIGSTAF (Breitbandiges integriertes Gefechtsstandfernmeldenetz) broadband integrated combat radio network provides broadband transfer for the German military networks. [22]

NATO TRANSFORMATION, INTEROPERABILITY WITHIN THE ALLIANCE

The nowadays widespread "infocommunication" expression includes the communicational and informatics tools and their applications. The new expression has been introduced because more and more technologies and tools are appearing which posses both communication and information abilities. In the case of the military infocommunicational systems one can state that the main inductor of the progression is no longer the military sphere; the military applications are increasingly making use of the civil services and systems, an increasing amount of data is being transferred and the bandwidth of systems is continuously growing. The tendency is the development of well equipped forces with smaller staff numbers and increased mobility, between which, thanks to the infocommunicational systems, the cooperation is tighter and tighter. [23]

For the better utilization of the opportunities provided by the information technology national and NATO programs are being started. Two from the seven main objectives of the Allied Command Transformation (ACT), established for the improvement of the NATO abilities (NATO transformation), are the Information Superiority (IS) and the NATO Network Enabled Capability (NNEC). [24] Numerous programs are meant to contribute to the network-centric, knowledge based transformation of the army, e.g. the American AKM (Army Knowledge Management). The AKM contains the strategy for the access of the network-centric army. For the achievement of the objectives it is necessary to use and redesign the network-centric network IT tools, the pre-existing knowledge base, the services and the strategies. Moreover, it is necessary to develop new regulations or, for example, to organize the education. [25]

In the NATO terminology the communication security is COMSEC, the informatics security is INFOSEC. For the protection of C2 systems the C2P (Command and Control Protect) expression has been introduced, which means the protection of C2 systems. The threats against the system can be intentional (intentional attack against the informational system), unintentional (e.g. user error, failure), structural-constructional (e.g. the security imperfections of the applied hardware and software elements), natural (e.g. extreme temperature, moisture, or earthquake). [26] The attacks reaching the system can be physical (damaging the physical components of the informational system), computational (e.g. viruses, the modification of data bases), theft (e.g. login codes, protected data), electronic (e.g. jamming), or attack with directed energy. The defensive C2P measures are decreasing the vulnerability of C2 systems.

The objective of the C2P (Command and Control Protect-Network Security Management, C2P-NSM) is to integrate the signal processing, technical development, security discipline and intelligence in order to ensure the authenticity, confidence and availability of information and the functionality of the system. With respect to this, one can distinguish defensive, detection and reacting measures. The MSN procedure means a real-time reaction to network penetrations. During the detection the MSN procedures discover the violation of security procedures, which results in a reaction. The reaction may vary from the recording of the error detection, through the redirection of the network traffic, ending with the replacement of network keys. The C2P-NSM tools are carrying out the monitoring of the system and the detection of the congestions, and are isolating the system from the hostile attacks, detecting the malicious codes and destructive systems, analyzing and estimating the threats.

In order to ensure their interoperability, the interconnection of military information systems has been becoming more and more important. [27] The NATO developments are being directed towards the establishment of a multinational, modularly built army of small dimensions which requires the increased cooperation of the individual (national, military service) systems. The imperfections of interoperability are worsening the efficiency of the task executions. NATO programs and trainings have been started and standards have been prepared in order to improve the cooperation between the systems. Within the NATO, it has been an important task in the past as well to regulate the connections between the systems (NATO interoperability management plan, NIMP and NATO interoperability planning document, NIPD). These programs have been controlling the modes of bit- and character-oriented message exchange between the systems, and their extension has become necessary by now.

The NATO C3 Interoperability Environment (NIE) [28], standing under development currently as well, is meant to cover the complex area of the interoperability inside the NATO. The NIE is

composed by four layers. [29] The policy layer means the uniform NATO interoperability policy, the directive layer covers the main directives of interoperability, and the guidance layer contains the instructions related to the conversion of the information system. The supporting layer contains the architectures of information systems, the testing infrastructure of the interoperability environment, the tools supporting the interoperability and the national interoperability profiles and controllers.

The objective of the NATO C3 Technical Architecture [30] is the support of the national technical architectures by offering uniform common standards and technical building blocks. It contains every fundamental component by means of which the NATO interoperable national technical architecture can be constructed. It contains the monitoring of the development, architecture models, fundamental standards (open communication standards usable for the NATO), NATO C3 common standards, and NATO C3 common operational environment.

The Multilateral Interoperability Programme is meant to support a better cooperation between the information systems of the member states. Its objective is the development of the uniform communication mechanism and data model between the individual national information systems (C2IS). [31] The national systems of the countries participating in the MIP are able to interconnect by means of the unified C3 information exchange data model and mechanisms. The base of the common message exchange is the SMTP internet electronic mail protocol. [32] In forms of file attachments it is possible to transmit text, sound and video materials as well. [33]

SUMMARY

Utilizing the possibilities offered by information technology, many military programs have been started since the nineties in order to support the development of the informational army. These programs are usually complex and expensive. The individual national defense forces, or in many cases the military services have been separately developing protected information systems, but in practice it became clear that the cooperation between these is indispensable for the efficient work. A system integrating these systems, like the GIG program of the USA, has appeared as a new concept.

One of the objectives of the NATO transformation is the development of the information based army, for the sake of which the supporting NATO standards have been introduced. For the protection of NATO C2 systems the C2P measures are being used. This complex measure system supplies a flexible protection for the protected NATO information systems.

During the coalition operations, the communication between the coalition forces is of primary importance. The practical experiences show that the cooperation between the systems must be improved. The interoperability between the military information systems is supported within the frame of NATO by the Interoperability Environment, the Multinational Interoperability Program and the NATO C3 Technical Architecture. Beyond these numerous practices help in defeating the interoperability-related difficulties. Further standards and data models developed by NATO are available for the developers of protected military systems.

The gaining ground of information technology in the defense sphere is reflected by the increase of the sums invested in military information systems, the gaining ground of the tools possessing military information abilities, and the increasing number of military standards and

announcements related to the development of information systems, information protection and the interoperability of the information systems.

BIBLIOGRAPHY

[1] http://www.nytimes.com/2004/11/13/technology/13warnet.html?ex=1182225600&en=7fad78af7d8ff32f&ei=5070, 2007. 06. 11.
[2] http://www.globalsecurity.org/military/library/policy/army/fm/24-12/Ch7.htm, 2007. 06. 11.
[3] Ködmön József: Kriptográfia, Az informatikai biztonság alapjai, a PGP kriptorendszer használata – Budapest: ComputerBooks Kiadó, 1999, ISBN: 9636182248 1. o.
[4] http://www.ittk.hu/infinit/2004/1118/tech1.html, 2007. 06. 17.
[5] http://www.mitre.org/news/the_edge/july_01/miller.htm, 2007. 06. 17.
[6] http://www.gordon.army.mil/AC/Spring/Spring%2002/GIG.htm, 2007. 06. 17.
[7] http://www.globalsecurity.org/military/library/budget/fy2001/dot-e/army/01wint.html, 2007. 06. 11.
[8] http://www.military-information-technology.com/print_article.cfm?DocID=1741, 2007. 06. 11.
[9] http://www.nationaldefensemagazine.org/issues/2001/Oct/Armys_Future.htm, 2007. 06. 11.
[10] http://www.agent.ai/?folderID=166&articleID=1570&ctag=&iid=, 2007. 06. 11.
[11] http://www.cdef.terre.defense.gouv.fr/publications/doctrine/doctrine01/US/etranger/art17.pdf, 2007. 06. 11.

[12] http://www.theregister.co.uk/2003/03/21/the_pentagons_tactical_internet/,2007. 06. 11.
[13] http://www.army.mil/fcs/network.html, 2007. 06. 13.
[14] http://www.army.mil/fcs/whitepaper/FCSWhitepaper(11_Apr_06).pdf , 2007. 06. 13.
[15] http://en.wikipedia.org/wiki/Defence_Information_Infrastructure, 2007. 06. 13.
[16] http://www.theregister.co.uk/2007/03/08/bowman_cpac_pasting/, 2007. 06. 13.
[17] http://en.wikipedia.org/wiki/Bowman_(communications_system)#BISAs, 2007. 06. 13.
[18]http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1016&zoneid=47, 2007. 06. 13.
[19]http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=340&zoneid=47, 2007. 06. 13.
[20] http://www.thalesonline.com/landjoint/Press-Room/Press-Release-search-all/Press-Release-search-result/Press-Release-Article.html?link=3E69743D-6161-1074-4E00-29234117060F:central&locale=EN-gb&Title=Microsoft+and+Thales+join+forces+to+promote+Comm%40nder%2C+the+new+integrated+C4I+solution+&dis=1, 2007. 06. 16.
[21] Új honvédségi szemle, 2005/12, Taktikai vezetési rendszer – FAUST
[22] http://de.wikipedia.org/wiki/BIGSTAF, 2007. 06. 13.
[23] Mikita János: A katonai infokommunikációs rendszerek fejlődésének főbb irányai. – Bolyai Szemle, 2001/1. (143-152.o.)
[24] Juhász György-Gáspár Tamás-Babos Tibor: Transzformáció: a NATO válasza a 21. század kihívásaira. – Új Honvédségi Szemle, 2006/3. (15-32.o.)
[25] http://www.globalsecurity.org/military/library/report/2003/htar-chapter16.pdf, 2007. 06. 12.
[26] http://www.globalsecurity.org/military/library/policy/army/fm/24-7/ch5.htm,, 2007. 06. 11.
[27] http://mip-site.org/publicsite/03-Baseline_2.0/MEB2R-MIP_End_of_Block_2_Report/MEB2R-NL-MSG-Edition2_1%20%20060608%201400.pdf, 2007. 06. 14.
[28] http://www.stsc.hill.af.mil/crosstalk/2001/08/moxley.html, 2007. 07. 02.
[29] http://194.7.80.153/website/book.asp?menuid=15&vs=3&page=volume1%2Fch02.html, 2007. 07. 02.
[30] http://www.stsc.hill.af.mil/crosstalk/2001/08/moxley.html, 2007. 07. 02.
[31] http://www.fgan.de/fkie/site/c40_f12_en.pdf, 2007. 07. 03.
[32] Dr. Munk Sándor: Az informatikai interoperabilitást támogató megoldások a NATO-ban, Új honvédségi szemle, 2006/09
[33] http://www.mip-site.org/011_Public_Home_Concept.htm, 2007. 07. 03.