Cyberspace Security Threats Evaluation System of the Republic of Poland

Joanna Śliwa, Przemysław Bereziński, Rafał Piotrowski
Ul. Warszawska 22A
05-130 Zegrze
POLAND

{j.sliwa, p.berezinski, r.piotrowski}@wil.waw.pl

ABSTRACT

Critical infrastructure of each country spans every domain of the economy and people's lives. One of the dimensions of the critical infrastructure is cyber domain, which is getting more and more important in modern societies. The level of dependency of the physical infrastructure on the virtual world is so big that cyber attacks can be as harmful as conventional attacks. Cyber domain is one of the most important elements influencing the operational state of critical infrastructure elements and, when not protected well, can jeopardize continuity of the country's core business. It is therefore of the highest importance to identify the elements that the country depends on and prepare all organizational and technical means to lower the risk that the threats may materialize. The article presents the idea, architecture and proof-of-concept implementation of Cyberspace Security Threats Evaluation System of the Republic of Poland (CyberEva) for national security management. There has been described its role in the area of cyberspace situational awareness at a national level.

1.0 INTRODUCTION

At the last NATO Summit organized in Warsaw, 2016, the alliance has officially recognised cyberspace as a military operational domain. This means that the NATO can respond with conventional weapons in case of a severe cyber attack, for instance a cyber attack against the critical infrastructure. Offensive cyber operations targeted at one of the NATO states can have real world consequence. Therefore it is essential to improve the awareness of the allied nations of the threats resulting from the cyber domain and their potential impact.

The EU has also recognized the need for cyber situational awareness (SA) and responded with policy and legislation proposals in the form of directives, plans and strategies [1][2][3] enforcing continuous monitoring of the national cyberspace that may be subject of cyber attacks. The key cyberspace players like banking, energy supply, transport, Internet services as well as public administration should report incidents (identify, assess and manage the risks) to the national network and information security (NIS) competent authorities to enable common cyber situational awareness for decision makers.

Based on the European Union (EU) recommendations, national directives, acts, and programs have been incorporated by the Member States (e.g. in Poland [4][5]). They assume that the governments have a significant role in assuring a safe cyberspace, but since major parts of the cyberspace are owned and operated by the private sector, cooperation between both sides is necessary. One of the steps towards the improvement of the cyber situational awareness on the national level in Poland was establishing of the project titled Cyberspace Security Threats Evaluation System of the Republic of Poland for national security management (aka CyberEva). The article presents the background, architecture and proof-of-concept implementation of CyberEva together with its role in the area of cyberspace situational awareness and decision making process at a national level. The role of CyberEva is commented both from the point of view of the requirements and regulations of the European Union as well as the Republic of Poland.

2.0 CYBERSPACE – REQUIREMENTS AND REGULATIONS

2.1 Cyberspace – new definition in Polish legislation

The requirements on the security incidents management defined by the EU have reflection in Polish regulations. The cyberspace definition has been introduced in Poland in August 2011 by several legal acts. According to these acts cyberspace is a space where processing and exchange of information created by the information and communications technology (ICT) systems takes place. This definition has been further detailed to describe 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. These acts grant state institutions a special privileges in the case of arising of a threat, which may affect country's operation as a result of cyberspace activities.

2.2 Cyberspace Protection Policy of the Republic of Poland

In June 2013 the Ministry of Administration and Digitization in cooperation with the Internal Security Agency released the document titled "Cyberspace Protection Policy of the Republic of Poland"[4]. The policy 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.

These overarching objectives encompass organizational activities that must be supported by technical solutions. They require the possibility to perform continuous cyberspace security management on the level of the government administration and coordinate the response activities that would minimize the risk of harmful situations on the national level. The security management process must however be started on the level on the ICT infrastructure elements (very often – private companies) that are obliged to report up to the government administration about the identified threats. 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? This information is usually very sensitive for each company and may be used against them resulting in e.g. the loss of reputation. In this aspect institution collecting such sensitive data must be in a position of a great trust.

2.3 National Critical Infrastructure Protection Programme (NCIPP)

The detailed National Critical Infrastructure Protection Program (NCIPP) [6] was adopted by the Council of Ministers in Poland on 26th March 2013. The goal of the NCIPP is to improve security and resilience of Polish critical infrastructure. 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 the government, critical infrastructure owners and operators.

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 NCIPP defines a hierarchical model of the NCI which clearly supports the idea of the country being dependent on 11 Systems. Each System is then composed of Sectors, Institutions, Components and Processes (see Figure 2-1).

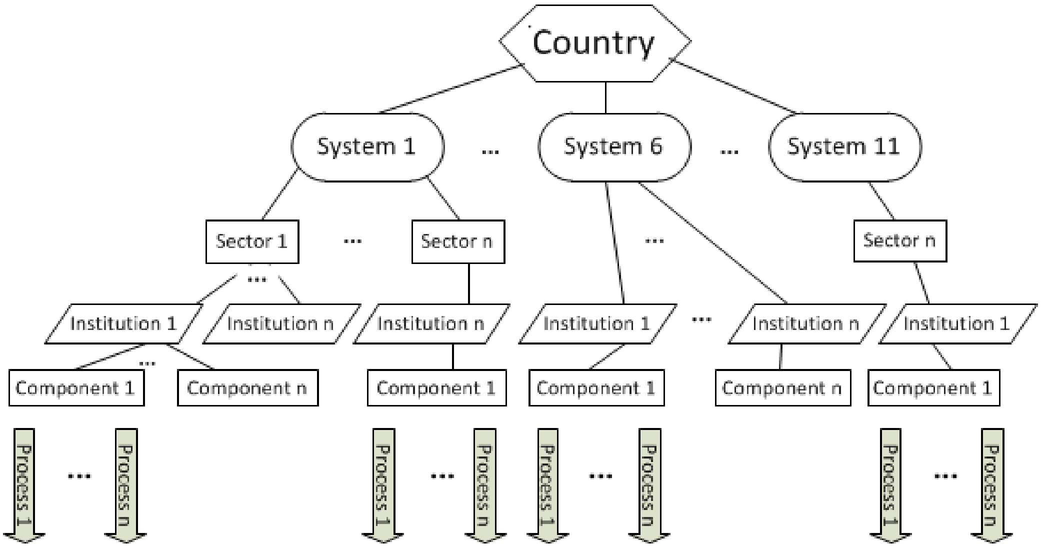


Figure 2-1: The structure of Polish critical infrastructure

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

3.0 CYBERSPACE SECURITY THREATS EVALUATION SYSTEM

In response to the 5th objective of the Cyberspace Protection Policy of the Republic of Poland 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” (project No DOBR-

BIO4/011/13221/2013) – CyberEva. CyberEva has been carried out by the consortium of 3 entities: Military Communication Institute (leader), Enamor International Ltd. and PBP Enamor Ltd. Potential beneficiaries of this project are Ministry of Digital Affairs, Internal Security Agency, Government Centre for Security and National Security Bureau.

CyberEva is a country-level cyber security evaluation system which supports decision making process. It incorporates risk assessment and risk management functions. In terms of the SA the system supports:

- Perception – CyberEva provides monitoring of the level of risk associated with potential cyber attacks (vulnerabilities and weaknesses) and observed incidents. NCI owners and operators are supposed to report periodically results of risk assessment and continuously – inform about identified incidents. Incidents' acquisition in CyberEva is supported by cyber-threat catalogue based on CAPEC – see section 3.1.
- Comprehension – On the basis of the input data CyberEva runs risk propagation algorithm that enables assessment of the risk related to possible cyber attacks on the whole critical infrastructure (see Section 3.2). Different visualization options are possible – see section 3.4. CyberEva provides impact analysis that enables to assess the situation after a severe cyber attack (see section 3.3).
- Projection – CyberEva allows to perform what-if analysis on the copy of the model simulating potential threat escalation as well as looking for the most vulnerable elements and testing the results of different mitigation options – see section 3.3.

Successful implementation of the system will enable the improvement of cyber situational awareness and decision support for administrative units responsible for the national security.

The Cyberspace Security Threats Evaluation System consists of three subsystems: Risk Assessment Subsystem (RAS), Situation Assessment Subsystem (SAS), and Decision Support Subsystem (DSS). It is also equipped with an interface to external systems supplying it with data about actual risk and threat levels (through so called KSZiWIZ – not deployed yet) (see Figure 3-1).

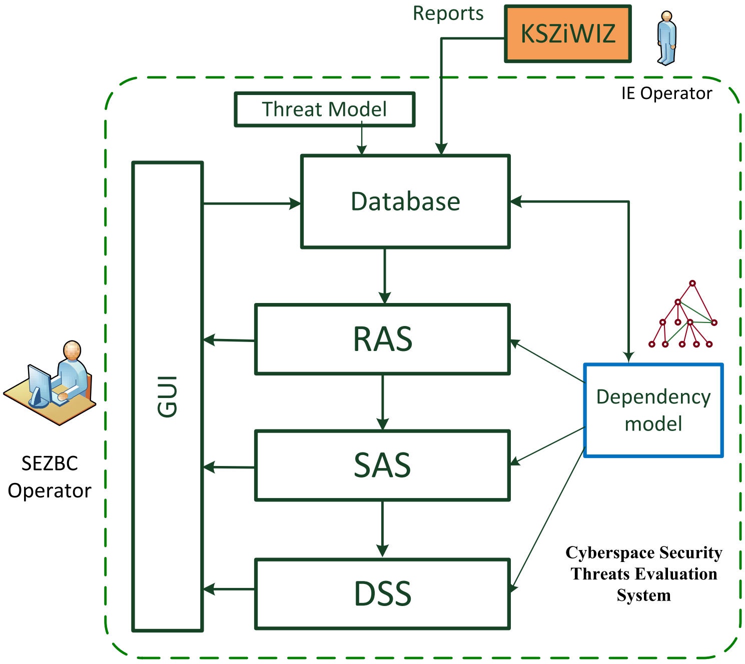
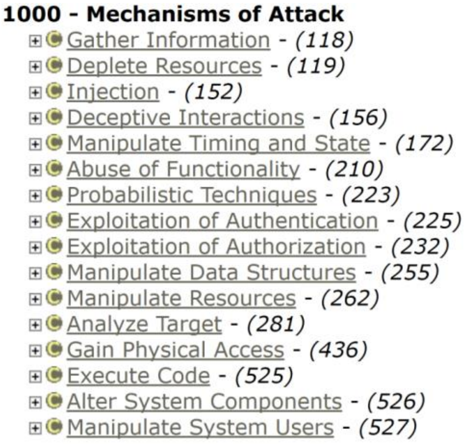


Figure 3-1: Cyberspace Security Threats Evaluation System architecture

3.1 Cyber threats model

In the course of the project there was proposed the cyber-threat model enabling uniform classification and description of the identified risks reported by administrators of the critical infrastructure (CI) elements. This model bases on Common Attack Pattern Enumeration and Classification (CAPEC) [7]. It provides an openly available catalogue of attack patterns along with a comprehensive schema and classification taxonomy, classified in an intuitive manner, along with a comprehensive schema for describing related attacks and sharing information about them. It was agreed and supplemented according to Polish 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.



1000 - Mechanisms of Attack

⊞ ● Gather Information - *(118)*
⊞ ● Deplete Resources - *(119)*
⊞ ● Injection - *(152)*
⊞ ● Deceptive Interactions - *(156)*
⊞ ● Manipulate Timing and State - *(172)*
⊞ ● Abuse of Functionality - *(210)*
⊞ ● Probabilistic Techniques - *(223)*
⊞ ● Exploitation of Authentication - *(225)*
⊞ ● Exploitation of Authorization - *(232)*
⊞ ● Manipulate Data Structures - *(255)*
⊞ ● Manipulate Resources - *(262)*
⊞ ● Analyze Target - *(281)*
⊞ ● Gain Physical Access - *(436)*
⊞ ● Execute Code - *(525)*
⊞ ● Alter System Components - *(526)*
⊞ ● Manipulate System Users - *(527)*

Figure 3-2: Main attack categories of CAPEC taxonomy

User interface used by CI administrators enables to create two kinds of reports:

- reports about system vulnerabilities (based on penetration testing and risk analysis – e.g. like described in [9]) and
- reports about identified incidents (materialized threats)

according to CAPEC classification that are input data to the CyberEva. The level of granularity in attack classification and description depends on the knowledge of CI administrator and may also include references to Common Vulnerabilities and Exposures (CVE) database. Common classification of attacks enables generation of statistics based on information delivered in attack reports (e.g. most often used vulnerabilities, types of attack etc.).

3.2 The method for risk analysis and threat assessment

CyberEva incorporates country-level risk assessment and risk management functions together with a support of decision making process. Risk Assessment Subsystem (RAS) is one of the most important elements of CyberEva. It employs an algorithm which takes into account system vulnerabilities (potential threats, possible effects resulting from threat materialization and security mechanisms used for attack counteraction) measured periodically by critical infrastructure elements' administrators, and incidents identified by security controls (reports). Constituent parts of the aggregated risk metric are propagated according to the predefined Dependency Model, which models mutual relationships between elements of the monitored infrastructure. It is similar to the tree-like structure, although non-hierarchical relations are also modelled (see. Figure 3-3).

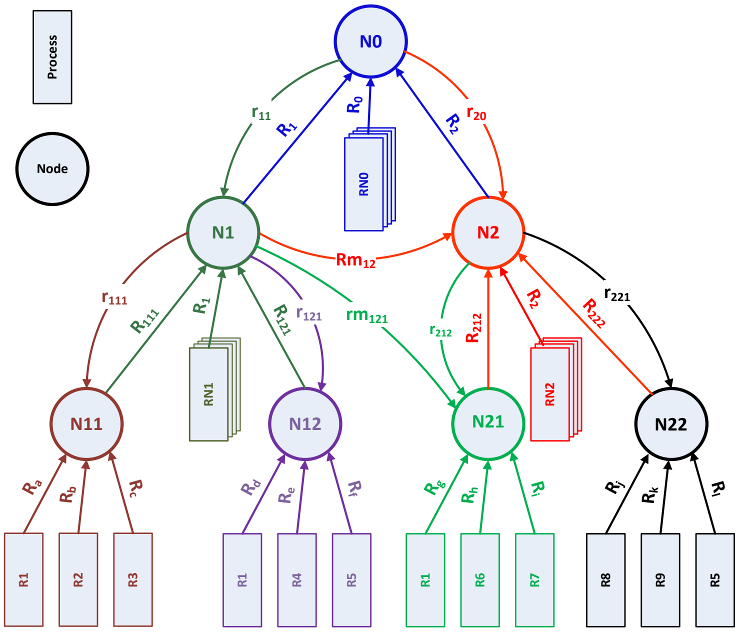


Figure 3-3: Dependency Model for risk propagation

There are six levels in the model, namely, country-level, sector-level, system-level, institution-level, component-level and process-level (accordingly to the Polish CI model presented in Figure 2-1). Particular elements resembling CI elements are represented by nodes. Relations describe an influence of one element to the other (dependencies). Each relation has its direction and weight which describes the strength of the influence (or impact). In CyberEva the model is built manually based on data coming from national institutions and private companies responsible for the maintenance of Polish critical infrastructure. Analysis performed by RAS is done bottom-up. The risk propagation mechanism is based on a weighted average (see Figure 3-4).

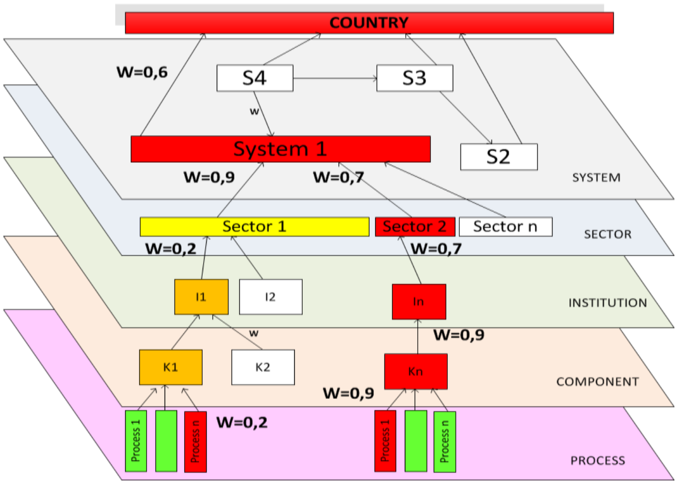


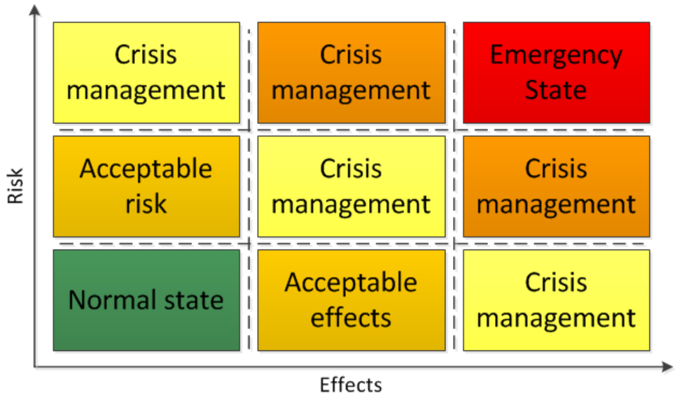
Figure 3-4: Risk propagation on the Dependency Model

3.3 Decision support in the case of cyber threats' materialization

The results of risk assessment algorithm are the risk values calculated for each node and presented on a graph-view 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 some kind of response is necessary. This response should minimize the risk propagation effects.

To support decision makers with a projection part of the situational awareness, a what-if mechanism has been employed (see DSS in Figure 3-1). It allows to simulate results of particular threat escalation as well as effectiveness of a mitigation plan. In such simulations an operator is able to manipulate the risk level of each node as well as the strength of relations in the model.

In order to support response part in a more high-level way (in case of a large-scale cyber-attack/incident or high risk of cyber threats' materialization) the Situation Assessment Subsystem (SAS) has been proposed. It implements the situation assessment algorithm, which bases on the predefined 27 Key Indicators derived from the Act of 21 June 2002 on the state of emergency. The Key Indicators for a high-level reaction are grouped into 3 categories: state of emergency, state of natural disaster or martial law criteria. For each group a separate analysis is performed which assesses the effects of the attack (its results in the real world). The dominance of the Key Indicators from one group and passing a predefined threshold allows to recommend introduction of particular state of emergency.



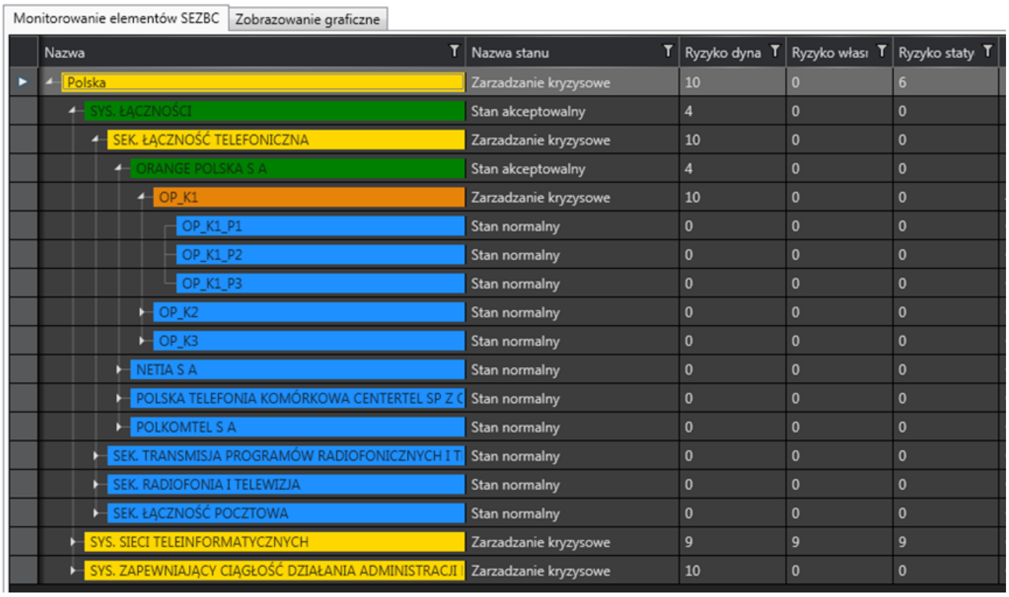
Crisis management	Crisis management	Emergency State
Acceptable risk	Crisis management	Crisis management
Normal state	Acceptable effects	Crisis management

Figure 3-5: Situation assessment decision matrix

3.4 User – facing visualization and presentation of results

A great challenge in building GUI and visualisation of the actual situation in national cyberspace was to select the most intuitive and clear way of presenting the actual risk level including information about the hierarchy of the monitored elements as well as non-hierarchical dependencies between them in such a way to be able to understand the actual root cause. Moreover, the number of the monitored nodes, which may reach even few thousands, had to be taken into account.

In the *monitoring mode* the system enables three methods of risk presentation: Tree view (see Figure 3-6), 'centric' view (see Figure 3-7) and map view (with geo-localisation of particular elements of the physical infrastructure).



Nazwa	Nazwa stanu	Ryzyko dyna	Ryzyko włası	Ryzyko staty
Polska	Zarzadzanie kryzysowe	10	0	6
SYS. ŁĄCZNOŚCI	Stan akceptowalny	4	0	0
SEK. ŁĄCZNOŚĆ TELEFONICZNA	Zarzadzanie kryzysowe	10	0	0
ORANGE POLSKA S A	Stan akceptowalny	4	0	0
OP_K1	Zarzadzanie kryzysowe	10	0	0
OP_K1_P1	Stan normalny	0	0	0
OP_K1_P2	Stan normalny	0	0	0
OP_K1_P3	Stan normalny	0	0	0
OP_K2	Stan normalny	0	0	0
OP_K3	Stan normalny	0	0	0
NETIA S A	Stan normalny	0	0	0
POLSKA TELEFONIA KOMÓRKOWA CENTERTEL SP Z (	Stan normalny	0	0	0
POLKOMTEL S A	Stan normalny	0	0	0
SEK. TRANSMISJA PROGRAMÓW RADIOFONICZNYCH I T	Stan normalny	0	0	0
SEK. RADIOFONIA I TELEWIZJA	Stan normalny	0	0	0
SEK. ŁĄCZNOŚĆ POCZTOWA	Stan normalny	0	0	0
SYS. SIECI TELEINFORMATYCZNYCH	Zarzadzanie kryzysowe	9	9	9
SYS. ZAPEWNIAJĄCY CIĄGŁOŚĆ DZIAŁANIA ADMINISTRACJI	Zarzadzanie kryzysowe	10	0	0

Figure 3-6: Monitoring mode – Tree view

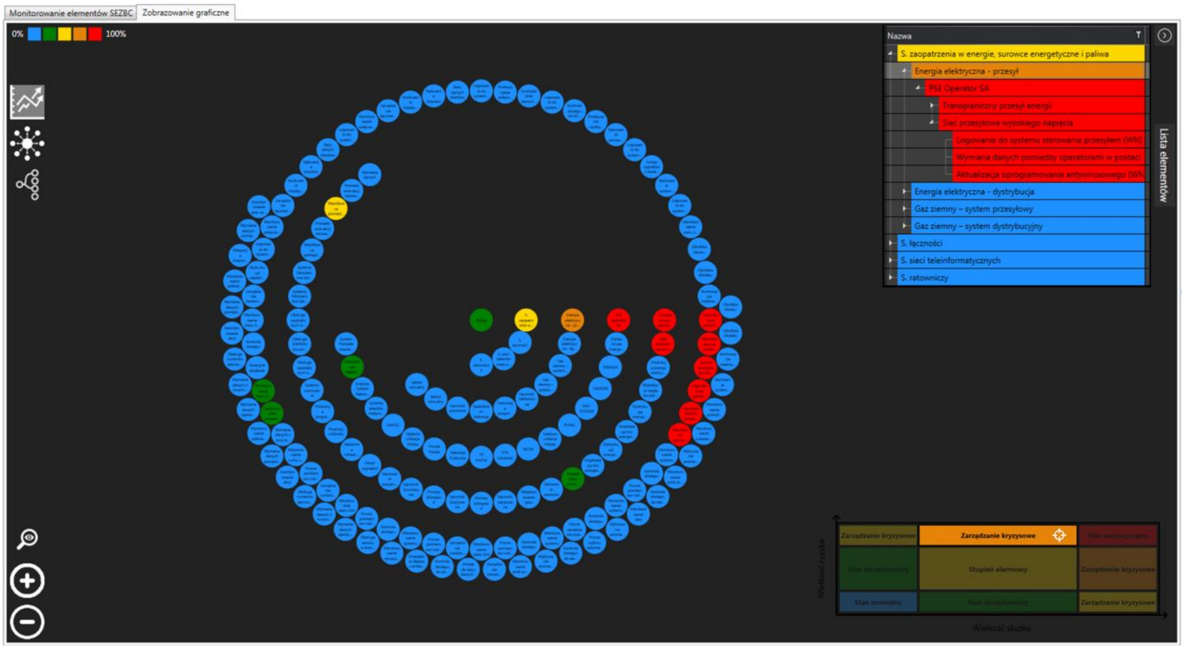
The Tree view presents hierarchical list of the monitored critical infrastructure (following the System – Sector – Institution – Component structure, see Figure 2-1) and detailed information about the risk (scale: 0 to 10) associated with particular node on each level of hierarchy. Three values of risk can be visualized:

- risk resulting from internal vulnerabilities of the node (own risk),
- propagated risk resulting from internal vulnerabilities of the dependent nodes (static risk),
- cumulative value of risk being a sum of:
  - own risk (risk from internal vulnerabilities of the node),
  - static risk (risk from vulnerabilities propagated from dependent nodes),
  - risk resulting from incidents identified in the node and propagated from dependent nodes.

Each element’s colour indicates simply the actual level of cumulative risk for the node. The thresholds for the risk level, that are then indicated by colours, are configurable and may be changed by the user.

In our approach the risk is propagated according to the in the risk Dependency Model (Figure 3-3). The Tree view does not present non-hierarchical dependencies defined in this model, but enables to ‘drill down’ investigation what is the reason of high risk level in the specified/particular system or sector. Moreover, it is possible to filter the elements in the tree view according to the rules defined by the user (e.g. show elements having risk higher than 5).

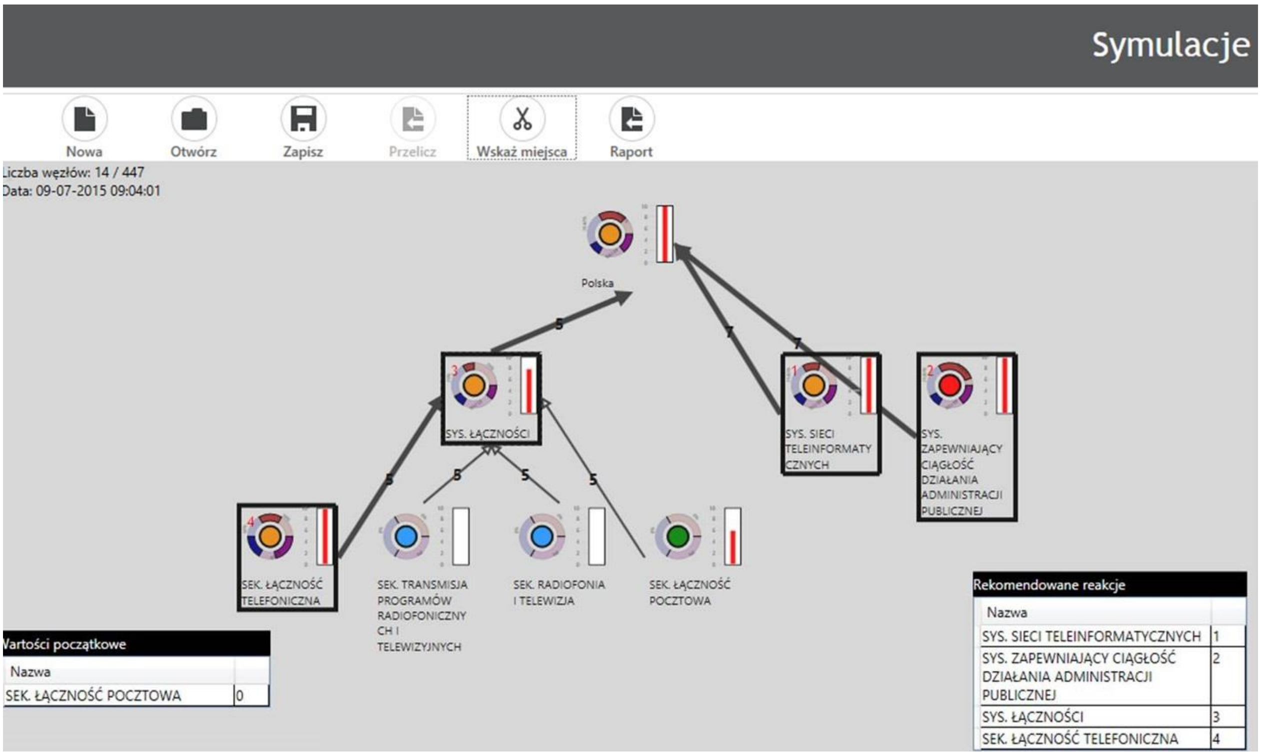
The Centric view (see Figure 3-7) enables visualization of all elements which are monitored starting from the top Level (country) visualized in the centre, to the lowest level (Processes) – external circle. It also shows non-hierarchical dependencies between elements, which may have crucial impact on risk propagation process.



Nazwa
- S. zaopatrzenia w energie, surowce energetyczne i paliwa
  - Energia elektryczna - przesył
    - PSE Operator SA
      - Transgraniczny przesył energii
      - Siec przesyłowa wysokiego napięcia
        - Logowanie do systemu sterowania przesyłem (WN)
        - Wymiana danych pomiedzy operatorami w postaci
        - Aktualizacja oprogramowania antywirusowego (WN
  - Energia elektryczna - dystrybucja
  - Gaz ziemny – system przesyłowy
  - Gaz ziemny – system dystrybucyjny
- S. łączności
- S. sieci teleinformatycznych
- S. ratowniczy

Figure 3-7: Monitoring mode – Centric view

Depending on the user access control rights/credentials CyberEva may present only selected part of the monitored infrastructure which is in their area of interest. The authorization mechanism provides the possibility to grant access to particular part of the model and particular action to be performed on it (similarly to [8]).


Symulacje
Nowa
Otwórz
Zapisz
Przelicz
Wskaż miejsca
Raport
Polska
SYS. ŁĄCZNOŚCI
SYS. SIECI TELEINFORMATYCZNYCH
SYS. ZAPEWNIAJĄCY CIĄGŁOŚĆ DZIAŁANIA ADMINISTRACJI PUBLICZNEJ
SEK. ŁĄCZNOŚĆ TELEFONICZNA
SEK. TRANSMISJA PROGRAMÓW RADIOFONICZNYCH I TELEWIZYJNYCH
SEK. RADIOFONIA I TELEWIZJA
SEK. ŁĄCZNOŚĆ POCZTOWA
5
7
7
5
5
5
5
1
2
3
4

Liczba węzłów: 14 / 447
Data: 09-07-2015 09:04:01

Wartości początkowe

Nazwa	
SEK. ŁĄCZNOŚĆ POCZTOWA	0

Rekomendowane reakcje

Nazwa	
SYS. SIECI TELEINFORMATYCZNYCH	1
SYS. ZAPEWNIAJĄCY CIĄGŁOŚĆ DZIAŁANIA ADMINISTRACJI PUBLICZNEJ	2
SYS. ŁĄCZNOŚCI	3
SEK. ŁĄCZNOŚĆ TELEFONICZNA	4

Figure 3-8: Simulation mode – what – if analysis

The *Simulation mode* (see Figure 3-8) in CyberEva enables to create a copy of the model and to search for recommendations what should be done to minimize risk propagated to higher levels of the NCI. The system identifies nodes which had the greatest influence on the risk reflected on the country level. It marks them using bold lines and prioritizes with priority index (marked in red). The whole critical path is also underlined. Analysis of the possible actions on the country level can result in high – level reactions (e.g. changing the weight of relationship between connected elements or internal risk reduction).

The user working with the *Simulation mode* may change weights of dependencies between particular nodes of the model or reduce internal risks in selected elements and see how the changes are reflected in risk propagation. This way the *Simulation mode* enables modelling of various scenarios, including escalation of threats, which may be necessary in validation of the Dependency Model.

4.0 CONCLUSIONS

Situational awareness in the area of cyber threats targeted at the critical infrastructure is crucial for the security of each country. Given the fact that severe cyber attack can be seen as an offensive act of aggression and result in conventional military response, it is necessary to create mechanisms and procedures to monitor the cyberspace and understand the level of risk related to the possibility of cyber attacks appearance and their possible impact on the country’s operation.

The Cyberspace Security Threats Evaluation System (CyberEva) supports risk assessment on the national level providing the first level of situational awareness for decision makers. However credibility of information delivered by CyberEva depends on the supplying data sources and accuracy of the Dependency Model describing existing critical infrastructure elements. Consequently, only proper adjustment of the dependencies among the nodes 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 dependency of one system on another (e.g. heath care on power supply) is necessary in order to fine-tune CyberEva and allow the right level of its sensitivity.

It should be noted that CyberEva is unique because it 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 tries 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 different perspective on the cyber defense and risk assessment than security teams of particular companies/institutions. Moreover, CyberEva is trying to assess possible impact of malicious activities in real life.

Perception, comprehension and projection provided by CyberEva will support administrative units responsible for the national security. In the near future CyberEva will be verified by prospective users and then hopefully deployed in target localization.

REFERENCES

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL Brussels, 7.2.2013

[2] EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive, Brussels, 7 February 2013

[3] Proposal for a 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, COM(2013) 48 final - 7/2/2013 - EN ; http://ec.europa.eu/maritimeaffairs/policy/maritime_spatial_planning/documents/swd_2013_65_en.pdf

[4] Cyberspace Protection Policy of the Republic of Poland, Warsaw, 25 June 2013,

[5] National Critical Infrastructure Protection Programme, 2013, http://rcb.gov.pl.

[6] Description of Project “Cyberspace Security Threats Evaluation System of the Republic of Poland for national security management”, project No DOBR-BIO4/011/13221/2013,

[7] Common Attack Pattern Enumeration and Classification (CAPEC), Mitre Corporation, https://capec.mitre.org/

[8] J. Sliwa, B. Jasiul, T. Podlasek and R. Matyszkiel, "Security Services Efficiency in Disadvantaged Networks," *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, Glasgow, Scotland, 2015, pp. 1-5, doi: 10.1109/VTCSpring.2015.7146075

[9] M. Szpyrka, B. Jasiul, K. Wrona, F. Dziedzic, "Telecommunications Networks Risk Assessment with Bayesian Networks", Computer Information Systems and Industrial Management: 12th IFIP TC8 International Conference, CISIM 2013, Krakow, Poland, September 25-27, 2013, pp. 277-288, doi: 10.1007/978-3-642-40925-7_26