"HENRI COANDA"
AIR FORCE ACADEMY
ROMANIA

GERMANY

"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY
SLOVAK REPUBLIC

INTERNATIONAL CONFERENCE of SCIENTIFIC PAPER
AFASES 2011
Brasov, 26-28 May 2011

COMMUNICATION AND INFORMATION SYSTEMS WITHIN THE CRISIS MANAGEMENT

Marcel LINEK

Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš, Slovak Republic

Abstract:

Considering the current security risks, a need arose to define critical infrastructure as a part of the infrastructure which, once destroyed, would make the developed countries face up severe economic and political consequences. Accordingly, a need arose for an appropriate security of this infrastructure in the case of terrorist attacks. Naturally, this also implies a need for implementation of modern and secure communication and information capabilities in both military and non-military operations on the territory of the SR (NATO) within the crisis management.

A coherent approach to the issue of protection and security of modern deployable ICT systems in both military and non-military operations on the territory of the SR (NATO) within the crisis management operations is a part of a complex issue and as such it requires elimination of other risks related to particular environment and circumstances, like natural disasters, emergencies, industrial accidents, physical wear out of installations (networks and facilities), lack of strategic supplies and scarce raw materials, use of mass destruction weapons, organized crime, spread of contagious diseases and many others.

Modern deployable ICT systems must be able to ensure efficient and failure free operation of all the communication and information elements of the system, be that the elements already employed or the elements to be implemented in a foreseeable future. This prerequisite is closely linked with the needs and requirements of deployable units earmarked for military and non-military emergency operations so that the successful accomplishment of the allied tasks is ensured.

Keywords: communication and information systems, crisis management, protection, security, interoperability and flexibility

Considering the current security risks, a need arose to define critical infrastructure as a part of the infrastructure which, once destroyed, would make the developed countries face up severe economic and political consequences. Accordingly, a need arose for an appropriate security of this infrastructure in the case of terrorist attacks. Naturally, this also implies a need for implementation of modern and secure communication and information capabilities in both military and non-military operations on the territory of the SR (NATO) within the crisis management.

Terrorism focuses primarily on carrying out attacks against civilian population and against the critical infrastructure of the state, with the aim to inflict heavy casualties and extensive damage, to instill fear and create atmosphere of insecurity. In addition to traditional threats to critical infrastructure like natural disasters, negligence, technology breakdown resulting in emergencies and accidents, unauthorized access and intrusion into computer systems or other criminal acts, a

phenomenon of terrorisms poses a new threat to security. A serious threat that modern terrorists efficiently use is a threat of the information and communication technology systems of the Allied forces being disabled, ruined or severely damaged.

A coherent approach to the issue of protection and security of modern deployable ICT systems in both military and non-military operations on the territory of the SR (NATO) within the crisis management operations is a part of a complex issue and as such it requires elimination of other risks related to particular environment and circumstances, like natural disasters, emergencies, industrial accidents, physical wear out of installations (networks and facilities), lack of strategic supplies and scarce raw materials, use of mass destruction weapons, organized crime, spread of contagious diseases and many others.

Modern deployable ICT systems must be able to ensure efficient and failure free operation of all the communication and information elements of the system, be that the elements already employed or the elements to be implemented in a foreseeable future. This prerequisite is closely linked with the needs and requirements of deployable units earmarked for military and non-military emergency operations so that the successful accomplishment of the allied tasks is ensured.

Security of modern ICT systems in the crisis management operation should focus, besides many others, on protection against terrorist attacks, with the following being the most likely forms of attacks:

- ***a direct action*** – a direct armed physical attack against a target, carried out by the armed terrorist groups,
- **a *bomb attack*** – an attack that is most likely to be carried out by an individual or a small group, using a non - conventional explosive charge (i.e. other than aerial bombing),
- ***CBRN attack*** – an attack using chemical, biological, radiological or nuclear agents
- ***Cyber attack*** – an attack aimed to destroy data or to ruin a computer system or to cause irreversible damage to a computer system/a computer program, normally via the Internet
- information operations – attacks aimed at gaining or misusing the information or attacks aimed to influence the information based processes (e.g. to influence a computer system in a way that it seems to be fully operational, however, the data used are being manipulated), whereas one's own information and computer systems are fully protected.

A paramount need to provide a secure environment for modern deployable ICT systems is a corollary of the fact that the current level of informatization in defence sector is very high. Equally, there is a critical need for informatization of the allied units deployed in military and non-military emergency operations on the territory of the SR (NATO).

The basic characteristics of a modern, fully deployable mobile ICT system that would be employed in military and non-military operations within the crisis management operations are as follows:

- mobility,
- modularity,
- interoperability,
- reliability,
- fully automated system,
- security,
- deployability,
- stability and endurance,
- open architecture,
- full autonomy and independence on the existing stationary infrastructure,
- the system needs to be easily and quickly put into operation.
- flexibility.
- others.

Modern ICT system should be designed as a mobile system and should not require a manual change of configuration every time that a position of one or more communication (information) subsystems (entities) is changed. Mobility should be based on fully distributed systems and dynamic distribution of data. Individual elements of ICT system should be fully functional also as autonomous entities without a need to communicate through central

management system. Mobility of the system must ensure that ICT is ready to be deployed under various climatic and geographic conditions, that is to say all over the world.

Another characteristic feature of a modern deployable ICT system is modularity. Modularity should facilitate a simple replacement or adding the HW components (devices) or even the whole blocks of machinery. With a view to available and reliable logistic support, the system should use just one type of HW components (e.g. server memory, the same type notebook, phones etc.). Software modularity should facilitate extended functions through new modules (entities) and provide a basis for integration of further customer's systems depending on the type of operation (mission).

A modern deployable ICT system with its broad portfolio of interface, modularity and fully distributed design must be able to adjust and adapt to any environment with standard interface. Interoperability of the system in question should be based on an open architecture and on portfolio of standard commercial and military interface installed in communication nodes (entities). A mobile ICT, equipped with a supporting tool X.500 protocol and transformation of directory services into a standard shape, should be capable of cooperating with many other ICT systems, be that military or non-military systems. At the same time it should be able to cooperate in the field of provision of individual information and communication services.

Individual entities of a deployable ICT system should be equipped with devices that ensure high reliability. HW components must be selected with regard to a wide scale usage, extensibility and scalability, reliability, unification with an adequate available technical support. Life-cycle of all the commercial HW components should be minimum 3 years and the individual manufacturers of HW components should provide both warranty and post warranty service, depending on geographical deployability of the system. A form and way of service to be provided should be arranged prior to deployment.

A modern deployable ICT system must be designed as a fully automated system and should not require change of configuration of individual ICT subsystems every time when the individual components of the system in question (entities) change their position. Equally, the processes of application of service packages should be automated. Low maintenance costs and easily available logistics should be ensured through the use of the so-called COTS (commercial) unified and easily available technologies and through standardization of components and interface.

A modern deployable ICT system will only be as safe and secured as its every component, entity or subsystem with the access to the system in question, be that through radio network, LAN or WAN. The use of Gate Personal Firewall, antivirus and antispyware solutions is an intrinsic part of modern ICT systems and an implied duty. Nowadays, at the time of global Internet, when remote working becomes more and more popular, which results in a need to connect to the home network through remote Internet connection, the operational systems of individual subsystems and applications must be properly maintained, operated, updated and secured. Every day the new security risks to software applications emerge, as well as threats to operation systems and applications that pose a genuine risk of ICT systems coming under attack, which might result in abuse of data or abuse of identity of users, even in serious

damage to or disabling of the ICT system as a whole, or some of its components.

The issue of automated repairs and update of operation systems and the individual information subsystems in modern deployable ICT systems is a complex one, and as such it requires maximum attention to be paid by a supplier and by a buyer of the ICT in question. Nevertheless, the system should be, at least, capable of the following:

- identification of a level of quick maintenance (update) and service packages
- testing of a quick maintenance on a pilot group of computers
- distribution of a quick maintenance to the selected groups of computers, information subsystems and the individual entities, based on the needs of the unit in question
- evaluation of a success rate of update and installation of service packages (patches)
- return to the original condition of the component, subsystem or individual entities in the case of problematic or inefficient update

A modern deployable ICT system must be designed as modular one, with a possibility to extend the ICT system (subsystem) in question and add the other communication or information elements, entities and subsystems. At the same time, there should be a possibility to integrate the system or subsystem in question into the other national or international ICT systems. The ICT system should provide a basis for integration of the other customer's systems. The system should have a sufficient capacity to address the needs of employment, super temporarily if possible, and should facilitate the use of applications on the existing HW device.

The scale of a system solution of a modern deployable ICT system should enable:

- building a communication (radio) subsystem,
- building IT subsystem,
- administration of users and defining rights on particular levels (a user, administrator, server administrator, etc.),
- file and press related services, direct or shared,
- local and remote configuration of workstations,
- remote installation of workstations,
- remote control of workstations and servers,
- videoconferences and presentation services,
- provision of electronic mail, as a minimum POP3, IMAP, SMTP, X.400,
- directory service according to a standard X.500, with a possibility of a connection to external systems,
- redundant architecture for the selected components (entities) of a system or subsystem,
- services DNS, DHCP (administration of IP directory plan),
- automated patch management of the OS and PC for the core parts of the system,
- replication of the domain information,
- replication of a file system among the individual entities or subsystems,
- server data back up using disk fields,
- remote control of servers without a need of a running one,
- hardware necessary to meet the user's requirements,
- software necessary to meet the user's requirements,
- provision of a platform for implementation of the other communication systems,
- making GPS coordinates available for the other systems or units.

A communication system should be designed to provide safe and secured mobile voice and data services through different information subsystems and radio systems with net devices and applications joined in support of communication between units within the crisis management. A communication system should provide LAN and WAN networks for the whole mobile

communication network, as well as connection to external LAN and WAN networks.

IT subsystem of a modern mobile communication system should be designed to minimize usage of WAN communication. In IT subsystem, the QoS services must be implemented that would, in critical situations, ensure that the defined type of voice and data communication is preferred. IT subsystem should be designed in a way that would ensure that WAN communication would provide the user with the following possibilities:

- replication on level AD (Active Directory) – implementation of directory services,
- file replication of DFS module (Distributed File System),
- HTTPS communication with the management,
- remote control of PC and servers,
- fully functional electronic mail (e-mails),
- access to intranet/internet,
- centralized patch management.

All the above mentioned services to be provided by IT subsystem must be optimized as to the use of WAN communication.

Likelihood of unpredictable asymmetric military and non-military threats is typical of the current security environment as well as of future security environment. With this type of threat, a rapid response becomes a vital prerequisite to success in crisis management operations. These operations require timely, flexible and agile command and control capabilities, supported by an interim local network and information infrastructure that must be fully deployable, easy to put in operation and easy to operate. It must also be resilient, stable, reliable, safe and secured.

The experience from NATO operations – primarily from Afghanistan and West Balkans – have shown that for an efficient crisis management it is inevitable, in the field of CIS, to provide units with modern deployable ICT systems based on proprietary HW and SW solutions, that would guarantee security of voice and data services in NEC-oriented environment. These systems must be based on a fully distributed modular and promptly deployable system that would create basic conditions for successful conduct of both the military and non-military crisis management operations.

REFERENCES

1. Szabo, S.: Command and control (C2). In The Slovak Armed Forces. July 2008 (2008), p. 23. Available at: Internet: <http://www.mosr.sk/slovakia-in-nato?>.
2. Szabo, S.: The course of the state policy in the field of defence science and defence technology up to 2010. In *Vojenské reflexie*, Vol. 3, No. 2 (2008), p. 5-13. ISSN 1336-9202.
3. Szabo, S.: Defence Policy and Defence Planning. In *Euro-Atlantic quarterly*. Vol. 3, No. 2 (2008), p. 22-23. Internet: <www.eaq.sk> ISSN 1336-8761.
4. Nečas, P., Olejník, F., Szabo, S.: Information warfare and security. In *Zarzadzanie bezpieczenstwem: Miedzy-narodowa konferencja naukowa.* Kraków, 11 - 13 May 2000. Kraków : Profesjonalna szkola biznesu, 2000. p. 75-82. ISBN 83-7230-040-2.
5. Nečas, P., Szabo, S., ADAMČÍK, F.: Information Operations/Combination Warfare in Simulated Environment. In Simulácia a modelovanie v *PVOS/ Simulation and modeling in the field of AD: Specialized military workshop with international participation* : Liptovský

Mikuláš, 21 October 2005. Liptovský Mikuláš : KPVO, Armed Forces Academy of General M. R.Štefánik v Liptovskom Mikuláši, 2005. 9 p. ISBN 80-8040-271-X.