NATIONAL STANDPOINTS

Project - Resilience of Critical Infrastructure Protection in Europe (RECIPE)

Financed through Union Civil Protection Mechanism, prevention and preparedness projects in the field of civil protection and marine pollution 2014

Date of update: 24 August 2015

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

TABLE OF CONTENTS

ABBREVIATIONS/ACRONYMS

DUZS	National Protection and Rescue Directorate
DG ECHO	Directorate General for Humanitarian Aid and Civil Protection of the European Commission
EU	European Union
EC	European Commission
ISMS	Information Security Management System
CI	Critical infrastructure
NCIC	National critical infrastructure centre
RECIPE	Resilience of Critical Infrastructure Protection in Europe
CSAB	Central state administration body
ISMS	Information Security Management System
VVG	University of Applied Sciences Velika Gorica

1. PROJECT SUMMARY

Project coordinator: National Protection and Rescue Directorate

Project partners:

- University of Applied Sciences Velika Gorica
- University of Belgrade, Faculty of Security Studies
- Swedish Civil Contingencies Agency

Area of implementation:

- Republic of Croatia
- Republic of Serbia
- Kingdom of Sweden

Objective of the project: Strengthening resiliency of critical infrastructure protection systems at national and European levels through improvements to methods of management and critical infrastructure protection.

Source of co-financing: European Commission – Directorate General for Humanitarian Aid and Civil Protection (http://ec.europa.eu/echo/).
In accordance with the Grant Agreement, value of the Project amounts to 408.675 €, with the co-financing rate of 75% (306.506 €).

Financing instrument: Civil Protection Financial Instrument – Call for proposals 2014 for prevention and preparedness projects.

Duration of the project: 1 January 2015 – 30 June 2016

2. PURPOSE AND OBJECTIVES OF THE PROJECT

Failure of functioning of the fundamental support systems of our society such as energy, transport, daily consumables such as food and water, financial and healthcare system – to list only a few of them – involves a possibility of widespread harmful effects on:

- ✓ Well-being of population and environment
- ✓ Functioning of industry and the economy
- ✓ Liberty and ability of governments to function and operate

The field of critical infrastructure protection is one of key priority areas of the European Union. From the point of view of the European Union, the critical infrastructures are defined as: "An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions[1]." Croatian definition reads as follows: "National critical infrastructures are systems, networks and structures of national importance whose cessation of operation or cessation of delivery of goods or services might have serious consequences to national security, human lives and health, property and environment, safety and economic stability and ongoing functioning of government[2]."

In 2013, the Republic of Croatia adopted regulation in the field of critical infrastructure protection, specifically: Critical Infrastructures Act, Ordinance on methodology for critical infrastructure operation risk analysis and Decision on determination of sectors from which central government administration bodies identify national critical infrastructures and critical infrastructure sector ranking lists[3].

In May 2014, a Consortium consisting of partners from the Republic of Croatia, the Republic of Serbia and the Kingdom of Sweden participated in an European Commission call for proposals for prevention and preparedness projects in the field of civil protection and unexpected marine pollution, submitting a project proposal in the field of critical infrastructure protection called "Resilience of Critical Infrastructure Protection in Europe", abbreviated as RECIPE.

Implementation of the Project is performed in the Republic of Croatia, the Republic of Serbia and the Kingdom of Sweden, and project implementation partners are: National Protection and

---

1 Article 2 of the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345/75, 23.12.2008).

2 Article 3 of the Critical Infrastructures Act (Official Gazette, number 56/13).

3 Critical Infrastructures Act (Official Gazette, number 56/13); Ordinance on methodology for critical infrastructure operation risk analysis (Official Gazette, number 128/13); Decision on determination of sectors from which central government administration bodies identify national critical infrastructures and critical infrastructure sector ranking lists (Official Gazette, number 108/13).

Rescue Directorate as the coordinator, University of Applied Sciences Velika Gorica from Velika Gorica, University of Belgrade, Faculty of Security Studies from Serbia, and Swedish Civil Contingencies Agency. The project was launched on 1 January 2015, and it is scheduled to end on 30 June 2016. Project website www.recipe2015.eu.

Since critical infrastructures comprise the mainstay of development of the modern society, their inadequate or inappropriate protection represents a challenge both to national as well as security, economy and stability of the European states and the European Union as a whole. Despite efforts of the European Commission and the Member States, there is no unified degree of development or consensus regarding methods of protection of European critical infrastructures at the level of the European Union.

The purpose of the RECIPE project is to facilitate establishment of a platform for exchange of experience and best practices among professionals and states currently at different levels of critical infrastructure protection.

The above is planned to be achieved through: improvements to communication and cooperation among relevant public and private sector stakeholders, more active involvement of academic community as well as strengthening of scientific and research activities in the field of critical infrastructures risk management.

The main objectives and interest of the partners in this project is to develop several applicable and efficient models for:

- ✓ **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**

Approach to the project task and expected results

Resilience of Critical Infrastructure Protection in Europe project is divided into four components/activities, specifically:

- ✓ Panel discussions (performed in the first half of 2015)
- ✓ Joint workshops (planned to be performed in the second half of 2015)
- ✓ An international scientific conference (planned to be performed in the first half of 2016)
- ✓ Follow-up strategy

In June 2015, two single-day panel discussions were organised – two in Zagreb and two in Belgrade – which served as the basis for shaping of national standpoints towards assessment of

current national legislation and practice, their bases and shortcomings as well as opportunities for improvement and an analysis of regulations and practice in the field of identification and interdependence of critical infrastructures in relation to requirements laid down in Council Regulation 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

The joint workshops by the project partners – where participants shall exchange experience and good practice based on the national standpoints formed at the panel discussions, which should ultimately result in Instructions/Guidelines for better and more efficient management of critical infrastructures.

The international scientific conference shall bring together the achieved results and provide conclusions for development of critical infrastructure protection policies in general, with an emphasis on public-private partnerships in the field of critical infrastructure protection, establishment of mechanisms for exchange of sensitive data/information among participants in the critical infrastructure protection system and establishment of preconditions for development of a national Centre for critical infrastructures in the Republic of Croatia and the Republic of Serbia.

Further forms of cooperation and solutions for other needs in the critical infrastructures management system shall be defined through the follow-up strategy, for example education and training.

Overall expected results of the project are:

- ✓ Easier exchange of knowledge and experience between countries
- ✓ Increased awareness of risks threatening critical infrastructures
- ✓ Increased disaster event prevention knowledge base
- ✓ Improved communication among national and international stakeholders
- ✓ Strengthened mutual support and cooperation among all relevant public and private sector partners
- ✓ Increased scientific and research activity in the field of critical infrastructures risk management
- ✓ Guidelines for establishment of optimal critical infrastructures risk management systems in partner states
- ✓ The guidelines are made available to the European Commission for further dissemination and use.
- ✓ Increased resilience and level of protection of European critical infrastructures as a result of improved coordination and cooperation among the stakeholders
- ✓ Established methodology for assessment of system protection based on a systematic approach

- ✓ Defined long-term strategy for critical infrastructures management in the encompassed states
- ✓ Defined needs for further education and training of public and private sectors (education programmes, exchange of professionals)

3. ANALYSIS OF THE EXISTING SITUATION

In 2013, the Republic of Croatia enacted the Critical Infrastructures Act, Ordinance on methodology for critical infrastructure operation risk analysis and Decision on determination of sectors from which central government administration bodies identify national critical infrastructures and critical infrastructure sector ranking lists. Community acquis contained in the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection has been transposed into the legislation of the Republic of Croatia through the Critical Infrastructures Act.

The aforementioned Act regulates rights, authority and obligation of the Government of the Republic of Croatia, the National Protection and Rescue Directorate and the central state administration bodies, as well as authority, rights and obligations of owners and managers of critical infrastructures in identification, determination and protection of national critical infrastructures and ensuring their continuous operation. 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 operation risk analysis defines risk analysis procedures, determines cross-sectoral benchmarks, risk identification method, defines criteria for assessment of criticality, defines threat analysis and scenario development procedures, prescribes measures and criteria for identification of vulnerabilities and determines risk calculation methods.

The Government of the Republic of Croatia has determined eleven (11) sectors where national critical infrastructures are identified, authorised the National Protection and Rescue Directorate to monitor, assess threats and propose operational and other measures to assess criticality and propose measures for critical infrastructure protection and management.

Central government administration bodies appoint a security coordinator for critical infrastructure and his deputy for each critical infrastructure sector in its purview, while owners/managers of critical infrastructures are required to appoint a security coordinator for the critical infrastructure 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 existence of a legislative framework, critical infrastructures in the Republic of Croatia are not identified at the moment and the need to protect them and ensure their continuous preventive operation as well as operation in emergencies has not been assessed. Therefore the critical infrastructure protection and management system in the Republic of Croatia is in an initial stage of its development. Considering insights into the above process gained by now, it may be assumed with a high degree of confidence that the Government of the Republic of Croatia shall

certify a specific number of critical infrastructures, proposed by competent central government administration bodies, at the time of performance of this project which shall certainly provide an additional impetus and discourse of action to the RECIPE project stakeholders.

4. PUBLIC-PRIVATE PARTNERSHIPS IN THE FIELD OF CRITICAL INFRASTRUCTURE PROTECTION

Summary

The objective of the project is to establish a platform for public-private partnerships in the field of strengthening of resilience and critical infrastructure protection, which shall provide logic and principles for the following areas of interest: cooperation concept, projects, security and improvements to the normative framework.

Introduction

"Public Private Partnerships (PPPs) can provide effective ways to deliver infrastructure projects, to provide public services and to innovate more widely in the context of these recovery efforts" reads the Communication from the European Commission on principles of developing public private partnerships[4]. It follows from the above that public private partnerships in Member States of the European Union are certainly a needed and desirable practice.

Within the meaning of Regulation No 1303/2013 of the European Parliament and of the Council of 17 December 2013[5], public private partnerships represent forms of cooperation between public bodies and the private sector, which aim to improve the delivery of investments in infrastructure projects or other types of operations, delivering public services through risk sharing, pooling of private sector expertise or additional sources of capital. In that sense, public private partnerships can be an effective means of delivering operations which ensure the achievement of public policy objectives by bringing together different forms of public and private resources.

In accordance with the Public Private Partnership Act of the Republic of Croatia (Official Gazette, number 78/12, 152/14), a public private partnership is a long term contractual relationship between public and private partners, with the objective of construction and/or reconstruction and maintenance of a public structure, for the purpose of providing public services from the framework of competence of the public partner, where the private partner assumes obligations and risks from the public partner in connection with the construction process and at least one of two risks – risk of availability of the public structure and risk of demand.

---

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (2009) "Mobilising private and public investment for recovery and long term structural change: developing Public Private Partnerships".

Regulation No 1303/2013 of the European Parliament and of the Council of 17 December 2013 laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund and laying down general provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund and the European Maritime and Fisheries Fund and repealing Council Regulation (EC) No 1083/2006.

In present-day "Western" society confronted by an increasing number of security challenges, it is necessary to strengthen cooperation as well as exchange of knowledge and best practices among relevant stakeholders because it is increasingly apparent that states most often cannot independently satisfy apparent growing demand for strengthening of resilience and protection of vital interests without cooperation with all centres of social power. It is obvious that states need support from other sectors in the society, and public private partnerships have gained prominence in recent years as an exceptionally beneficial form of cooperation.

A public private partnership, as a model relationship between public and private sectors, is based on identification and application of benefits potentially available to the public and private sectors through pooling of resources as well as expertise (knowledge) with the purpose of improving and satisfying needs of the community. Such partnerships may combine advantages of both sectors, harmonising social and public responsibility and effective management, financial capabilities and "enterprising spirit" carried by the private sector. The above may result in higher quality and greater efficacy of protection of public interests in the field of critical infrastructures. However, without any habit of joint action, and moreover mutual preparedness to cooperate, such critical infrastructure protection models cannot be adequately fulfilled.

In the Republic of Croatia, the Critical Infrastructures Act provides, inter alia, a basis for consideration of serious consequences to economic stability as a critical factor which may be affected by cessations of operation or cessation of supply of goods or services due to impacts on the national critical infrastructure, pointing one to consider partnerships in the foregoing segment.

In the broadest sense, a public private partnership is often defined as a joint initiative of public and private sectors where each entity contributes to the system specific resources and participates in planning and decision-making. That is precisely what should be aimed for in public private partnership systems in the field of strengthening of resilience and critical infrastructure protection.

The private sector channels its resources and skills through public private partnerships to providing of goods and services traditionally provided by government services. Thus, a new quality is created in the relationship between the state and the private sector through a balanced distribution of tasks in functioning of the society.

According to a group of authors (Marenjak, S. et al., 2007) in the aforementioned partnership, focus should also be at specific elements and/or guidelines for successfulness and sustainability of cooperation aimed at implementation of the objectives of strengthening of resilience and critical infrastructure protection, specifically:

1. Defining roles and responsibilities – public private partnership contracts should regulate obligations and rights of public and private partners while respecting the basic principles in preparation and implementation of public private partnership projects, i.e. principle of public procurement, principle of public interest and principle of cost effectiveness.

2. Application of resources – aimed at reduction of criticality and/or increased resilience of infrastructures, public private partnership stakeholders should involve resources available to them (e.g. capital), as already addressed by the Public Private Partnership Act, and that should be a part of relevant contracts. In addition to the existing public and private financial resources, it is necessary to plan possible use of European structural and investment funds in support of public private partnerships in accordance with Regulation of the European Parliament and of the Council No 1303/2013 and/or in accordance with applicable law, especially laws on government supports and public procurement.
3. Openness to development of capacities and changes – if the need for institutional changes arises in the process of critical infrastructures risk management at the level of the service provider or the government body.
4. Realistic expectations – it is necessary to develop integrated solutions which shall have a longer "life cycle", which are not benefiting from imposition of exceptionally short timeframes. Short term plans with limited timeframes result in solutions which are difficult to implement. More significant institutional changes which guarantee quality require time. Also, it is not realistic to expect that inclusion of the private sector over a short period of time shall compensate for shortcomings regarding resources or in activity of public institutions in general.

It should be taken into consideration that there are certain differences in the approach to the concept of cooperation between partners in a public private partnership. For instance, "profit motives" of privately owned companies may arise, or the public sector may impose "bureaucratised" thinking and decision-making thus discouraging its counterparty. In order to overcome possible differences, it is important to focus on a greater goal which should be achieved, namely strengthening of resilience and protection of critical infrastructures, along with awareness that cooperation of "public and private", despite potential complicating factors, brings advantages such as, for example, more efficient implementation – the private sector has knowledge and resources to implement determined objectives over a short period, which sometimes presents the public sector with difficulties because of diverse circumstances.

The need to utilise public private partnerships in strengthening of resilience and protection of critical infrastructures may be found in several strategic documents in the field of national security of the Republic of Croatia. National Strategy for Prevention and Combating Terrorism (Official Gazette, number 139/08) states that "development of public private partnerships with the business community in promotion of economic stability and security in relation to danger of terrorism, especially in critical infrastructure protection and prevention and combating funding of terrorism. Development of public private partnerships shall be fostered in the field of cooperation in detection of terrorist activities, especially in the field of prevention of financing of terrorist organisations, providing information to and education of public on terrorism, protection of information technology, communications, transport, energy and industrial infrastructure,

cooperation in training of the business sector to respond to terrorist attacks and remedy consequences of terrorist attacks."[6] Additionally, proposed Draft Strategy of Cybernetic Security, one of the stated goal is that it is necessary to "Strengthen public private partnerships and technical coordination in processing of computer security incidents." A clarification states that "In the sector of critical infrastructure, determined by the aforementioned Decision of the Government of the Republic of Croatia on determination of sectors from which central government administration bodies identify national critical infrastructures and critical infrastructure sector ranking lists, it is necessary to foster public private partnerships through sectoral competent central government administration bodies in order to ensure unhindered operation for business entities who represent owners/managers of the critical infrastructures. In that sense, it is necessary to determine appropriate supervision and coordination procedures, as well as procedures for exchange and provision of required security information. Exchange and provision of information is performed among sectoral principals and owners/managers of critical infrastructures, with bodies competent for computer security incidents in the fields of public electronic communication and information technology infrastructures and services, as well as bodies competent for criminal prosecution. Technical coordination in processing of computer security incidents is performed through cooperation of bodies which have developed capability to respond to such type of incidents[7]."

In summation, it may be said that public private partnerships are engagement of resources to achieve common interests with the ultimate objective of preparation and achievement of development of a specific region. Strengthening of resilience and protection of critical infrastructures, considering their national importance, should undoubtedly be in the focus of development of the Republic of Croatia, and public private partnerships should be one of principal mainstays of performance of the above.

The concept of cooperation of the public and private sectors in strengthening of resilience and protection of critical infrastructures

The concept of cooperation of the public and private sectors in strengthening of resilience and protection of critical infrastructures may be built upon a multitude of diverse foundations and criteria.

A working group of the Centre for European Policy Studies deems that there should be a great need for an overall vision of what should be achieved by critical infrastructure protection first. Afterwards, a strategy is needed, as well as strong political commitment (determination) to achieve the results which are aimed at. The above should then be shared with all stakeholders as well as owners and managers of critical infrastructures in order to promote awareness for such an approach. The vision, strategy and awareness represent foundations of any successful critical

6 Section 34.c) of the National Strategy for Prevention and Combating Terrorism.

7 Working draft Stategy.

infrastructure protection policy. Afterwards, assuming the foregoing has been achieved, establishment of foundations for cooperation of the public and private sectors follows, including: (1) Development of standards and dissemination of the best practices; (2) Promotion of education and training; (3) Promotion of research and development; and (4) Exchange of information (Hammerli & Renda, 2010:75-76).

Generally, and especially in the course of RECIPE project, it is necessary to ensure that representatives of the most significant economic entities (potential national critical infrastructures), professional and academic community, Croatian Chamber of Economy, Agency for Investments and Competitiveness and numerous other collocutors are included in addition to the network of national security coordinators from the central government administration bodies in order to discuss and propose the optimal concept of cooperation.

Public private partnership projects in strengthening of resilience and protection of critical infrastructures

Even though a public private partnership is not the ideal model for all infrastructural projects, every possibility for joint action should be considered wherever possible and mutually justified. Construction of missing, maintenance and improvement of resilience of existing as well as protection of critical infrastructures is easier to achieve through public private partnerships than through care of the public sector only.

The public sector should strive towards greater, more innovative and long term financing of infrastructural projects by the public sectors, but it is necessary to analyse and consider interests of the private sector with great care to avoid creating an impression of a one-way partnership.

Public private partnerships allow transfer of project risks from the public sector to the private sector. In that respect, public private partnership projects deem risks (for example failures) to be risks of the private partner who is required to revise design documents and then also assume risks of performance of the future structure. Besides that, it is the approach which brings mutual advantages – including development, modernisation and maintenance of large infrastructures through private financing. Such discourse requires the following principles: contracting of long term projects (frequently longer than 30 to 40 years) by the public sector, includes public and private financing, request to include the private sector in obligations of the public sector (procurement, construction, management, maintenance and similar activities), establishment of risk and obligations sharing models during the partnership[8]. In the Republic of Croatia, the above is regulated by the Public Private Partnership Act and in future, one should strive towards the greatest possible number of projects implemented in accordance with this model. That is also supported by positive examples of fourteen projects, twelve of which are in use for many years, available for inspection through the Register of Projects at the Agency for Investments and Competitiveness website.

[8] John Forrer, James Edwin Kee, Kathryn E. Newcomer and Eric Boyer: "Public Private Partnerships and the Public Accountability Question" in Boyer, E. et al. (2014:4).

Objective of the RECIPE project is to collect and exchange the best practices regarding public private partnerships which shall serve to strengthen resilience of and protect national and European critical infrastructures.

Matters of security and public private partnership in critical infrastructure protection

National critical infrastructures represent a significant area of national security of any state. Therefore, the Republic of Croatia has also recognised the foregoing in development of the new National Security Strategy where inadequate protection and failure to recognise source of threats against national critical infrastructures are emphasised as representing a significant security risk to the national security of the Republic of Croatia.

In the countries of the West, critical infrastructures are majority-owned by the private sector which is therefore required to care for their protection. Precisely because of that, public private partnerships represents an excellent platform to exchange knowledge, information and to advance critical infrastructure protection in the Republic of Croatia.

Since the private sector in the West owns and/or manages more than 80 percent of national critical infrastructures (the proportion in the Republic of Croatia is currently unknown), it is understandable that the private sector is best acquainted with their weaknesses and advantages and it is required to strengthen resilience and protection of critical infrastructures, therefore cooperation of the public and private sectors in the above area is necessary for the public sector.

Improvement of normative framework of operation of private partnership projects in strengthening of resilience and protection of critical infrastructures

Establishment of a normative framework is always a demanding and inspiring task which should allow regulation of a specific field, as well as open up space for further activities, new ideas and methods of implementation of legislative provisions. Also, the normative framework should facilitate a stimulating approach for new investments and development of new values.

Since that is an exceptionally significant field in the area of national security of the Republic of Croatia, it is necessary to expand public discussion on the above with the objective of obtaining the best possible proposals for improvements to the normative framework, specifically the one regulating the field of public private partnerships in order to make it as clear as possible, more flexible and open to new investments and the maximum possible cooperation of the public and private sectors.

Solutions for improvements to the existing normative framework shall be proposed in the course of the RECIPE project.

Conclusion of the chapter

After an analysis of the critical infrastructure protection system through the prism of public private partnerships, the above imposes itself as one of significant principles of strengthening of resilience and protection of critical infrastructures. Accordingly, because of the most effective possible application of benefits of such interaction of the public and private sectors, the following considerations should be applied:

1. Taking into consideration significance of critical infrastructures to national and public security and stability and functioning of the state, it is necessary to expand the existing legislative (normative) framework in the area of public private partnerships, specifically:
   - The field of critical infrastructures should be included in provisions of the Critical Infrastructures Act, and public private partnerships should be addressed by the Critical Infrastructures Act.
   - The procedure of submission and approval of public private projects, including small value public private partnerships, should be adapted in the field of critical infrastructures.
   - Sectoral government administration bodies having sectoral competence for individual critical infrastructures should be included in monitoring and supervision of public private partnership projects.
2. Government administration body competent for coordination of critical infrastructures risk management activities develops a plan and proposal of public private partners projects whose objective is to increase resilience/security of those critical infrastructures in cooperation with sectoral government administration bodies having competence in sectors of the critical infrastructures and owners/managers of the critical infrastructures.
3. In the course of planning of public private partnership projects whose objective is to increase resilience and protect critical infrastructures, the possibility of use of European structural and investment funds should be taken into consideration, especially in the part pertaining to public private partnerships.

References

Strategies and acts

Croatian Parliament (2002) *National Security Strategy of the Republic of Croatia*, available at: https://www.soa.hr/UserFiles/File/Strategija_nacionalne_sigurnosti_RH.pdf, (accessed on 20 June 2015).

Croatian Parliament (2013) *Critical Infrastructures Act*, available at: http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, (accessed on 20 June 2015).

Croatian Parliament (2014) *Public Private Partnership Act*, available at: http://www.zakon.hr/z/198/Zakon-o-javno-privatnom-partnerstvu, (accessed on 20 June 2015).

Government of the Republic of Croatia (2008) *National Strategy for Prevention of and Combating Terrorism*, available at: http://www.propisi.hr/print.php?id=8677, (accessed on 29 June 2015).

European Union documents

European Commission (2009) *Mobilising private and public investment for recovery and long term structural change: developing Public Private Partnerships*, available at: http://www.ajpp.hr/media/5197/priop.pdf, (accessed on 20 June 2015).

European Parliament and Council (2013) *Regulation No 1303/2013 of the European Parliament and of the Council of 17 December 2013 laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund and laying down general provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund and the European Maritime and Fisheries Fund and repealing Council Regulation (EC) No 1083/2006*, available at: http://www.mingo.hr/public/documents/Uredba_EU_parlamenta-i-Vijeca_1303-2013.pdf, (accessed on 2 July 2015).

Authored works

Boyer, E. et al. (2014) *Public-Private Partnerships and Infrastructure Resilience, How PPPs Can Influence More Durable Approaches to U.S. Infrastructure*, http://www.uschamberfoundation.org/sites/default/files/article/foundation/PPPs%20and%20Infrastructure%20-%20NCF.pdf, (accessed on 24 June 2015).

Hammerli, B. & Renda, A. (2010) *Protecting Critical Infrastructure in the EU*, Brussels: Centre for European Policy Studies, http://www.ceps.eu/ceps/dld/4061/pdf, (accessed on 5 February 2014).

Marenjak, S. et al. (2007) *Javno-privatno partnerstvo i njegova primjena u Hrvatskoj (Public private partnership and its application in Croatia)*, available at: http://hrcak.srce.hr/file/24932, (accessed on 20 June 2015).

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

Summary

Handling of sensitive information on national and European critical infrastructures is performed in accordance with special regulations in the field of information security and international treaties. However, it has been determined in practice that the existing regulations are not enforced completely, therefore it is necessary to undertake additional activities in order to increase efficacy and security in exchange of information related to critical infrastructures.

Introduction

Present time is marked by an intensive development of information sciences which is closely related precisely to use of terms such as information, information security, personal and confidential data, right to privacy etc. This type of information society is marked by information as its basic resource, and it is encountered in various situations. In this framework, information is defined as data which has context and value for stakeholders. The main characteristics of every information are confidentiality, integrity and availability[9].

Confidentiality of an information represents the property that it is only accessible to the authorised user who is formally entitled to it.

Integrity of information is the property describing inability to change contents and form of the information, as well as immutability of procedures used to process and manipulate it without permission of owners of the information.

Availability of information represents the property that the information must be available to the (authorised) user in the required location, time and form.

Information has a specific degree of classification determined based on contents carried by the information, thereby automatically determining the method of handling of the information and scope of users who may use it in a specific way.

Since information is a fundamental resource of any system, including the critical infrastructure protection system, it is necessary to prescribe frameworks and requirements which must be satisfied in order to render the system functionally usable and to achieve compliance with information properties and classification requirements.

[9] HRN ISO/IEC 27001:2014 standard

In accordance with the Critical Infrastructures Act, sensitive information comprises data on critical infrastructures which have been designated as classified information in accordance with a special regulation. Information related to determination of individual critical infrastructure an European critical infrastructure represent classified data and are designated by a corresponding degree of confidentiality. Criteria for designation of degrees of confidentiality is prescribed by the Government of the Republic of Croatia through its decisions.

Handling of sensitive information on national and European critical infrastructures is performed in accordance with special regulations in the field of information security and international treaties.

Use of information within the framework of critical infrastructures

Existence and implementation of security of critical infrastructures is based, inter alia, on use of an information system in all stages. Since critical infrastructures are of special significance to states, it is obvious that the information system must comply with specific requirements in order to ensure planned and expected security management thereof.

Accordingly, it is necessary that the information system complies with two components:

a) Organisational-technological level ensuring functional management of critical infrastructures, and
b) Security level ensuring fulfilment of security requirements, primarily in order to meet requirements related to classification of information used within the framework of management of critical infrastructures

The organisational-technological level is normally conditioned by vision and capabilities, primarily financial ones, and since it is not a subject of consideration, it shall not be addressed specifically here.

The crucial problem, regardless of technological design of the information system, represents preservation and improvement of the security level of the information system. Information handling method (including generation, processing, transfer, delivery, storage, and destruction of obsolete ones) is primarily determined by classification. A higher level of classification requires a more serious approach, in every aspect, to preservation of security of information related to critical infrastructures.

According to the Data Confidentiality Act[10], method of determination, as well as rights and data handling methods, are prescribed for each level of classification.

[10] Data Confidentiality Act (Official Gazette number 79/07 and 86/12)

Method of preservation of information security, as the basis for compliance with classified information handling requirements, is optimally achieved by implementation of an Information Security Management System.

In other words, implementation, certification and supervision of the ISMS provides a satisfactory degree of confidence in preservation of critical infrastructures information security.

In implementation of the ISMS, government bodies and public administration bodies must comply with the Information Security Act[11], while the other stakeholders in the system of protection and management of critical infrastructures should apply and implement requirements laid down by HRN ISO/IEC 27001:2014 standard. Application of this standard is completely in compliance with the Information Security Act.

The following should be provided for the purpose of fulfilment of information classification needs:

a) Implementation of the Information Security Management System
b) Certification of the information security system
c) Ongoing verification of compliance with the Information Security Act and/or HRN ISO/IEC 27001:2014 standard requirements
d) Increased awareness of all stakeholders related to information security of critical infrastructures through education
e) Qualification of those directly participating in management of critical infrastructures for proper conduct and implementation of information security requirements through education and training

For the purposes of the foregoing, critical infrastructure protection stakeholders should develop a model of efficient management of information in the field of critical infrastructures management.

Development of a communication system model and a model ensuring availability of information

Mutual cooperation of all critical infrastructure protection stakeholders, systems for their communication and exchange of sensitive information, as well as general availability of information on critical infrastructures are important segments of the complete critical infrastructures management system.

In the course of its activities already performed, the RECIPE project has recognised the following needs:

[11] Information Security Act (Official Gazette number 79/07)

a) Development of the joint data and information transmission system to establish more efficient coordination and cooperation in all government bodies and institutions.
b) Development of the national critical infrastructures database and
c) Establishment of a web GIS browser on the critical infrastructures

While taking into consideration all needs recognised so far, as well as needs which may potentially be recognised in the further course of the project, a conceptual communication system model and a model ensuring availability of information should be developed.

Conclusion of the chapter

Based on the presented material, it is concluded that the following should be performed:

1. Implementation of the ISMS for all beneficiaries and owners of critical infrastructures
2. In order to establish efficient information management in the field of critical infrastructures management and harmonisation of procedures for exchange of that information among stakeholders, it is necessary to develop a model of efficient management of information in the field of critical infrastructures management.
3. Establishment of a cross-sectoral working group of representatives of central government administration bodies and other stakeholders in the critical infrastructures protection and risk management system is proposed for the purpose of development of the model referred to in Section 2.
4. Critical infrastructure security coordinators and advisors for information security of central government administration bodies and legal persons should propose determination of the lowest degree of confidentiality which shall ensure protection of interests which might be compromised by unauthorised disclosure of that data/information (Article 12 of the Data Confidentiality Act) to the owner of the data/information.
5. The security coordinators and advisors for information security of competent central government administration bodies should propose amendments to the ordinance on protection of data confidentiality and develop criteria for determination of degrees of confidentiality for data within the scope of critical infrastructures in accordance with Article 10 of the Data Confidentiality Act.
6. The conceptual communication system model and a model ensuring availability of information should be developed while taking into consideration all needs recognised in the course of the project.

References

Acts

Croatian Parliament (2013) *Critical Infrastructures Act*, available at: http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, (accessed on 20 June 2015).

Croatian Parliament (2007) *Data Confidentiality Act*, available at: http://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka, (accessed on 20 June 2015).

Croatian Parliament (2007) *Information Security Act*, available at: http://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti, (accessed on 20 June 2015).

Standards

Croatian Standards Institute (2014) *HRN ISO/IEC 27001:2014 standard (information security)*

6. ESTABLISHMENT OF PRECONDITIONS FOR DEVELOPMENT OF A NATIONAL CENTRE FOR CRITICAL INFRASTRUCTURES

Summary

The objective of the project is to develop a conceptual model of comprehensive protection and management of critical infrastructures in the Republic of Croatia which shall define prerequisites for establishment and development of the National Centre for Critical Infrastructures and provide fundamental principles for the following areas of interest: improvements to the normative framework, improvement of the existing and development of new methodologies and development of measures for identification of criticality classes and application of necessary protection measures.

Introduction

The normative framework of critical infrastructure protection in the Republic of Croatia has been determined by the Critical Infrastructures Act[12] and corresponding subordinate legislation[13,14]. The Critical Infrastructures Act determines competence of nine sectoral ministries over individual sectors of critical infrastructures and security coordinators and their deputies have been appointed for each sector of the critical infrastructures. The critical infrastructures management and protection system is still in its early stage of development and only some system elements foreseen by the normative framework have been implemented by now[15].

[12] Critical Infrastructures Act (Official Gazette, number 56/13)
[13] Ordinance on methodology for critical infrastructure operation risk analysis, Official Gazette number 128/13
[14] Decision on determination of sectors from which central government administration bodies identify national critical infrastructures and critical infrastructure sector ranking lists, Official Gazette number 108/13
[15] Panel discussions "Analysis of situation and needs in the national critical infrastructure protection system" – report to the European Commission, RECIPE project, Zagreb, June 2015

During RECIPE project activities performed by now, two panel discussions have been held with their topic of "Analysis of situation and needs in the national critical infrastructure protection system" and as their result the main directions of further activities were defined, as described in greater detail in further text of this chapter.

DEVELOPMENT OF A NATIONAL CENTRE FOR CRITICAL INFRASTRUCTURES

The Critical Infrastructures Act determined obligations and competences of the Government of the Republic of Croatia, sectoral ministries and the central government administration body whose scope of work includes protection and rescue operations (DUZS) in critical infrastructure protection. Through practical implementation of the aforementioned Act, it was determined that the established critical infrastructure protection system cannot successfully address demands in terms of organisational and operational solutions as well as in respect of the existing human resources, taking into consideration complexity and scope of processes and procedures in the field of management of critical infrastructures. Taking the above in consideration, as well as the fact that efficient critical infrastructures risk management is of the greatest interest for national and public security, there is no doubt that it is necessary to establish a central national service whose fundamental task would be prevention, integrated operation and increasing efficacy in the field of critical infrastructure protection.

In terms of structure and organisation, there are several possible models to establishing the foregoing service in the Republic of Croatia, for instance:

- National centre for CI as an organisational unit at the DUZS
- National centre for CI as an organisational unit in another central government administration body
- National centre for CI organised within services and offices of the Government of the Republic of Croatia
- National centre for CI as an independent government administration body

Within the RECIPE project, the following tasks have been recognised as those the critical infrastructures centres should perform:

a) Collecting, analysis and exchange of information among critical infrastructures protection/risk management – in this sense the centre would be the central point for coordination of critical infrastructures security coordinator network in CSABs and operators of critical infrastructures
b) Submission of proposals and development of regulations in the field of critical infrastructure protection
c) Supervision and directing identification and development of sectoral critical infrastructures risk analyses

d) 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 central government administration bodies
e) Organising education and training in the field of critical infrastructure protection, in cooperation with other stakeholders in critical infrastructure protection
f) Establishment and functioning of a central point for planning, preparedness and responses in emergencies in the field of critical infrastructure protection
g) Coordination and monitoring of public private partnership projects in the field of critical infrastructure protection
h) Establishment and functioning of a contact point for European critical infrastructures

In further course of the project, examples of good practice from countries which have highly developed awareness on the need for critical infrastructure protection and significantly developed systems for its protection shall be analysed, and several versions of organisation model of the national centre for critical infrastructures shall be proposed.

Advancement of the normative framework, advancement of the existing and development of new methodologies

The RECIPE project is aimed at providing a platform for assessment of quality of normative framework design and practice related thereto in the field of critical infrastructure protection, including advantages and shortcomings as well as opportunities for improvements. In the course of project activities performed so far, it has been assessed that the normative framework offers areas for improvements, for instance in segments such as place and role of security coordinators in sectoral ministries and opening up the areas for appropriate incentives to those business entities which shall be recognised as national critical infrastructures[15].

It is necessary to develop a critical assessment of the normative framework, identify any existing omissions ("lacunae") in its documents, consider efficacy of the foreseen system in respect of duration of individual processes, consult registered and potential owners of critical infrastructures in order to determine their views of issues regarding implementation of the system as well as develop a model which shall allow sectoral ministries to determine a structure and required number of critical infrastructure protection standpoints with corresponding job descriptions and specify their competences and responsibilities.

The Ordinance on methodology for critical infrastructure operation risk analysis defines risk analysis procedures, determines cross-sectoral benchmarks, risk identification method, defines criteria for assessment of criticality, defines threat analysis and scenario development procedures,

prescribes measures and criteria for identification of vulnerabilities and determines risk calculation methods. Since critical infrastructures in the Republic of Croatia have not yet been identified in accordance with provisions of this Ordinance, there is no exact information on successfulness of its application. Notwithstanding of that, it is possible to assess quality of the prescribed methodology and the need for its possible improvements through various types of simulations[15].

The need to develop a risk management methodology in addition to the existing risk analysis development methodology has been recognised through RECIPE project analyses carried out by now. Since ISO standards have become generally accepted and the most widely applied global standards in a great number of human activities, and since it is a fact that a large number of provisions of the Critical Infrastructures Act and the Ordinance on risk analysis development methodology is in compliance with provisions of HRN ISO 31000:2012 standard[16], a logical conclusion imposes itself that the risk management methodology should be in compliance with that standard. Risk management should also ensure business continuity in accordance with HRN EN ISO 22301:2014 standard[17].

Furthermore it is necessary to develop a proposal of improvements to the existing risk analysis development methodology and a conceptual model of the risk management methodology.

Development of benchmarks for identification of criticality classes and application of necessary protective measures

Identification of those infrastructures which are critical in all eleven determined sectors of critical infrastructures is a great challenge and one of the main tasks in development of a comprehensive critical infrastructures management system in the Republic of Croatia[15].

In the process of identification of critical infrastructures, structural ministries should answer which serious consequences to the national security, serious consequences to human lives and health, serious consequences to property and environment, serious consequences to security and economic stability and serious consequences to ongoing functioning of the government may occur. In order to facilitate the answers to the questions, it is necessary to determine benchmarks to determine which consequences are serious. Existing experience and recommendations provided by the European Union and other Member States should be considered in the process.

The processes aimed at determining the benchmarks and identification of critical infrastructures, also including required risk analyses, should be performed by sectoral ministries. However, human resources of the sectoral ministries do not comprise a sufficient number of persons with required competences to perform the aforementioned procedures thus the activities of the

[16] HRN ISO 31000:2012 standard
[17] HRN EN ISO 22301:2014 standard

RECIPE project carried out so far have recognised the need for an additional education of human resources in all critical infrastructure sectors.

In order to achieve all of the above, it is necessary to develop a concept of a model for determination of sectoral benchmarks and a concept of a model of a modular education in the area of critical infrastructure protection.

Conclusion of the chapter

Based on the determined objective of the project proposal and everything presented in this section, the following conclusions are determined. They also represent further contents of project activities of the RECIPE project in the segment of establishment of prerequisites for development of the National Centre for Critical Infrastructures:

1. Propose multiple alternatives of the model of organisation of the national centre for critical infrastructures while taking into account examples of good practice from countries which have highly developed awareness on the need for critical infrastructure protection and significantly developed systems for its protection, and perform a multi-criterion analysis of advantages and shortcomings of the proposed models.

2. Identify any existing omissions in the normative framework documents, consider efficacy of the foreseen system in respect of duration of individual processes, consult registered and potential owners of critical infrastructures in order to determine their views of issues regarding implementation of the system as well as develop a model which shall allow sectoral ministries to determine a structure and required number of critical infrastructure protection standpoints.

3. Propose required improvements to the existing risk analysis development methodology and the conceptual model of the risk management methodology.

4. Develop a concept of the model for determination of sectoral benchmarks and a concept of a model of a modular education in the area of critical infrastructure protection.

References

Acts and regulations

Croatian Parliament (2013) *Critical Infrastructures Act*, available at: http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, (accessed on 20 June 2015).

European Council (2008) *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,* available at: http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32008L0114&from=EN, (accessed on 20 June 2015).

National Protection and Rescue Directorate (2013) *Ordinance on methodology for critical infrastructure operation risk analysis*, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2013_10_128_2792.html, (accessed on 20 June 2015).

Government of the Republic of Croatia (2013) *Decision on determination of sectors from which central government administration bodies identify national critical infrastructures and critical infrastructure sector ranking lists*, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2013_08_108_2411.html, (accessed on 20 June 2015).

Standards

Croatian Standards Institute (2012) *HRN ISO 31000:2012 standard (risk management)*

Croatian Standards Institute (2014) *HRN EN ISO 22301:2014 standard (Societal security – Business continuity management systems)*

RECIPE project documents

RECIPE project (2015) *Panel discussions "Analysis of situation and needs in the national critical infrastructure protection system" – report to the European Commission*, Zagreb, June 2015