recipe 2015

Humanitarian Aid
and Civil Protection
ECHO/SUB/2014/696006

RESILIENCE OF CRITICAL INFRASTRUCTURE PROTECTION

GUIDELINES

RESILIENCE OF CRITICAL INFRASTRUCTURE PROTECTION

GUIDELINES

Source of co-funding: European Commission - Directorate-General for Humanitarian Aid and Civil Protection (DG ECHO http://ec.europa.eu/echo/).

In line with the Grant Agreement, the total Project value is € 408.675, with the co-funding of 75% (€ 306.506).

Funding instrument: Financial Instrument for Civil Protection - 2014 Call for Proposals for the preparedness and prevention projects.

EXCHANGE OF EXPERIENCE AND BEST PRACTICES

Varying levels of critical infrastructure protection in the relevant partner countries will enable the countries with developing or deficient critical infrastructure protection systems to profit from the achievements of the country boasting a developed critical infrastructure protection system such as the Kingdom of Sweden.

Best practices collected through RECIPE 2015 project are published in these Guidelines and will be implemented in each partner country. Instructions/Recipes on how to achieve a more efficient critical infrastructure risk management published in the Guidelines are also envisaged to help other and future EU Member States in their efforts to improve their own infrastructure protection.

RECIPE Project Team

CONTENTS

ABBREVIATIONS

CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
NPRD	National Protection and Rescue Directorate, Republic of Croatia
EU	European Union
ECI	European critical infrastructure
FB	Faculty of Security Studies University of Belgrade, Republic of Serbia
MSB	Swedish Civil Contingencies Agency, Kingdom of Sweden
NCCI	National Centre for Critical Infrastructure
PPP	Public-private partnership
RECIPE	Resilience of Critical Infrastructure Protection in Europe
VVG	University of Applied Sciences Velika Gorica

GENERAL PART

1. SUMMARY

Critical infrastructure is the backbone in the development of the contemporary societies; its deficient or inadequate protection may pose a threat to the national, regional and European security, economy and stability. Notwithstanding various efforts done by the European Commission and the Member States in this respect, there is no uniform level of development throughout the EU, nor is there consensus on the model of protection of the European critical infrastructure.

Since the state represents the central point in any critical infrastructure protection system, its biggest interest is that critical infrastructure, irrespective of the ownership structure of a critical infrastructure facility or network, operates uninterruptedly, thus ensuring smooth functioning of the community. From this perspective, it is necessary to raise the awareness and proper understanding of the importance of critical infrastructure within the strategic management of the state and its institutions. In fact, it is rather impossible to develop a functional critical infrastructure protection system if stakeholders are unaware of its criticality for the vital societal functions.

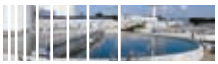
These guidelines are based on the experiences and good practices of the Kingdom of Sweden and other countries with developed protection measures of critical infrastructure, taking into account the situation in the Republic of Croatia and the Republic of Serbia. The guidelines are made with the aspect of further supporting the development of critical infrastructure protection in these two countries, as well as other countries that have just started or are about to start developing the critical infrastructure protection system, particularly the neighbouring countries. The guidelines are based on three areas of critical infrastructure protection, namely: Public-private partnership in the protection of critical infrastructure, Challenges and mechanisms of sensitive information exchange among the stakeholders in critical infrastructure protection system, and Setting preconditions for the development of national critical infrastructure centres.

ENERGY

COMMUNICATION AND INFORMATION TEHNOLOGIES

TRANSPORTATION SYSTEM

HEALTHCARE AND PUBLIC HEALTH



WATER MANAGEMENT

AGRICULTURE AND FOOD

FINANCE

CHEMICALS

PUBLIC SERVICES

NATIONAL MONUMENTS AND HERITAGE

SCIENCE AND EDUCATION

1.1. PROJECT RECIPE DESCRIPTION

Deficient or inadequate critical infrastructure protection may affect the national, regional and European security, economy and stability. Notwithstanding various efforts done by the European Commission and the Member States in this respect, there is no uniform level of development throughout the EU, nor is there consensus on the model of protection of the European critical infrastructure.

"Resilience of Critical Infrastructure Protection in Europe" (RECIPE) is a project co-funded by the European Commission - Directorate-General for Humanitarian Aid and Civil Protection and implemented in the Republic of Croatia, the Republic of Serbia and the Kingdom of Sweden, with the participation of the Consortium partners:

- The National Protection and Rescue Directorate, Republic of Croatia (project coordinator)
- University of Applied Sciences Velika Gorica,
- The Faculty of Security Studies of the University of Belgrade, and
- The Swedish Civil Contingencies Agency.

The project started on January 1, 2015, and will end on June 30, 2016. For more details visit the official website **www.recipe2015.eu**

The aim of the Project is to facilitate the establishment of a platform for exchange of experiences and best practices between experts and countries that have different levels of critical infrastructure protection development.

The main objectives are to develop several applicable and efficient models for:

- Public-private partnership in the field of CIP,
- Establishment of the mechanism for classified information/data exchange in the CIP system,
- Setting of preconditions for the establishment of National CI Centres.

This will be achieved through the improvement of communication and cooperation between relevant public and private sector stakeholders, more active involvement of the academic community as well as strengthening of the scientific research activities in the field of critical infrastructure risk management.

The Project includes four types of activities: panel discussions, joint workshops, the international scientific conference and follow-up strategy.

Four one-day **panel discussions** (two in Belgrade and two in Zagreb) analysed the current national legislation and practices, their strengths and weaknesses, possibilities for their improvement and the analyses of regulations and practices in the field of identification and interdependencies of critical infrastructures. This finally resulted in the National Standpoint documents which were used as the basis for **joint workshops** of international stakeholders for the exchange of their experiences and best practices. The results of joint workshops have been integrated in the present Guidelines for a better and more efficient critical infrastructure protection management. The obtained data, information and shared experiences were used to offer several different models for achieving all the aforementioned Project objectives, for the Republic of Croatia and for the Republic of Serbia respectively. The models were also included in the Feasibility Studies conducted by independent and neutral analysts. The results of the Feasibility Studies were used as specific guidelines/instructions in this document.

The Project Team expects that the **International Conference** will integrate all the results of the efforts made throughout the Project and provide conclusions for the Follow-up Strategy. The **Follow-up Strategy** will define the future activities and cooperation models in the CI management protection system related to the main objectives of the Project.

RECIPE 2015 Guidelines offer a collection of best practices related to the critical infrastructure protection system. The purpose of these instructions is to enable a more efficient critical infrastructure risk management and to help other and future EU member States in their efforts to develop and improve their own infrastructure protection.

The best practices collected throughout RECIPE 2015 Project are published in these Guidelines and will be implemented under adequate conditions in each partner country.

1.2. RESULTS OF JOINT WORKSHOPS

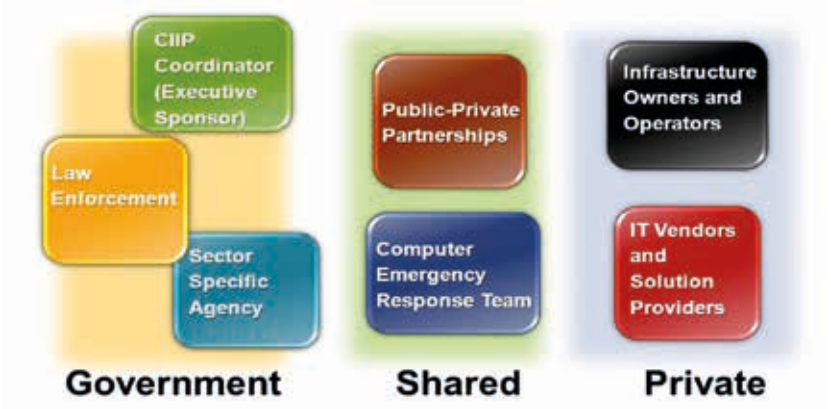
The first Joint Workshop of project partners, Serbian and international CIP experts was held on 13th of October 2015 in Belgrade, Republic of Serbia. The Second Workshop of the project partners and Croatian and foreign experts was held on 15 October 2015 in Zagreb, Republic of Croatia.

The aim of both workshops was to discuss National Standpoints created during and after the national Panel Discussions (June-September 2015), in order to fill in the potential gaps in the CIP system in Republic of Serbia and Republic of Croatia through the exchange of experiences and best practices presented by the international experts. The particular attention was placed on the presentation of the state and development of the CIP system in the Kingdom of Sweden.

The expected results were: "best practices shared", "recommendations provided", "awareness on more efficient solutions raised".

The discussion was mainly focused on three main project aims:

1. Public-private partnerships in the field of critical infrastructure protection,
2. Establishment of mechanisms for exchange of sensitive information/data among participants in the critical infrastructure protection system,
3. Establishment of preconditions for development of the national Centre for critical infrastructures.



1.2.1. SERBIAN WORKSHOP RESULTS

With regard to the definition, identification and legal regulation of the field of critical infrastructure in the Republic of Serbia, the Law on Critical Infrastructure would establish a regulatory framework for defining, identifying and protecting the national and European critical infrastructures in Serbia, whilst its bylaws should provide practical solutions and criteria for the identification and prioritization of critical infrastructure. The Action Plan for Chapter 24 in the Serbia-EU accession negotiations recognizes the Ministry of Internal Affairs of the Republic of Serbia as the authority responsible for the future Law. Within the Ministry of the Interior, the Sector for Emergency Management is the body that shall coordinate the activities on the establishment of an interdepartmental working group that will define the national CIP policy.

The future Law on CI, together with other laws relevant to the CI, should contain the provisions of the European Directive on the identification and designation of the European critical infrastructures and the assessment of the need to improve their protection (Directive 2008/114/EC). In this regard, it is necessary to make amendments in the CIP-related parts of the National Security Strategy of the Republic of Serbia, National Strategy for Protection and Rescue in the Emergency Situations and in the Law on Emergency Situations, to implement the existing Data Secrecy Law and to adopt the Law on Information Security (the work on its draft commenced more than three years ago), and the Regulation on Encryption and Cyber Security Strategy.

In the identification of critical infrastructure sectors and facilities, it would be desirable to start from the national level, and resist the temptation of making a list of sectors too broad and impractical. The next step would be to identify critical infrastructure facilities at lower levels, at the urban and local level. Preliminary identification and classification of critical infrastructure facilities may be done even before the law is adopted, provided the criteria and departmental sector analysis are defined. Another important thing will be to identify the "front desk" for the critical infrastructure issues. It should be kept in mind that, taking into account the economic situation in Serbia and its need to attract foreign investments, overregulating should be avoided.

There are varying experiences among the EU countries, related to the identification of CI sectors and facilities. As a matter of example, in Sweden and the Netherlands the critical infrastructure sectors (in Sweden - Vital

Societal Functions) and assets are identified at local, regional and national level, whereas in Italy there has not been official critical infrastructure identification and the main focus is on cyber security.

Similar differences can be observed in the field of threat, vulnerability and risk assessment. Sweden implements the all-hazard approach, but the focus is on crises and natural disasters, not on wars or political issues. In Finland, there is a tendency to delegate threat analysis to regional level, with the disturbances in electricity network identified as the biggest risk at the national level, followed by public health. Due to its geographical position below the sea level, the all-hazard approach is also prevalent in the Netherlands, with threat assessments being conducted both at the national and the regional level.

With regard to the public-private partnership in the field of CI resilience strengthening and protection, the Law on Public-Private Partnership regulates this area, but it does not explicitly mention the term 'critical infrastructure'. Even though the percentage of privately owned CI assets and facilities is still lagging behind the EU average, it is expected to grow in the coming period. There are still many gaps in provisions of this Law and its implementation that need to be addressed.

In the Southeast Europe, the awareness of all-hazard approach is at a very low level, especially in the private sector, which may represent a serious obstacle for the establishment of successful public-private partnerships (PPP). The strategic management in companies needs to take into account the privatization trends in the field of security. Unfortunately, all the countries in the region are always one step behind the multinationals and lag behind with the legislation. Non-compliance with the all-hazard approach could also be the cause of significant consequence of the disasters in the region and globally.

Significant problems are observed in the process of public procurement. Outsourcing of the private security companies reduces the expenses for the corporate security, but the choice based on the cheapest offer only creates additional problems. In addition, in some important companies and facilities (energy sector), corporate security is positioned low on the organizational ladder, and not recognized as important by top management, thus not having a say in the decision-making process.

In the process of CI risk management, PPP may encounter further obstacles, as the private owners and operators often have different perceptions, priorities and interests. The state needs to define the "skeleton of the basic threats/hazards" of which the CI operators will be in charge. For complex threats the state institutions should be engaged. The state can offer tax incentives for companies that perform safety and security activities well.

Public-private partnership can be a funnel through which the results of research and development projects and activities can reach operators and owners. The EU produces a lot of research in the safety and security field and it is difficult for everything to be implemented, so experimental capabilities are also very important for the projects. National governments need to ensure that operators act in line with the best available knowledge.

With regard to the establishment of the mechanisms for sharing of sensitive information within the Critical Infrastructure Protection system, it is often the question whether there is more harm if the information is not sent, and therefore useless, or sent and potentially shared with non-authorized parties. In Serbia, sharing of sensitive/classified data is regulated by the Data Secrecy Law which is often not implemented. However, it must be stressed that this is still a grey area in many developed EU countries and that there is an apparent lack of procedures and protocols.

There are varied experiences in other EU countries regarding the sharing of sensitive information. For instance, the Croatian legislation requires all information related to the critical infrastructure to be classified, which creates a number of problems, such as the identification of information and the obligation to obtain the security certificate to deal with sensitive information.

The classification of information and data must be done, but it may hamper the PPP arrangement and prevent the smooth flow of information. In Finland, there are four levels of confidentiality – state secret, secret, confidential and restricted. Business secrecies within companies can be marked as secret, confidential and restricted. There is no standardized corporate practice in this regard. In Finland and the Netherlands, some companies mark the information with colours – "traffic light protocol", which is a convenient, albeit "light" solution. Those sectors that do not use it simply rely on trustfulness of the people involved. The Netherlands' experience says that in sectors and facilities there should be designated

persons in charge of the information exchange, who will remain in the position for a long time, as trust takes time to be built.

Sharing of sensitive information is among the most problematic issues not only in Serbia, but even in the highly developed countries such as the Netherlands, Finland and Sweden, due to the lack of standard operating procedures and protocols. The trust between private and public sector will take time to be established, and it can be particularly problematic in cases where critical infrastructure assets are in foreign ownership.

With regard to the preconditions for setting up the national critical infrastructure centres, functionalities of the NCCI should be clearly defined as the first step, as it will make it easier to decide whether it should be established within an existing institution or as an independent body. The National Centre for Critical Infrastructure must have coordinating, consulting and research aspect.

The establishment of NCCI will need to be done in at least two phases. In the first phase, a centre will not be able to answer all critical infrastructure related issues, but it should connect the business, research and government sectors. In phase two, the wanted outcomes may be attained.

The newly established Directorate for Risk Management and Emergency Situations will at the beginning deal with all issues pertaining to critical infrastructure protection, but in the future this role may be taken by a separate National CI Centre.

1.2.2. CROATIAN WORKSHOP RESULTS

During 2013, the Republic of Croatia enacted the Critical Infrastructures Law, Ordinance on Methodology for Critical Infrastructure Operation Risk Analysis and Governmental Decision on Determination of sectors from which central government administration bodies identify national critical infrastructures and critical infrastructure sector ranking lists (11 sectors).

Community Acquis contained in the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of the European critical infrastructures and the assessment of the need to improve their protection have been transposed into the legislation of the Republic of Croatia through the Critical Infrastructures Law.

The aforementioned Law regulates the rights, authorities and obligations of the Croatian Government, central state administration bodies and the National Protection and Rescue Directorate as the system coordinator, as well as the authority, rights and obligations of the owners and managers of critical infrastructures in identification, determination and protection of national critical infrastructures and ensuring their business continuity. The need to protect them against all types of threats, ranging from natural and anthropogenic disasters to threats of terrorist activities is particularly defined. The Ordinance on Methodology for Critical Infrastructure Risk Analysis defines the risk analysis procedures, determines cross-sectoral

benchmarks (defined by the Law) and risk identification method, defines criteria for assessment of criticality, threat analysis and scenario development procedures, prescribes measures and criteria for identification of vulnerabilities and determines risk calculation methods.

The Law also stipulates that the central government administration bodies appoint a security critical infrastructure coordinator and a deputy for each critical infrastructure sector. purview, while the owners/managers of critical infrastructures shall appoint a security critical infrastructure coordinator who is responsible, in the course of critical infrastructure protection, for communication in security matters between the owner/manager and the competent central government administration body.

Despite the existence of a legislative framework, critical infrastructures in the Republic of Croatia have still not been identified and the need to protect them and ensure their continuous preventive operation as well as operation in emergencies has not been assessed, even though the deadlines given in the Law have been surpassed. Therefore, the critical infrastructure protection and management system in the Republic of Croatia is in its initial stage of development.

All significant changes require time for their implementation, and this is also true for the establishment and development of the functional system for strengthening of resilience and critical infrastructure protection in the Republic of Croatia. The RECIPE project has already, at this stage, proven to be very significant for the efforts made in the Republic of Croatia and confirmed that the Republic of Croatia is on the right track and should continue to follow it.

The workshops that took place in Zagreb confirmed the facts that the main aims of the project (Public-private partnerships in the field of critical infrastructure protection; Establishment of mechanisms for exchange of sensitive information/data among participants in the critical infrastructure protection system; Establishment of preconditions for development of the national Centre for critical infrastructures) are interrelated and complementary areas which cannot be viewed or developed separately, but need to be considered and worked on using a holistic approach. The aforementioned will be the course that the Republic of Croatia will continue to take.

With regard to the public-private partnerships in the field of strengthening of resilience and critical infrastructure protection, it was concluded that the representatives of the Republic of Croatia would try to strengthen the legal provisions of the critical infrastructure area in the Public-Private Partnership Law, as well as the public-private partnership in the Law on Critical Infrastructures. As far as the establishment of cooperation between public and private sector is concerned, it was suggested

to take the direction of establishing a platform based on which all interested stakeholders could take part, working on the "win-win" principle. Taking into account that the development and notions of social relations in south-eastern Europe are somewhat different from the similar societal norms in Sweden, the Netherlands and Finland, a pragmatic attitude was suggested in that the public sector, when establishing the cooperation with the private sector in the area of critical infrastructures should open, or offer certain "benefits" with the aim of finding common interests of cooperation.

In the part that dealt with the exchange of sensitive information, the attitude adopted was to investigate the possibility of using "HITRONet" communication network which serves to connect different public legal bodies through common computer-communication infrastructure. "HITRONet" is a multi-user and multi-service communication network of the Croatian Government.

The need to develop new protocols for the exchange of sensitive information was mentioned as the next step. Even though it was deemed that the Republic of Croatia has enough experts and knowledge for such a task, the international experience acquired through the RECIPE project will be very significant for the comparison of quality of national and international solutions. All participants supported further use of international standards and their increased integration in the solutions that the Republic of Croatia will need in the future.

With regard to the national Centre for critical infrastructures, out of four suggested organizational approaches in the National Standpoints of the Republic of Croatia, two were deemed as the most appropriate ones during the workshop: The Centre as the body of the Croatian Government, and the Centre as an organizational unit within the National Protection and Rescue Directorate. Both proposals are elaborated in more detail in order to serve as the foundation for the development of models and their comparison in the Feasibility Study which is an important part of the RECIPE project. The workshop participants confirmed the earlier stands stated in the National Standpoints about the duties that the Centre should be tasked with and agreed with the view that the Centre needs to be established and developed in phases and that the functionality comes before placement.

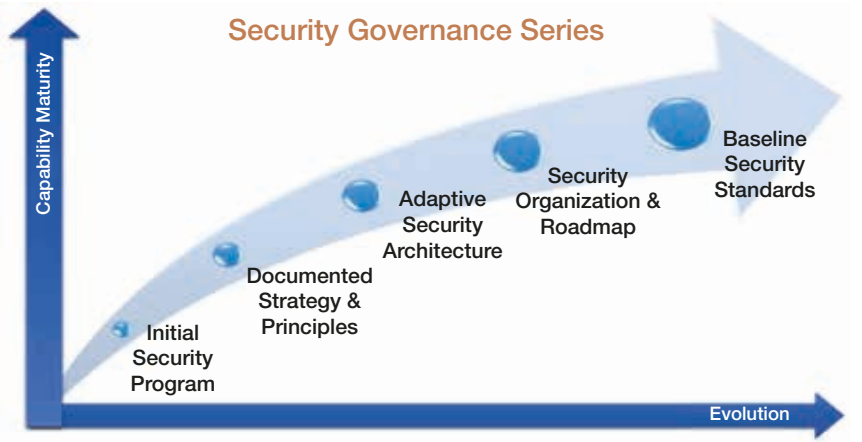
1.3. RESULTS OF THE FEASIBILITY STUDIES

The feasibility studies both for the Republic of Serbia and the Republic of Croatia were done on the basis of the national CIP models, submitted by the academic project participants, the Faculty of Security Studies University of Belgrade, the University of Applied Sciences Velika Gorica, and the National Protection and Rescue Directorate. The models were developed on the basis of international workshops held in Belgrade and Zagreb, which were attended also by experts from Sweden, Finland, Italy, Slovenia, Hungary, the Netherlands, Montenegro, Bosnia and Hercegovina, and the European Commission Joint Research Centre. In addition, once the results of the workshops were formulated, they were again discussed with the relevant national stakeholders, and the final results have been incorporated in the model.

The creation of an appropriate system of critical infrastructure protection constitutes an extremely demanding task for any country. Critical infra-

structure is, due to its basic mission to cover those parts of the system that are necessary for the normal functioning of the wider social community, very difficult to cope with. The complexity of the security environment and threats that arise for the functioning of this infrastructure put an extremely challenging task before the state, its bodies and CI operators themselves. The limited financial, human and organisational resources in the area of critical infrastructure protection constantly push the priorities of individual organisations or companies which manage critical infrastructure to the margins.

Critical infrastructure appeared in the EU as a term in the last twenty years. Terrorist threats, cyber-risk and natural disasters have set the need for setting CIP in the highest priority of the state regulation. Of course, it is necessary to realise that the system approaches to the regulation of such an area differ from country to country. The diversity in the perception of threats, past experiences, the soundness of the state structure and the degree of private ownership in the companies themselves which manage critical infrastructure is reflected through a variety of approaches and solutions carried out in this area by the individual states. This differentiation of approaches can also be seen at the European level, where it is very difficult to come up with coordinated actions in the field of the European critical infrastructure protection.



The Republic of Serbia and the Republic of Croatia belong to the group of countries where the organisation of the state and legal order stem from the European continental tradition. In this context, the state represents the central point for the regulation of relationships in terms of the authorities and responsibilities of the institutions in regulating individual social processes. These certainly include managing and ensuring continuous activity on strengthening of CIP system.

Surely, it cannot be said that both countries have zero experience with the provision of appropriate security environment for a continuous control of key buildings, institutions and processes which are necessary for the functioning of the social community. The fact is that a big part of the processes and activities that we know today under the definition of critical infrastructure protection was covered by other processes in the field of the protection of facilities important for defence operations, institutions and companies which were important for the society and have been subject to a specific statutory definition of organisations which, as a result of their activities, had to have mandatory protection. A lot of related processes can be found in the field of normative regulations which governed the field of civil protection and the management of the consequences of natural disasters.

All of this clearly indicates that there is no way to argue that both countries have no experience in the field of protecting key facilities, institutions and processes that are nowadays terminologically defined as critical infrastructure.

Not only in the Republic of Serbia and in the Republic of Croatia, but also in the majority of transition countries there has always been a mainly inadequate understanding of the term critical infrastructure and the process itself, which are brought together in their operation. A proper understanding of this process in relation to the system, which was until recently established in the transition countries, represented a key moment which with the correct understanding accelerated the system measures in the field of regulating critical infrastructure protection. Of course, during this transition period, due to the changes in socio-political relations directed to the market economy, in the extent of stakeholders that are important

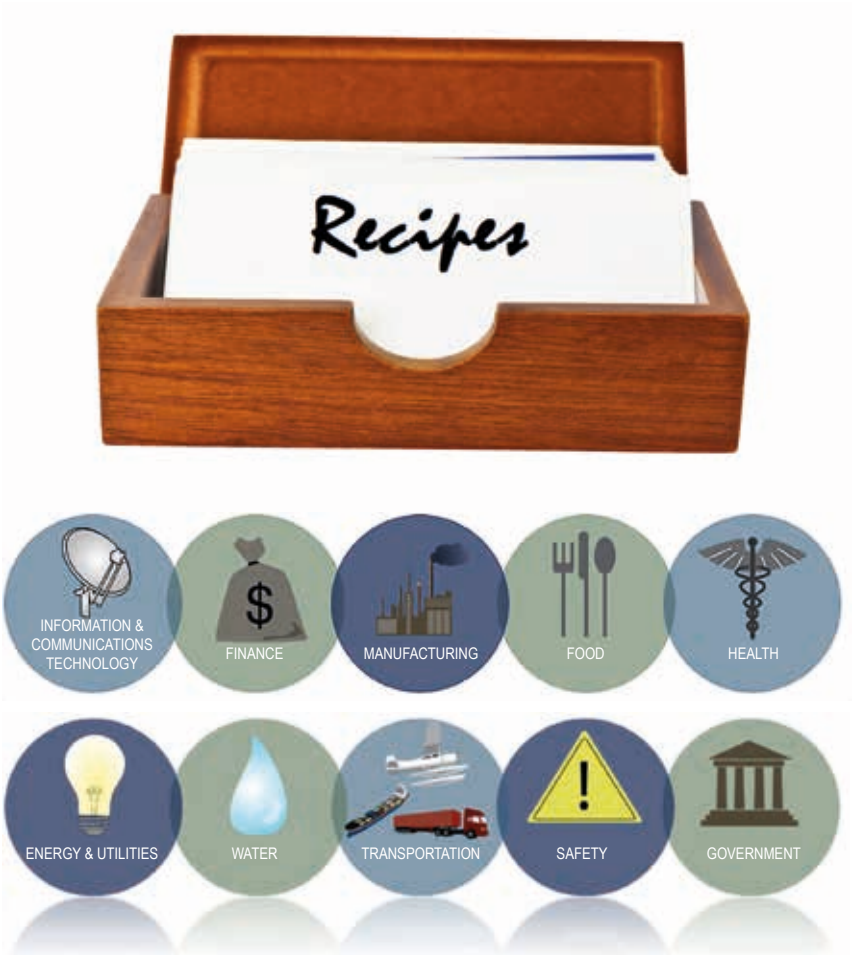
for the effective operation of the system of critical infrastructure, private capital appeared which is becoming one of the key factors in the ownership of companies which manage critical infrastructure. This represents one additional element which is crucial in the perception of changes in the system which was in place prior to the transition.

Due to the above mentioned, the processes and effective models of public-private partnership are the key to a successful system of critical infrastructure protection. The system of critical infrastructure protection can only be successful assuming a win-win combination, where all the stakeholders understand the positive aspects of the regulation of the critical infrastructure protection system, and are from this point on ready to invest the necessary efforts and other resources in building this system.

SPECIFIC PART

2. RECCOMENDATIONS

Since the Republic of Serbia and the Republic of Croatia are at different development levels of critical infrastructure protection system, further in the text certain recommendations will be presented for each country respectively. This can certainly be of use to all the countries that are only now establishing their own system or have recently started with the process, as well as provide other countries with the possibility of verifying whether some recommendations may serve as the supplement to their current mechanisms within critical infrastructure protection.




DIRE STRAITS
COMPAQ

2.1. ESTABLISHMENT OF THE PLATFORM FOR PUBLIC-PRIVATE PARTNERSHIP

The Project goal in this field has been identified as the establishment of a platform for public-private partnership related to the following points of interest: concept of cooperation, projects, security and improvement of the legal framework.

Establishing a proper system of public-private partnership in the area of critical infrastructure protection is a constantly ongoing process which practically never ends. However, this component is one of the utmost importance for the effective establishment and the functioning of critical infrastructure protection system.

Public-private partnership is among the key factors in the critical infrastructure protection process. In the majority of Western developed countries, around 80% of critical infrastructure is privately owned. Although there are no precise figures for Serbia, Croatia and Southeast Europe, that percentage is undoubtedly lower. However, the increase in the percentage of privately owned critical infrastructure facilities is expected, taking into account the global trends of market liberalization. In line with this, the recommendations are:

1. Taking into account the importance of CI for national and public security, stability and functionality of the state and the government, it will be necessary to broaden the existing legal framework related to the public-private partnership with the following provisions:
    - The concept of critical infrastructure should be incorporated in the Law on Public-Private Partnership, and the concept of PPP should be more strongly incorporated in the future Law on Critical Infrastructure as well;

- Adjust and simplify the procedure of submission and approval of public-private partnership project proposals, including small-value PPPs in the critical infrastructure protection field;
- Involve the state bodies (in particular the State PPP Commission, comprised of representatives of various ministries, including those that will be certainly recognized as competent and responsible for CI sectors) in the monitoring and control of public-private partnership CI related projects.

2. Taking into account the large number of critical infrastructure sectors and facilities and the experience of countries that have already adopted this paradigm, it is impracticable to equally protect and build resilience of all critical infrastructure facilities. In order to avoid this it would be necessary to prioritize already identified CI Private actors, primarily the owners and operators of the privately owned critical infrastructures, can provide a valuable contribution to this process.

   In the Southeast Europe, the awareness of all-hazard approach is at a very low level, especially in the private sector, which may represent a serious obstacle for the establishment of successful public-private partnerships. The recommendations are that it is necessary to work on the elimination of weak points, strengthen the measures of prevention and preparedness and interconnect the systems so that the entire community would be more resilient and better prepared for the risks to which it has been exposed.

   Big challenges are observed in the process of public procurement and outsourcing principles in the field of security. The recommendations are that, apart from raising the awareness about the importance of the process of critical infrastructures protection, it is necessary to also introduce the provisions that would stress the importance of a system comprising stricter and higher standards of delivering goods and services than in the case of regular procurement.

   In the risk management process, public-private partnership may encounter further obstacles, as the private owners and operators often have different perceptions. For instance, in Romania, the potential private owners and operators need to notify the government about their future ownership or management of the identified critical infra-

structure facilities, and the government has two months to give their approval. This example may certainly be a useful recommendation for the countries in transition, where the highest standards and norms of protecting vital national interests have not yet been established. Therefore, one could ask themselves a hypothetical question: 'If the state protects its frontiers and the territory against external threats, what does it do to protect its key infrastructures from being taken over on the stock markets by individuals or companies that are not friendly or in harmony with the national interests of the respective state.

In France, critical infrastructure assets (the French term being 'vital infrastructure') are narrowed down to a number that can be protected in a satisfying manner, and then public and private sectors work together on their protection.

In Finland, there are more than two thousand prioritized companies in the system. The Kingdom of the Netherlands does not have a Law on Critical Infrastructure, but despite this the area is managed well and successfully. They have determined 13 sectors in which it is possible to identify and designate the national critical infrastructure, and they have prescribed the quantification of criteria for the identification of critical infrastructure. Despite the non-existence of the Law on Critical Infrastructure, the cooperation among the stakeholders within the system is very good and carried out on the principle "networks and trust" (basic principle is "win-win situation").

Hungary has nine critical infrastructure sectors, half of which have been analysed. Within them, a little over a hundred facilities, networks or systems have been identified and designated as a national critical infrastructure.

Some countries legally oblige the operators to state how they engage security companies. Private companies want to implement their business-driven decisions and keep secrecy about as much information as possible. This is certainly a practice that needs to be considered thoroughly when referring to the countries in transition.

Since the private sector is engaged in direct benefit from the partnership, we recommend the "Business Continuity Planning" platform for their involvement. The following recommendations outline the direction that the public sector should take in order to stimulate the interest of the private sector in joint cooperation such as: provision of knowledge, experience and guidance; explanations and enhancements of elements of the information system and risk and threat warning system; advising on standardization and best equipment according to the information available to the public sector from the cooperation with other countries, international organizations and particularly with the EU institutions; opening of various networks and possibilities to the private sector; enabling the perception of vulnerability and resilience to risks and threats in space through standardized questionnaires to private companies; offers for joint education, trainings and exercises.

Moreover, public-private partnership can be a funnel through which the results of research and development projects and activities can reach the operators and owners. The EU produces a lot of research in the safety and security field and it is difficult for everything to be implemented, so experimental capabilities are also very important for the projects.

In developing strategic and legislative frameworks for public-private partnership it is necessary to ensure the widest possible participation of proposals. Hereinafter, it will be required, in addition to providing an appropriate level of awareness, to clearly define the authorities and responsibilities. This is an important basis for the establishment of long-term trust among all partners in the process of critical infrastructure protection in every country.

The practice has shown that there are different ways of realizing the cooperation between the public and private sectors in CIP, ranging from mandatory to voluntary participation. In case of voluntariness it is also necessary to clearly impose certain limits and arrangements in the functioning of the national forum for critical infrastructure protection. The

cultural dimension of the agreement on the important/sensitive information exchange, which will not be aimed at the general public, will also have major importance. This factor is of great importance and it is impossible to regulate it only by adopting certain legal frameworks under the Law on Public-Private Partnership or the Law on the Protection of Classified Information, or the protection of business secrets.

It is important to recognize that at least two of the key categories of information have been discussed, namely, the information that is essentially important for ensuring national security and on the other hand, the information that represent important business data in the business environment, which may reduce the competitive advantage of the company that manages critical infrastructure.

2.1.1. RECOMMENDATIONS FOR THE REPUBLIC OF SERBIA

The main recommendations address the following areas of activities: The concept of cooperation between the public and private sectors for strengthening the critical infrastructure resilience and protection; Establishment and improvement of the normative framework with the view of strengthening of CI protection and resilience; Identification and prioritization of CI using the mechanism of public-private partnership; Public-private partnership projects aimed at strengthening the critical infrastructure protection and resilience; Public procurements; Awareness raising, training and education.

The concept of cooperation between the public and private sectors for strengthening the critical infrastructure resilience and protection

Since the Law on Critical Infrastructure has still not been adopted in Serbia, first of all it will be necessary to clearly define what is understood under 'critical infrastructure', 'critical infrastructure protection' and 'resilience'.

Therefore, the first joint task of public and private sector will be raising the awareness among all stakeholders, especially among the CI owners and

operators. The main role in the awareness raising will need to be played by the academic sector and the state institutions, which are best acquainted with "good practices". During the critical infrastructure identification and prioritization, as well as during the drafting of CIP strategy or guidelines, the highest possible number of stakeholders needs to have their say, as otherwise "top-down" decisions may not be implemented in a satisfying way.

In order to achieve successful "bottom-up" approach, the national forum should be established as a platform for discussing all aspects of critical infrastructure identification and prioritization, critical infrastructure protection and resilience. The forum will consist of representatives of both public and private organizations and institutions. Provided the preceding steps have been completed, it will be necessary to establish the foundation of cooperation between the public and private sectors which includes the following:

Establishment and improvement of normative framework with the view of strengthening of CI protection and resilience

The establishment of normative framework is an extremely demanding work that will facilitate the regulation of a certain field, and in addition open the ground for further action, new ideas and models of implementation of legal regulations. In addition, normative framework should provide a stimulating approach for new investments and creation of new values.

First of all, reference here is to the adoption of Law on Critical Infrastructure that will regulate this field, as well as to bylaws pertaining to this law. Furthermore, this refers to amendments in other laws (Law on Public-Private Partnership, Law on Defence, Data Security Law, Law on Information Security, Law on Private Security, etc.) and strategic documents (National Security Strategy, Cyber Security Strategy, Strategy for Terrorism Prevention, Strategy of Socially Responsible Business...), directly or indirectly related with critical infrastructure protection and resilience, and also regulate public-private partnership in this field.

Identification and prioritization of CI using the mechanism of public-private partnership

After the critical infrastructure related law and bylaws have been adopted and the critical infrastructure sectors and facilities identified, the following step will be prioritization, as not all CI sectors and facilities are equally critical from the aspect of the disruption of their operations or interruption of supplies of goods and services.

Taking into account the large number of critical infrastructure sectors and facilities and the experience of countries that have already adopted this

paradigm, it has been concluded that it would be impracticable to equally protect and build resilience of all critical infrastructure facilities. Private actors, primarily the owners and operators of the privately owned critical infrastructures can provide a valuable contribution to this process.

Public-private partnership projects aimed at strengthening the critical infrastructure protection and resilience

Although public-private partnership is not an ideal model for all infrastructure projects, it is necessary to consider a joint action wherever possible and mutually justified. The construction of the missing critical infrastructure capacities, maintaining and improving the resilience of the existing ones, and the critical infrastructure protection, are easier to achieve through public-private partnerships in relation to the options of the public sector.

The public sector should aim at a larger, more innovative and long-term financing of infrastructure projects by the private sector, but also carefully consider the private the sector interest, in order to avoid the impression of unidirectional partnerships.

Public-private partnership projects facilitate transfer of risk from the public to the private sector. This approach brings benefits such as the development, modernization and maintenance of large infrastructure facilities through private funding.

Public procurements

Public and private sector in the field of CIP should work together on the improvement of public procurement practice, which has often been under the professional, academic and public scrutiny due to its deficiencies. Public institutions and private owners and operators of critical infrastructure should design the provisions for future Law on Critical Infrastructure and amendments to the existing Law on Public Procurements where public procurements in the field of critical infrastructure would be separately added, due to their importance for security and safety of the society and economy.

Awareness raising, training and education

Public institutions and private organizations (including public and private academic institutions) should work together on raising awareness of the concept of critical infrastructure and critical infrastructure protection among decision makers and general public. In addition, academic institutions, together with state institutions and in consultations with private sector, should create trainings and education activities (seminars, workshops, examinations, etc.) for critical infrastructure protection practitioners. In this field it will be important to keep up to date with international research and "good practices".

2.1.2. RECOMMENDATIONS FOR THE REPUBLIC OF CROATIA

The main recommendations address the following areas of activities: Public-private partnership projects; Development and improvement of methodology for identification of critical infrastructure; Training; Counselling; Exercises.

Public-private partnership projects

The mentioned proposal contains a suggestion to consider and implement the following three processes: 1.) Preparation and audit of the model of public-private partnership; 2.) Initiating projects of public-private partnership; 3.) Monitoring and supervision of the project of public-private partnership in CI protection. In the mentioned proposed processes, it is essential to include public-private partnership in the system; it is essential to include sectoral security coordinators and academic and research community among the participants. Although extreme connection between all three key priorities of the RECIPE Project has already been emphasised during project activities (workshops and panels), it also needs to be point out that the public-private partnership is considered to be most effective if the central point of its coordination is National Centre for Critical Infrastructure which represents the pivotal stronghold in the establishment of a high-quality and comprehensive Critical Infrastructure Protection system.

Development and improvement of methodology for identification of CI

The development of new approaches in the field of CIP and their introduction in the operational use must be a continuous and ongoing process. The dynamic security environment is constantly changing, which raises challenging dilemmas for the planners and developers of critical infrastructure protection. Four key processes that tackle the methodology for the

identification of critical infrastructure, cross-sectoral and sectoral criteria, methodologies for risk assessment and methodology for risk management are defined in the foreseen proposal. A real and effective methodology can significantly contribute to the reality of planning and defining the measures required to determine minimum standards and the critical infrastructure scope and the measures necessary for the implementation of critical infrastructure protection. All this is strongly linked to the planning and use of resources that need to be given to the operationalisation of plans and results. For all four proposed processes, it is recommended to include sectoral CI security coordinators as well as managers / owners of critical infrastructure.

Training

Training is one of the key segments of the success of each system. Staff potential is highly important for successful implementation of the processes. Hence, there is an urgent need to implement training for all levels and groups of staff involved in critical infrastructure protection. For this purpose, it is necessary to integrate various forms of training and use a variety of methods including e-learning. The changes in the dynamic security environment force us to update the training contents constantly. In this part, the recommendations refer to two key processes in which the emphasis needs to be placed on the integration of the participants and educational institutions as performers. Knowledge and experience transfer among a wide circle of expert public. Two processes in this part are of special importance: Training of CI security coordinators in sectors and training of managers / owners of critical infrastructure.

Counselling

Counselling is an added value which is introduced into the system of critical infrastructure protection. It is used for certain specific processes, when special knowledge which can be applied in a particular environment is required. Counselling is also provided to assist the CI security coordinators in the sectors as well as the management structure. Two key processes in this part are: Counselling of security coordinators in sectors and coun-

selling of managers / owners of critical infrastructure. It is of special importance, to include external experts in the processes, apart from other participants.

Exercises

Exercise is an added value that is introduced into the system of critical infrastructure protection and it is used where there is a need for special knowledge which can be applied in a particular environment. Through exercises, the preparedness and capacity of the various structures in the system of critical infrastructure protection could be tested and checked. Exercises induce direct practical training of theoretical procedures and foreseen plans. Exercises should be based on real situations, because the more e they get closer to reality, the more effective will be their results. In this regard two processes have been singled out: Implementation of exercises for CI security coordinators in CI sectors and implementation of exercises for CI managers / owners. In both processes it would be essential to include external experts, scientific research institutions, and other stakeholders in the CIP management system among participants.

2.2. ESTABLISHMENT OF MECHANISMS FOR EXCHANGE OF SENSITIVE INFORMATION/ DATA AMONG PARTICIPANTS IN THE CRITICAL INFRASTRUCTURE PROTECTION SYSTEM

In the era of informatisation, the protection of information plays an extremely important role in the systemic approach to risk management for the operation of critical infrastructure. In the field of information security linked to critical infrastructure, the holistic approach needs to include all the necessary steps to ensure the establishment and functioning of the system for the protection of sensitive data.

Therefore, in conceiving and establishing of the mechanism for sensitive information exchange, l three aspects of the functionality of such system should be taken into consideration:

- confidentiality of information, which means insuring that certain information could be available only to the authorized users and up to the level of classification of their authorisation;
- the integrity of information, so that their content and form cannot be changed without the approval of the information owner;
- availability of information, reflected in the possibility that authorized users could obtain adequate information on the site and at the point of time when it is needed.

The reason for this is the fact that the functioning of the entire critical infrastructure protection system is based on the consistent use of the information system. Any error, inconsistency and unreliability of the functioning of the information system implemented to protect the critical infrastructure, or the failure to satisfy all three mentioned security components may lead to disastrous consequences.

In order to achieve an effective protection against potential attacks on the critical infrastructure, or threat to the security of the information system in critical infrastructure protection should necessarily be considered. This implicitly leads to the fundamental requirement of preservation and continuous improvement of the information system security which is used for the sensitive information exchange in the field of critical infrastructure protection.

2.2.1. ESTABLISHMENT OF MECHANISMS FOR EXCHANGE OF SENSITIVE INFORMATION/DATA IN THE REPUBLIC OF SERBIA

In sharing of sensitive information, it is often the question whether there is more harm if the information is not sent, and therefore useless, or sent and potentially shared with non-authorized parties. In Serbia, the sharing of sensitive/classified data is regulated by the Data Secrecy Law which is oftewn not implemented. However, it must be stressed that this is still a grey area in many developed EU countries and that there is an apparent lack of related procedures and protocols.

The sharing and treating of sensitive and classified information is performed in accordance with the Data Secrecy Law ("Official Gazette of RS", No. 104/2009). The problems that Serbia is facing are reflected in the following shortcomings: the lack of horizontal and vertical connection of participants responsible for the protection of sensitive information, insufficient recognition of the importance of categorization of classified data and sensitive information, diverse procedures in the protection of personal and business data, lack of capacity for protection of sensitive information, an vague role of the Ministry of Construction, Transport and Infrastructure, lack of skilled personnel in the Ministry to deal with the critical infrastructure issues, the lack of permanent education of managers in the field of critical infrastructure and information protection, the lack of awareness of people in charge of the critical infrastructure of their own role in data and information protection, lack of knowledge of procedures for information and data sharing with other stakeholders, insufficient harmonization of data protection practices with international standards, etc.

The following suggestions are offered for overcoming the abovementioned shortcomings:

1. With a view to establishing the efficient exchange of classified and sensitive documents and data between the participants in the field of critical infrastructure risk management, as well as harmonizing the exchange procedures with owners/operators of

critical infrastructures, it is necessary to create "Standard operative procedure (SOP) for classified and sensitive data and documents".

2. For this purpose, we suggest the establishment of intersectoral working group of stakeholder representatives from the system of critical infrastructure protection and risk management.
3. Accelerate the process of inclusion of private security sector in the TETRA communication system and in the "112 Service".

The term 'sensitive information' in Serbia is not legally recognized, and it covers various forms of data regulated by different legal regulations. Sensitive information in Serbia can imply secret data (regulated by the Data Secrecy Law), personal data (regulated by the Law on Protection of Personal Data), or business/professional secrets (The Law on Protection of Business Secrets, regulations on intellectual property), etc.

The exchange of sensitive information in the CIP system will mostly deal with professional secrets, which does not enter the domain of secret data, so it will have to be regulated further – by amending the existing Data Secrecy Law and the Law on Protection of Business Secrets, respectively. The law that will be most relevant for critical infrastructure systems is the recently adopted Law on Informational Security. Article 6 of the Law identifies ICT systems of particular importance, which are related to the energy, transport and telecommunications infrastructure sectors. The Law also stipulates the establishment of the National and specific centres for security risk prevention in ICT systems (National and Special CERT). In addition, we recommend that the future Law on Critical Infrastructure or Strategy/Guidelines for critical infrastructure protection contains a provision concerning the definition and exchange of CIP related sensitive data.

Suggested channels for exchange of critical infrastructure protection related sensitive data are protected networks and paper communication.

The definition of critical infrastructure protection related sensitive information, channels and techniques of data exchange, as well as identification of persons who may have access to them should be discussed at the national forum which will gather both public and private stakeholders.

It is important that the exchange of sensitive information enters the future curriculum for critical infrastructure protection professionals' trainings and certification.

2.2.2. ESTABLISHMENT OF MECHANISMS FOR EXCHANGE OF SENSITIVE INFORMATION/DATA IN THE REPUBLIC OF CROATIA

In the Croatian legislation, most of the information related to critical infrastructure is required to be classified, which creates a number of challenges. The exchange of information may go through secret systems and channels, but which data will enter it, especially in cases involving public-private partnership, has until now remained unresolved. According to the Croatian Law, sensitive data are those data about critical infrastructure that are designated as classified in accordance with the special Law. In order to obtain access to them, both private and public sector personnel require security certificate which implies very long procedure. Therefore, a problem arises when one needs to transfer the information to another who does not possess the certificate. The recommendations in this part are directed toward the necessary simplification of the matters related to the sensitive data exchange. The owners of the data should not insist on unnecessarily high levels of data confidentiality in order to avoid blocking system. Certain recommendations in relation to the duration of issuing the security certificates could be given but this is an essentially security issue which is affected by a number of variables. Instead, the recommen-

dations are oriented towards rising of the general awareness of all the participants in the sensitive data exchange process about the method and conditions of the system functioning all the way to timely submission of the request for issuing of the security certificates.

The essential issue for the Republic of Croatia is whether it is even necessary to establish an information network for the exchange of sensitive information among stakeholders in the system due to a series of facts which are not immediately apparent such as: accreditation of such network, the issues of industrial security, the manners in which information circulate among all stakeholders, etc. These issues are important particularly because there are countries which, despite the existence of the information networks, still use the paper correspondence. Finland, for instance, is an example of such a functioning. The recommendations for a country like the Republic of Croatia which is setting up all the system functionalities should first consider the format of the information to be shared, paying less attention to the information confidentiality levels. Also, if Croatia opts for the establishment of the system, i.e. platform for sensitive data exchange, it is necessary to perform this in compliance with specific international standards such as ISO standards in the area of the exchange of sensitive information, which are currently being developed globally.

In the discussion about the concepts of sensitive data exchange, other experts have different opinions about the differences in the protection of sensitive information approach that belong to the domain of public and national security. On the other hand, the need to protect business information, which is the particular interest of the business sector, is not emphasized enough. The recommendation is that in the matters of sensitive data exchange, it is certainly necessary to focus on all the necessary sources of sensitive data, but not on some of them primarily. In this regard, it is necessary to highlight the example of the Republic of Hungary that has developed its own special software for the exchange of sensitive information among all stakeholders of the system.

The Croatian model of information security is based on the strategic and normative documents. The analysis of the existing legislation showed that

it contains all the necessary foundations which enable the practical establishment of the information system of transmission of key data in the field of the critical infrastructure protection.

Croatia has opted for the model of building a critical infrastructure protection system using the top-down principle. Eventually, wherever the National Critical Infrastructure Centre would be located (currently two possible solutions are being considered), the proposed organizational structure that is organized from the highest point is appropriate and expected. The highest strategic place is organizationally represented by the Government of the Republic of Croatia managing the system through the National Council and National Critical Infrastructure Centre, all the way down to the critical infrastructure managers as the lowest point of the system. The related requirements for the establishment of an information system are common, but include the necessary basis, which would allow the beginning of the establishment of the proposed information system. Since Croatia has limited financial resources that she could allocate to a larger extent for the establishment of an expensive sensitive data exchange system, the suggestion is to study in detail the practices of other countries and to use all the available financial instruments of realization – State budget of the Republic of Croatia and application for international funding.

When considering the technical solutions, special attention should be paid to the establishment of two-way independent parallel communication system which represents an appropriate way for achieving security and business continuity in the event of failure of certain communication channels. The encrypted form via the VPN protocol provides a sufficient level of security of data transmission according to their value and importance. Of course, it will be hereinafter necessary to define the level of encrypted solutions, which will also entail the choice of the technological solution that among other things will have to be compatible with the current system in use in the State Administration.

Among other requirements, it is particularly necessary to highlight the competence of the personnel that will be needed for the establishment of this system. The layout – the framework and content - of the training system of all participants in the CIP system is still missing. In part, this is defined below under the tasks of the National Centre for Critical Infrastructure.

In the context of the proposed tasks of the National Centre for Critical Infrastructure in the exchange of key data, the things are foreseen in the appropriate format. Most challenges, in addition to adequate financial resources, will be raised in the adequate definition of the information that will be eligible for the transmission through this information system. The recommendations suggest strict compliance to the definition of the information that is defined in the Law on the Protection of Classified Information and other related documents. This issue will definitely appear in that part of the information that defined by the strategic management as business secret in the companies (operators). This part can also lead to some challenges, due to the competitive relationship, where there will be more operators on the market that deal with the same or similar content. These challenges may result in deterioration of an appropriate public-private partnership and will be reflected on the quality of cooperation. Although the Republic of Croatia introduced a "top-down" approach in the introduction of the CI protection system, it is precisely this factor of public-private partnership that is very important and will also influence the introduction of the systemic exchange of the key data. For this reason, it is necessary to pay particular attention to these elements.

Further recommendations suggest formation of the National Centre for Critical Infrastructure within National Protection and Rescue Directorate and developing the sensitive data exchange system. This is contributed by the following positive indicators. NPRD already carries out a key part of tasks in the field of coordination and development of the critical infrastructure system in the Republic of Croatia. This has to be continued with even greater intensity in the future. The knowledge and experience acquired by the employees of National Protection and Rescue Directorate in the field of the establishment and functioning of the system of critical infrastructure will be the key generator of the skills necessary also for the future establishment and functioning of the National Centre for Critical Infrastructure and the related tasks in the field of the key data ex-

change. The National Protection and Rescue Directorate has developed certain segments of the information system, which will be in this case possible to upgrade to the corresponding whole. This has to be continued further. The legal basis in the field of the classified information protection and management of cyber threats is in Croatia quite properly set. Because of that, the recommendations are oriented to a small supplement in the field of systemic Law on Critical Infrastructure Protection. In the context of government administration institutions, a sufficient number of trained human resources operate in the field of information security, which will bear the focus on the completion of a secure information system for the transfer of critical information related to critical infrastructure protection. In this spirit, it is recommended to raise the level of knowledge and quality of all those engaged in these activities.

2.3. ESTABLISHMENT OF PRECONDITIONS FOR DEVELOPMENT OF THE NATIONAL CENTRE FOR CRITICAL INFRASTRUCTURES

Any system of critical infrastructure protection requires a central coordinating institution and a central point which brings together all the necessary processes in the field of critical infrastructure protection, in other words national CIP centre.

The RECIPE Project partners agree that functionalities of National CIP Centre, both in Serbia and in Croatia, should be clearly defined right from the start, in order to facilitate the decision later whether it should be established within an existing institution or as an independent governmental body. The partners also agree that National Centre for Critical Infrastructure must have both consulting and research aspect. Instead of simple information collection and distribution, the Centre needs to have capacities for their analysis and for supervision of the implementation of the Law on Critical Infrastructure at the national level. As a good example and potential model for the future NCCIs in the region, the partners recommend the United Kingdom Centre for Protection of National Infrastructure.

In Italy, there is no Critical Infrastructure protection Centre, but there is Civil Protection Centre and the Situation Room (Sistema) of the Civil Protection Department. A specific desk is dedicated to critical infrastructure operators who sit together with representatives of "Carabinieri", Institute for Earthquake Forecasting, Institute for Meteorology, etc. The Operative Committee is the body that ensures joint management and coordination during the emergency. It gathers when the Situation Room becomes a crisis unit and the calamity directly involves the Department of Civil Protection.

All the Project participants are convinced that National Centre for Critical Infrastructure protection is necessary for successful functioning of the critical infrastructure protection system and that it will be necessary to develop it in both countries.

2.3.1. RECOMMENDATIONS FOR THE REPUBLIC OF SERBIA

In line with the recommendations of Directive 2008/114/EC, there is a need for the establishment of the National Centre for Critical Infrastructure which would serve as the national contact point for the protection of European critical infrastructure. The National Centre would be legally responsible for activities in the field of critical infrastructure protection. In addition, the recent Law on Informational Security stipulates the establishment of National and Particular CERTS.

It is believed that the establishment of the National Critical Infrastructure Centre will need to be performed in at least two phases. In the first phase, the Centre will not be able to respond to all critical infrastructure related issues, but it should connect the business, research and government sectors by creating a National Forum or Experts Network comprised of critical infrastructure experts from the academic, institutional and corporate sectors, as an informal body. In phase two, a formalized structure – Centre, may be established with the fully operational functionalities.

The future National Centre for Critical Infrastructure needs to have operative, consulting, analytic and inspection aspects. The Operative department would issue directions and react in certain situations, whilst the Inspection department should have competences to issue sanctions. Aca-

demic community should be involved in the work of the National Centre as it can greatly help with research projects, exchange of good practices, strategic and "lessons learned" approach, creation of analyses, which has been the shortcoming of many Serbian institutions in the past couple of decades.

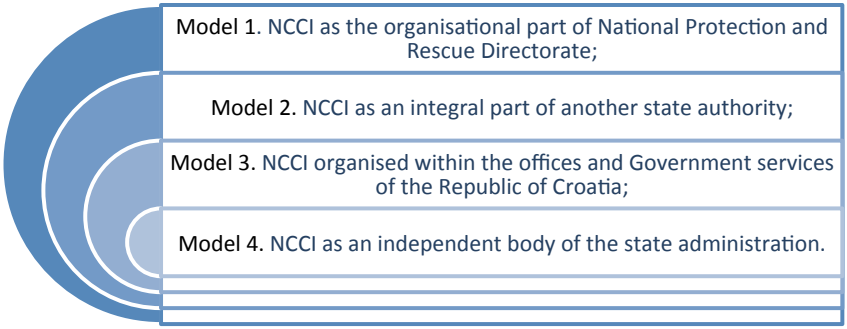
Instead of simple information collection and distribution, the Centre needs to have capacities for their analysis, as well as capacities for supervision over the implementation of the Law on Critical Infrastructure at the national level. National Centre for Critical Infrastructure should have the following functionalities:

- Coordination of CIP stakeholders and creation of the holistic CIP system;
- Coordination of critical infrastructure protection operations at national level;
- Coordination and monitoring of public-private partnership projects in the CIP field;
- Critical infrastructure and CIP related data collection, analysis and exchange;
- Review, harmonization and improvement of the relevant legal framework;
- Supervision of the implementation of the legal framework;
- Serving as the national contact point for the European Critical Infrastructure;
- Monitoring and guidance over the risk assessment efforts in various CI sectors;
- Monitoring and guidance of risk assessment, business continuity planning and security planning performed by CI owners and operators;
- Education and trainings in the field of CIP, together with other stakeholders;
- CI related emergency planning, preparedness and response.

Whether this Centre should be a separate agency or an organizational part of the existing state bodies remains an open question. However, an important milestone in this regard is the merging of the Office for Redevelopment and Flood Relief and the Sector for Emergency Management (a part of the Ministry of the Interior) as the Directorate for Risk Management and Emergency Situations, envisaged by the draft Law on Risk Management of Natural Disasters, which come into force from January 1st, 2016. National Centre for Critical Infrastructure could be organized as a department/sector of the Directorate for Risk Management and Emergency Situations, or just as one of its functionalities, at least in the beginning. Other options, such as the establishment of the National Centre for Critical Infrastructure as an independent government agency, a part of a relevant ministry (the Ministry of Interior or the Ministry of Construction, Transport and Infrastructure) or the Office of the National Security Council and Classified Information Protection would be less effective and more difficult to implement. There is a possibility that the Ministry for Emergency Situations is established, in which case the National Centre could be established under its jurisdiction.

2.3.2. RECOMMENDATIONS FOR THE REPUBLIC OF CROATIA

At the beginning of the RECIPE Project, the considerations related to the position of NCCI were within the frame of four possible solutions:



During the course of the project, all four possibilities were discussed and analysed. Discussion results identified two models as relevant, requiring

deeper analysis for further implementation, namely Model No. 1 and Model No. 3.

After thorough analysis, comparison and evaluation, the Feasibility Study has shown that the optimal development for the Republic of Croatia is within the proposed Model No. 1, i.e. National Centre for Critical Infrastructure as the organisational part of the National Protection and Rescue Directorate.

This conclusion is particularly supported by the fact that Model No. 1 would imply a continuation of the current systemic measures for the final regulation of the situation in the field of critical infrastructure protection. At this point, the rational deployment of the solution is a very important factor that greatly helps in supporting the decision, especially due to the fact that the Republic of Croatia is going through the important structural reforms, which will require a large amount of various resources, in order to increase the operability, suitability of coordination and other professional references, the rationality of investment for building this system will have a great influence on the choice of suitability. Through cost-benefit analyses, it is could be demonstrated that the input in this solution is a lot lower, and the results are as expected, much higher due to the continuation of the current processes as well as the existing resources. The next important factor favouring the Model No.1 is the analysis of processes, which shows that the critical infrastructure protection system is very much associated with the Civil protection system or protection and rescue system and disaster mitigation, or with civil protection system. In this context, the functions of the National Centre for Critical Infrastructure could very closely rely on those processes that are already running and are effectively tested within the National Protection and Rescue Directorate. This segment provides more effective and certainly more high-quality operation of the new organisational structure, which would be a logical continuation of already set bases. At the level of general activities and functions, it was recognized that the National Centre for Critical Infrastructure should be tasked with the following:

Gathering, analysis and exchange of information among stakeholders of the critical infrastructure risk management/protection – in this sense the Centre would be the central point for coordinating the network of security critical infrastructure coordinators in central state administration bodies and for coordinating critical infrastructure operators.

Proposing and drafting regulations in the area of critical infrastructure protection.

Supervising and directing identification and development of sectoral critical infrastructures risk analyses

Supervising and directing the course of development of risk analyses and security plans and plans for business continuity of owners/managers of critical infrastructures (operators) in cooperation with the state government administration bodies

Organizing education and exercises in the area of critical infrastructure protection, in cooperation with other stakeholders in critical infrastructure protection.

Establishing and functioning of a central point for planning, preparedness and response in emergencies in the area of critical infrastructure protection.

Coordinating and monitoring public-private partnership projects in the area of critical infrastructure protection.

NCCI would be the contact point for the European critical infrastructure.

Recommendations and suggestions for a National CIP Centre at the level of individual processes and their participants are the following:

Development and update of the normative framework of management

The current legislation is partially adequate and requires some amendments, especially if the chosen model for the organisation of the National

Centre for Critical Infrastructure is Model No.1. Within the mentioned proposal, altogether five processes are recommended that need to be implemented into the work of NCCI: 1) Adapting the changes and amendments of the Law on Critical Infrastructure

(It is essential to include public-private partnership in the mechanisms and to include managers of critical infrastructure among participants); 2) Proposing the changes and amendments to define critical infrastructure sectors (It is essential to include public-private partnership in the mechanisms and to involve the CI managers among the participants - without them an appropriate analysis which would imply the reality of legal provisions and their potential for practical implementations could not be carried out); 3) Proposing the changes and amendments to define critical infrastructure priorities list (taking account of public-private partnership in the mechanisms; when integrating critical infrastructure operators, one has to make sure that the priority is not affected by the narrow interests of critical infrastructure operators;); 4) Making changes and amendments to the Ordinance on methodology of Critical infrastructure business risk analysis (it is essential to include critical infrastructure operators); 5) Drafting and review of cross-sectoral criteria.

Coordination of stakeholders activities in the CI management system

In addition to the CI security co-ordinators, it is necessary to point out that effective coordination needs to be taken into account as one of the key segments for the effective transfer of information, as well as the CI operators. Public-private partnership has an extremely important role in this context.

Within this proposal, it is necessary to consider the implementation of the following four processes: 1) Coordination of work of the CI security co-ordinators at the National Protection and Rescue Directorate/NCIC. There is an urgent need to add common coordination of all coordinators among the cooperation mechanisms. Good mutual knowledge of coordinators can save many of the systemic problems in the field of communication and transmission of information; 2) Coordination of the activities of the CI owners/operators in the CIP process. This is one of the key

processes of strengthening public-private partnership; 3) Coordination of activities with other EU Member States; 4) Coordination of activities with the EU bodies.

Collection, analysis and information exchange

It is necessary to invite for participation the representatives of institutions responsible for the protection of classified information and cyber security in the Republic of Croatia. The establishment of appropriate system to share key information constitutes the major cost that can deter the strategic management from the intention to support the fulfilment of this task with the relevant resources. In this respect, four recommendations are given for the processes to be considered and implemented: 1) Database management on national and European CI. It will also be necessary to include security co-ordinators in the process of cooperation, in order to verify the relevance of the information in their areas of jurisdiction. This applies to international partners just as well, where a central coordination point confirms the suitability of the information for a particular country; 2) The development and upgrading of standard operating protocols for the exchange of key data (definitely add security sectoral coordinators, managers and international partners among the participants.); 3) The system for key data exchange management (definitely add representatives of the relevant state institutions among the participants, such as the Office for National Security and other authorities responsible for data protection and cyber security.); 4) Management of information security for key data exchange (the same as under item 1).

2.4. CREATING NORMATIVE AND STRATEGIC FRAMEWORKS IN STRENGTHENING RESILIENCE AND PROTECTION OF CRITICAL INFRASTRUCTURES

All project participants agreed on the necessity for the clear normative framework which will support the effective cooperation, exchange of information and protection of critical infrastructures by all stakeholders of the system. It was noted that certain countries, such as the Kingdom of the Netherlands, do not have a Law on Critical Infrastructures, but they have identified critical infrastructure sectors, identified and designated critical infrastructures, with the properly organized system of their protection. The Republic of Italy does not have a clearly defined national normative framework for determining national critical infrastructures, but they have legal provisions which envisage the identification, designation and protection of the European critical infrastructures.

For the successful outcome of the project, the experiences of the Kingdom of Sweden are especially valuable, as well as the consideration of the development of their critical infrastructure protection system. The Swedish emergency preparedness system is based on the principle of duty and responsibility and the need for mutual cooperation in order to minimize vulnerabilities and increase the capacities for action during emergencies. Accepting such an approach represents added value within the project.

The Swedish area of interest and activity is based on protecting the vital social functions and critical infrastructure, where multiple factors (development of national and international public policies, development and application of information and communication technologies, economic development, development of science and technologies, security issues, population and demographic issues and challenges, climate changes, globalization, privatization, efficiency, timeliness, etc.) are taken into account when considering the challenges. Such a broad picture and consideration of the areas of interest is definitely wider than the current discourse in the Republic of Serbia and the Republic of Croatia and will serve as a signpost, indicating the direction that needs to be taken in the future, once the conditions have been met. The observed system is based on three strategic

principles: System approach, All-hazards approach, Observation before, during, and after the occurrence of emergencies and disasters. The system has certain sectors and subsectors of vital social functions which need to be protected, so the prioritization of sectors has been determined.

For establishing a normative framework it is important to consider the space and time context, the mission and vision of each country, serving as the basis for setting up organizational implementation models.

2.4.1. RECOMMENDATIONS FOR THE REPUBLIC OF SERBIA

The field of critical infrastructure protection should be regulated by laws or some other binding legal documents as the topic is, by definition, of critical importance for the wellbeing of citizens and economy of the state. A specific Law on Critical Infrastructure should be in place in order to define, identify and protect the European and national critical infrastructure

sectors and facilities, as well as to offer the glossary of standardized critical infrastructure related terminology. In addition, bylaws would provide practical solutions and criteria for the identification and prioritization of critical infrastructure, as the first step.

The Law should designate the responsible bodies for the implementation of legal provisions and for taking legal measures against the stakeholders who do not comply with the law. In Serbia, the Sector for Emergency Management of the Ministry of the Interior is the body that shall coordinate the activities on the establishment of an interdepartmental working group that will define the national CIP policy.

The future Law on CI, but also other laws relevant to the critical infrastructure, should contain the provisions of the European Directive on the Protection of Critical Infrastructure (Directive 2008/114/EC). Consequently, it will be necessary to make amendments to the CIP-related parts of the National Security Strategy of the Republic of Serbia, National Strategy for Protection and Rescue in the Emergency Situations and the Law on Emergency Situations, implement the existing Data Secrecy Law and the newly adopted Law on Information Security (which stresses the importance of the energy, transport and telecommunication infrastructure), as well as adopt the Regulation on Encryption and the Cyber Security Strategy.

The bylaws to the Law should establish the criteria for identification and prioritization of critical infrastructure sectors and facilities. They should also provide a clear answer about who the "front desk" for the critical infrastructure protection and other critical infrastructure related issues is.

The Law should contain provisions related to the public-private partnership (in particular public procurement procedure) and exchange of sensitive information. Other relevant legal and strategic documents in this field (Data Secrecy Law, Law on Private Information, Law on Public Procurement, Law on Public Private Partnership, etc.) should incorporate the provisions and articles related to the critical infrastructure.

Finally, it should be kept in mind that, taking into account the economic situation in Serbia and its need to attract foreign investments, overregulation should be avoided.

2.4.2. RECOMMENDATIONS FOR THE REPUBLIC OF CROATIA

The need has already been recognized for the Republic of Croatia, and especially during the project it has been confirmed that the normative framework needs to be further developed and the development of the national strategy in the area of critical infrastructures and the corresponding action plan or national plan for the strengthening of resilience and protection of critical infrastructures needs to be considered.

The project has enabled the Croatian representatives to gain new insights into the best practices and the course of development of the critical infrastructure protection outside Croatia. Certain important notions such as public-private partnerships in the critical infrastructure protection and the area of national IT critical infrastructures are incorporated in the newly adopted strategic documents relating to national security – National Strategy for the Prevention and Suppression of Terrorism (Official Gazette, 108/15) and National Cyber Security Strategy and Action Plan for the Implementation of the National Cyber Security Strategy (Official Gazette, 108/15). Both documents were adopted at the beginning of October 2015, incorporating knowledge and experience also gained during the RECIPE Project.

The vision of the Croatian experts about the "top-down" approach to the building of the critical infrastructure protection system has been confirmed also through the Feasibility Study. The Study indicates that the "top-down" approach is the most appropriate at this point, as the country has to take, within its organisational levels, significant legal and substantial steps for the final establishment of an effective model of critical infrastructure protection. Understanding of this approach is particularly necessary in the phase of installing adequate regulatory frameworks for the operation of this system, and more importantly in the step of defining the criteria for determining critical infrastructure in specific sectors.

The Republic of Croatia has also stated in its strategic documents that it

ensures through various levels of national security mechanisms the implementation of its national interests and above all the establishment of a secure environment for their development. The National Security Strategy is currently in the phase of re-defining the strategic factors for ensuring national security. The area of critical infrastructure protection will in any case have to be re-introduced among other important areas. The importance of critical infrastructure protection is evident also from other legal and strategic documents which are directly or indirectly tied to the area of critical infrastructure. The most important statutory provision at the strategic level is certainly the Law on Critical Infrastructure. It needs to be stressed, though that the Republic of Croatia has some difficulty with direct implementation of the accepted legal solutions into practice. In certain parts, legal provisions are only partially implemented.

However, this is a factor that is characteristic of most countries in transition. There are several reasons behind this and the most obvious one is that the adoption of the Acquis has required very extensive adaptations and changes in legal solutions, but there was not enough time and resources for the full implementation of the statutory system requirements. An important factor could certainly be found in political environment and (the lack of?) direct awareness of the importance of critical infrastructure protection for the smooth functioning of the wider community. Strategic management of companies and the ruling policy enable the proper operation of critical infrastructure, with the whole series of challenges posed by the difficult environment, difficult to put on very important places on the list of their priorities. However, the objectives pursued by the proposed model of operation of critical infrastructure protection are realised in the important part.

In order to improve the normative framework and its implementation, the following provides recommendations for the Republic of Croatia that are also applicable for any countries that are currently in a similar situation as to the development of their normative frameworks. It will serve as a reference point for the countries such as the Republic of Serbia that will soon have to deal more actively with the establishment of a normative framework in the CIP field. As for the countries that have a longer-lasting practice in this field, it can serve as a reminder of the ideas to be re-considered.

Identification of critical infrastructure

Given the fact that CI identification process has not yet been fully implemented in the Republic of Croatia, it represents one of the critical processes for the effectiveness of the establishment of a comprehensive system of critical infrastructure protection. The proper definition of the criteria and the setting of the national and European critical infrastructure protection require the cooperation of all parties concerned. In this regard, it is necessary to re-emphasise public-private partnership that is adequately strengthened through these processes. Within this proposal, the recommendations suggest the implementation of additional three processes, apart from those that have already been normatively organised / stipulated in the Republic of Croatia:

1) Validation of the designed cross-sectorial criteria in the process of identifying critical infrastructure (it is essential to include public-private partnership and managers of critical infrastructure into the mechanisms.);

2) Proposing European critical infrastructure in the Republic of Croatia (including public-private partnership, CI managers and the competent authorities of neighbouring countries

3) Supervision over the implementation of cross-sectorial criteria (including methods of control, counselling and evaluation and demonstrations of good practices among the mechanisms. It is essential to include the CI managers among the participants.).

Risk Assessment

In the context of this proposal, two processes are anticipated to adequately assess the risks to the continuous operation of critical infrastructure. This process is of utmost importance for the solid foundations and functioning of any system. The risk assessment related to continuous operation of critical infrastructure is the basis from which all the necessary systemic measures for the proper risk management subsequently derive. Two basic processes that are geared towards sectoral coordinators and CI managers are planned for that. It should be understood that these processes are very closely related, and it is impossible to run them separately. The mentioned processes are:

1) Control and guidance of sector risk assessments in the National Protection and Rescue Directorate (transmission of guidelines and standards and good practices in the mechanisms has great importance, just as consultancy, evaluation and participation of representatives of relevant institutions and other experts.);

2) Control and guidance of making security plans of owners / operators of critical infrastructure in cooperation with the National Protection and Rescue Directorate (it is essential to include public-private partnership in the mechanisms also with transmission of guidelines and standards and good practices, monitoring and evaluation).

Monitoring and verification

In the context of this proposal all the necessary processes for the proper monitoring and checking the condition of the field of critical infrastructure protection are provided for. Annual reporting and analyses on the state of the national and European critical infrastructure are essential indicators for the upgrading of the integrity of the system and monitoring the situation. The legislative and executive branches of authority provide relevant data to enable control of the efficiency and functioning of the comprehensive system of critical infrastructure protection. The mentioned processes are: 1) Making an annual report on the number, criticality and carried out dimensions of critical infrastructure protection; 2) Making an annual report on the number of ECI by sectors and the number of interested countries that are dependent on certain critical infrastructure.

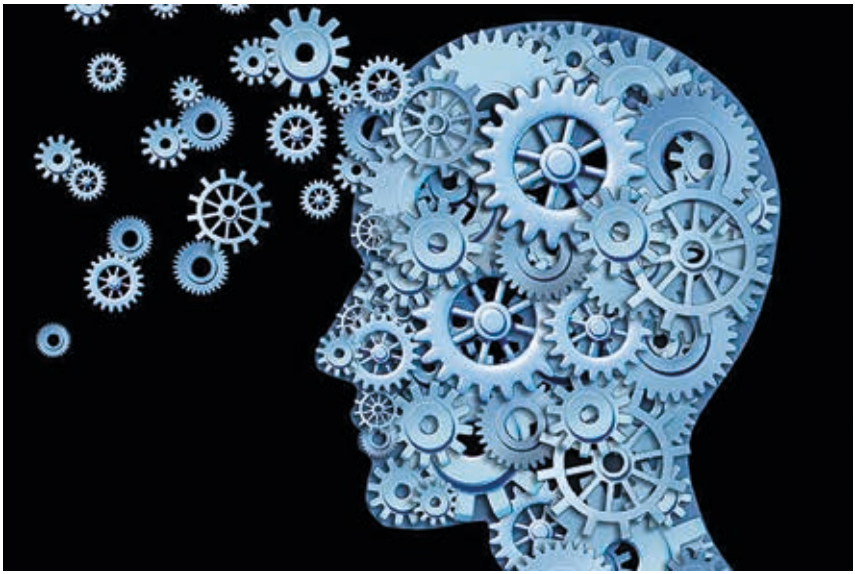
CONCLUSION

3. CONCLUSION

In the field of critical infrastructure protection, there are several "grey" areas that deserve particular attention due to the lack of uniform experiences and even "good practices", despite their importance for setting up of an efficient and functional CIP system.

First of all, what sectors, subsectors and facilities do we identify as critical? How broad and deep should we go? If everything is critical, then nothing is critical. From the experience of EU countries which have performed the identification, the number of sectors identified as critical is around ten.

Regarding ECI, Directive 2008/114/EC applies to two sectors - energy and transport. Most studies have shown that IT and finances have extremely high level of interconnectedness and interdependency with other sectors, so they should be included in the list.



As a large part of critical infrastructure is either owned or operated by private actors, it is necessary to establish a successful model of public-private partnership (PPP) in this field. First of all, it is of utmost importance that stakeholders are fully aware of all aspects of critical infrastructure protec-

tion, educated and fully trained for the implementation of protection and resilience measures and activities.

The most efficient way to attain this would be to involve private sector in critical infrastructure protection related decision and strategy making from the very beginning. Therefore, there should be two-way communication and cooperation between state institutions and academia on one side, and on the other side critical infrastructure owners and operators. Well educated critical infrastructure owners and operators will also create better and more robust public procurements.

The establishment of the proper model of the public-private partnership is a key dimension for the successful establishment of a comprehensive and effective system of critical infrastructure protection in each country. Without having established this cooperation, all attempts are doomed to low-level performance and non-systemic measures which requires increased needs of investments.

Building a proper system of public-private partnership is a constantly ongoing process, which practically never ends. However, this component is one of utmost importance for the effective establishment of critical infrastructure protection system. In a process of making strategic and legislative frameworks in each country, it is necessary to ensure the widest possible participation of solutions and proposals. It will be required, in addition to providing an appropriate level of awareness, to clearly define authorities and responsibilities. This is an important basis for the establishment of long-term trust among all partners in the process of critical infrastructure protection.

Based on detailed analysis of all factors we suggest developing a National Centre for Critical Infrastructure as an organizational part of the existing state body which has already taken some activities in critical infrastructure protection. A strong argument for this is the fact that the input in this solution is a lot lower, and the results, however, expected to be much higher due to the continuation of the current processes. This recommendation is also confirmed by the analysis of processes that should be performed by the National Centre for Critical Infrastructure in general, which shows that the system of critical infrastructure protection is tightly associated with the protection and rescue system/civil protection system. In this context, the operation of National Centre for Critical Infrastructure can rely very closely on those processes that are already running and are effectively tested by the existing bodies.

The establishment of the National Centre for Critical Infrastructure may be carried out in at least two phases. In the first phase, a centre will not be able to address all critical infrastructure related issues, but will serve as a platform (formal or informal) to connect the business, research and government sectors. In phase two, all needed functionalities may be attained.

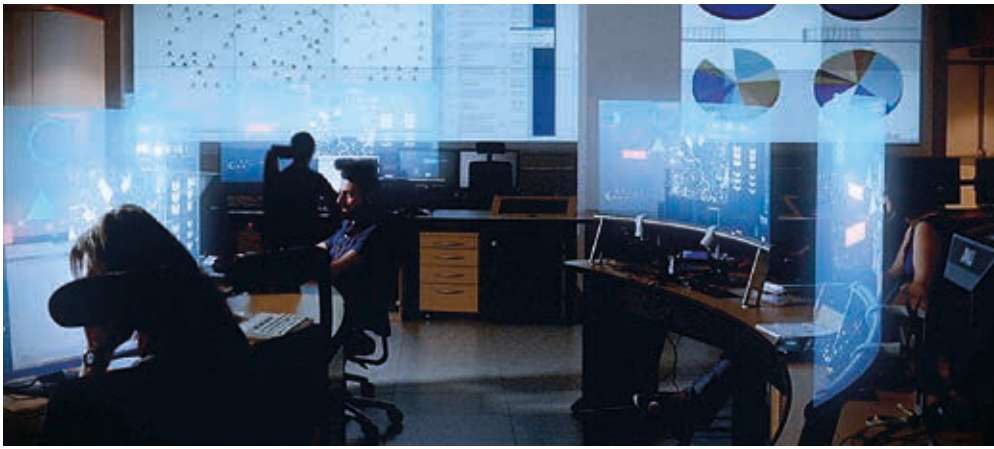
Considering the establishment of the National Centre for Critical Infrastructure, it is necessary to take into account that the exchange of sensitive information is a delicate subject not yet addressed in a satisfying and uniform manner. Information exchange among all stakeholders is extremely important for the functioning of the security system of critical infrastructures and it is one of its basic components, since the absence of data exchange leads to the absence of a functional system of critical infrastructure protection.

Generally, for the compliance with the stipulated classification and for achieving of efficient data exchange, the legal obligation of pronouncing all data related to critical infrastructure as classified should be considered and they should be categorized according to objective need of classification. This would simplify the data exchange system from the scope of critical infrastructures. Access to data for the exchange would be simplified for the data that objectively need not be classified. Thus, higher efficiency of critical infrastructure protection and risk management system would be achieved. Data that should be classified regarding their content would as such continue to be available only to those persons who need them in order to perform the activities related to critical infrastructure and they have to have the certificate for one of the secrecy degrees.

The information system that would be used for sensitive data exchange is in any case heterogeneous and encompasses several platforms: ICT, paper documents, courier transfer, etc. System that would rely only on one technological mode of CI sensitive data exchange is much more sensitive and less reliable than the implementation of several parallel and technologically different aspects. Therefore, in considering the practical solution for the organization and implementation of critical infrastructure, the sensitive data exchange should include and analyse all the technologically available approaches, and based on the risk assessment, a combined system with at least two technological levels should be selected.

For an integrated approach to establishment and improvement of the critical infrastructure sensitive data exchange, it is optimal to use the solutions based on international norms of information security, primarily

ISO 27001. This defines the recognizable concepts and approaches to the solutions of critical infrastructure sensitive data exchange, and as such they are necessarily harmonized with the national legislation. The implementation of this approach to the preservation of security of sensitive data exchange satisfies all the technological forms. Besides, this approach is fully compatible with the solutions of information security established by every contemporary serious business organization, regardless of the ownership and activity. The implementation of a security system of critical infrastructure sensitive data exchange based on this ensures proactive management and satisfactory degree of planned and achieved security.



Regarding several proposals of the organizational approach of critical infrastructure management system, the approach to security of critical information exchange is independent of the final solution which ensures full flexibility. For the solution of the exchange of sensitive data, the first and most important step is to define which data will be exchanged. Since the organization of critical infrastructure management is conceived as "top-down", the decision should be made whether all analytical data will be processed and stored in every critical infrastructure and only the results communicated and exchanged, or all the processing data will be kept in the central base. It would be rational to establish a distributed database system with analytics about the sensitive data in every critical infrastructure, and according to the vertical and horizontal communication and exchange, use the results in a defined form and level of classification.

Finally, since the Directive 2008/114/EC stipulates the existence of contact points for critical infrastructure protection in each country, it would be important to set up a National Critical Infrastructure Centre in all Member States and neighbouring countries. Its position in the organizational structure of the national critical infrastructure protection system may vary, but it is important that such centres have at least similar functionalities – coordination, consultation and research – as a minimum.

duzs
DRŽAVNA UPRAVA ZA ZAŠTITU I SPAŠAVANJE

[ФБ]
УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ
UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

VELEUČILIŠTE VELIKA GORICA
UNIVERSITY of APPLIED SCIENCES VELIKA GORICA

MSB Swedish Civil Contingencies Agency