Security Education as a Fundamental Pillar of Critical Infrastructure Protection and Resilience

HROMADA MARTIN, LUKAS LUDEK

***Abstract*:** The increasing society dependence on the technologies also increases the society dependence on the critical infrastructure as the basis of ensuring and maintaining the society functional continuity. Logical consequence of this fact is the security and safety measures/standards development in relation to their potential to minimize the impacts of identified risk. For the fulfillment of that argument, however, it is necessary to constitute the security education that would provide a basis for security liaison officer education whose skills and knowledge would become fundamental for the operator security plan elaboration. Article therefore defines the challenges and objectives that should be achieved by security education and optimal structure of security education in relation to critical infrastructure protection and resilience. Security education structure will be based on the critical infrastructure resilience evaluation methodology as a security research output. To better understanding of the fundamental relationships between defined parameters it will be the methodology and robustness as its part presented.

***Keywords*:** Critical infrastructure protection, Resilience, Robustness, Security Education, Operator Security Plan, Security Liaison Officer.

I. Introduction

PROTECTION of critical infrastructure is a relatively new branch of application of management functions by state. Due to the results of the analysis of security threats the technological development and society's dependence on energy, products, networks, commodities leads to formulation of the required degree of protection. Modern states solve those problems by multi-level solution. The defining of national critical infrastructure program is usually first step. The legislative pillar is cornerstone of critical infrastructure defining, its components and how to ensure its protection. The organization of critical infrastructure protection is basic part of these programs. Functionality of critical infrastructure determines the effectiveness of state security system. Functionality creates conditions for providing external and internal security measures and protection of population.

The current problem of critical infrastructure protection is interdependence between critical infrastructure sectors. Internal dependence occurs at several levels, mainly physic, cyber and organization levels. It arises due to financial flows, energy flows, information flows. Countries and people need a systematic solution. This increased the importance of security education development, in connection with the optimization of critical infrastructure protection and resilience.[1]

A. Terminology definition

'*critical infrastructure'* means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions,

'*European critical infrastructure*' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure,

'*risks analysis*' means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure,

'*sensitive critical infrastructure protection related information*' means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations,

'*protection*' means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralize a threat, risk or vulnerability,

'*owners/operators of ECIs*' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive,[2]

'*resilience*' is understood „The ability of systems, infrastructures, government entities, businesses, and society to adapt to adverse events, to minimize the impact of such events

This work was supported by the Ministry of Interior of the Czech Republic under the Research Project No. VG20112014067 and by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

M. Hromada. He is with Faculty of applied informatics, Tomas Bata University in Zlin, Czech Republic. (e-mail: hromada@fai.utb.cz).

L. Lukas. Author was with University of Defence in Brno, Czech Republic. He is now associate professor with Faculty of applied informatics, Tomas Bata University in Zlin, Czech Republic. (corresponding author to provide phone: +420-576035248, e-mail: lukas@fai.utb.cz).

(keeping the system running), and also to anticipate future adverse events and be able to prevent them.[3]

II. Security Education Perspectives

Above mentioned subject should fulfill the basic knowledge and training requirements to Security Liaison Officers. The next perspective should be seen through the facilitation the process of creating relevant documentation by owners and operators of critical infrastructure. The following can therefore be seen as a perspective of security education and identification of the areas of critical infrastructure protection and resilience, which should be covered by this education process.

A. Security Liaison Officers

The Security Liaison Officer shall function as the point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority.

Each Member State shall assess whether each designated ECI located on its territory possesses an OSP or has in place equivalent measures addressing the issues identified in Annex II of the Council Directive 2008/114/ES (European Critical Infrastructure OSP PROCEDURE). If a Member State finds that such an OSP or equivalent exists and is updated regularly, no further implementation action shall be necessary.

B. European Critical Infrastructure OSP PROCEDURE

The operator security plan ('OSP') procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an ECI OSP procedure is set out in Annex II.

The OSP will identify critical infrastructure assets and which security solutions exist or are being implemented for their protection. The ECI OSP procedure will cover at least:

a) identification of important assets;
b) conducting a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact; and
c) identification, selection and prioritisation of counter-measures and procedures with a distinction between:
   a. permanent security measures, which identify indispensable security investments and means which are relevant to be employed at all times. This heading will include information concerning general measures such as technical measures (including installation of detection, access control, protection and prevention means); organisational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems,

graduated security measures, which can be activated according to varying risk and threat levels.[4]

III. Critical Infrastructure Resilience Evaluation Methodology

As it was discussed in the introduction, the status of security education is an essential aspect of increasing the level of protection and resilience of critical infrastructure. In the context of this argument, the methodology for resilience evaluation was established as the lynchpin of control activity, where the methodology, its structure and demands for control authority creates new challenges on the educational fields in relation to the protection and resilience of critical infrastructure. To understand the process of resilience evaluation it will the above mentioned methodology be presented.

Critical infrastructure elements and elements system resilience evaluation respects the principles of critical infrastructure resilience evaluation. Depending on the purpose, the evaluation should be done as an external or internal resilience of critical infrastructure element or elements. It should be based on knowledge of nature and basic functional, technological and spatial attributes of the evaluated critical infrastructure elements. The self-evaluation of the critical infrastructure element resilience should be based on risk analysis and countermeasures quality extent assessment for shared risks effects elimination or degraded function restoration. In the external evaluation, the evaluator prepares and independent risk analysis, in the internal evaluation, the results of the risk analysis, prepared in the critical infrastructure entities crisis preparedness plan, may be used. Furthermore, the described methodology is destined for an external critical infrastructure elements resilience evaluation.

Critical infrastructure element resilience evaluation includes the following phases:

a) System analysis of evaluated critical infrastructure element,
b) Analysis and Risk assessment,
c) Determination of evaluated areas Of security/safety,
d) Determination of the attributes and indicators calculation,
e) Calculation of critical infrastructure element resilience,
f) Evaluation of critical infrastructure element resilience.

A. System analysis of evaluated critical infrastructure element

System analysis of evaluated critical infrastructure element generally identifies:

a) Main/objective function (output, product, service) of evaluated object (s)/CI elements,
b) procedural or functional architecture, presenting an overview of key processes that ensure the element target function
c) topological structure of the evaluated object, definition of the basic structure, elements and relations, including maintaining topology, if the CI element is part of network structure, the evaluation is done

separately ,

d) technological architecture of CI element - the list of technologies that are in the CI element used to its target function secure,
e) production correlation and time-sensitivity – level of lacking production
f) number of employees.

B. Analysis and Risk assessment

The output of the analysis and risk assessment process is a list of risks that have the highest potential for degradation of the target function. These risks are essential for the process of determining the areas of security and critical infrastructure resilience evaluation in terms of risks coefficient expression.

The position of the two-phase process of analysis and risk assessment is important both in terms of determining the values of the risk coefficients, as well as other robustness evaluation process.

Two phases approach itself is based on the needs risk prioritization in relation to their potential impact to operational continuity of critical infrastructure in the perspective presence of domino effects or synergistic effects.

C. Determination of evaluated areas of security/safety

The definition and specification of the areas of security is a crucial stage in the critical infrastructure resilience evaluation process and it should be based primarily on the analysis and prioritization of risks. Set of identified risks and the need for their reduction or mitigation determines the specific security areas. This method objectively identifies the areas of security, where the final specifications and the definition should be made by responsible entity that requires resilience evaluation.

Based on the current state of knowledge, following security/safety areas were for further resilience evaluation process selected:

a) Physical security,
b) Information Security
c) Administrative Security
d) Personnel security,
e) Fire safety
f) Health and safety at work,
g) Technologies safety, etc.

D. Determination of the attributes and indicators calculation

Securing the process of resilience evaluation is associated with a necessary expression of the parameters values involved in the structural robustness, robustness, security and preparedness. The parameters and their values affect the final value of critical infrastructure element resilience.

Consequently it is possible to calculate the value of the basic resilience indicators. The basic indicators expressing the significant resilience factors are:

a) The Risk value (parameter / coefficient) H_{RZ} - the potential impact of risk on the CI functionality,
b) The Correlation value (parameter / coefficient) K_{SO} – expressing dependences and links between the different areas of CI,
c) The Structural robustness (parameter / coefficient) K_{SR} – elements ability to withstand the effects of negative factors due its structure, system performance and characteristics of technology,
d) The Security robustness (parameter / coefficient) K_{RO} – referring to the status and level of security measures ensuring the mitigation of risk exposure,
e) The preparedness value (parameter / coefficient) K_{PR} – ability to provide an element response to an exceptional event / incident and restore the CI element required functions.

Robustness coefficient evaluation

The robustness expressed by $K_{RO,}$ represents strength, durability, resistance to deformation. It is the ability to resist and withstand the effects of negative events without significant function degradation. In this methodology is the element robustness divided into structural robustness and security robustness. These two areas respectively their expression formulates a relationship for the evaluation of the system robustness:

$$K_{RO} = K_{RZ} * K_{SR} \quad (1)$$

where:

K_{RO} - is the robustness coefficient,

K_{RZ} - is the structural robustness coefficient,

K_{SR} - is the security robustness coefficient.

Security robustness coefficient evaluation

Evaluation of security robustness coefficient K_{RZ} in relation to the evaluation of resilience is seen in a wider context. Security robustness coefficient expresses the extent and quality of the critical infrastructure element security in connection with identified risks. Individual measures according to the nature and effect are grouped into specific areas of security. It is an area of physical security, information security, administrative security, personnel security, etc. For each type of critical infrastructure elements should the responsible entity recommend the different security areas. The security robustness coefficient basically consists from:

- level of physical security M_{FB} - which is an expression of the extent and quality of the measures taken in the critical infrastructure element physical security,
- level of information security M_{IB} - which is an expression of the extent and quality of the measures taken in the critical infrastructure element information security,
- level of administrative security M_{AB} - which is an expression of the extent and quality of the measures taken under the critical infrastructure element administrative security,
- level of personal security M_{PB} - which is an expression of the extent and quality of the measures taken in the critical infrastructure element personnel security.

Importance (weight) of individual security areas respectively components of the security robustness is as individual as the status and importance of robustness and preparedness in relation to the selected critical infrastructure element resilience. Importance determination respectively the weights determination of security robustness individual components is realized using pairwise comparison (Fuller triangle).

In the case of any two security robustness components comparison of the n components, we select all combination of two elements of n, where the total number of combination is equal to:

$$K = \frac{n * (n-1) * (n-2)!}{2!\,(n-2)!} = \frac{n * (n-1)}{2} \quad (2)$$

Figure 1: Example of Fuller triangle

Mark the count of circled 1 by m_i symbol, where the weights may be calculated by following equation:

$$V_i = \frac{m_i}{\sum_{i=1}^{k} m_i} = \frac{m_i}{K} \quad (3)$$

Mathematical expressions of weights determine the safety respectively security areas that are relevant for the evaluation process which influence the final value of the resilience (in the case that the weight of administrative security is 0, it is clear that we would not evaluate the measures provided by this security area).

For the process of security robustness evaluation process has been formulated following relationship:

$$K_{RZ} = M_{FB} * V_{FB} + M_{IB} * V_{IB} + M_{AB} * V_{AB} + M_{PB} * V_{PB} \quad (4)$$

where:

V_{FB} - is the weight of physical security,

V_{IB} - is the weight of information security,

V_{AB} - is the weight of administrative security,

V_{PB} - is the weight of personal security,

M_{FB} - concerns the determination of the quality of the physical security measures,

M_{IB} - concerns the determination of the quality of the information security measures,

M_{AB} - concerns the determination of the quality of the administrative security measures,

M_{PB} - concerns the determination of the quality of the personal security measures.

Structural robustness coefficient evaluation

Resilience of critical infrastructure element is the ability to ensure functionality in terms of external and internal factors effects. Different resilience value should have a point featured element (building, room), another surface element (agricultural fields, complex reservoirs), another line element (pipeline, pipeline) and another element with the network nature (Radiation Monitoring Network). The level of element resilience is related to the security measures, but also reflected the systemic, structural and technological characteristics. Critical infrastructure element with network character structure will be able to withstand the effects of natural disasters without serious function degradation, if it will be able in terms of its structure, redirect the flow of technology and alternative way to bridge the shortfall of transit components. To determine the degree of influence is necessary to reflected those characteristics that are part of normal operation and are immediately available to use and do not require extensive activation of forces and means. These characteristics determine the structural robustness of critical infrastructure element.

In the process of assessing structural robustness it is possible to use so-called the macro-view approach. Widely distributed critical infrastructure element deployed on a large territory (region, country) is more vulnerable than a point element (Department Building). The probability that it will deal with the effects of natural disasters is higher, also has given his blanket deployment of more vulnerabilities.

Structural robustness of critical infrastructure element expresses the ability to withstand the effects of negative factors due to its structure, system and technology properties. It also includes the ability to withstand the effects of negative factors without function degradation, potential of deploying the

redundant subsystems to isolate the failure (to prevent their spread) and flexibility to redirect service. In relation to this fact, the critical infrastructure elements have the character of the building, technological unit, staffed technical system, processes, systems or services, the assessment of structural robustness should be determined by a multi-criteria evaluation.

The evaluation process is represented by scoring of the main attributes that determine the magnitude of the structural robustness. The structural robustness coefficient K_{SR} varies in the interval 0.8 – 1. Structural robustness coefficient K_{SR} expresses the influence of topological structure, complexity and other properties or characteristics of the deterioration of protective measures effect of evaluated critical infrastructure element. If the coefficient of structural robustness K_{SR} is lower, the more attention should be paid to emergency preparedness. Main attributes by which the evaluation of the structural robustness should be performed include:

- type of topological structure,
- complexity,
- number of key technologies
- flexibility
- redundancy
- perimeter protection.

The values of topology index I_t, complexity index I_s, key technologies index I_{kt}, flexibility index I_f, redundancy index I_r and perimeter protection index I_{po} are listed in following table.

Type of topology	point		area			line		network
	> 1000 m2	< 1000 m2	> 1 km2	1 – 10 km2	< 10 km2	> 10 km	< 10 km	method
	●	●	●	●	●	●	●	●
Complexity	simple (under 10 employees)			medium (10-100 employees)			complex (over 100 employees)	
	●			●			●	
Number of core technologies	0-2 of technology			3-4 of technology			5 or more technologies	
	●			●			●	
Flexibility	no					yes		
	●					●		
Redundancy	no					yes		
	●					●		
Perimetric protection	unprotected			local			complete	
	●			●			●	

Figure 2: Decision-making table of topology index evaluation

The resulting coefficient of structural robustness K_{SR} is calculated using a formula which respects the "Pareto rule"

$$K_{SR} = 0{,}8 + \frac{I_t + I_s + I_{kt} + I_f + I_r + I_{po}}{60} \qquad (5)$$

K_{SR} - structural robustness coefficient

Network topology index I_t evaluation

Evaluation process of structural robustness is an important reflection of element topology. Topology evaluation of point, line and area is relatively simple. The situation is different in relation to elements with network topology. Network topology acquired considerable number of forms. The difference is mainly in topological structure type, number of nodes, interconnection density, the existence of key nodes, etc. A simple network with a central node is more vulnerable than large networks without a central node. In case of central node disruption or destruction, providing for critical infrastructure element key processes, it will escalate to collapse of the entire network functionality, therefore, the structural robustness of such a critical infrastructure element is low. To ensure the necessary degree of resilience, it is necessary to realize a larger number of measures in order to eliminate this disruption.

Topology index evaluation I_t for network is realized by multi-criteria approach. The attributes that will be reflected in the topology index are type of topological structure, the total number of nodes, the number of key nodes and the average number of edges (connections) per node. These attributes have been chosen as the basic characteristics of the networks due important reflection in their resilience. These include the network flexibility that is an attribute rated as one of the indexes of structural robustness in the overall assessment.

On the basis of an expert assessment has the greatest weight the topology type, the number of key nodes, number of nodes and the average number of edges per node. The evaluation is realized by pointing method. The resulting value is determined by adding the points identified for each category of attributes.

Topology type reflects the typical model of interconnected nodes. The basic types of topologies include bus, star, tree and polygonal structure. The star is characterized by the existence of a central node. When the network central node collapse the network should disintegrate and critical infrastructure element stops working. For this reason, it is necessary to assess the star topological structure regressively. On the contrary, it is necessary to do progressively assessment in relation to the polygonal structure in which the failure of one node do not seriously affects the operation of the network. Topological structure index of bus type (bus) I_t is assigned by 0 points, topology (star, circle) are assigned by 4 points, 8 points are related to tree topology and topology of polygon takes value of 12 points. In some cases it is not possible to unambiguous classification of the topological structure due its different nature. The network core can be connected polygonal and peripheral parts of the network have the character of a star. In this case, it is appropriate to reflect the proportion of individual topologies.

Number of key network nodes expresses the vulnerability of networks due to the elimination of important, key nodes. A key node is considered to be one whose elimination would significantly degrade the functionality of the entire network. The key nodes are those which are central elements or major transit nodes. Regular transit node is one that is connected to the adjacent nodes at least 1.6 times on the edges than is the average number of neighbors per node. If the network has only

one key node is vulnerable and the index of key nodes I_{ku} takes the value 0, two key nodes are equal to the value of 3 points, three key nodes are equal to 6 points and 4 or more key nodes is the I_{ku} equal to 9 points. Same value has the network without any key node.

Number of nodes expresses the extent of the network. The number of network nodes is relevant for the elimination of one node reflection in the functionality of the evaluated critical infrastructure element. Network with the number of nodes to 5 are more vulnerable than the networks with number of nodes more than 50. The network range effect to its robustness is measured by the total number of nodes index I_c . For networks with the total number of nodes to 5 takes the index value of 0, for the network with the nodes number in the range of 6-15 nodes the value is 2, the network with the number of nodes in the range of 16-40 nodes I_c takes the value 4, and network with number of nodes more than 40 knots I_c has a value of 6 points.

The average number of edges (connections, links) on one node is an attribute that expresses the density of the network. Higher parameter value expresses the fact, that the network is denser and more easily ensure transmission path redirection. The attribute is also used to determine the key nodes of the network. Index of edges average number per node I_h is calculated as the arithmetic average of the number of edges (connections) for all evaluated network nodes. If the index value reaches average number of edges per node I_h values up to 1.6 of edge, is assigned an index value of 0 points. The index I_h where the average number of edges is from 1.7 to 2.2 edge is attributed to 1 point, for the index I_h where the average number of edges is from 2.3 - 3 edges is attributed to 2 points, for I_h where the average number of edges is higher 3 edges is the index value 3 points.

Selected index values I_s, I_{ku}, I_c and I_h are listed in the table. The whole value of topology index is for a network topology derived from the calculation of the network index I_b .

$$I_b = I_s + I_{ku} + I_c + I_h \quad (6)$$

Type of topology	bus ●	star / circle ●	tree ●	polygon ●
Number of core nods	1 node ●	2 nodes ●	3 nodes ●	4 nodes and more or none ●
The number of nodes	to 5 nodes ●	6 - 15 nodes ●	16 - 40 nodes ●	over 40 nodes ●
The average number of edges per node	to 1,5 edge ●	1,6 - 2,2 edges ●	2,3 - 3edges ●	more than 3 edges ●

Figure 3: Decision-making table of network topology index evaluation

Table 1: Conversion Table I_b to I_t

I_b - points	topology index I_t
0 – 7	0
8 – 15	1
16 – 22	2
23 – 30	3

Subsequent evaluation process is same and it continues to coefficient of structural robustness K_{SR} calculation.[5]

E. Calculation of critical infrastructure element resilience

Multi-criteria evaluation is the most appropriate method for critical infrastructure element and elements resilience evaluation. The method allows implementing a comprehensive evaluation of relatively independent indicators and parameters. It uses a semi-quantitative expression of the size of individual indicators. Its disadvantage is the lower level interpretation of resilience degree, but it allows to include evaluated critical infrastructure element into the corresponding range of resilience level. Evaluation result, however, does not specify how long a critical infrastructure element can withstand the influence of negative factors. The advantage is to evaluate the countermeasure quality to selected risks.

It is obvious that the multi-criteria evaluation should relate to the areas of security, which have a positive impact on the level of resilience (robustness and preparedness), including their components. Each area of security, having a positive impact on the robustness and preparedness should be assessed in relation to the established standards (criteria), for selected area through checklists. A comprehensive evaluation requires expressing the value (coefficient) of the risk and its relationship and impact to the value of resilience in relation to selected element or sector of critical infrastructure. This highlights the fact that the total value of resilience under evaluated system is the average value of resilience in relation to i-th risk. For a complex multi-criteria evaluation of selected CI element or elements resilience was established mathematical relationship:

where:
$$ODP = \frac{\sum ODi}{xi} \quad (7)$$

ODP - selected CI element resilience value
ODi - CI element resilience value in relation to selected i-th risk
xi - number of selected risks
Mathematical expression of CI elements resilience in relation to the i-th risk:

$$ODi = \frac{(1-H_{RZi})+(1-K_S)+(K_{RO}*V_{RO}+K_{PR}*V_{PR})}{3} \quad (8)$$

where:
H_{Rzi} - the value of i-th risk,
K_S - correlation parameter,
K_{RO} - robustness parameter,
V_{RO} - robustness weight,
K_{PR} - preparedness parameter,
V_{PR} - preparedness weight,
Equations $(1-H_{RZi})$ and $(1-K_S)$ reflect the fact, that risk and correlation value negatively affect the value of the critical infrastructure element resilience.
The presented facts are the basis for the final evaluation of the critical infrastructure element or group of elements resilience in the relevant sector.

F. Calculation of critical infrastructure element resilience

As already described in the preceding text, the final phase of resilience evaluation is the inclusion of the resulting values in the following table, which also verbally (qualitatively) describes the determination of the resilience level.

Table 2: Resilience evaluation table

Resilience evaluation	Value of ODP	Verbal rating	The minimum value of the robustness	The minimum value of the robustness of security	The minimum value of preparedness
Great (A)	0,8– 1	system is ready for all identified risks, none risks was neglected	0.5 as a result of the relationship $K_{RO}*V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0.5 as a result of the relationship $K_{PR}*V_{PR}$
Very good (B)	0,6 – 0,8	system is ready for all of the important identified risks	0.4 as a result of the relationship $K_{RO}*V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0.4 as a result of the relationship $K_{PR}*V_{PR}$
Good (C)	0,4 – 0,6	systém is ready for the most of important identified risks	0.3 as a result of the relationship $K_{RO}*V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0.3 as a result of the relationship $K_{PR}*V_{PR}$
Enough (D)	0,2 – 0,4	system is ready for the most of the identified risks	0.3 as a result of the relationship $K_{RO}*V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0.3 as a result of the relationship $K_{PR}*V_{PR}$
Unable to resist (E)	0 – 0,2	system is not ready for the majority (more than half) of the identified risks	0.2 as a result of the relationship $K_{RO}*V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0.2 as a result of the relationship $K_{PR}*V_{PR}$

The presented methodology is a comprehensive approach to evaluate the resilience, where various factors respectively expression and formulation of individual coefficients or relevance of the created mathematical model was verified on selected critical infrastructure element. Based on these facts, it can be stated that the application of the principles and philosophy of the risk assessment and management may be the basis for an evaluation system of critical infrastructure resilience. For practical verification of mentioned methodology we used standards, which grew out from a separate security research project in relation to the selected critical infrastructure sectors. It obvious that for an objective resilience evaluation of the selected critical infrastructure element group or sector is needed the establishment of security standards and requirements which are sectorial specific, assuming their definition and acceptance of a leading governmental authority.[6]

IV. Education Program Structure

The following text will present the basic subjects demands of an educational program, which will ultimately enable the fulfilment of the philosophy and requirements of the regulatory state administration body in relation to assessment of resilience. In connection with the structure of the resilience evaluation methodology is the assumption that the basic subjects of security will be focused on the defined areas of security. The text will describe subjects and their focus and requirements. Also it is divided to technical and management subjects.

A. Technical subjects

Systemization of the security industry

The aim of the course is to provide overview knowledge from the area of security industry, which should enable deeper study in other special courses. This course focuses on the issues of the security industry with the accent on its basic elements: Guarding services (Protection of property and persons), Transport of money, valuables and processing cash money, Control desks of centralized security, Technical security services, Private detective services, Official secrets.
The student has knowledge on the security industry in the Republic, has expertise in commercial security services and security industries, as well as to define the growth of CSI and its expansion, is able to define the different sectors and services in the SI.My review of the valuation problem of security risks, the basic operations provided guarding services, security analysis and audits. Student is well informed in the regulations and standards of classified information protection.

Mechanical barrier systems

The course introduces into the issues of mechanical preventive and protective systems used in the commercial security industry, which are approved by the Association of Czech security companies, are certified by the respective specialized institutions in the CR and are in accordance with the requirements of the EU.
The student has knowledge of basic concepts, classifications of elements of mechanical barrier systems, their basic function and use in practice. Students are able to design in MZS (MBS), mechanical protection for the shield, and the perimeter of that object. Interpret the design problem of mechanical barrier system in accordance with related technical means (I & HAS, CCTV) is able to understand the legislation and current trends characterize mechanical barriers in the EU and the world.

Technological equipment of security industry

The goal of course is to teach students the principles, construction and use of basic principles of technical equipment used to ensure the asset protection. The course is divided into two parts, first part explains the principles and properties of selected motion detectors, fire detectors and leak chemicals.

Emphasis is placed on understanding the transformation of the physical phenomenon of a security incident into the alarm signal. There is emphasized the continuity with alarm systems, fire, CPD. The second part of the course focuses on support systems for ensuring the security and physical security, such as digital cameras, camera systems, GPS receivers, GSM systems, and security X-rays systems, drugs and explosives detectors. Emphasis is placed on understanding of the operation principle of equipment and systems, their properties and use for security purposes.
Students will learn to use electronic security technology to protect of property. Student will be able to link individual elements and systems into a coherent and functional system. Student can explain how the elements and systems work. Student will be able to configure and set the operating mode of each electronic security device.

Physical Security - Electronic elements

The course provides knowledge from the area of electronic systems used for building protection in commercial security industry, especially electronic (electrical) security signal devices, fire protection signaling, closed-circuit TV systems (CCTV), attendance and access systems, electronic guard of goods and some other auxiliary guarding systems. The knowledge must enable applications, including global assessment and solution design. Part of the course is laboratory exercise and field training.
Students will learn to use electronic security technology to protect of property. Student will be able to link individual systems into a coherent and functional system. Student can explain how the systems work. Student will be able to configure and set the operating mode of each electronic security device.

Information security

Aim of the course is increasing of knowledge about value of information, it strategic purpose in knowledge community world. Students receive knowledge about risks which are dangerous for present IT systems. Students get information about realizing organization security policies with close relationships to security decomposition of information system.
Student has knowledge about security risks depending on working with information; and methods for his elimination.
Student manages to understand security structures of companies and knowledge about this structure on high level, which is necessary for active and constructive input to this structure. Student is able to use common security technologies.

Design of Security Systems

The subject is aimed at gaining knowledge about alarm systems, about the mode their project. Student will acquire knowledge about technical requirements to alarm systems and about the basic phase of projection.
Student has knowledge about technical requirements to alarm systems and about the basic phase of projection alarm systems.

Computer Viruses and Security

The aim of this subject is to introduce aspects of computer security to students like computer viruses and its classification, virus defending activities, virus generators, spam, phishing, hacking, etc.
The student has knowledge about fundamentals of information theory. The student is well informed in methods of information theory.
Electronic alarm systems and physical access systems
The purpose of the subject is to learn the students with the technology of the current card systems, which utilize magstripe, chip, RFID or wiegand cards for the purpose of the control of the physical access.
Student gains detailed knowledge about technology of magstrip, chip and RFID cards. The student will be able to work with a simple microprocessor system, which is being used for readout and handling of different card readers. The student will also learn to work with physical access system Winpack.

Modelling of Crisis Situations

The goal is to gain knowledge in area of crisis or emergency incidents management and critical infrastructure protection. Theoretical knowledge focused on the legal aspects of emergency incidents management and critical infrastructure protections are complemented by practical approaches to modelling the impact of incidents through information support.
Students acquire basic knowledge in crisis management, the present legislation, emergency response, risk analysis and critical infrastructure protection. From a practical point of view will gain knowledge in the process of security documentation elaboration and use of information support for simulating the effects of the emergency incidents.

B. Management subjects

Legal order

This is a profiling course that enhances the level of the students' legal education and knowledge of the application of individual legal standards to the area of protected social relationships. Through this knowledge the legal basis is applied to the security, legal and administration activities in the state administration, local authorities and in the private security sector - security industry. The knowledge is directed at the frequent legal areas of the Czech legal order with an accent on the constitutional, civil and family laws, business and trade laws, labor and misdemeanor laws. The topics also include specific features of public administration, state administration and internal security of the country. In connection with the European Union the course deals with the community law and its historical background, and also provides basic knowledge from the area of private security.
Students are familiar with the basic interpersonal relationships, knows the history and theory of law.

Commercial security technology

The aim of the course is to introduce the main issues of commercial security. The topics are: introduction into the protection of property and people, legal base of this protection, basics of the prevention in the protection of property and people, security hazard, security analysis (expertise), security prognosis, security project (organizational, regime, etc.); forms, methods, means, power and auxiliary power of the protection of property and people, methodology of this protection, European training module. The specialized part deals with the issues of crisis planning; situation, value and risk security analyses, issues of the transport of cash money and other valuables, etc.
The student has the knowledge about bases of commercial security technology, is well informed in security issues, can separately analyses and synthesize the security situation and work in terrain, is able to lead, know the law, can work with human resources, has basic knowledge in forms and methods of work in commercial security industry and know the basic technical means in this field.

Criminological technology and systems

The course deals with the problems of security-legal activities, completes the knowledge gained in other relevant courses with an accent on interdisciplinarity, e.g. law and psychology. During the course the output skills of the students are followed which are necessary for standard activities in private security services. The introductory part concentrates on communicative skills; students gain the information and arguments that enable them to effectively deal with questions of the social role of criminological practice.
The knowledge of this discipline will provide users, especially within the security agencies, instruments of scientific knowledge and understanding of advanced technical and tactical methods used in practice

Techniques of detective activities

The aim of the course is to introduce topics following the opening thesis in the sphere of private detective services (PDS), develop basic legal aspects of private detective activity (PDA), forms, methods and means used in PDA (more closely in the previous course chart). In the field of specialization, the students are familiarized with issues of interest of submitter (client) protection in the framework of business co-operation; detective preservation of economic interests; detection of latent economic criminality, including commercial intelligence issues.
Students obtain consequential and equitable knowledge and information in connection with topics following the basic thesis in the sphere of private detective services (PDS); development of legal aspects of private detective activity (PDA), forms, methods and means used in PDA. Within the scope of the specialization, the students are familiarized with issues of protection of interests of submitter (client) in terms of business co-operation; detective protection of economic aspects; detection of latent economic criminality, including issues of commercial (non-state) intelligence.

Management of Security Engineering

The content of Management of Security Engineering is focused on the need of students to acquire basic knowledge of company management, organization and economics. The aim is to prepare students for the creative application of knowledge in terms of specific companies.
Students will adopt the ability to apply elementary concepts of the enterprise management. Students will be able to read elementary financial statements and use it for managerial decisions. Students will be able to understand the contemporary business environment and will be able to use basic economic and managerial tools.

Ergonomy and Psychology of Security

The aim of the course is to introduce the ergonomy (essential part of human activity optimization), which deals with system of working interaction, and define their mutual bindings and effects. In the field of occupational psychology and its safety, issues of stress and traumatic situations, methods of their solution and communication principles in stress situations will be explained.
Students will obtain knowledge in selected fields of ergonomy, they will master the interactions ongoing mainly in working systems, including their mutual bindings and effects. The students will also master the issues of work psychology and its safety (stress and traumatic situations, ways of their solution and communication principles in stress situations).

Integrated Rescue System, Crisis and Information Management

The course goal is to expand students' knowledge of IRS, crisis and information management. The course is divided into three parts; the first discusses the challenges IRS law, its components, including the issue of contingency plans. The second part of the course is focused on crisis management system of the CR, the issue of contingency plans and protection of the population. The final part of the course is oriented to the area of information management.
The student has knowledge about determination, the composition and structure of the IRS and state emergency management system of the CR. Student can specify the basic measures in dealing with emergencies. Student identifies the basic information needs for crisis management. Student specifies the criteria and measures of information management.

Security Futurology

The course deals with an issue of future development of security in regions, territories, fields and social groups. Further, creation of concrete scientific prognosis of safety situations development by forecasting the issue of the

worldwide safeguard of people especially by the international terrorism in social dimension of international relations, by the solution of so-called security dilemma in international relations, by the philosophy of safety future, by the research in security conflicts, and by the security systems of interim measures of protection is described. The transeurasian security system is also mentioned.
The student has the knowledge about statistics in security activities, analyses and synthesis of security projects and planning. The student is well informed in predicting the security of future of mankind, and they are able to apply gained knowledge if foreseeing the security situations. The student is also qualified for handling with prognostic materials.

Entrepreneurial Law in the Commercial Security Industry

Entrepreneurial Law in the Commercial Security Industry is profile subject, which increases student level laws education and knowledge itself possibility application severally laws norm into area save asocial relation, on top unfocused on undertakings. Subject creation possibility for application severally norm in administrative doing in state well, autonomy, and business doing. Measure schoolwork them oriented how on ground knowledge theory laws, so and on frequently return Czech laws system with accent on law constitution, civil, business and trade law and law work.
Students are familiar with the basic knowledge in various legal disciplines. The standards used mainly commercial law for ordinary everyday practical work. [7,8,9]

V. Conclusion

Article “Security Education as a Fundamental Pillar of Critical Infrastructure Protection and Resilience” discusses the security education position in context of critical infrastructure protection and resilience, mostly in relation to maintenance of vital societal functions and society functional continuity. Introductory part of the text moves from terminological definition of selected problematic to security education objectives and challenges. Third part was the developed methodology of critical infrastructure resilience evaluation description, where the robustness definition was described in wider context. Methodology is also seen as the philosophical basis of establishing the objective education program subject structure within the security education. Defined subjects structure is divided into management and technical subjects. This defined subject structure is fundamental for critical infrastructure protection and resilience and its part of study program “Security Technologies, Systems and Management” at Tomas Bata University in Zlin.

Acknowledgment

This work was supported by the Ministry of Interior of the Czech Republic under the Research Project No. VG20112014067 and by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

References

[1] [1] LUKÁŠ, L., HROMADA, M. Management of Protection of Czech Republic Critical Infrastructure Elements, In: 13th WSEAS International Conference on Automatic Control, Modelling & Simulation (ACMOS´11), Recent Researches in Automatic Control, Lanzarote, Canary Islands, Spain, , p. 306-309, 2011, ISBN: 978-1-61804-004-6
[2] [2] EU. Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In Council directive 2008/114/EC. 2008, 345, s. 75-82. Available from WWW: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:en:PDF
[3] CRN Report, Focal report 6, Risk Analysis, Resilience – trends in Policy and Research, Commisioned by the Federal Office for Civil Protection Zurich, pp.25. April 2011
[4] HROMADA, M.,Povinnosti prevádzkovateľa Európskej kritickej infraštruktúry/The European Critical Infrastructure Operator Duties, In: Security Magazín, No. 95, p. 52-55, 2010, ISBN – 1210-8723
[5] HROMADA, M., LUKAS L., The Status and Importance of Robustness in the Process of Critical Infrastructure Resilience Evaluation, The 13th annual IEEE Conference on Technologies for Homeland Security (HST ’13), held 12-14 November 2013 in Greater Boston, Massachusetts. Pp. 589-594, ISBN 978-1-4799-1533-0
[6] LUKAS L., HROMADA, M. Metodika hodnocení odolnosti vybraných prvků a sytému prvků kritické infrastruktury, Univerzita Tomáše Bati ve Zlíně, Zlín, 2013, 75s.
[7] TBU, FAI, Security technologies, systems and management, Bachelor study program structure, online: http://ects.utb.cz/plan/7030?lang=en.
[8] TBU, FAI, Security technologies, systems and management, Master study program structure, online: http://ects.utb.cz/plan/7041?lang=en.
[9] Hromada M., Lukáš L., Critical Infrastructure Protection and Resilience as an Actual Challenge of Security Education, Computers and Technology in Modern Education, Kuala Lumpur, Malaysia, April 23-25, 2014, p. 62-69, ISBN: 978-960-474-369-8
[10] Ševčík J., Lukáš L., Aggregate coefficients of the Intelligent Video Surveillance Systems, Apploed Computational Science, Proceedings, of the 13th International Conference on Applied Computer and Applied Computational Science, Kuala Lumpur, Malaysia, April 23-25, 2014, p. 56-61, ISBN: 978-960-474-368-1

Martin Hromada - Was born in 1983. In 2008 completed a master's degree in security technologies, systems and management at the University of Tomas Bata in Zlin, where he currently serves as an internal PhD student. The object of his interest in the protection of critical infrastructure in terms of technological aspects, modelling and simulation.
Ludek Lukas - (LTC ret.) was born in 1958. He graduated university studies in 1981 at Military Technical University in Liptovsky Mikulas (Slovakia) and doctoral studies in 1993 at Military Academy in Brno (Czech Republic).
During his working at the Military Academy in Brno (1991 - 2005) he held the function of lecturer, group leader, head of department and vice rector for study affairs. He currently works at the Tomas Bata University in Zlín as associate professor. His scientific research, publishing and educational activities are focused into area of C2 communication and information support, information management, physical security and critical infrastructure protection.