“NICOLAE BĂLCESCU”
LAND FORCES ACADEMY

The 21st International Conference
The Knowledge-Based Organization

TECHNICAL SCIENCES

CONFERENCE PROCEEDINGS 3

11-13 JUNE 2015

“NICOLAE BĂLCESCU” LAND FORCES ACADEMY
PUBLISHING HOUSE
SIBIU, 2015

ICT SECURITY OF A STATE

Mirosław SMOLAREK, Marek WITKOWSKI,

The General Tadeusz Kosciuszko Military Academy of Land Forces, Wroclaw, Poland,
m.smolarek@wso.wroc.pl, m.witkowski@wso.wroc.pl

Abstract: *The paper presents the impact of the reliable ICT systems on efficient and safe functioning of a state. Moreover risks which faced communication and information systems have been presented. Furthermore authors proposed their own solutions that may improve the level of security of transmitted information. Then they indicated ICT systems that can be used for providing continuous and flawless exchange of information, with particular emphasis on the need of protection of information from unauthorized access, modification or destruction. Also some suggestions have been proposed for the modernization of IT systems, which could improve the secure dataflow and ensure continuous exchange of information between the components responsible for the security of the state.*

Keywords: Information and Communication Technologies, ICT systems, secure communication, state security management system

1. Introduction

Well-functioning communication systems are particularly important for military as well as non-military structures, which are actively involved in safeguarding the security of a state. Means used in communication and information technology are often called ICT critical infrastructure of the state, and are essential for the safe and uninterrupted functioning of the country. Ensuring the proper functioning of this type of infrastructure would contribute to the smooth flow of information and providing safety for the management systems used for efficient administrating of the state-run institutions and other aspects of national security. Thus, the institutions and organisations responsible for the security of the individual components of the system will be able to receive and provide real-time information about the anticipated and real dangers and hazards. On this basis it should be possible to conduct proper decision-making processes and take the appropriate measures and actions adequate to the given situation. Well-coordinated reaction and quick response to the arising threats could ensure restoring conditions from the pre-crisis time.

2. Threats for ICT security

Accidental or organized (targeted) attacks on ICT systems and networks can occur in many forms, for example as:

- damages caused to fixed ICT infrastructure;
- interference in radio frequencies;
- electronically distributed viruses, worms, Trojan horses, malware, spyware, etc.;
- blocking access to vital services (governmental, public administration, military, law enforcement or finance systems);
- hacking into databases, applications or other programs;
- destabilizing or taking complete control

over ICT systems;

- forging crucial data (e.g. election results).

Above presented possibilities of attacks, not only in cyberspace, are only some examples of methods used for destabilisation of communication and information technology systems. Furthermore the methods which are used nowadays to achieve the goals by various groups, organizations or terrorist extremist factions, are still under development. That is why persons and institutions responsible for ICT security have to be prepared for new forms of attacks in the future.

With the current saturation of information equipment and the use of the Internet as a main mean for data transfer – one can state that computers are one of the most significant threats to ICT security. This new type of hazards in the network-centric environment are referred as “cyber threats” or commonly a term “cyber terrorism” is used. Particularly significant cyber threats can include those that are directed to incapacitate critical infrastructure of the state. The aim of the "electronic attack" can be military and non-military structures of a particular country or group of countries. The most dangerous cyber-attacks are those which are aimed against ICT infrastructure responsible for the flawless functioning of the following systems responsible for:

- national security management**;**
- protection and defence of the state;
- crisis management;
- warning and alarming**;**
- state and local government;
- support (e.g. the economic, social etc.);
- widely understood control and monitoring (e.g. in the energy or transport sectors).

In above mentioned systems appropriate protection measures should be taken, that will ensure their functioning in all conditions in order to prevent damage to or destruction of ICT critical infrastructure. Ensuring continuous communication between the elements which are responsible for the security of the state is particularly important in situations of imminent threat to the state and its citizens. Therefore it is essential to ensure the appropriate level of security for data communication systems and the efficient exchange of information.

As mentioned earlier, the serious threat to these systems are the risks that may occur in cyberspace. Such threats may arise as a result of unintentional or intentional acts of a different nature, extent and intensity that can be targeted to a specific country or system.

Therefore, the fight against cybercrime should be conducted in an organized way and have dimensions which range from national to international levels. For example, the fighting against cyber-attacks could be organised in framework of cooperation between various organisations, institutions, departments and agencies that are responsible for the state security. Moreover, the continuous exchange of information about the potential risks should also take place at the level of international institutions and organizations. As an example of such cooperation one could mention the European Cybercrime Centre (EC3) at Europol. The organisation collects and processes data on cybercrime, and then distributes the crucial pieces of information to the member states of the European Union [1].

The risk assessments prepared by EC3 allow to maintaining databases, conducting analysis, forecasting and identifying trends in potential threats. Information obtained in this way may be beneficial for improving the effectiveness of an early warning system against cyber-attacks.

The protection of information systems against potential dangers is called by a collective term “cyber security”. In protecting the web community are involved several agencies, institutions and organizations, which were set up in order to respond to security incidents on the Internet. The main international bodies are:

- ENISA (European Union Agency for Network and Information Security) [2];

- CERT (Computer Emergency Response Team) [3];
- CSIRT (Computer Security Incident Response Team) [4];
- IWPITC (INTERPOL Working Parties on IT Crime) [5];
- CCDCE (Cooperative Cyber Defence Centre of Excellence) [6].

Joint actions for IT security, improve the effectiveness of the fight against cybercrime. Appropriately structured cooperation, exchange of experience and the threat databases could provide better protection and conduct continuous operations in case of crisis situations. Therefore, a very important task for the protection ICT systems used by the structures responsible for the security of the state is a comprehensive approach to the subject of study.

3. Counteraction to the threats

Effective prevention of ICT infrastructure against the potential dangers requires proper organisational measures and use of reliable IT systems which should ensure:

obtaining information about the structure and location of the criminal or terrorist groups;

- acquiring data about preparation for potential attacks, venues and endangered objects;
- processing of the obtained pieces of information;
- collection and storage of data regarding potential enemy groups, their methods, techniques and principles of operation;
- exchange of information between counterparts responsible for the security of the state, with simultaneous ensuring safety procedures and protection of databases against unauthorized access.

Implementation of the above mentioned undertakings and information processes requires the use of modern information and communication technologies, information management programs and other modules (applications) which could enhance and support decision making processes. Having a reliable means of communication, especially in a time of appearing of military and/or non-military threats, should provide immediate notification of the authorities who are responsible for ensuring safety in emergency situations.

Obtained information will also allow to dispatch appropriate forces and means for the area in which the threat appeared. Comprehensive approach to the issues related to ensuring the exchange of information should base on a reliable telecommunications infrastructure for the needs of national security. Furthermore, if the ICT systems should be compatible with the systems of other countries and in addition an exchange of information at the international level should be provided. This approach will ensure the continuity of operating of institutions, bodies and services which are responsible for the security of the state and its citizens.

Interference in the trans-mission of information or a complete incapacitation of ICT systems may adversely affect the process of making adequate decisions. Moreover, this kind of disturbance could contribute to a significant delay or total lack of response to arising threats. Improper flow of information between the governing and executive bodies may result in a lack of coordination in organised assistance and contribute to the escalation of the threats. Therefore, it is essential that ICT systems, used by the authorities responsible for national security, should be reliable and have to be a subject to special protection.

4. Proposed changes for ensuring ICT security

One can state, that issues related to cyber security, should focus on the following areas:

- technical;
- physical;
- human resources;
- organisational;
- legal.

Only such a comprehensive approach to the above-described areas could ensure uninterrupted data transmission in all circumstances. This applies to the transfer of the necessary information about the aforementioned activities between the decision-making bodies at the local, national as well as international levels. According to the above-mentioned areas, the model of the ICT systems for emergency situations should be based on a variety of IT equipment and media transmission devices. This approach should ensure the efficient exchange of information between military and non-military authorities, public administration representatives, security and public order services.

This task, however, requires a systematic attitude to issues related to the construction of a modern infrastructure. The preparation of such infrastructure is not an easy task, because it demands a detailed analysis, specialized studies and considerable funding for such projects. However, this approach will help to determine the most reliable IT systems that ensure efficient flow of information in all circumstances.

Based on their own research, the authors suggest that building of such systems should be not limited only to one group of data transfer and communication equipment sets and transmission channels (lines), but rather various and non-conventional solutions should be applied. The use of different means and devices of communication and broadcasting media, should ensure incessant circulation of information. This is due to the fact that in the case of damage or destruction of one data communications system (e.g. during cyber-attack) it should be possible to transfer the information by other, even “older” means, and communications channels to the decisive bodies responsible for the security of the state.

The ICT means that can be used for efficient and secure exchange of information are:

- wired communication systems - based largely on fixed communications lines, which operate on the basis of fixed infrastructure. To this group one can include all kinds of telephone switchboards, telephones and fax machines, which are the main transmission medium for cable networks;
- wireless communication systems - which transmit information by use of radio waves. These are mainly: radio stations, radiotelephones, mobile and satellite phones and services;
- information systems - these are mainly computers, laptops, and tablets with the secure software systems, applications and support software. To this group one can add devices such as: printers, plotters, scanners and telefaxes.

All the above-mentioned groups of communications means, ICT systems and telecommunications infrastructure (fixed and wireless) must be prepared for simultaneous and/or alternative use for information exchange between the institutions which are responsible for the security of the state. Although it is particularly important to increase the amount of wireless communication equipment, because this type of devices can operate in virtually all environmental circumstances. This is due to the fact that such devices use electromagnetic waves for transferring information, which are not dependent on fixed infrastructure or the Internet. In addition, both radiotelephones, as well as mobile and satellite phones have their own power supplies, so they will be able to operate in the moments when the national power grid is damaged or destroyed. Another advantage of wireless means is that they can be used in places where wired systems ceased to function or even when in a given area does not exist a fixed comms infrastructure.

Modern IT infrastructure built for the needs of national security should be primarily based on mobile communications components that provide:

- rapid deployment and establishing communication as well as proper operation of ICT networks;

- dynamic reconfiguration of used systems and networks in the event of damage or destruction of the ICT infrastructure;
- automatic exchange of databases between the parts of the safety management systems of the state;
- secure information flow.

The components of the infrastructure designed to ensure the flow of information can be built on the following elements:

- the Internet network WAN and LAN type to ensure encrypted data transmission;
- access servers with authentication of the access to the resources;
- network integrators of IP-WAN – which allowing the exchange of data via radio link and stationary lines;
- integration blocks - that allow the automatic exchange of data and voice messages between wired and wireless systems;
- subscribers' terminals;
- access stations;
- radio broadcasting centres;
- radio reception centres;
- retranslation radio transmitters;
- radio base stations;
- broadband radio stations;
- personal radio stations;
- IP radio stations;
- directional radio links;
- mobile phones;
- satellite phones.

Efficient flow of information between all the elements responsible for safety could reduce to a minimum the time for developing a decision and for rapid action which could support increasing the level of security of the state in crisis situations. Therefore, ICT systems, which are used for the collection, processing, transmission and storage of information for national security, must be protected adequately and be secured against unauthorized access, modification, or obtaining information by unauthorized persons.

5. Conclusions

The use of information protection measures in ICT systems should guarantee confidentiality, integrity and continuous availability and access to stored data only by authorized persons. Limited access to sources of information may delay the decision making process and thus lead to the spread of risks. In order to avoid such situations should be necessary to introduce measures of efficient protection in order to guarantee the security of information as well as quick access to it. Such actions should limit opportunities for access to the important data for national security by unauthorized persons, as well as to make the unauthorized changes in the databases or protect systems from deliberate destruction of information. Only professionally designed electronic systems and properly constructed IT security policy could ensure the proper protection of information and enable the efficient functioning of the state in case of the threat for state's critical infrastructure. Well-designed information security policy should contain documented sets of rules, best practices and procedures, in which the organisation determines how to protect their assets, own systems and processed information [7].

Currently every country tries to protect their ICT systems. In case of Poland such provisions were determined in "Cyberspace Security Policy of the Republic of Poland", which defined that with special protection should embraced ICT systems that are operated by the government, the legislative authorities, the judiciary, local government, the strategic state safety systems as well as businessmen and individuals [8].

Conducting the well-organized and coherent IT security policy requires formulation of a legal and organizational framework in order to build a system of effective coordination and information exchange between all elements of national security management system and enable collaboration within the framework of international agreements. Only a coherent system could provide the efficient exchange of information and effective management in case of extraordinary emergency situations. Providing of the required level of ICT security should also ensure the protection and defence of country's critical infrastructure.

References

[1] https://www.europol.europa.eu/ec3

[2] http://www.enisa.europa.eu/

[3] http://www.cert.org/

[4] https://www.csirt.org/

[5] http://www.interpol.int/

[6] https://ccdcoe.org/

[7] PN-ISO/IEC 27002:2014-12

[8] Cyberspace Protection Policy of the Republic of Poland, Warsaw 2013.