Cyberspace Situational Awareness in National Security System

Rafał Piotrowski, Joanna Sliwa,
Military Communication Institute
C4I Systems’ Department
Zegrze, Poland,
r.piotrowski@wil.waw.pl, j.sliwa@wil.waw.pl

Abstract — Todays’ world is based on two main dimensions: a real one and cyber one that are mutually connected and interdependent. People’s business and private lives use cyberspace on a daily basis. Counties’ economies with private and public sector companies use the Internet for their business and operation. However the systems connected to the Internet are subject of multiple threats that may cause not only vulnerable information leakage but also loss of reputation or damage of the critical infrastructure. That is why the authors emphasize the need of constant monitoring of the systems that may be subject to cyber-attacks. The article presents the concept and architecture of Cyberspace Security Threats Evaluation System of the Republic of Poland (SEZBC) for national security management. There have been described its role at a national level in the area of cyberspace situational awareness and decision making process. The role of SEZBC was commented both from the point of view of the requirements and regulations of the European Union as well as the Republic of Poland.

Keywords-component: cyberspace national security, risk analysis, critical infrastructure, cyber situational awareness.

I. INTRODUCTION

Recently, the Internet and cyberspace has had an increasing impact on all parts of human life. All areas of our life depend on information exchanged mainly via Internet. The Internet enables global information sharing without barriers between communities. In conjunction with communications technology it has become the driving factor of the world’s economy growth. Many systems and sectors such as finance, energy and transport base on the information systems with the continuous access to the Internet. However, these benefits come with a price. The information systems are affected by Cybersecurity incidents, increasing in frequency and magnitude, becoming major threat to safety and the economy [1]. They can result in losses not only in the reputation of the companies but also financial losses or even threaten the smoothness of the countries’ operation.

Cyberspace should be protected from non-intentional and intentional malicious activities and incidents. In this area governments have a significant role in assuring a free and safe cyberspace. However most often major parts of cyberspace are operated by the private sector. New technologies, like cloud computing or e-banking, demand security assurance, because they are vulnerable to accidental or cybercrime incidents. The victims of cybercrime activities are the government and public institutions, the private sector and common citizens. Attackers are using very sophisticated methods for espionage, stealing money or critical business information as well as blocking access to business services. Because of these new threats governments and companies have started to develop own cybersecurity strategies.

In 2013 the European Commission published Cyber Security Strategy [1]. It was the first document covering many aspects of EU’s policy in the area of cyberspace. The goal of this strategy is to strengthen the security of the EU’s information systems and to stimulate economic growth by common Internet utilization. The Strategy defines the priorities for EU international cyberspace policy. It bases on freedom and openness as fundamental rights in cyberspace. It assigns that responsibility for more secure cyberspace depends on all participants of the global information society, from governments to common citizens. Development of EU cyber security should involve international cooperation between military and civil agencies responsible for national as well as private sector safety. Security of the Internet as a global network demands cooperation between countries to detect and mitigate cyber threats. This strategy defines roles and responsibilities necessary for the effective protection of the cyberspace. The private sector should play a leading role in the management of the Internet. Protection of the cyber domain includes actions both in the civilian and military area. Cybersecurity assurance is a common responsibility of all cyberspace players. Over the last two decades several initiatives have been developed in this area.

The national institutions and agencies have created Computer Emergency Response Teams, called CERTs (e.g. CERT EU, CERT Polska, CERT GOV). They are responsible for the defense against and responses to cyber-attacks. The CERT Polska team is handling security incidents and cooperates with similar units worldwide. Cert EU works at an international level. CERT.GOV.PL - The Governmental Computer Security Incident Response Team (established in 2008) is responsible for protection of public administration units against cyber-threats. Its area of responsibility includes IT systems and networks which may influence the lives and health of people, existence of national heritage and the environment,
lead to considerable financial loss, or disturb the operation of public authorities.

In 2004 the European Network and Information Security Agency (ENISA) has been established. Its aim is contributing to ensuring a high level and developing a culture of network and information security (NIS) within the EU. ENISA cooperates with the Commission, the Member States and, consequently, the business community in meeting the requirements of network and information security, including present and future EU legislation.

Nowadays the proposal of “Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union” [4] is agreed among member states. It makes member states, key internet providers and critical infrastructure operators obliged to secure their systems. Moreover, these parties are required to manage the risks to their networks and to report important security breaches. Each country and designated national authority for network and information security (e.g. CERTs) should improve readiness and engagement of the private sector in cyberspace risk management. The key cyberspace players like banking, energy supply, transport, Internet services as well as public administrations should assess and manage the networks and information systems risks. They should share the identified risks with the national NIS competent authorities to enable common cyber situational awareness for decision makers. The directive enforces the following measures [4]:

- Each Member State must adopt a NIS strategy and designate a national NIS competent authority with adequate financial and human resources to prevent, handle and respond to NIS risks and incidents;
- It is necessary to create a cooperation mechanism among Member States and the Commission to share early warnings on risks and incidents through a secure infrastructure, cooperate and organise regular peer reviews;
- Operators of critical infrastructures in some sectors (financial services, transport, energy, health), enablers of information society services (notably: app stores e-commerce platforms, Internet services, cloud computing, search engines, social networks) and public administrations must adopt risk management practices and report major security incidents on their core services.

The above requirements create the baseline for executive regulations’ modification. The current regulatory framework requires only telecommunication companies to adopt risk management steps and to report serious NIS incidents. The EU is going to contribute efforts to strengthen Critical Information Infrastructure Protection (CIIP) cooperation networks involving governments and private sector. Moreover these efforts should be supported by research and development and academia in the EU. To avoid duplications, the EU is exploring possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defense and other information infrastructures on which the members of both organizations depend.

II. CYBERSPACE

A. Cyberspace – new definition in Polish legislation

The requirements on the security incidents management defined by EU have reflection in Polish regulations. In August 2011 in Poland several acts introducing the definition of cyberspace went into effect (in accordance with Article 2 paragraph 1b of the Act from 29th August 2002 on martial law and the powers of the Supreme Commander of the Armed Forces as well as the Commander’s subordination to the constitutional authorities of the Republic of Poland). This act grants state institutions a special authorization in the case of arising of a threat, which may affect country’s operation as a result of cyberspace activities. According to them cyberspace is a space where processing and exchanging information created by the information and communications technology (ICT) systems takes place. There was also introduced the term Cyberspace of the Republic of Poland (CRP) as a cyberspace within the territory of the Polish state and beyond, in places where the representatives of the RP are operating.

B. Cyberspace Protection Policy of the Republic of Poland

In June 2013 the Ministry of Administration and Digitization in cooperation with the Internal Security Agency published final document titled “Cyberspace Protection Policy of the Republic of Poland” [5]. This document appoints the Governmental Computer Security Incident Response Team CERT.GOV.PL as the primary CERT in the area of government administration and the civil area. In the area of CRP security its main task is to protect organizational units of public administration of the Republic of Poland against cyber threats, with particular emphasis on attacks targeted at infrastructure, including ICT systems and networks, destruction or disruption of which could pose a threat to human life, health, national heritage and the environment to a significant extent, or cause serious property damage and disrupt the functioning of the state. In the military, this role is realized by “Departmental Centre for Security Management of ICT Networks and Services.”

The policy [5] defines the following objectives:

- Increasing the level of security of the State ICT infrastructure.
- Improving the capacity to prevent and combat threats from cyberspace.
- Reducing the impact of incidents threatening the ICT security.
- Determining the competence of entities responsible for the security of cyberspace.
- Creating and implementing a coherent system of cyberspace security management for all government administration entities and establishing guidelines in this area for non-state actors.
Creating a sustainable system of coordination and exchange of information between the entities responsible for the security of cyberspace and the cyberspace users.

Increasing awareness of the cyberspace users on the methods and safety measures in cyberspace.

From the practical point of view the question is how to attract private sector to share data about risks and incidents which they observe in their systems and networks they are responsible for? These information are usually very sensitive for each company and may be used against them resulting in the loss of reputation. In this aspect institutions collecting such sensitive data must be in a position of great trust.

C. National Critical Infrastructure Protection Programme (NCIPP)

On 26th March 2013 National Critical Infrastructure Protection Program (NCIPP) was adopted by the Council of Ministers. The goal of the NCIPP is to improve security and resilience of critical infrastructure in Poland. To reach this goal the critical infrastructure protection systems are to be built. The protection of national critical infrastructure (NCI) bases on a shared responsibility across all levels of government and critical infrastructure owners and operators. According to NCIPP “the critical infrastructure shall be understood as systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance for the security of the state and its citizens, as well as serving to ensure efficient functioning of public administration authorities, institutions and enterprises”.

In short, critical infrastructure elements are necessary for minimal and smooth operation of the economy and the state.

In Poland critical infrastructure incorporates 11 systems, which have fundamental importance for national security and for citizens as well as smart operation of public administration, institutions and business. Critical infrastructure incorporates the following systems:

- Energy, fuel and energy supply system,
- Communication system,
- Tele-information network system,
- Financial system,
- Food supply system,
- Water supply system,
- Health protection system,
- Transportation system,
- Rescue system,
- System ensuring the continuity of public administration activities,
- System of production, storing and use of chemical and radioactive substances, including pipelines for dangerous substances.

The model is hierarchical and the system level is the second in the overall hierarchy. Each system may be then composed of Sectors, Institutions, Components and Processes (see Figure 1.).

Over 500 elements have been identified as critical infrastructure in Poland, but the list is not publically available.

III. CYBERSPACE SECURITY THREATS EVALUATION SYSTEM

A. The concept

In response to 5th objective of Polish Cyberspace Protection Policy (chapter II B) the National Centre for Research and Development (NRCD) launched the project titled “Cyberspace Security Threats Evaluation System of the Republic of Poland for national security management system” - SEZBC (project No DOBR-BIO4/011/13221/2013). Military Communications Institute (as a leader of the consortium) realizes this project in cooperation with Enamor International Ltd. and PBP Enamor Ltd. The potential beneficiaries of the system appointed by NCRC are: Ministry of Administration and Digitization, Internal Security Agency, Government Centre for Security and National Security Bureau.
The aim of the project is to work out the concept of Cyberspace Security Threats Evaluation System (SEZBC) and develop its demonstrator for national security management system. Successful realization of the project will enable the improvement of cyber situational awareness and decision support for administrative units responsible for national security. It can be realized with the supply of tools for current monitoring of the situation in cyber space and cyber threats’ assessment, early warning attack prevention and decreasing its side effects. In particular this system will support decision making process in terms of declaration of the state of emergency in case of cyber-attack/incident or high risk of cyber threats’ materialization.

The main results of the project are:

- Cyber-threats’ model.
- The methods for risk analysis and threat assessment.
- The model of decision support subsystem in the case of cyber threats’ materialization.
- The criteria of threats situation assessment with the purpose of proposing the state of emergency.
- The concept of the system for information exchange between the entities responsible for the security of cyberspace and the cyberspace users in support of cyber situational awareness capability (so called KSZIWIZ).
- Realization and pilot deployment of the demonstrator enabling evaluation of cyber security threats of the Republic of Poland cyberspace.

The general SEZBC architecture is depicted in Figure 3.

### B. The architecture

SEZBC consists of three subsystems: Risk Assessment Subsystem (RAS), Situation Assessment Subsystem (SAS), and Decision Support Subsystem (DSS). SEZBC is also equipped with an interface to external systems supplying it with data about actual risk and threat levels (proprietary implementation until KSZIWIZ is finally deployed).

In the course of the project there was proposed the cyber-threat catalogue enabling uniform classification and description of the identified risks. It bases on Common Attack Pattern Enumeration and Classification (CAPEC) classification developed by Mitre [8]. It provides an openly available catalogue of attack patterns along with a comprehensive schema and classification taxonomy. It was agreed and supplemented according to Internal Security Agency recommendations. Detailed description of the threats includes the vulnerability it exploits. The attack patterns are descriptions of common methods for exploiting software providing the attacker’s perspective and guidance on ways to mitigate their effect. This formalized way of attack description brings value for architectural risk analysis and guidance for the security architecture. Hierarchical CAPEC representation helps to navigate through the list and find a specific attack pattern or to show the relationships amongst different patterns. The threats identified and classified in the catalogue include links to Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE) databases.

Figure 2. shows potential data sources for SEZBC. System is ready to receive data from KSZIWIZ, implemented currently as a proxy between SEZBC and other data source elements. KSZIWIZ in fact will be a separate autonomous system. Although its implementation has not been decided yet, its concept was proposed in the project. As data source elements there are proposed: public administration (all levels), critical infrastructure operators, business sector and individual cyberspace users.

The key requirement for the proper SEZBC operation and its ability to present actual situation is that reliable and up-to-date information from data source elements feed particular components of the system.
C. Risk Assessment Subsystem (RAS),

Risk Assessment Subsystem is the most important element of SEZBC. It employs individual risk assessment algorithm taking into account potential threats, possible effects resulting from threat materialization and security mechanisms used for attack counteraction. RAS takes into account mutual relationships between elements of the monitored infrastructure (Relationships model). These relationships result from hierarchical (see Figure 1.) and non-hierarchical connections between the elements (e.g. vulnerability of the process influences the risk to a component; unavailability of the critical process may cause unavailability of the whole component, etc.). The Relationships Model (RM) has a form of a graph where nodes are infrastructure elements and arcs describe the relationship (influence of one element on another) (see Figure 5). Each arc is characterized by direction and weight describing the strength of the influence.

The model is very important in a global approach to risk assessment for the purpose of cyber threat monitoring for the Republic of Poland. Without it this would be impossible to verify and assess the level of cyber security risk on the country level.

The results of risk assessment algorithm are the risk values calculated for each node and presented on a graph or scorecard. In this way decision makers are aware of actual risk propagation values, which is especially important for nodes having high risk level, where reaction is necessary. This reaction should minimize risk propagation effects.

D. Situation Assessment Subsystem (SAS)

Situation Assessment Subsystem implements situation assessment algorithm, which bases on predefined decision criteria. These criteria derive from the Act of 21 June 2002 on the state of emergency, where 27 criteria for emergency state declaration are defined. They are grouped into 3 categories: state of emergency, state of natural disaster or martial law criteria. If side effects of the attack (its results in real world) influence in majority one category (e.g. state of emergency) then the declaration should concern this state.

SAS takes into account results of RAS calculation derived from actual identified incidents and attacks as well as effects of a real cyber-attack. The effects of cyber-attack in real life are evaluated by a person responsible for attack/incident notification in the range from 0 (lack of impact) to 10 (full impact). SAS produces recommendation for the decision makers of which state should be declared in a given situation (if any). The quality of this recommendation is strongly dependent on the input information quality (reliability of the relationships model and its parameters, precision of the systems’ vulnerability level assessment and potential threats, and effects assessment in a real life).

E. Decision Support Subsystem (DSS)

Decision Support Subsystem provides visualisation of the results of RAS and SAS in the following ways:

- graph view
- tree view
- decision matrix
- detailed report.

DSS enables to recommend possible reactions’ for actual situation (on the country level) and simulate reaction scenarios. Simulation may comprise also of incident/attack escalation scenarios and their influence on situation progress in the area of risk propagation or recommended state of emergency.
IV. CONCLUSIONS

In order for the process of cyber security assessment on the national level to be successful it is necessary to provide solutions for all requirements presented in chapter II B, especially “Creating a sustainable system of coordination and exchange of information between the entities responsible for the security of cyberspace and the cyberspace users”. This makes the critical infrastructure elements’ ICT systems’ administrators evaluate potential threats to their systems, secure them properly, deploy cyber-attacks’ detection systems and share information about the detected incidents. Proposed Cyberspace Security Threats Evaluation System enables risk assessment on the national level where infrastructure elements’ relationships model is used. However credibility of information delivered by SEZBC depends on the supplying data sources, and accuracy of relationships model describing existing critical infrastructure elements forming the most important element of the cyberspace of Poland. Consequently, proper adjustment of the interdependencies among the elements of the model will ensure accurate propagation of the risk and possible effects of cyber-attacks which, in effect, will result in a proper state of emergency recommendation. That is why a thorough analysis of the vulnerabilities of the existing infrastructure elements as well as the influence of one system into another (e.g. power supply to health care) is necessary in order to fine-tune SEZBC and allow the right level of its sensitivity.

In should be noted that SEZBC is unique because is approaches the assessment of risk to the materialization of attacks and exploitation of vulnerabilities in ICT systems not only locally, but on the national basis. It is trying to trace incoming events in order to assess the situation in case of a global or massed attack on different branches of economy. It looks from another perspective on the cyber defense and risk assessment than security teams of particular companies. Moreover it is trying to assess possible effect of malicious activities in real life.

Cyber situational awareness picture created in SEZBC will support administrative units responsible for national security. In the near future SEZBC will be verified by prospective users and then hopefully deployed in target localization.

REFERENCES