CYBER SECURITY WITHIN THE GLOBALIZATION PROCESS

Milan PODHOREC

University of Defence, Faculty of Economics and Management,
Brno, Czech Republic

The contribution focuses on the issue regarding security of information shared within the decision-making processes concerning control activities and information protection, which represents a key factor in the cyberspace. One of the main principles, which are considered as the basis for network operations and information sharing under the conditions of environment digitalization for users, lies in security and protection of mutually interconnected networks. Information superiority on the one hand and meeting requirements for secrecy and security on the other hand will result in high demands on personnel and implementation of cyber security and protection measures.

Key words: *Communication and information systems, Cyber security and protection, Information.*

1. INTRODUCTION

The environment which influences the security of states undergoes dynamic changes. Its foreseeability decreases due to the increasing interconnection of security trends and factors. The threats, their sources and bearers are of both state and more and more non-state and supranational character. Internal and external security threats mingle and the differences between them are being removed. The importance of a complex approach is increasing; it combines military and civilian tools including diplomatic and economic resources to prevent threats and to mitigate their adverse effects. The requirements for readiness to respond to sudden threats in time and effectively are also increasing. They are related to the trends in the global environment which reinforce their potential and increase the possibility of their propagation from the relatively remote areas of local or regional conflicts and strained relations. The balance of the security environment is affected by the increasing goals of new global and regional participants. The distinctive feature of the current environment is the fact that the instability and conflicts beyond the European border may also have direct impact on our security. The main guarantee is the membership of NATO and EU and good relations with neighbouring countries. Main threat sources are critical attitudes towards the base values of the society, the doubtful concept of a democratic legal state and the negation of basic human rights and freedoms. Both states and increasingly non-state participants and various groups and

their supporters may be bearers of these attitudes. [1]

Through prevention and coping with common threats the security became a key factor in supporting the quality of life in the European society and in protecting critical infrastructures. The internal security strategy has been adopted with a view to facilitate the road ahead for Europe, to combine present activities and to set out principles and instructions for future activities. Therefore, it is vital for the internal security strategy itself to be able to conform to both the requirements of citizens and the challenges of the dynamic and global twenty-first century.

2. SECURITY OF COMMUNICATION AND INFORMATION SYSTEMS IN THE GLOBALIZATION PROCESS

The present age can be called information age. Information superiority is also one of the main goals of NATO transformation processes. The Czech Republic as an Alliance member has to pay special attention to improving information support of operations in peace as well as in coping with crisis situations. New trends vest in massive emergence of communication and information technologies and modern tools related to them to provide security

and services. The aim is to eliminate problems in operating communication and information systems and to achieve high resilience, reliability and effectiveness. Based on the analysis of security environment of the Czech Republic specific threats for its security can be identified. The Czech Republic, as a responsible member of international organizations, also considers such security threats which do not affect directly its security, but threaten its allies. Cyber attacks rank among these threats. In this respect, the official view of cyber attacks is as follows: The increasing dependence on information and communication technologies raises the vulnerability of the state and its citizens towards cyber attacks. These attacks may represent a new form of warfare or may have criminal or terrorist motivation and may be used for society destabilization. The leakage of strategic information, interferences in information systems of state institutions or strategic businesses and companies which support state basic functions may threaten strategic interests of the Czech Republic. [2]

3. CONCEPT OF THE CZECH REPUBLIC CYBER DEFENCE

The problems of the Czech Republic cyber defence were \model known as the Plan-Do-Check-Act or the PDCA. It may be applied to

all ISMS processes according to this norm. **Figure 1** illustrates how the ISMS accepts requirements for information security.

The ISO/IEC 27001 norm provides the entire model for implementing principles which modify risk assessment, the proposal and implementation of security, security management and repeated security evaluation. This international norm supports the adoption of procedural approach for establishment, implementation, operation, monitoring, maintenance and improvement of ISMS in an organization.

For an effective operation of an organization it is necessary to identify and control many interconnected operations. The operation which uses sources and which is controlled for the purpose of transformation of inputs to outputs may be considered to be a process. An output from one process often forms directly an input for the next process. The application of the process system in an organization together with the identification of these processes, their mutual operation and control may be designated as a *"process approach"*. In using the process approach for information security management, as it is presented in this norm, the stress is laid on:

- Insight into the requirements for information security of an organization and the need to define the policy and goals of information security;
- ISMS implementation and adoption of measures in the context of organization activities risk management;
- ISMS efficiency monitoring and reviewing;
- Continuous improvement of the system on the basis of physical metering.

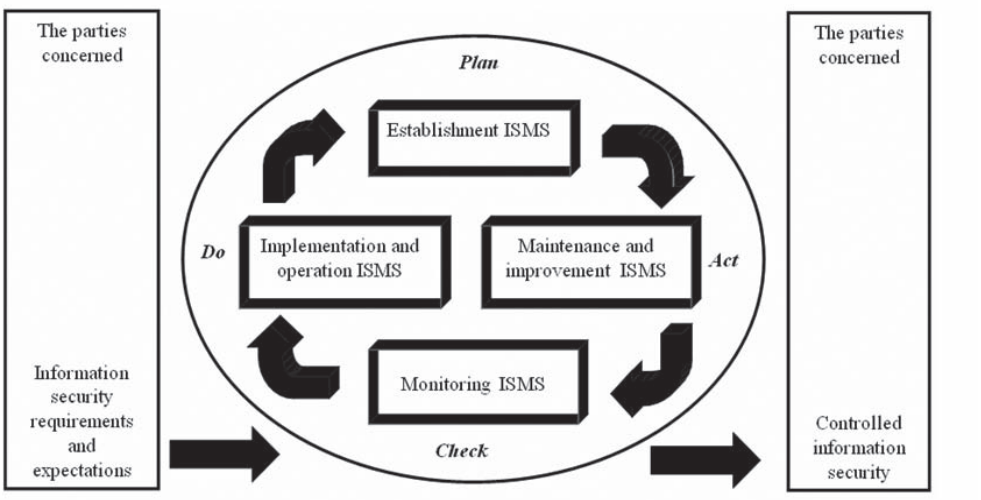

Fig. 1. The PDCA model applied to ISMS processes

4. REQUIREMENTS FOR INFORMATION SECURITY

Information, supporting processes, systems and networks are important assets of an organization. Defining, implementing, supporting and improving information security may be essential for maintaining capability of an organization. Organizations and their information systems are threatened when they are subject to security threats from different sources including computer frauds, espionage, sabotage, vandalism and fires. The sources of damages, such as computer bugs, hacker attacks and denial-of-service attacks, are more frequent and their hazardousness and sophistication are increasing. Information security is important from the viewpoint of critical infrastructure protection in both the private and the public sector. In both sectors information security is important for service availability and, at the same time, for avoiding or minimizing risks. Interconnecting public and private networks as well as sharing information sources increase the difficulty of access control. The tendency towards the distributed processing and information sharing may weaken the effectiveness of central control performed by specialists.

Many information systems were not designed to be safe. Security which may be achieved through technical resources is inadequate and should be completed with adequate management and procedures. Careful planning and analysis of any detail are necessary to determine the measures to be taken. Information security management, therefore, requires at least some participation of all employees of an organization. It may also include cooperation of an organization, third parties, users and other external entities. Last but not least, some advice from specialists of other organizations may be useful. It is necessary for an organization to define its safety requirements. The three main sources are as follows:

1) The first source is the assessment of risks which threaten an organization with regard to its global strategy and aims. Within the risk assessment the threats and the probability of their occurrence are identified. The threats may act against activities and vulnerability and may be misused. It is necessary to make an estimate of their potential impact.

2) The second source includes the requirements of laws, by-laws and norms, contractual stipulations as well as local conditions which an organization, its business partners, contractors and service providers have to follow.

3) The third source includes specific principles, goals and requirements for information processing which an organization created to support its activities.

5. PREPARATION, TRAINING AND EDUCATION OF PERSONNEL IN THE FIELD OF CYBER SECURITY

The ability and readiness of personnel to fulfil assignments in the environment of information technologies and in the integrated environment will require different levels of knowledge and skills from each user depending on his/her tasks within the forces structure. It is necessary to specify the depth

of knowledge of information technologies in the information environment with regard to the level of particular military professional's, specialist's needs which will be mentioned in the concept and will define the requirements for personnel specification. The quality and continuous recruitment of armed forces is a task of personnel marketing which will enable the selection of appropriate personnel for the categories of workers required for building capabilities in the field of cyber security. They are as follows:

- Efficient workers to support task accomplishment;
- Workers capable of inventing and implementing new procedures, and
- Workers for research and development.

For the second and third category it will be necessary to enlist the personnel with qualities which cannot be attained through training only, namely for time reasons. Education of military professionals in military schools has and will have an unsubstitutable place in relation to the development of information technologies. In the field of information technologies the development of education must also be supported more in the educational and training institutions of the Ministry of Defence of the Czech Republic. The accredited form of soldiers´ training is realized based on the study programs which have been developed in compliance with the Act on universities of the Czech Republic and is performed at the University of Defence. The non-accredited form of soldiers' training is carried out in career and special courses for officers, warrant officers and non-commissioned officers. The non-accredited form of soldiers' training is carried out at the Military Academy in Vyškov and in military educational and training institutions. In the area of future officers' training it will be especially the provision of required information qualification for all graduates from the University of Defence who will be capable of accomplishing demanding tasks in the future information environment. In the selection of applicants for the study at the University of Defence one of the criteria of the university entrance examination (in addition to the English language knowledge, physical condition, medical fitness and psychological resistance) will also be the level of knowledge and skills in the field of information technologies. Depending on the gradual development of resources and environment, the cyber security problems should be included in the following areas:

- Curricula at military schools to achieve insight into the conceptual basis and its impact on the development of operational capabilities;
- Curricula and training programs in educational and training institutions with a view to achieve qualification to handle particular hardware and specific operational procedures.

Solving the problems of cyber defence and system security in departments will be realized using personnel and resources of departments, especially at the centre of Computer Incident Response Capability (hereinafter referred to as CIRC), and project and operation security managements. With regard to cyber defence specificity and related system security problems it is necessary to provide high

qualifications for personnel who have sufficient previous work experience in the field of information and network technologies. The objective is to enlist and stabilize personnel with adequate knowledge and attainments (specialists in the field of information technologies whose knowledge also includes the field of system security) that will support the accomplishment of cyber defence tasks.

The main objective in the field of training and education is to provide an integral system of training. It is necessary to create conditions for the preparation, training and education of both specialists in administration and operation in the field of cyber defence and system security and users of information systems. The training of technical staff has to be aimed at the increase in capabilities for preventing, searching and coordinated responding to computer threats and incidents. As to the users of information systems it is required to increase security awareness in their use and to achieve the desired level of knowledge, skills and habits aimed at minimizing security incidents.

6. CONCLUSIONS

In connection with the threat of cyber attacks the priority of the government is to provide security and protection of information and communication systems included in the critical infrastructure of the Czech Republic using the government coordinating team for immediate reaction to computer incidents (Computer Security Incident Response Team – CSIRT). This team is a part of the national and international early warning system. The Czech Republic supports the building of such systems which enable widespread cooperation of all participants, i.e. also those who are not a part of public service and contribute to the exchange of experience acquired in coping with cyber incidents at national and international levels. The government supports legislative as well as non-legislative measures to be in compliance with the principles of information society development and the strategy of cyber and information security. [5]

The government supports uncompromising observance of security standards in information and communication systems operated by public authorities. It also supports further education focused on cyber and information security since the general public may be the most vulnerable element of the entire system. It defines the methods of protecting the sensitive information which is handled in the information systems operated by public administration authorities, namely the information systems required for supporting the state critical infrastructure. The Czech Republic is actively engaged in developing measures against cyber threats within international organizations, namely EU and NATO. It supports the reinforcement of international judicial and police cooperation with the aim to capture cyber attack perpetrators. The Czech Republic also joins the initiatives supporting the creation of international legal standards modifying the problems of cyber security. [6]

REFERENCES

[1] Security strategy of the Czech Republik. Praha: 2011, 20 s. ISBN 978-80-7441-005-5. [czech], p.7.

[2] Idem, p.9.

[3] Liang Qiao, Al Santoli, Xiangsui Wang, (2002) Unrestricted Warfare, NewsMax Media, Inc.

[4] ISO/IEC 27001-Information Security Management Systems.

[5] Security strategy of the Czech Republik. Praha: 2011, 20 s. ISBN 978-80-7441-005-5. [czech], p.13.

[6] Idem.

[7] ISO/IEC TR 13335-1,2,3,4,5 Information technology - Guidelines for the management of IT Security - Part 1,2,3,4,5.

[8] Strategie vnitřní bezpečnosti Evropské unie:Brusel: 2010, 32 s. ISBN 978-92-824-2674-6. [czech].