Protection of Critical Infrastructure

Miloslav Seidl, Ladislav Šimák
Faculty of Special Engineering of the University of Žilina, Slovak Republic

Visegrad Fund

Improving the security level belongs to the actual tasks of the contemporary society. The critical infrastructure security is part of these processes. The security environment and its influence on the security. The task of the state and public administration in protecting the critical infrastructure. The influence of the individual critical infrastructure elements for achieving the required citizens´ standard of living. The experience of neighbouring countries from the critical infrastructure protection. The tasks of science and research in the area of increasing the resistance of the critical infrastructure.

Keywords: Critical infrastructure, sectors and elements of the critical infrastructure, security, security system, security environment, risks, threats, public administration, transport, protection, operability.

Complex increasing the security level is currently one of the most important tasks which the whole society, the governments of individual states but also the management of every firm is faced with. At the same time to achieve safe life and sustainable improvement of the standard of living is the objective of all people. The security has ceased to be interpreted as a state of preparedness for averting a possible military attack, but it is perceived as an ability to ensure continuous development of the society and to fulfil the society-wide goals. The protection of the selected most important elements of the infrastructure which has a principal influence on a problem-free operation of the society and achieving the required standard of living of the citizens is an important part of these activities. This part of the infrastructure designated as critical is a condition for fulfilling the basic economic, social and political functions of the state.

The critical infrastructure represented especially by the sector of telecommunications, power industry, transport but also the food industry, health care through it essence fulfils the basic tasks of the modern state. If any of these vitally important areas fails, the collapse can spread to other sectors because they are mutually linked and dependent on each other. In the current world which is very closely linked by the information, telecommunication, transportation and other networks, it is very probable that serious failures or breakdowns will cause damages not only in the state where they arise but very probably also in others, not only the neighbouring countries. The critical infrastructure protection became therefore a global challenge which is to be approached unambiguously from the multination point of view.

1. SECURITY OF CRITICAL INFRASTRUCTURE

The system approach to ensuring the required level of security and sustainable development of the society represents ensuring the security and sustainable development of the human society elements (states, nations, institutions of the public administration, the elements of the critical infrastructure, legal entities, groups of persons as well as individuals who create the system) and on the other hand ensuring the security of the links and information flows between the elements of the system which can be dominant for the situation of

the human society (the legal environment, social environment and relations, interpersonal relations,…).

Improving the level of security of the process for fulfilling the stated goals belongs to the basic tasks of the leading employees on all levels of the state administration, territorial self-government, the managers of the entrepreneurial subjects in manufacturing and services as well as the representatives of various associations and organisations aimed at the public inspection. They achieve it through identifying the risks in any area of the human activity including the risks threatening the operability of the critical infrastructure, their complex analysing and assessment in all society life areas and through searching for way of their reduction. The process of assessing and managing risks in the conditions of the critical infrastructure has to be permanent; it has to run continuously and to create conditions for continuous improvement of the activity results of the relevant subjects. The area of the critical infrastructure's security and risk which endanger it is mutually interconnected and it is to be understood in a complex way. That is why it is inevitable to investigate the security environment, to assess concrete risk and actual threats and to optimise the processes of their permanent reduction.

Generally, the term security designates an objective state defined by the environment, conditions, elements and their relations in which the given subject does not feel threatened. The term security is defined in a whole range of scientific works, legal standards as well as various popular materials in different ways. In the terminological dictionary of the crisis management the term *security* is defined as follows:

The **security** is a state of the social, natural, technical, technological system or another system which in concrete internal and external conditions enables fulfilling the stated functions and their development in the interest of people and the society.

The security has its internal as well as external dimension. The **internal security** expresses a state of security of those elements and relations which are inside of the given system against the external security. It is also based on the interpretation of he subject's state and the ability to reduce the risks which can be a source of threats. Its protection also consists in the preparedness and ability of the system to be activated due to reducing the probability of the rise of a crisis phenomenon which would threaten the fulfilment of the stated goals and its development.

The **external security** is based on the level and character of the elements and relations of the external threat and parallely on the influence of various protection elements of the social life (military, political, economic,…). Its protection consists also in the preparedness and ability of the system to perform against other subjects which affect its security and in the qualities of its elements as well as collaborating subjects being able to participate in achieving the required level of security (determinateness, properties and possibilities to create various security sub-systems or institutions).

The structured character of the security is shown from the point of view of the extent in its vertical hierachisation (it is derived from the system of governing a territory, from the global viewpoint up to the individual citizen) and from its horizontal classification (its basis is in the professional division of the human activities). The **vertical structure of security** contains a whole range of the security levels whose importance is not derived only from the size of the territorial or organisational unit which it expresses but also from the angle of view of the subject assessing the situation.

On the other hand the **horizontal division of security** is connected with individual areas of the human activity but also with the environment people realise their activities. The optimal development of the state is impossible without achieving a certain level of the political, military but also economic, information, technical and technological as well as energy security. A substantial part of the segments of the horizontal division of security belongs to individual sectors of the critical infrastructure.

2. SECURITY ENVIRONMENT AND ITS INFLUENCE ON CRITICAL INFRASTRUCTURE SECURITY

In the process of assessing the security level of any system, equipment, process or activity it is

inevitable to define correctly its security environment. The complex and objective assessment of the security environment enable to take optimal measures for maintaining or improving the security level and the sustainable development of the society. To know the security environment on one hand and the possibilities of the state on the other hand enable correct heading of the security policy.

Defining the term security environment is not univocal. Similarly as the security also the security environment has its complicated vertical and horizontal structure. The security environment performs on one hand in the framework of the global environment, the environment of the international organisations or states and on the other hand in the framework of various systems creating the society structure and fulfilling their basic functions which are interconnected by mutual links and activities in the area of security.

The security environment is thus a space where the security is realised, in which it has developed and is developing otherwise a threat for the security, interests, activities, values of the international society, a concrete state, various forms of the social groupings, legal entities or individual citizens arises. However, this part of the security environment mostly performs as a condition for changes in the security of individual systems, in a smaller extent as their cause. The security environment is at the same time created by the qualitative and quantitative parameters (factors, indicators), the characteristics of the system itself whose relation change to each other as well as in relation to the conditions is as a rule the basic cause of the security changes as a state and the change of perception and experiencing the security.

For the needs of investigating the processes connected with the critical infrastructure protection the security environment can be defined as follows:

The **security environment** is a changeable complex of the external and internal conditions, factors, relations and activities which determine the changes of the state of security and whose perception, knowledge and experiencing finds its expression in the behaviour of the social subjects.

The security environment has always a concrete character. In spite of frequent repeatability or similarity it performs and changes in concrete geographical, territorial, time, demographic and historical conditions which take a form of real socio-economic, political, military, cultural and other determinants of the security. At the same time these determinants are enforced in confrontation with concrete social subjects which more or less affect the security environment.

The security environment can be classified according to several criteria. One of them is the placement of the element which affects the security level. When defining the internal and external security environment we assume that the environment is not a complex of mutually acting factors, influences and elements beyond the boundaries of the given system but simultaneously also a complex of factors, elements and influences which are part of the given system or perform inside of it. The involvement of a concrete element to the external or internal security environment is relative; it is dependent on the system extent into which we involve it.

The internal security environment relates to detecting the internal security and order in the state (protection against criminality and organised crime,…). The term internal security which is represented by the internal security environment has been recently connected with the term social vulnerability (it concerns especially the most advanced and richest cities with high concentration of inhabitants and people become an easy target of the violent criminal activity). However, it is also connected with the protection against natural disasters whose sources are in individual regions different and for which the institutions of the public administration do not expend the same resources. The internal security environment is also dependent on the structure of industry, on the prevention of industrial accidents and on the technical and technological maturity of the country and its citizens.

The external security environment relates to detecting the external security and defence of the state (protection against military threats by other states or military coalitions). Except for this it is affected by the character of the external threats including natural disasters and global disruption of the environment. The external security environment is based on the ability of the subject to influence other subjects in the effort to maintain the required security level.

The trends of the internal security and possible scenarios of reactions to these trends unambiguously show that the society strives in a greater extent to build complex security systems based on the exchange of information on the global scale. The information society is endangered by a whole range of risks and its vulnerability has a quality changed in a fundamental way. The security is thus more and more dependent on the data accessibility and failure-free function of the communication system and technologies. The unsolved problems in this area can result in the rise of extensive crisis phenomena whose negative impacts can by their extent resemble the crisis of the military character.

The internal security of the modern society cannot be defined from the position of the national or even regional or sector security and it cannot be created like this. The internal security has to be substantiated by the global framework conditions and control tools. The never ending changes of the security threats and consequences require implementing new methods of identification, e.g. modelling and simulation. At the same time we have to develop new legitimate procedures how to respond to the security threats, long-term management, warning, adaptation and acceptation.

The required level of the internal security is not only the task of the state. The economy and especially sectors and subjects operating the critical infrastructure have their responsibility. And finally, the level of the internal security is determined by the responsibility of every citizen – both on the level of capability and will to protect our own persons but also on the level of helping the others. It requires a change of approach to the danger and risk. Only if the society understands the necessity of the collective security, the citizens will be willing to adopt the limitations in the crisis situations. [18].

The security environment is also classified according to the extent, importance and distance of the events which have a direct impact on the security situation of the territory assessed. Every emergency as well as actual risks and real threats have their territorial and dynamic side which affect the development of the security environment of the given state or region. In compliance with these facts the external security environment can be defined as immediate, close and remote security environment.

The immediate security environment includes the neighbouring states or regional integration groupings. The natural but also industrial accidents which have supranational character (e.g. the consequences of disaster in nuclear facilities) possess here a specific place. The development of the security environment is up to a certain level affected by the quality of the relations between states and the foreign policy of the state but also the level of the internal security environment of the neighbouring country.

The close security environment includes the European region (the EU states but also other countries on the European continent as well as various types of political, economic or military groupings, e.g. EEC, NATO and others). The influences of the natural and industrial disasters play an important role also on this level. The development of the security environment level is influenceable only in a limited extent, in dependence on the character and importance of the concrete risks and threats.

The remote security environment contains the main areas of interest of the world and European powers (e.g. influencing the security environment in the area of mining strategic raw materials, etc.). In this area it is inevitable to assess the global climatic changes and their effect of the society or also the global effects of the nuclear disasters. The development of the security environment on this level can be affected only minimally. It is carries out in the form of international negotiations on the ground of international organisations, e.g. the UN. (Zeman, 2003)

3. ANALYSIS OF SECURITY ENVIRONMENT IN RELATION TO CRITICAL INFRASTRUCTURE

The security environment of each reference subject consists of a whole range of elements. A part of them creates the internal security environment and another one represents the external security environment. The fulfilment of the security interests of the reference objects requires formulating and implementing specific strategies and policy. However, it is impossible without complex knowledge of the security environment which permanently develops and changes.

The analysis of the security environment is a process of defining the basic interests and activities of the reference object and identifying the risks and

threats which can disrupt their security and fulfilment of the planned goals. Subsequently it is inevitable to state also the most appropriate measures for their reduction or complete removal.

The interests resulting from the protection of the most important values of the reference object are divided into vital and important interests according to the Security Strategy of the Slovak Republic from 2001. Except for this, in several professional studies and also in the Security Strategy of the Czech Republic the term "further interests" or "long-term interests" are introduced. If we take into account just this classification the extent of the interests which are to be protected is very extensive. According to one part of experts it is necessary to consider the threats for security those ones which have an existential character for the reference object, it means they are vital threats and also the general public perceives them in this way. The security in this context is exclusively understood as certainty of maintaining the existence.

The measures for reducing the assessed security threats have the goal to minimise the risk, i.e. to reduce the probability of the rise of negative phenomena disrupting the security and to reduce the size of the damages which could arouse the possible rise of them as well as the means used for minimising this risk and damages. These measures become part of the security policies and strategies. They are used for materialising the threat and become part of the security environment.

The internal security environment contains also undesirable components which represent especially:

- the structural threats which result from the existence of the reference object itself,
- the current threats which arise due to a common or non-scheduled performance of the reference object.

The security analysis is carried out in the environment of uncertainty which is given by the dynamics of the security environment and complexity of the security systems of individual reference objects as well as their environment. The objective of the security environment analysis is to acquire material for the political process whose goal is to achieve the required security level.

The object of the analysis is assessed in the conditions of subjective uncertainty which means that there is lack of information about the phenomenon investigated. This type of uncertainty is connected with the rate of knowledge of the competent employees. The subjective uncertainty cannot be fully removed because it is almost never possible to acquire relevant information for the given reference framework. However, on the other hand we have to speak also about the objective uncertainty. It results from the facts that the security analysis is aimed at phenomena which objectively still do not exist. The total removal of uncertainty is impossible in spite of the fact that effective strategies are able to minimise the uncertainty or to transform it to the risk.

In the security environment analysis the uncertainty is linked with the level of the risk and here the risk represents the probability rate of the threat materialisation. On the other hand it is inevitable to assess not only the probability of the rise but also the quantitative extent of the given negative phenomenon. From the point of view of assessing the security environment in relation to the protection of the critical infrastructure is thus necessary to state not only the probability of the rise of an non-scheduled phenomenon but also the extent of the negative impacts on the society.

During the analysis of the security environment we create a model approximately corresponding with reality according to which it subsequently possible to formulate the security policies and strategies. The effort is to capture and describe the reality as complexly as possible, i.e. to describe those elements, links and processes in the security environment which affect it most distinctively or have a potential to affect the reference object in the future. The analysis of the security environment usually consists of two key parts – the description of the actual situation and the prognosis of the security environment in the future.

The task of the description is the primary illustration of the security situation, i.e. the current state of the security environment. It can also comprise historical facts which clarify the current situation and can help formulating the generalisation and theses about the development in the future. The description unusually includes the qualitative assessment and the most important thing is to pay attention to the relevant information about the elements and links. However, no

description can reproduce the security environment in its whole complexity. The social analyses in general catch only those elements of the real environment which can be caught and described by common communication means or through verbal and statistical descriptions.

When prognosing the future development we distinguish the linear forecasts (one cause arouses one reaction or subsequently one resulting phenomenon), the divergent forecasts (one cause arouses several reactions which lead to several resulting phenomena) and the convergent forecasts (several causes performs in a cumulative way and arouses one resulting phenomenon) which enable to foresee the development of the future actions and processes. (DeRosnay, 1979). Prognosing is the second phase of the complex analysis of the security environment. In its framework it is important to single out the rational players in the security environment, i.e. first of all other players of the international relations and relevant subsystems of the reference object and on the other hand the natural forces performing in an irrational way with a reduced possibility of forecasting. When estimating the future development we can forecast and complexly describe the phenomena and processes connected with the natural forces only with difficulties, however, we can anticipate them. Also the sources of the industrial accidents with the impacts on the assessed environment and combinations of the natural forces with effects of the industrial accidents of great extent can irrationally perform in a similar way.

The methods of analysing the security environment are the same as the risk assessment of the territorial units. One of the basic qualitative methods which enable to work out the development of the future actions and processes is the method of creating scenarios. It is utilised by the bodies of the public administration for assessing the internal security environment but also when forecasting the international events. This method enables to optimise gradually the development of the actions and processes and subsequently the individual scenarios. Its is also suitable to reduce the rate of subjectivism by using the methods that are based on the team knowledge of a wider security community.

An important issue in the process of assessing the security environment is to define the risks and threats. Several methods that are based on the quantitative, semi-quantitative or qualitative tools and materials are used for these activities. The quantitative procedures are based on real quantifiable inputs which are results of statistical investigations. On the other hand the semi-quantitative and qualitative inputs are based especially on the expert estimation. The semi-quantitative procedures require data which is estimated and subsequently structured into intervals. The qualified estimations which are most frequently utilised in the framework of the security environment analysis can be transformed through semi-quantitative procedures and can be expressed in a more exact way.

The biggest shortages of any analysis are the credibility and ability to describe the followed phenomenon in a real way. In the case of the analysis dealing with security and development, this problem is emphasised by the great extent and by the work carried out in this area until now. In the security studies there is only one single clear turning line which represented by the end bipolarity, however, the discipline is internally divided due to an unclear object of investigation and the starting point of the individual procedures. These facts cause that to set up an exhausting overview of the theories dealing with the impact of the security problems on the development of the individual components and branches of the society and the development of increasing or decreasing the security rate is extraordinarily difficult. This is also decisively important e.g. for investigating terrorism which represents a multidimensional threat. This fact arouses the opportunities to realise the analyses through various types of theories – from the psychological, sociological, geopolitical and mathematical up to the economic ones.

4. SECURITY ENVIRONMENT OF THE SLOVAK REPUBLIC

The security environment of individual countries differs from each other in dependence on the position of the given country in the international system and also on the extent and level how the individual security sectors are built. When analysing the security environment it is inevitable to take into account the geographical position of the reference object, i.e. the concrete state or region.

In the case of the Slovak Republic the geographical factors are the main determinant of the security environment development because just they distinguish it largely from the actual providers of the key analyses of the security environment, e.g. the EU or NATO. In the conditions of Slovakia the security environment analysis is often taken over from international institutions or other internationally and politically important countries. The reason is moreover the size and position of the country in the international environment but also a feeling of false subsidiarity.

For these reasons but also for other political grounds, e.g. maintaining sovereignty and moral integrity, it is necessary to create our own security environment analyses which should be based on the specific position of the Slovak Republic compared with the average of the EU and NATO countries, but connected to the global development and important regional as well as global trends.

The security environment is in Slovakia assessed in the process or during alteration of the Security Strategy of the Slovak Republic. Last time this process was realised in 2005. Except for this, every year we work out and on the level of the central bodies of the state administration the Report about Security of the Slovak Republic is discussed. The Report about Security of the Slovak Republic for 2010 was worked out on the basis of the provision § 2, letter a), section 3 of the law No. 110/2004 Coll., about performing the Security Council of the Slovak Republic in the time of peace according to which the Security Council of the Slovak Republic assesses and once a year submits to the government of the Slovak Republic the report with proposals of measures. The report was worked out by an interdepartmental working group under the gestion of the chairman of the Security Council of the Slovak Republic according to the Methodology for Working out Reports about Security of the Slovak Republic approved by the resolution of the Security Council of the Slovak Republic No. 238 from 26th November 2008.

The report was based on materials which were worked out and submitted by the relevant ministries, other central bodies of the state administration, state bodies as well as the security councils of the regional offices in the seat of the region according to the approved content structure of the material. The external and internal aspects of the security situation are the content of it. It briefly assesses the security level of the Slovak Republic and the realisation of its security interests. It shows the main shortages which can negatively affect the security of the citizen and state. The main priority of the activities of the ministries, other central bodies of the state administration and the bodies of the local state administration in the issues of security became the realisation of the tasks resulting from the elaboration of the Policy Statement of the Government of the Slovak Republic to their concrete conditions.

The government of the Slovak Republic has declared it will constantly pay attention to ensuring security of Slovakia. The Security Council of the Slovak Republic as the advisory body of the Slovak government coordinated together with the ministries, other central bodies of the state administration and other state bodies the preparation of the documents solving the state security. The submitted report shows the security of the Slovak Republic has been ensured. The methods of coping with problems and risks are expressed continuously in the whole material and in the proposals of measures. Such a regular objective assessment ensures not only a permanent overview about the state of security, but if necessary, it enables also early correction of the goals and tasks of the security policy from the level of the Slovak government with impacts on improving the security system of the Slovak Republic. The final part suggests the measures for improving the state of security in the Slovak Republic in the further time period.

Slovakia works out the analyses of the security environment especially for the needs of the central bodies of the state administration which belong to the supranational and international structures and concentrate on the regional security level and do not reflect the specific local conditions. The regional security level should take an important, however, not the absolute part of the attention of the country's security community. This fact results from the following basic assumptions:

- the immediate geographical surroundings of the Slovak Republic includes several latent threats, especially the eastern frontier with Ukraine,
- also threats of the global character where belong the economic crises but also the threats from cyber space, cyber terrorism

and terrorism in general are a reference framework of the Slovakia's security.

The basic step of analysing the security environment is its primary description. The actual risks and threats are identified in its framework. The description can be based on the historical facts which explain the actual situation and can participate in generalising the materials for prognosing the future development. It means it has a form of a qualitative assessment which is based on relevant information about the elements and links occurring in the assessed environment. However, the description of the security environment has only a limited utilisation and means only the orientation inside the problem and the preparation of a part of materials for usage in the framework of more exact procedures.

According to the current security strategy the security environment of the Slovak Republic is characterised and parallely affected by the following facts:

- the Slovak Republic is geographically and by its historical, cultural, political, economic and other linkages part of the Euro-Atlantic space,
- by its membership in the UN, OSCE and other organisations and groupings the Slovak Republic actively contributes to the effort of the international commonwealth to maintain the peace and security in the world,
- by accession to NATO the Slovak Republic became part of the system of collective defence and security,
- by accession to the EU the Slovak Republic acquired guarantees of the political and economic stability,
- entering the OSCE the Slovak Republic became integrated to the economically most advanced countries of the world,
- the geopolitical position of the Slovak Republic in Central Europe determines the security policy of the Slovak Republic,
- the membership of the Slovak Republic in the international organisations changed its security position in a principal way and created new conditions for realising its security interests. (Bezpečnostná stratégia, 2005)

The security environment of Slovakia is affected by the external and internal threats. According to the type and character of the threat some of them perform together from the external as well as internal environment. They often overlap and affect each other and it is impossible to separate them. The correct assessment of information acquired about the external and internal threats is a very important element for adopting a suitable set of measures for improving the state security. That is why this area is currently paid increased attention.

The external parameters which impact the security environment of the country are substantially affected by the global changes and trends which Slovakia is not always able to influence. We fail to remover the traditional global problems as poverty, lack of foodstuffs, possible pandemics or the danger of the world war, etc. and parallely the political potential of the new substantial global problems arises, e.g. the issue of climatic changes and accessibility and utilisation of the raw material sources. Currently the weakening of influence on the political and economic affairs of the traditional power centres (including the EU) goes on continuously. On the regional as well as the global level the influence of the so called new powers – e.g. China, Turkey, Iran, India and Brazil increases and the destabilisation of some strategically important countries, e.g. Pakistan deepens. The consequences of the global economic crisis – reduction of funds, increasing prices of foodstuffs and growing social frustration resulting from the high unemployment rate create assumptions for political changes in several Arabic countries, including the states in the north of Africa. The ethnical and religious unrests persist in a lot of regions in the world and procuring of military capacities with unpredictable consequences for the international stability continues.

The threat of the conventional military attack against the Slovak Republic is low; the non-military, asymmetric threats are more probable. The trends of stagnation of the illegal immigrants moving across the Slovak territory are confirmed, however, the effort of migrants to acquire a legal entrance to the Slovak territory increases. The threat of criminal activity of the illegal migrants persists. The risks connected with the activities of the organised crime and demonstrations of

radicalism and extremism are on a comparable level as in the previous time period. Disrupting the deliveries of strategic raw materials, illegal proliferation of weapons including those of the mass destruction and materials for their construction and the information war including the misuse of the cyber space and social networks still belongs to the threats for the Slovak Republic. Until now no immediate terrorist threat or involvement of people to preparation of a terrorist attack abroad has been recorded in the Slovak territory.

A new phenomenon of the current period is the impact of the financial and economic crisis on the EU. The last events in Europe concerning the solution of the debt crisis have caused falls of the governments in Ireland, Portugal, Spain, Italy, Greece, Slovenia, but also in Slovakia. The further development in this area is unpredictable and it is confirmed by the opinions of the foremost European politicians. Though Germany and France exert enormous effort to maintain the eurozone, if it goes bankrupt, the existence of the EU itself is threatened and this fact would bring serious economic consequences. The European leaders have to realise the extent of the crisis which can lead to unpredictable situations. In spite of the political peace in Europe, the financial and economic crisis can cause serious existential problems especially in the smaller EU countries. In general the following risks and threats can endanger the security environment in Slovakia in the nearest future:

- the terrorism represents for Slovakia a strategic global risk,
- the war conflicts whose source can be the regional conflicts and subsequences of some activities of the important player in the international politics threatening the stability of the international law system,
- the global financial, debt and economic crisis,
- the inadequate armament,
- the proliferation of the weapons of mass destruction and some dangerous technologies,
- the international organised crime,
- the radical nationalism and extremism – disrupting the stability of the social and political system of the Slovak Republic as well as its international position,
- the illegal and uncontrolled migration,
- the activities of the foreign intelligent services can perform against the interests of the Slovak republic as well as its citizens outside the territory of the country,
- the cyber attacks against the information and communication systems,
- the countries which fail, poverty and economic imbalance,
- the negative impacts of globalisation,
- the unequal political, economic, social and cultural development,
- spreading of pandemics, epidemics and dangerous contagious diseases as well as contagions of animals threatening the health of inhabitants and animals,
- the raw material and energy dependence on the vitally important resources,
- the climatic changes,
- the ecological changes,
- the natural and technological disasters with the cross-border impact and impact exceeding the regional boundaries,…

The aforementioned threats have an impact on the internal security. In the recent period in the Slovak territory there has not been recorded neither any immediate terrorist threat nor any involvement of persons to a terrorist attack abroad. Regarding to the attitudes concerning the foreign countries as well as the political ones and the participation of the Slovak Armed Forces in the operations of the international crisis management there is a risk of probable attacks not only against the Slovak citizens operating in the crisis regions but also against inhabitants and object in the Slovak territory.

Separating the external and internal security environment is necessary also from the point of view of the methodological research of influences leading to changes of both sides of security. However, the character of the current and future threats wipes away the imaginary frontier between their unambiguous affiliations to the external or internal dimension of security. One of the decisive causes is the globalisation of all areas of the society.

Opening the European space (which is desirable) not only in the framework of the EU member states but also for the non-members of the EU including the third world principally changes

the danger of threatening security and puts also its internal dimension over the framework of the individual countries´ territorial boundaries. As a matter of fact the EU from its rise considers the issues of the external and internal security as common problems of all member states. The European Security Strategy defined already in December 2003 belongs among the basic documents dealing with these issues. It defines as the key threats terrorism, proliferation of the weapons of mass destruction, regional conflicts, failure of the function of the state and organised criminal activity.

One of the latest EU documents in the area of security is the proposal of the strategy for the internal security submitted by the Council of Europe in February 2010. The strategy deals with three basic issues: [17]

- identifying common threats and challenges,
- defining common policy of the internal security and principles of its implementation in the conditions of the individual countries,
- defining the European security model which is based on common obligations and tool used.

The following main common threats identified in the strategy:

- the terrorism in every form as a significant and continuously developing threat of security,
- the serious and organised criminal activity as drug trafficking, people trafficking, weapons, violent criminal activity, child pornography, legalisation of incomes from the criminal activity, document counterfeiting and other forms,
- the cyber criminality as a global cross-border anonymous threat of every information system,
- the cross-border criminal activity of a less serious or economic character, however, affecting the everyday life of people,
- the violence among young people connected with sport events,
- the disasters caused by nature as well as people, most frequently forest fires, earthquakes, floods, storms, droughts, power cuts, failures of information and communication technologies, etc.
- the traffic accidents a whole range of other common phenomena.

In spite of respecting the common procedures concerning the issues of the internal security, the security environment of every country has a certain specific character. Of course, it does not exclude the need to pay attention to all aspects and threats of the internal security, however, in an extent differentiated according to the real conditions of the country.

The events connected with continuing climatic changes which have a potential to hit extensive areas of the state, especially floods and storms, become more and more frequently serious factors that are able to destabilise the economics and affect the security environment negatively. Serious secondary threats as disruption of infrastructure, interruption of supplying with the vital energy, etc., are connected with it. The rise of such situations can negatively affect also performance of individuals and groups of persons in the affected territories.

As the last events connected with reports of the physicians show, also the long-term unsolved society-wide problems can have a negative influence on the security environment in the Slovak Republic. The health care belongs to the problems affecting the general public. The seriousness of the situation is underlined by the fact that the Slovak government declared the state of emergency (29th November 2011) for ensuring the inevitable health care according to the § 5 of the constitutional law No. 227/2002 Coll., about security of the state during war, state of war, martial law or state of emergency.

Another problem of this type is the so called “Roma issue” which has been solved for a long time only in a buck-passing way and without any conception. If the current approach of the top representatives of the Slovak Republic continues we can expect a break-out of extensive unrests in Slovakia in a time horizon of 10 – 15 years.

Besides the aforementioned facts the main internal threats can be considered as follows:

- disrupting the infrastructure of the power engineering, transport and telecommunications,
- the low law enforcement,

- the industrial technical and technological threats,
- deteriorating of the environment quality,
- the clientelism.

Based on these facts we can say that the global, European and Central European security environment from the point of view of the Slovak Republic shows no signs of a possible direct terrorist threat. Currently the economic crisis is the most negative factor. It causes economic imbalance and has a direct impact also on our domestic policy and the deteriorating level of employment rate in Slovakia. Other factors as proliferation of weapons of mass destruction, regional conflicts, radical nationalism, deliveries of crude oil and natural gas, etc. do not pose any negative effect on the security environment in Slovakia. The internal security environment is most affected by the political development, unemployment, long-term failing to solve serious society-wide problems (health care, Roma issue, corruption, etc.), migration of citizens and floods. Paradoxically, one of the factors negatively affecting the internal security environment is also unsuitable legal environment which ambiguously, inconsistently or by no means solves the area of the critical infrastructure.

5. ENSURING OPERABILITY AND PROTECTION OF CRITICAL INFRASTRUCTURE IN THE SLOVAK REPUBLIC

The state is a political and power organisation whose features are the state territory, citizenship, existence of law and order, existence of a relatively independently acting subject of international law as well as domestic law, political organisation of the society comprising the whole society and the system of the public power bodies and sovereignty. It is an institutional expression of the political power and the main body in the society. The state is first of all an institutionalised power, i.e. also an institution in which this power is embodied.

Every state fulfils a whole range of functions where belong the legal function represented by creating and maintaining the legal, political, economic and social order, the social, cultural and also security function whose task is the protection of the nationals, their rights and freedoms against internal as well as external threats. These functions are achieved through executive, legislative and judicial power. The bodies of the state administration, the parliament, system of courts, armed forces, armed security brigades, emergency systems and others are formed for its fulfilment in practice.

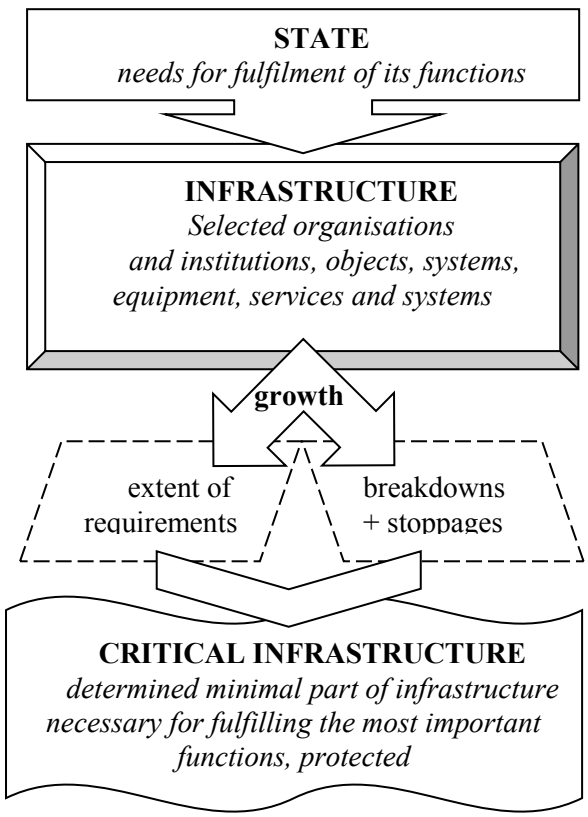
The relation of the state and citizen, the state and society or also the sate and its legal units is the essence of the public administration. The public administration as a whole represents an important power which organises and secures the fulfilment of the socio-economic tasks. The public administration through its activities, goals, tools and methods ensures the fulfilment of the stated social, political and socio-economic interests of the state. The objects, methods and goals of the public administration are involved in the legal order of the state and are concretised in the individual practical activities of the public power bodies. The public administration and its bodies carry out the administration of the state in the public interest. If a certain area exceeds the boundaries of the private ownership and the interests concern also other cooperating subjects in the given society, this area becomes public. Those institutions, which realise the public administration, carry it out as an activity which legally and based on laws must be done as a thing of the common interest. The law ensures the legal position of the public-law subjects with the necessary financial provision.

Based on the legal authorisation the state administration can be carried out by the state administration bodies as well as bodies of the local self-government or the bodies of the public corporations. For performing the state administration it is inevitable for a state administration body to be armed with powers and has to possess the factual and local or personal authority in the framework of which it implements the scope of authority.

The state has to ensure the optimal conditions for the inhabitants in any situation including the crisis situations. The current society gradually with the improvement of the technical and technological means used for ensuring its everyday needs and the extensive implementation of the information and communication technologies becomes more and more dependent on them. Today we cannot imagine our life without regular supplies of electrical energy, water, heat, without transport and

telecommunication services, the high quality health care and enough foodstuffs and other needs of everyday use. These basic needs of the inhabitants and the life standards are ensured through a widely branched infrastructure. The basic links between the state, its infrastructure and critical infrastructure are shown in the figure 1.

A quantity of interconnected structural elements which maintain the whole structure in the form of a functional unit is considered the infrastructure (from ten French word *infra-structure,* literally: what is under buildings) in the most general sense of the word. This term is used for artificially created structures in a whole range of lines of business. In the framework of ensuring the population we usually use a narrowed term – the public infrastructure which contains the transport infrastructure, the technical infrastructure of buildings, the community facilities as well as public places created and utilised in the public interest. In the interest of the society it is inevitable to administer the public infrastructure, to ensure its regular maintenance and development.



Source: *authors*

Fig. 1 Infrastructure and critical infrastructure of the state

The mankind is thus still more and more dependent on the functionality and sufficient performance efficiency of the public infrastructure. This dependence requires still larger and larger resources expended by the state as well as the entrepreneurial subjects to achieve the required level of security and ensuring uninterrupted functionality of the public infrastructure which is a risk point in the framework of society's preparedness to resist various crisis phenomena. The increased risk is also the extent of linkage and mutual dependence of the individual public infrastructure elements which is negatively affected also by the alteration of the property rights from the state to private persons, atomising the property relations and the entrance of the foreign capital to this area of business. These are the reasons why a part of the public infrastructure has a cardinal importance for the state performance and for ensuring quality life inside of it. This part of infrastructure is called the critical infrastructure.

The terminological dictionary of the crisis management says that the infrastructure particularly includes the objects of special importance, other important objects, selected information and communication means, premises for production and supplying with water, electrical energy, crude oil and natural gas and other parts of the state property as well as property of the legal entities and natural persons determined by the Slovak government or other competent bodies of the state administration which are inevitable for coping with the crisis situations, protection of inhabitants and property, for ensuring the minimal performance of the state economics as well as its external and internal security and which are to be particularly protected.

The area of protecting the critical infrastructure became an actual issue of the public interest especially due to the threat of the global terrorism. Also the EU began to deal with these issues intensively. In 2004 the total strategy for protecting the critical infrastructure which respected the fact that damaging or destroying part of the infrastructure in one member state can negatively influence other member states and the European economics as a whole began to be built. The new technologies (e.g. internet) and market liberalisation (e.g. for the supplies of power and natural gas) cause that a lot of infrastructure types

is part of a larger network. In these situations the protective measures are only as strong as the weakest segment is protected. It means that the protection level of individual infrastructures, sectors and elements should comply with their importance from the point of view of the complex state security, of ensuring the performance of the economy and ensuring the basic needs of the inhabitants.

The European Commission adopted on 20th October 2004 the material "Critical Infrastructure Protection in the Fight against Terrorism" where it submitted proposals how to improve the prevention against the terrorist attack against the critical infrastructure, preparedness and reaction to them on the European level. Subsequently, they adopted the Green Paper of 17th November 2005 on a European programme for critical infrastructure protection whose goal was to create a basic platform for an effective collaboration of the state administrations and operators of the critical infrastructure elements. According to the conclusions introduced in the Green Paper the effective protection of the most important infrastructure requires communication, coordination and collaboration on the intrastate level as well as the EU level among all involved subjects – the owners and operators of the infrastructure, professional bodies and industrial associations in collaboration with all governmental levels and the public. In December 2005 the Council for Justice and Home Affairs asked the Commission to submit the draft of the European Programme for Critical Infrastructure Protection and parallely it decided in the process of the critical infrastructure protection the threats caused by people, the technological threats and natural disasters will be taken into account, however, the priority will be the threat resulting from terrorism. In April 2007 the Council then adopted the conclusions about the European critical infrastructure where it emphasised the final responsibility of the member states in the framework of their national boundaries for managing measures for the critical infrastructure protection. In the effort to unify the procedure of the individual member states the Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection was issued on 8th December 2008. Its content brought a principal change in understanding the critical infrastructure protection when not the protection of people is in the foreground but the attention is increasingly paid to the protection of infrastructure and services. The Directive 2008/114/EC stated the date 12th January 2001 for the EU member states to adopt measures necessary for achieving compliance of fulfilling the tasks with this directive and they were to inform the Commission about the adopted measures and their relation to this directive.

The Directive 2008/114/EC defines the critical infrastructure as follows: *„The 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.*" (Council Directive, 2008).

In the Slovak Republic the law about the critical infrastructure was adopted on 8th February 2011. It stated the organisation and scope of authority of the state administration in the area of the critical infrastructure, the procedure for determining the critical infrastructure elements and the duties of operators in the area of protecting the critical infrastructure elements and responsibility for breaching these duties.

The state administration of the critical infrastructure is carried out by the government of the Slovak republic and selected central bodies of the state administration. The Ministry of Interior of the Slovak Republic is authorised to coordinate the state administration in the area of the critical infrastructure protection carried out by selected ministries according to their scope of authority. The individual ministries are responsible for the following sectors of the critical infrastructure:

- The Ministry of Economy of the Slovak Republic:
  - the sector energy engineering (mining industry, power industry, gas industry, crude oil and oil products)
  - the sector industry (pharmaceutical industry, metallurgy, chemical industry),
- The Ministry of Finance of the Slovak Republic:
  - the sector of the information and communication technologies,

- The Ministry of Transport, Construction and Regional Development of the Slovak Republic:
  - the sector transport (road transport, air transport, water transport, railroad transport),
  - the sector of electronic communication (satellite communication, networks and services of the fixed and mobile electronic communications),
  - the sector post (providing post services, payment system by post and procurement activity),
- The Ministry of Environment of the Slovak Republic:
  - the sector water and atmosphere (meteorological service, water constructions, ensuring drinking water),
- The Ministry of Health of the Slovak Republic:
  - the sector of health care.

The diagrammatic depiction of the relations between the players of the Slovak critical infrastructure – see the figure 2.

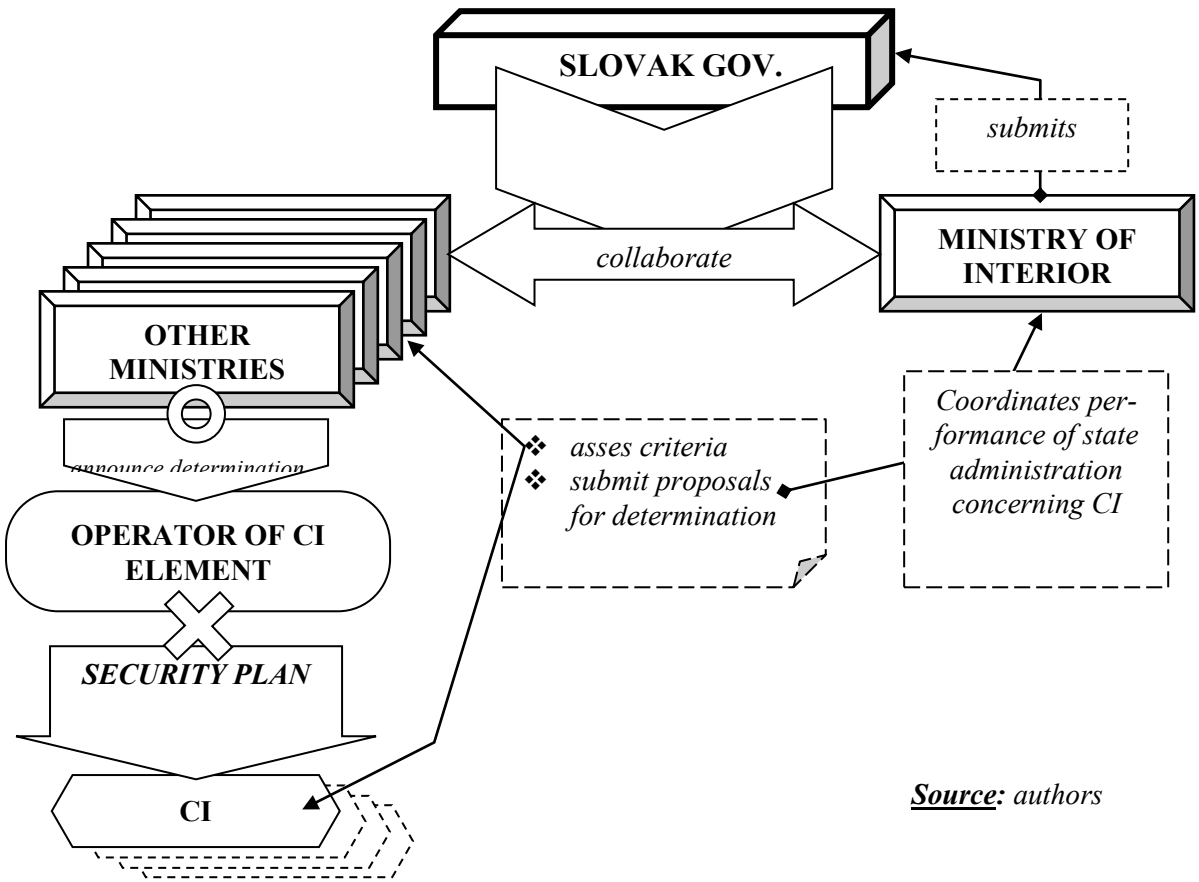


Figure 2 Determining CI elements in Slovakia

On the state top level the government of the Slovak Republic deals with the area of the critical infrastructure protection – it is a collective executive body. Its tasks are as follows:

- approving the critical infrastructure conception in which it determines the goals, priorities and tasks as well as methods for their realisation for the corresponding time period,
- approving the critical infrastructure programmes between the ministries for financial coverage of the tasks resulting from the law about the critical infrastructure,
- determining the criteria for ministries, the European sector criteria, the cross-section

criteria and the European cross-section criteria,

- deciding about determining the element and its categorisation to the sector as well as discarding the element from the sector.

The Ministry of Interior of the Slovak Republic works out in collaboration with other ministries in the competence of which the individual critical infrastructure sectors are a draft of the critical infrastructure concept which it submits for approval to the government. Subsequently, in collaboration with competent ministries it participates in working out the draft of the sector criteria, the European sector criteria, the cross-section criteria and the European cross-section criteria. Then the ministry submits it to the government with its standpoints.

The ministry then participates in the process of involving the critical infrastructure elements to individual sectors as well as in their discarding. Also in this area it cooperates with corresponding ministries and the decision-making is in the government's competence. As the administrator it works out in collaboration with the central bodies the draft of the ministry programme of the critical infrastructure which is also approved by the government.

Part of information used in the process of the critical infrastructure protection has a sensitive character. The task of the Ministry of Interior is to determine which information is to be involved to this category and to state responsible persons who can obtain this information. In this connection the ministry administers the non-public central register of the elements in the electronic form. The non-public register contains data about ranking the individual elements to the corresponding sectors and their detailed description including the statutory representative. Compared to majority of the neighbouring states Slovakia keeps part of critical infrastructure data secret which seems nowadays as a non-systemic measure.

The ministry also checks in collaboration with the corresponding central body the fulfilment of the duties for operators of the individual elements of the European critical infrastructure. In the framework of these tasks it coordinates the matters concerning the protection of the European critical infrastructure element with the corresponding member state and the European Commission and takes part in negotiations about these issues. It informs the Commission about the issues connected with the protection of the European critical infrastructure elements, about the number of the European critical infrastructure elements according to the sectors and about the number of the involved member states. Once or twice a year it submits a report to the Commission concerning risks, threats and vulnerable points in the sectors where the European critical infrastructure elements are. It also informs the corresponding state about discarding the elements of the European critical infrastructure from the sector and the reason for discarding. In the framework of its scope of authority it collaborates with the same institution abroad.

The individual ministries which take care about the corresponding critical infrastructure sectors work out a draft for the sector criteria and European sector criteria which is then submitted to the Ministry of Interior. In compliance with them and according to the procedure stated by the law they prepare a draft for determining the element and its ranking to the sector as well as the proposal for discarding the element from the sector. They collaborate with the operators who are informed about the decisions for determining the element and ranking the element to the sector as well as about discarding. These facts are continuously assessed. They work out the analysis of the sector risks and its updating which is submitted to the Ministry of Interior and in writing it gives opinion to the security plan and its updating.

Similarly, as the Ministry of Interior also the individual ministries which are responsible for the individual sectors of the critical infrastructure determine in collaboration with the operators the extent of the sensitive information and protect it according to the stated principles. They ensure the inspection activity in relation to the operator and submit to the Ministry of Interior a summary report dealing with the inspection of the operators. They solve breaching of law and the stated principles with the operators and in the extent of their scope of authority they can collaborate with a similar institution abroad.

The public power represents a force in the state which is able to ensure the formation, fastening and protection of the individual sectors and elements of the critical infrastructure through legal means including the forcible compulsion means.

Without the public power it would not be possible to ensure the required standard of living of the citizens and the social relations as well. Just the ability to ensure the order also by compulsion is one of the most important features of the social relation. The essence of the crisis management of the state, whose part is also the process of ensuring the protection and operability of the critical infrastructure, is based on a special mechanism of public power performance which consists of:

- implementing specific means for the public power performance,
- the specific institutional security provision of the state (security system of Slovakia).

The special tools of the crisis management are the certain authorisations of the state bodies and other subjects which consist in the possibility or duty to accept and carry out crisis measures aimed at solving the crisis situations with emphasis on the protection of people and property, i.e. minimising the damages and quick return to the situation before the crisis. Their part is also the restriction of the property rights and affecting the activity of the critical infrastructure operators.

A system of public power bodies and other elements of the crisis management which represent the security system of the Slovak Republic and are responsible for prevention of the rise of the crisis phenomena, for crisis planning and permanent preparedness for solving the arisen crises creates the specific institutional provision of the state. Also individual ministries which control the corresponding sectors of the critical infrastructure, the Ministry of Interior as the coordinator of the process of the critical infrastructure protection and the government which plays the decisive role in the area of the crisis preparedness fulfil concrete tasks connected with the critical infrastructure protection in the framework of the security system.

Providing the protection and functionality of the critical infrastructure and its elements is not only a task of the state and corresponding institutions of the public administration but also of the operators. The operator of a critical infrastructure element can be a company established in the scope of authority of the state or it can be a private company with participation of the domestic or foreign capital. The relation between the central body of the state administration and operator distinguishes also in connection to these property relations in the given element. The problem in this area is the fact that in the substantial proportion of the privatisation contracts there is anchored no duty to fulfil concrete tasks in the area of the crisis management.

In compliance with some measures of the economic mobilisation where belong (according to the law No. 179/2011 Coll., about economic mobilisation) e.g. organising the production and services, regulating the distribution and consumption of electricity and heat and the regulation of distribution and consumption of the natural gas, organising the supplies of vitally important products or vitally important goods, organising the health care, organising the transport, solving the lack of crude oil, organising the post services, the organisation of providing the electronic communication networks and electronic communication services would seem advantageous if the operators of the critical infrastructure elements were at the same time the subjects of economic mobilisation. However, this problem has not been solved in the corresponding legal standards.

A substantial part of the rights which the subjects of the economic mobilisation possess could reflect in increasing the protection level and functionality of the critical infrastructure elements. Here belongs e.g. the right (in writing) to ask the corresponding district office to release its employees from the working duties, to require from the district office to provide human resources and material means for fulfilling a concrete measure and a whole range of others.

The operators of the individual critical infrastructure elements are obliged to protect them against disruption or destruction. Due to fulfilling this task the operator has to assess the risks which threaten the security and functionality of the operated critical infrastructure element in a complex way and subsequently to work out a security plan which contains scenarios of the possible disruption of functionality or destruction of the assessed element and security measures adopted for its protection. They contain an integrated system based on mechanical preventive means, technical preventive means, security elements of the information systems as well as the

physical protection, inspection measures and their combination.

The critical infrastructure element operators have to discuss the worked out security plan with the corresponding central body of the state administration within six months from receiving the information about determining the element and its involvement to the sector and to implement it to practice. In the framework of implementing the security plan into practice the operators are obliged to inform their employees in an inevitable content with the security plan and minimally once per three years to train (on a model situation) the measures realised in the case of a threat which can cause disruption or destruction of the element.

In the process of updating the technological processes and building new systems of the property protection the operator is obliged to take into account also the character of the possible threat of the critical infrastructure element and the change in the security environment. Therefore the security plan is to be continuously assessed and the potential changes to discuss with the corresponding central state administration body. Subsequently the updated security plan can be introduced to practice.

The collaboration between the central state administration body and the operator of the critical infrastructure element is realised through a determined authorised person who is at the same time also the contact person if it is an element of the European critical infrastructure. The authorised person provides the corresponding central state administration body with cooperation in the issues connected with ranking the element to the corresponding critical infrastructure sector, with working out an analysis of the sector risks and the administration of the element register. The operators are furthermore obliged to inform immediately the corresponding central body about the changes in the area of their activity which can affect the determination of the element and its ranking to the sector, the sale of the element or another change of the property and legal relation to the element, the start of liquidation, the declaration of solvency or the permission for restructuring.

The operators have the right to receive the financial contribution for fulfilling the duties connected with carrying out the security measures for protecting the element if they were ordered to them by the corresponding central state administration body in the area of the critical infrastructure and at the same time they do not follow from the valid legal regulations.

6. CRITICAL INFRASTRUCTURE IN NEIGHBOURING COUNTRIES

In spite of the fact that the intensive and targeted attention to the critical infrastructure has been paid only for a relatively short time period of ten years, we can already follow certain trends and generalise the acquired information. The growing effects of the natural disasters in Central Europe represented especially by floods and partially higher speeds of the wind (windstorms, hurricanes) are one of it. The consequences of disrupting the infrastructure in these cases exceed the regional as well as national boundaries. Undoubtedly the sector of the information and communication technologies both from the point of view of failing people during utilisation of the information technique or erroneous software and targeted attacks of the hackers is a growing risk. In the future we must not underestimate the health risks connected with epidemics and pandemics. The mass diseases and quarantines can make the attendance of the object or equipment of the critical infrastructure non-functional and cause the subsequent chain reaction in other dependent sectors.

This mutual functional linkage of almost all critical infrastructure sectors it although a generally famous phenomenon but its extent and impact become apparent often only when a failure and infrastructure drop out occur. A lot of material, logical as well as virtual links, as a matter of fact, are not visible during failure-free operation of the infrastructure. However, it can be a very high level of dependence whose consequence is, as a rule, an undesirable domino effect. Its initiator can be even a tiny stimulus which seems to be harmless fromthe local point of view.

The goal of the critical infrastructure protection is to reduce and minimise the duration of the breakdown in dependence on the probability of the rise of failures or elimination of its elements on the national level. The critical infrastructure protection has to be ensured on one hand by concrete protection measures and on the other hand by collaboration of a quantity of elements which deal with the individual protection aspects.

Working out the conception of the critical infrastructure protection is a cyclically repeating process. It is based on the assessment of the existing competences and legal documents which state the goals of protection. A deeper analysis of threats and risks follows. Based on this analysis we assess up to what level the current measures ensure the required goals. If they are not sufficient, additional measures are added. Their adoption or adaptation is first of all a political issue. The result can be new tools for protecting the critical infrastructure. The practical implementation of the tools will test the level of the achievement of the goals for protection and a potential need of further changes.

The principles of the critical infrastructure protection can be formulated in several points (29):

- The integrated risk management – the programme of the critical infrastructure protection is based on a thorough assessment of the risks from which the measures in the area of the prevention (e.g. construction and technical planning, emergency planning), of the usage (e.g. physical protection, alarm systems, crisis communication), of the repairs (e.g. temporary repair of infrastructure) and of the recovery (e.g. reconstruction of infrastructure) are derived,
- The full spectrum of the risks – as a matter of fact, the risk assessment has to deal with all relevant risks (natural, technical, social) without preferring any of them,
- The resistance and flexibility are of great importance as the whole infrastructure is not uninterruptedly protected and is vulnerable. Therefore after disruption the return to the original state has to be as fast as possible. The infrastructure resistance is created by its robustness, availability of reserves, the capability and speed of realising supporting measures, the ability of the society to solve the crisis situations,
- Maintaining the proportionality – the adopted measures have to be proportional to the extent of the risk and required goals of protection therefore adequacy between the costs, protection, security as well as independence and legal rights has to be preserved (it must not cause the market deformation),
- The subsidiarity – the measures have to penalise the critical infrastructure operators as well as the public sector. Due to the fact that a big part of the critical infrastructure belongs to the private sector, special responsibility for measures and investments arises. Protecting its own elements of the critical infrastructure and support of operators is required from the public sector.

The prospects of the suggested and realised critical infrastructure protection measures are dependent on several factors. In the coming period also the following problems are to be solved here (30):

- The central problem is the mutual dependence and complexity of the critical infrastructure sectors. A possible contradictory moment inside of the sector can be the different level of the individual elements and sub-systems (e.g. the modern management system and obsolete physical management objects. The link between the sectors in the case of a drop-out of one sector causes the already mentioned cascade of failures of the dependent sectors; however, the size of the contact element between the sectors is not important at all.
- The internationalisation and coordinated collaboration is an objective consequence of the international market integration and unification of the technical standards. Especially the network sectors (transport, energy engineering) have to be regulated together. This regulation is necessary also from the point of view of various ownership of the critical infrastructure. It is to say that the measures for protecting the critical infrastructure serve – often in a greater extent – in favour of the neighbouring states,
- The long-term planning and maintenance of property is connected with usage and big financial demandingness of the critical infrastructure. Therefore the private operators insist on knowing the strategic development trends. A big challenge is not only to build a new infrastructure but also to ensure the maintenance and operation of the existing capacities.
- The variedness of the risks and new conceptions of protection require a permanent risk analysis. However, the great extent of risks almost excludes in practice their full elimination by every critical

infrastructure operator. Therefore there is a requirement for implementing the flexible protection conceptions which take into account all risk sources and solve them by improving the technical and social systems. The goal of this flexible conception is to reduce the consequences of a crisis phenomenon as well as fast recovery of the standard operation.

The common approaches and coordination of measures in the area of the critical infrastructure of the EU countries belong to the basic collaboration areas of the member states. Besides the inevitability to fulfil the adopted documents the real network connection of the decisive infrastructure sectors – energy engineering, transport and communication systems – is an objective need of collaboration. In spite of the partially different conditions of the individual states the achieved level of identification and protection of infrastructure is on a comparable level and this is valid in the case of immediately neighbouring countries.

One of the possible indicators is the comparison of the defined critical infrastructure sectors shown in the table 1. Beside Slovakia (SK) the table shows the countries with common boundaries, i.e. the Czech Republic (CZ), Poland (PL), Hungary (H) and Austria (A) and for comparison Germany (D).

Table 1 Comparing the critical infrastructure sectors in selected countries

Critical Infrastructure Sector	Country					
	SK	CZ	PL	H	A	D
Transport	X	X	X	X	X	X
Electronic communications	X					
Energy Engineering	X	X	X		X	X
Information and Communication Technologies	X	X	X	X	X	X
Post (Telecommunications)	X		X			
Industry	X			X		
Water and Atmosphere	X	X	X	X	X	X
Health Care	X	X	X	X	X	X
Food Industry and Agriculture		X	X	X	X	X
Financial Market and Currency		X	X	X	X	X
Emergency Services		X	X			
Public Transport		X	X	X		X
Production, warehousing and usage of chemicals and radioactive substances (including pipeline transportation of hazardous substances)			X		X	
Police and Defence				X	X	
Research					X	
Media and culture						X
Total of Sectors	**8**	**9**	**11**	**9**	**10**	**9**

Sources: [22], [24], [25],[26],[27],[28]

In the Czech Republic the coordinator of the tasks in the area of the critical infrastructure is the Committee for Civilian Emergency Planning as a working body of the Security Council of the state. The National Programme of Critical Infrastructure Protection is linked with the Complex Strategy to Solving Critical Infrastructure and is created parallely with this document. The law No. 430/2010 Coll., which amends the law No. 240/2000 Coll., about crisis management and other laws (crisis law) as amended became effective on 1st January 2011. The subject matter of the amendment of the crisis law is also to state the scope of authority and powers of the state bodies

and bodies of the territorial self-government units and the rights and duties of the legal entities and natural persons in the critical infrastructure protection. It incorporates the critical infrastructure protection to the crisis management and states all crisis management bodies (government, the Ministries of Interior, of Transport, of Industry and Trade, the Czech National Bank, the district bodies and other bodies in the area of the districts, the municipality bodies with extended scope of authority, legal entities and natural persons, subjects of the critical infrastructure) the tasks in relation to the critical infrastructure. It defines all basic terms – the critical infrastructure, the European critical infrastructure,, the element, the subject and critical infrastructure protection, the cross-sectional and branch criteria for determining the critical infrastructure elements. The Resolution of the Government No. 432/2010 Coll., about criteria for determining the element of the critical infrastructure concretises the cross-sectional and branch criteria for determining the critical infrastructure elements in all nine areas of the critical infrastructure.

In Poland the responsibility for the critical infrastructure is delegated to the government body Rządowe Centrum Bezpieczeństwa. The main legislative document is the law about the crisis management from 2007 which is gradually amended. In 2010 the issues concerning the critical infrastructure were incorporated to the law. It defines the European critical infrastructure, critical infrastructure and its systems and the critical infrastructure protection. The preparation of solution in the case of disrupting the critical infrastructure is part of the tasks in the area of civilian planning. The law obliges the duty to work out the nationwide crisis management plan and the same plans on the level of the region, district and municipality. These plans also include the characteristic of threats and risks in relation to the critical infrastructure, the procedures for solving tasks connected with the protection of the critical infrastructure and the tasks in the area of protection and recovery of the critical infrastructure. The law furthermore states the adoption of the national programme of the critical infrastructure protection. There are concretised duties for the heads of the regions, the mayor and the head of the municipality councils who are to organise the fulfilment of tasks in the area of the critical infrastructure protection. The structure, processing and updating the plans for the critical infrastructure protection is stated by the decision of the Council of Ministers from 30th April 2010.

CONCLUSION

The task of every state is to ensure the required level of the external as well as internal security. This task is fulfilled by a whole range of the specific measures of the state administration which creates the security system of the state and participates in realising the measures ensuring a continuous increase of the inhabitants´´ standard of living. The infrastructure of the country creates conditions for fulfilling the needs for life of the citizens and improves the life comfort. The disruption of the transport systems, interruption of energy supplies or supplies of food and water can be caused by the natural but also anthropogeneous factors. Due to them especially in the towns there can arise serious crisis situations which the state has to solve effectively and as quickly as possible. The European Union has been emphasising especially during the last decade the necessity to select and secure that part of the infrastructure which is the most important for the state as well as the citizens. The Slovak Republic began to deal with the area of the critical infrastructure only during recent years and for the time being it has a whole range of unsolved problems which affect the method and quality of ensuring the critical infrastructure operability. Solving these issues in the nearest future is the task of the state administration as well as the scientific and research institutions. The Faculty of Special Engineering would like to participate actively in fulfilling these tasks.

BIBLIOGRAPHY AND INFORMATION SOURCES

[1] BECKER, H.S. 1996. The Epistemology of Qualitativeresearch. In: JESSOR, Richard, COLBY, Anne, SCHWEDER, Richard (eds.). Ethnography and Human Development. Chicago: University of Chicago Press, s. 29-37. ISBN 0-226-39902-8

[2] BORRADORI, G. 2005. Filosofie v době teroru. Karolinum, Praha 2005. 188 s. ISBN 80-246-0907-X

[3] BUZAN, B., WAEVER, O., DE WILDE, J. 2005. Bezpečnost: Nový rámec pro analýzu.

Brno: Centrum strategických studií. ISBN 80-903333-6-2
[4] FRANK, L.: *Bezpečnostní prostředí České republiky* [on-line]. [cit.24.11.2011]. Dostupné na: http://www.mocr.army.cz/mo/obrana_a_strategie/1-2003cz/frank.pdf
[5] LAML, R.: 2008. Niekoľko poznámok k definícií bezpečnostného prostredia v Bezpečnostnej stratégií SR. Fórum pre medzinárodnú politiku. Mepoforum.sk
[6] LASICOVÁ, J. 2006. Bezpečnosť: Bezpečnostná agenda súčasnosti. Univerzita Mateja Bela v Banskej Bystrici, Fakulta politických vied a medzinárodných vzťahov. ISBN 80-8083-352-4.
[7] PROCHÁZKOVÁ, D.: *Bezpečnost je základní prioritou současnosti* [on-line]. [cit.24.11.2011]. Dostupné na:
[8] http://www.cemc.cz/aspekty/vyber_z_clanku/rizeni/dokumenty/11.pdf
[9] PROCHÁZKOVÁ, D.: *Komplexní pohled na problematiku bezpečnosti* [on-line]. [cit.23.8.2011]. Dostupné na:
[10] http://aplikace.mvcr.cz/archiv2008/2003/casopisy/vs/0435/konz_info.html
[11] ŠIMÁK, L. 2006: Manažment rizík. Žilina 2006. 116 s. ISBN 80-88829-13-5
[12] ŠIMÁK, L., HORÁČEK, J., NOVÁK,L., NÉMETH, Ľ., MÍKA, V. 2005.: *Terminologický slovník krízového riadenia*, ŽILINA 2005, ISBN 80-88829-75-5
[13] ŠKVRNDA, F., PAWERA, R., WEISS, P. 2008. Medzinárodná bezpečnosť. Bratislava: Vydavateľstvo EKONÓM. ISBN 978-80-225-2527-5
[14] ZEMAN, P: *Česká bezpečnostní terminologie*. 1. vyd. Brno : Vojenská akademie v Brně - Ústav strategických studií, 2003
[15] Bezpečná Evropa v lepším světě – Evropská bezpečnostní strategie [on-line]. [cit.24.11.2011]. Dostupné na: http://consilium.europa.eu/uedocs/cmsUpload/031208ESSIICS.pdf
[16] ČSN EN 31010 Managementrizik – Techniky posuzovánírizik, UNMZ, Praha, 2011, 80s.
[17] Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany (2006). [on-line]. 19 s. Dostupné na: http://www.minv.sk/?ochrana-kritickej-infrastruktury
[18] Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike (2007). [on-line]. 24 s. Dostupné na: http://www.minv.sk/?ochrana-kritickej-infrastruktury
[19] Návrh stratégie vnútornej bezpečnosti EÚ: „Smerom k európskemu bezpečnostnému modelu“, Brusel, 2010
[20] Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschlad, Berlín, 2008, ISBN 978-3-934401-18-1
[21] Smernica rady 2008/114/ES, z 8.12.2008 o identifikácií a označení európských kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu. In: úradný vestník Európskej únie, L345/75-82
[22] Správa o vykonávaní Európskej bezpečnostnej stratégie – Zaistenie bezpečnosti v meniacom sa svete, Luxemburg, 2009, ISBN 978-92-824-2432-2
[23] STN ISO 31000 Manažérstvo rizika Zásady a návod, SUTN, Bratislava, 2011, 40s.
[24] Zákon NR SR číslo 45/2011 z 8. februára o kritickej infraštruktúre
[25] Zelená kniha, 2005 o európskom programe na ochranu najdôležitejšej infraštruktúry
[26] Nariadenie vlády ČR o kritériách pre určenie prvku kritickej infraštruktúry č.432/2010 Sb.
[27] Ustawa o zarządzaniu kryzysowym z dn. 26.04. 2007 r., Dziennikustaw z 2007 r., Nr 89, poz. 590, z 2009 r. Nr 11, poz. 59, Nr 65, poz. 553, Nr 85, poz. 716, Nr 131, poz. 076, z 2010 r. Nr 240, poz. 1600
[28] Határozatok Tára 2008. évi 31. szám. Kritikus Infrastruktúra Védelem Nemzeti Programjáról
[29] K.: . In: *Der Soldat,* Wien,
[30] Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Berlin, BMI, 2009, 20 s., Artikelnummer: BMI09324
[31] Grundstrategie des Bundesrates zum Schutz Kritischer Infrastrukturen, Bern, BABS, 2009, dostupné na:
[32] http://www.bevoelkerungsschutz.admin.ch
[33] Der Schutz kritischer Infrastrukturen: Gegenwart und Zukunft, CRN Report, Zürich, CSS ETH, 2010, 23 s.
[34] This work was supported by the Slovak Research and Development Agency under the contract No.APVV-041-10.

Miloslav Seidl, Ladislav Šimák
Faculty of Special Engineering of the University of Žilina, Slovak Republic
Miloslav.Seidl@fsi.utc.sk
ladislav.simak@fsi.uniza.sk