PhD Eng. Maciej MARCZYK
Nationals Defence University
Brig. Gen. Chruściela 103
00-810 Warsaw, Poland
m.marczyk@aon.edu.pl,
ph 0048 22-6- 813-142

TITLE:
Opportunities for cooperation military tactical communications network to public networks in emergency operations in Poland

ABSTRACT:

The development of civilization, in addition to the clear benefits of the twentieth and twenty-first century, has also brought a lot of risks that may affect the public in the form of diversity crises. Effective coping with them is one of the determinants of modern society and guarantee the survival of humanity. Sources crises may be different in various ways affect the society. This can be caused among others crises: terrorist activities, environmental disaster or hostile economic impact of another state. Recognizing the importance of the problem of emergency response by presented in the article possibilities of cooperation of the army and the state civil service widely in the field of telecommunications (IT) and the use of military and public communication networks to manage operations during a crisis situation on the Polish territory. The author has made the analysis of an important issue which is the possibility of using IT networks and cooperation army tactical level and the network of publication for the management (command) implemented emergency response centers and the important organs of the crisis in our country. It must be assumed that the armed forces and the army largely will have a significant part in preventing the effects of different types of disasters. They will be an important link in the process of pursuing an emergency response management. For this reason, they must be able to implement some stages of emergency response at the same time the possibilities of cooperation with the local authorities. It follows that you should take steps to determine the suitability of land owned by military systems and networks in the field of emergency response management, as well as identify, by the possibility of using civilian systems and technologies for data and voice.
KEY WORDS: tactical communications network, public networks, emergency operations.

Introduction

In terms of the definition of national security in a crisis situation indicates that it is a state of growing instability, insecurity and social tensions, characterized by the violation of social ties, the possibility of losing control over events and escalation of threats, in particular, the situation is hazardous to life, health, property, cultural heritage or critical infrastructure, including incidents caused by terrorism. This condition also causes an intense, persistent and long-term deterioration in the functioning of society and the state. It is characterized by escalating danger of losing control of mitigating the effects of event (emergency) for each service, inspections and guards. This situation may also cause negative effects on the economy, and may also have an impact on foreign relations.

The basic document in this respect is the Act of 26 April 2007 *The crisis management* (Journal of Laws No. 89, item. 590). It shows the authorities competent for crisis management and the objectives and principles of action, as well as financing principles of crisis management tasks. The provisions of this Act shall also determine the nature of the crisis management operations public administration, which is part of national security, which is to avert crises, preparing to take over control of them through planned activities, to respond in case of emergencies and for reconstruction of infrastructure and restoration of its original character.

This was, among other things, reflected in the records of the National Security Strategy, where it is stated that the new challenges dictate the need for a comprehensive national emergency response system, responding to the contemporary threats to the security of both international and domestic. The relevant state institutions will lead efforts to establish an integrated system of management and supervision to him in the event of a crisis. It is necessary to consistently regulate the tasks and powers of the authorities and public institutions, and social organizations-acting tools for national security[1]. The document also indicated that the system of governance and management should be able to timely and effective response to any situation so that the scale of the threat adequately to allow the neutralization of the total.

The Act has already presented to the management indicated that the tasks and procedures are hereby to crisis prevention, preparing to take over control of them through planned activities and respond in case of emergencies implement the National Emergency Rescue System. This system is meant the structure and operation of government bodies and the Armed Forces[2].

The analysis of the assumptions and principles of the system showed that it consists of two major subsystems created by management authorities and the strength and means provided to act in emergency situations. These subsystems consist of the two mutually complementary components: non-military and military. Their role and participation in solving various crisis situations may be different, depending on the nature of the situation and their location and extent. In the case of a non-military crisis, caused by a natural disaster, natural or technical disaster, terrorist activities or other social phenomena leading role in the solution play an administration bodies and local government and civil forces and resources. In this case, part of the armed forces (elected bodies and the divisional command of military units) may be limited to assist in possible rescue operations in the liquidation of conse-

[1] National Security Strategy of the Republic of Poland, Warsaw (2007).
[2] Act of 26 April 2007 *The crisis management* (Journal of Laws No. 89, item. 590).

quences of emergency or maintenance of public order, and only in cases where the use of civilian proves insufficient, or impossible. However, during the crisis of a political and military (armed conflict, war) plays a leading role in the military subsystem.

The general assessment is considered that the essential parts of the system already exist. And the ongoing work of the normative and implementation focused on clarify the competences of individual cells, adjusting the relationship between them, organize and coordinate their action plans, remodeling solutions incompatible with the new realities and the creation of the missing pieces. Organizing an integrated management system and crisis management keep in mind its universal character. This means that in normal conditions it operates only when necessary. However, its development takes place only in an emergency, to the extent adequate to the scale (natural disaster, large disaster, a local armed conflict) to the highest readiness and maximum efficiency achieved during the biggest threat (during the war). Still, it should be one and the same system in which the basic composition, equipment and supplies (IT measures) do not change and are only replenished according to the needs of the situation and forecast of its development.

Topic analysis leads to the conclusion that the ideal solution would be to create a single integrated automated communication system that would work across all departments and entities involved in the management of its resources and the activities related to emergency surgery. Use in depending on the needs of the different types of networks would be the target data communication for exchanging information between the elements of the operation. IT networks could be built on the existing networks such as the level of tactical military troops land and other public networks (departmental and commercial), depending on what the requirements will be met by the participants in order to eliminate the crisis.

Opportunities for cooperation IT networks

IT networks used for the process of proving Army component is designed primarily to facilitate the exchange of information on distance (in various forms and in various ways) between relevant decision-making bodies and to improve (accelerate) the process of command. In a broader sense, IT networks organized for the purpose of process, the Army component command are also part of the whole system, communications of the Polish Armed Forces and State communications networks. Army IT networks are organized to provide a variety of comprehensive utilization of IT in all relationships command and control means destruction, collaboration, notification, warning and alarm. Capabilities and network structure depends on the adopted plan of action and tasks that are set for the troops.

IT networks army tactical level are set several subnet, differing in properties, specifications and sizes, suited to performing the function of sharing and exchange of information to varying degrees, depending on the technique used, the transmission of information. One of the indicators of the theory of combat NNEC[3] environment is a departure from the classical command system, and the departure from the hierarchy. The proposed network structure by the author different types of data communication networks are not assigned to any level of command, but a task that must support the militant group or item. These networks can be classified by the area in which they are developed for wide area networks and local area networks. Because of the high demand for the transmission of high-function amount of information, the basic matrix extensive networks in the process of Army component command is a radiorealy network supplemented by the cable network and satellite network. These networks should be assigned to the area activities (tasks area by the Army component) and not to the level of the which they are found. The main task of the network is to ensure an appropriate level of IT services in all bodies of command (decision) implements its tasks in the area where the backbone is developed and the storage and retrieval of information to authorized bodies of command.

The next component of the large networks, providing connectivity on the move over long distances, but with fewer opportunities transmission, radio networks are built HF and VHF using this type of radio. Network of HF and VHF radio will be used on the basis of the current in order to ensure communication and transmission doubling the limited amount of data for battlefield management systems. Network of HF and VHF radio are proven and reliable way to exchange information, but are characterized by a limited bandwidth and a small amount of data communication services. With a large amount of equipment owned the land forces component of HF and VHF radio abandonment of the means of communication seems to be pointless.

Topic analysis revealed that a separate component of IT networks organized process for the Army component command will local IT networks using broadband subunits radio networks operating in ad-hoc radio networks and network packet radio. These networks will be used for the provision of IT services to the subdivisions being on the move, in a small area. The main purpose of a network of local subdivisions should be exchange of information for battlefield management systems (share information on the location of their own troops and the enemy, consumption of resources and possible events).

The last element of telecommunication networks are local command posts and points of diversion. These networks can be created based on both measures cable (cable networks) as well as radio means (broadband radio networks with limited capacity and access work based on the 802.11 family protocols).

Considering the area of operation of the network including military networks can be made division following networks: LAN (Local Area Network called) local transmission network, MAN (Metropolitan Area Network called) - transmission metropolitan area networks, WAN (Wide Area Network) - extensive transmission network; The Internet - global network.

The Polish Armed Forces stationary use IT networks consisting of three main components: MIL-WAN network, network and network Internet SEC-WAN. The concept of organization communication for crisis management should base on the assumption of independence of the environmental conditions of the operation. You can use the infrastructure described in the article IT in the field of action, however, must deal with the failure rate or unavailability due to failures that have been made in the course of previous actions. The basic element, which should be guaranteed, is to implement mechanisms to create and share a full picture of the situation of the area of operations and the implementation of modern communication and information services. This solution will create a network of IT, which is characterized by exchange rate information (data) and at the same time allowing easy determination of the author and recipient of information.

[3] NATO Network Enabled Capabilities,

Modern telecommunication network should be characterized by: globalization, interoperability, cost-effectiveness and ease of management and maintenance. IT network services should include:

- constant observation of the situation in the area covered by the crisis;
- the possibility of a permanent exchange of information;
- exchange of e-mail;
- availability of network services and information services;
- can communicate via instant messaging;
- VoIP (Voice Over Secure Internet Protocol) technology, the main assumptions is the integration of traffic data transmission.

For future task forces gained full capacity to carry out operational activities in crisis because of their transformation should aim to increase maneuverability of troops and capabilities of telecommunication networks, and integrate logistics, expansion of civilian-military cooperation and more efficient use of troops (the ability in the following areas: systems, reconnaissance and intelligence operations in urbanized areas concerned).

All these projects aim to achieve information superiority, significant growth opportunities for autonomous action and finally to obtain operational capabilities, allowing the opposition to more and higher risks in today's crisis response operations. You should also pay attention to the possibility of co-operation of communication networks army component of other public networks while organizing crisis management system. Network infrastructure and information technology (NII, Networking and Information Infrastructure) is available to emergency operations now create four components:

- communications services (called Communication Services);
- IT and integration services (called Information and Integration services);
- information security services (called Information Assurance services);
- management services mentioned components (Service Management and Control Services).

The inclusion of any component in the non-military crisis management to network infrastructure and information does not mean that will change the owner of the entity managing this component. Military systems will be independently managed by their owners under the rules for military systems in the operation, which is one of the basic assumptions of the concept. However, the inclusion any component non-military system or component other ministries strength (police, border guards) will also be tantamount to agreeing to be bound by force in the joint crisis response operations, procedures and safety requirements. IT services are currently the most advanced IT component of the network structure, which is in direct relation with development and operation of the other components.

IT services component will be characterized primarily using the Internet Protocol (IP v. 6 and later[4]), which creates a common, secure transport mechanism for all types of information transmitted by all media transmission in data communication networks. IP transport services will operate in an environment which is characterized by the use of a wide range of transmission services (transport) and the need to support different types of quality of service in order to meet the requirements of individual applications.

The analysis in the commercial fixed infrastructure IT has shown that the basic infrastructure of the state are the backbone fiber optic network based on DWDM (Dense Wavelength Division called Multiplexing), owned by some of the largest telecommunications network operators, such as Polish Telecom, EXATEL SA (energy), TK Telkom, Poznańskie Centrum Superkomputerowo - Sieciowe. Many other operators, such as the Naukowo-Akademicka Sieć Komputerowa, Netia, the GTS uses its own links or leases it from the other aforementioned operators. The largest IT infrastructure has TP SA. The second largest national optical network with a total length of more than 20 thousand km. of fiber and bandwidth of 320 GB / s has EXATEL SA Another important provider of network access services, TK Telkom, has more than 6 thousand km. of fiber with a total capacity of 1.7 TBIT / s. Develop its own optical network and Polish academic centers under the PIONIER. This network is managed by the Poznańskie Centrum Superkomputerowo - Sieciowe now has a length of about 5.5 thousand km. of own network infrastructure (Figures 1-3)[5].

An analysis of services provided by public operators showed that they can be divided into three basic groups:

- protocol services using VPN (Virtual Private Network);
- services using Frame Relay;
- stream leased E1, E3 and STM.

VPN is a service that allows you to combine all the customer's location in a virtual wide area network. It is a service that allows you to create virtual wide area network client by sending private data over a public network operator. Client packet transmission is performed in such a way that the public operator nodes are transparent to this type of transmission. Older technology used to build wide area network service is Frame Relay, ATM-based technology. Frame Relay technology performs client's local area network on the basis of the statement of independent transmission channels in access transmission medium. Until recently, the common belief was that the armed forces are used latest technology in relation to public telecommunication networks and systems. Due to the existence until recently many research centers-acting tools for the military could be considered such statements to be true. However, changes in the doctrines of defense states, the reduction of the army and military research centers has meant that in many areas of technology and IT solutions used in the public sector are more modern solutions. An example of the rapidly developing field of science is right and telecommunications.

[4] IP v. 6 is to enable the creation of so-called. Internet of Things that will facilitate such secure logistics and improve the system power groups.
[5] http://www.pionier.net.pl/online/pl/projekty

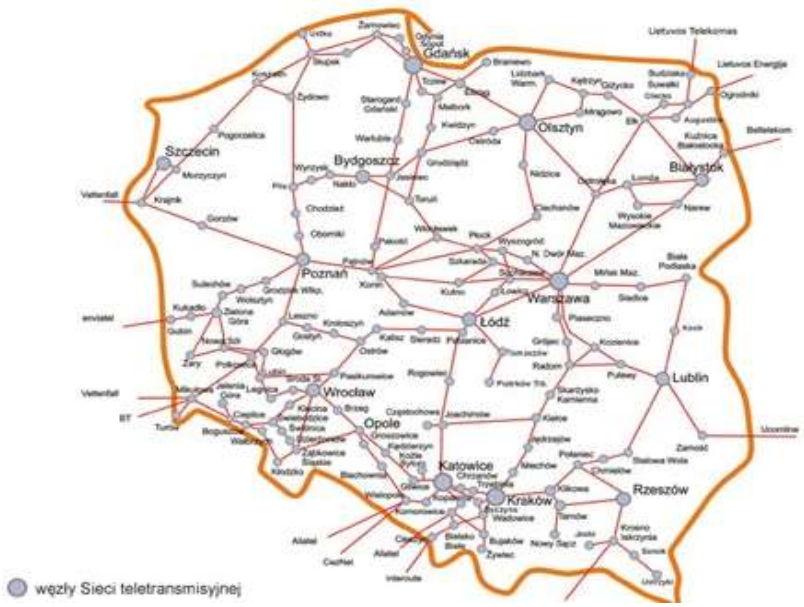

Fig. 1. Exatel S.A. - network infrastructure diagram

Source: http://www.exatel.pl

Fig.2. Telkom TK - network infrastructure diagram

Source: http://tktelekom.pl//files/swiatlowody_aktualne.gif

Fig. 3. Pionier - network infrastructure diagram

Source: http://ww.pionier.net.pl/online/pl/projekty/69

Summary

Cooperation between Army and regional public administrations in driving under the emergency response network using military communication is possible when public bodies will be equipped with these measures. The possibility of using the existing infrastructure is the greater, the more they are open systems. Studies have shown that the approach of COTS (commercial of the called shelves) by the use of commercial technologies in military systems, telecommunications, greatly facilitated the public work, departmental and military communication systems. It should be noted at the same time, it is observed continuously increasing importance of data transmission technology to the detriment of traditional telecommunications systems. The introduction of such a system based on the functioning of the network services IT is an inevitable process, which should be introduced in the Armed Forces and used for training and implementation of the tasks of the units of the Army. The beginning of this process is the introduction of the use in the Polish Army new simulation system JCATS (join combat and tactical simulation) and a tender for a new generation NCW platform (network centric warfare) – BMS (battlefield management system) .

Point management activities within the Group Emergency Response and Operational Group should have a direct and secure communication with superiors, subordinates, interacting elements, military and not-military in order to ensure the proper conduct of tasks. In crisis situations, should have the necessary tools in the form of forces and means of IT in order to respond to arising threats.

The Group Emergency Response and IT tasks should be performed by the best-trained soldiers professionally prepared to handle and use modern technology and equipment not only domestic production. Each network user has to be a professional recipient, equipped with a means of access to the network, and any IT equipped with a professional service provider network and control systems security transmitted in the information. In fact, an extensive network of IT will rational elements of crisis management and effective control over them.

It is also envisaged development of mobile telephony for crisis management and development of mobile computing products (personal devices, iPods, etc.) Personal Modern Commercial messaging (mobile phone, etc.) provide a much better service than military equipment. Commercial systems based on services, GSM, TDMA and CDMA will be used primarily as a network reserve (VoIP) and data support for the military (they will also be used by the soldiers of The Emergency Response Group mainly to coordinate activities and personal communication).

To mitigate the effects of crises should use all possible force and resources of the country, including IT systems. The rapid development revolutionized the approach to governance (management) and has allowed the introduction of a new quality of access to information. In relation to the information used in the management of emergency surgery systems and networks should ensure availability, reliability, safety, consistency, durability, and up to date information. The author believes it is necessary to:

- develop the concept of IT support for crisis management operation, the requirements of such a system should meet;
- develop and implement interfaces for collision-free communication information between different information systems of all actors involved in the operation of this type;
- development environment, which will harmonize existing activities various bodies and departments;
- develop a standard computer, which will form the basis for the formulation of future hardware and software specifications;
- term conceptual roadmap, and implementation;
- estimate the costs associated with all activities in this area and identify the sources of their funding.

Bibliography

1. Dela P., *Wsparcie informatyczne procesu dowodzenia*, NDU, Warsaw (2004).
2. Dela P., *Sieci teleinformatyczne w procesie dowodzenia komponentem WLąd*, NDU, Warsaw (2012).
3. Janczak J., Wołejszo J., Daniluk P., *Operacje informacyjne*, NDU, Warsaw (2005).
4. Janczak J. i inni, *Sieci komputerowe węzłów łączności wojsk lądowych*, NDU, Warsaw (2006).
5. Janczak J. i inni, *Wykorzystanie mobilnych sieci teleinformatycznych na stanowiskach dowodzenia szczebla taktycznego*, NDU, Warsaw (2008).
6. Nowicki K. i inni, Sieci LAN, MAN i WAN – protokoły komunikacyjne, FPT, Krakow (2003)
7. Kręcikij J., *Działania sieciocentryczne. Wybrane problemy*, NDU, Warsaw (2008).
8. Ustawa z dnia 26.04.2007 r. *O zarządzaniu kryzysowym* (Dz. U. Nr 89, poz. 590).