FINAL TECHNICAL IMPLEMENTATION REPORT

Resilience of Critical Infrastructure Protection in Europe (RECIPE)

Financed under European Union Civil Protection Mechanism Projects on Preparedness and Prevention Projects in civil protection and marine pollution 2014

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

1. TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS 3
2. GENERAL REMINDER OF PROJECT OBJECTIVES, PARTNERSHIP AND EXPECTED DELIVERABLES 4
3. GENERAL SUMMARY OF PROJECT IMPLEMENTATION PROCESS 6
3.1. GENERAL OVERVIEW OF THE PROCESS 6
3.2. COMPARATIVE ANALYSIS 8
3.2.1. Initial and Current Time Schedule 8
3.2.2. Planned and Used Resources 12
3.2.3. Expected and Actual Results 13
4. EVALUATION OF PROJECT MANAGEMENT / IMPLEMENTATION PROCESS 16
4.1. POSITIVE ASPECTS / OPPORTUNITIES 16
4.2. INTERNAL AND EXTERNAL DIFFICULTIES ENCOUNTERED 16
4.3. PARTNERSHIP / CORE GROUP COOPERATION (as appropriate) 17
4.4. COOPERATION WITH THE COMMISSION 17
4.5. COMMENTS ON THE EUROPEAN VALUE ADDED 18
4.6. LESSONS LEARNED AND POSSIBLE IMPROVEMENTS 18
5. ACTIVITIES 20
5.1. COMPARISON BETWEEN INITIALLY PLANNED AND ACTUALLY IMPLEMENTED ACTIVITIES, INCLUDING MONITORING, EVALUATION AND DISSEMINATION 20
5.1.1. Panel discussion 20
5.1.2. Joint workshops 21
5.1.3. International scientific conference 22
5.1.4. Follow-up strategy 23
6. PRESENTATION OF THE TECHNICAL RESULTS AND DELIVERABLES 24
6.1. DESCRIPTION OF INDIVIDUAL DELIVERABLES, PURPOSE OF THE DELIVERABLE, EVALUATION OF THE DELIVERABLE, VALUE-ADDED – IN PARTICULAR EUROPEAN VALUE – ADDED AND TRANSFERABILITY – OF THE DELIVERABLE, DISSEMINATION 24
6.1.1. Questionnaire 24
6.1.2. National standpoints 26

6.1.3. Feasibility study 27
6.1.4. Guidelines 28
6.1.5. Mobile application 28
7. EVALUATION OF THE TECHNICAL RESULTS AND DELIVERABLES 30
7.1. GENERAL LESSONS LEARNT 30
7.2. STRENGTHS 35
7.3. POSSIBLE CHALLENGES AND/OR IMPROVEMENTS TO BE TACKLED TROUGH FURTHER ACTION 36
7.4. RECOMMENDATIONS TO STAKEHOLDERS, PARTNERS, AUTHORITIES IN CHARGE, NATIONAL AND EU INSTITUTIONS 37
8. FOLLOW-UP 40
8.1. COMPARISON BETWEEN INITIAL AND CURRENT FOLLOW-UP MEASURES 40
8.2. ADDITIONAL FOLLOW-UP APPROACHES 44

ACRONYMS AND ABBREVIATIONS

AB1	First Beneficiary - University of Belgrade, Faculty of Security Studies
AB2	Second Beneficiary - University of Applied Sciences Velika Gorica
AB3	Third Beneficiary / Coordinator - National Protection and Rescue Directorate of the Republic of Croatia
CIP	Critical Infrastructure Protection
CIPR	Critical Infrastructure Protection and Resilience
CO	Coordinator - NPRD
CP	Civil Protection
EC	European Commission
ECI	European Critical Infrastructure
EU	European Union
FB	University of Belgrade, Faculty of Security Studies (Fakultet bezbednosti)
RH	Republic of Croatia (Republika Hrvatska)
MSB	Swedish Civil Contingencies Agency
NPRD	National Protection and Rescue Directorate of the Republic of Croatia (Državna uprava za zaštitu i spašavanje, DUZS)
RS	Republic of Serbia
SE	Kingdom of Sweden
VVG	University of Applied Sciences Velika Gorica (Veleučilište Velika Gorica)

2. GENERAL REMINDER OF PROJECT OBJECTIVES, PARTNERSHIP AND EXPECTED DELIVERABLES

Critical infrastructure is the basic facilities, networks and systems directly critical to the nation's economic activities being a vital asset for the functioning of the society. The number of infrastructure sectors and types of assets considered to be "critical" for purposes of a nation's security in modern times generally has been expanding. Hence, a deficient or inadequate protection of critical infrastructure, having interdependent and cross-sectorial character, may pose a threat with cascading consequences to the security and stability of the European countries and Europe as a whole. Borders represent a significant vulnerability to the critical infrastructure sectors and may act as chokepoints restricting or disrupting cross-border movement.

Critical infrastructure protection (CIP), therefore, aims to cover all the activities directed at enhancing the resilience of people, systems and physical infrastructure, whereas prevention plays a crucial role, be it at regional or international level. Such a culture of safety and resilience at all levels is best reinforced through a quality security management system enhancing partnership and collaboration between potentially affected stakeholders sharing ECI (European critical infrastructure).

However, despite various efforts made by the European Commission in this respect, uniform levels of protective security are still not present throughout the EU ('Multi-speed Europe'), and vulnerabilities persist. Instead of considering this imbalance a threat or a deficiency, this Project aims to turn it into an advantage providing opportunities for the exchange of different know-hows and best practices.

For this purpose, the Project involves EU Member States with varying levels of progress within CIP area, together with a candidate country so that the EU achievements can be spread beyond its borders for a strengthened security of all. The Project thus engages countries at three different levels of achievement as regards the critical infrastructure protection, namely Sweden, boasting significant progress and distinctive results in CIP, Croatia that has only just initiated CIP-related efforts and Serbia that is lagging behind and is in need of peer assistance in establishing its own CIP system.

The Project coordinator of RECIPE is NPRD (Croatia) and the partners are FB (Serbia), VVG (Croatia) and MSB (Sweden). The Project is implemented in Croatia, Serbia and Sweden.

The Project started on 01/01/2015 and ended on 30/06/2016.

The Project's total eligible cost is: 408.675 € (EC financial contribution: 75% of the total).

The most important Project deliverables are:

- Questionnaires which gave the insight in the current state of critical infrastructure risk management at the partner countries' national level and beyond;
- National standpoints of the Republic Serbia and Republic of Croatia regarding their CIP system development issues;
- Feasibility studies assessing best practice implementation applicability in the relevant partner countries' (Croatia, Serbia) CIP systems;
- The Guidelines with integrated best practices resulting from the workshops and assessed in feasibility studies;
- Book of proceedings as a result of the international scientific conference as the integrating goal of the Project summing up all the efforts done throughout the Project and providing conclusions for the follow-up strategy on CIP;
- The mobile application intended for the exchange of CIP stakeholder contacts (not only Project partners but any interested stakeholders).

3. GENERAL SUMMARY OF PROJECT IMPLEMENTATION PROCESS

3.1. GENERAL OVERVIEW OF THE PROCESS

The Project implementation process started on 01/01/2015 by establishing the contacts among the partners and with the European Commission. At the same time, internal partner meetings were organized in each of the participating partner countries where working groups were formed and tasks assigned. On 20/01/2015, the Project kick-off meeting took place in Brussels with the representatives of NPRD and FB.

The Project initial meeting was held in Zagreb on 25/02/2015. The representatives of all Project partners were present, the tasks were allocated, the administrative and financial issues, as well as the formation of management bodies, were discussed. The Project partners were asked to nominate persons in three management teams (overall Project management, Administrative management and Financial management) and in three committees (Assessment, Academic and Conference committee). The management bodies were established. It is attached to the Final Report (Annex I).

The Consortium Agreement was signed in April 2015. The Agreement sets out the general terms and conditions and provides a legal basis for all activities among partners that are necessary for the successful Project implementation. The Swedish partner asked for a modification regarding the legal issues of the Consortium Agreement and this was solved in the form of an Annex to the Consortium Agreement. At the same time, the Project plan with detailed division of the tasks was finalized.

The Project logo and Project web page were launched in May 2015.

The Assessment Committee prepared the Analysis Questionnaire adapting it to each respective country. The Questionnaire results served as the basis for panel discussions and other future activities.

The Questionnaire evaluation report was completed both for RH and RS and submitted on June 10, 2015 and the complete evaluation report was submitted to the Commission on July 15, 2015 in English. It is attached to the Final Report (Annex II).

The Project implementation process continued in July 2015 with the Project meeting held in Belgrade with the representatives of all the partner institutions (except for the Swedish partners). The results of the panel discussions were presented, and the development of the national standpoints as well as future steps and the upcoming activities of the RECIPE Project were discussed.

Other internal meetings were organized at the institutional level on the monthly basis in order to discuss the current activities and to monitor the Project progression.

Based on the conclusions drawn from the panel discussions, the Croatian and Serbian National standpoints on the aimed course of action were formulated. Their results were used in subsequent Project Actions. The National standpoints are attached to this Report (Annex III).

The following step in the Project implementation was the organization of joint workshops. The one in Belgrade was held on October 13, 2015 and the Zagreb one was held on October 15, 2015. The Project-based aim of the workshop was to discuss the national standpoints formed at the earlier national panel discussion in order to fill certain voids in the critical infrastructure system through the exchange of experience and good practices presented by experts from EU countries. Special attention was paid to the current state and development of the critical infrastructure protection system in the Kingdom of Sweden. Both workshops in Zagreb and in Belgrade fulfilled all set goals and justified the participants' expectations. All participants gained new knowledge and were made familiar with the best practices and successful solutions in other countries. They shared experiences on different problems in the implementation of certain segments and, in doing so gained valuable insights into the challenges that require special attention. The workshop reports are attached to this Report (Annex IV and Annex V).

At the same time, the expert from the Slovenian Institute for Corporate Security Studies was chosen to conduct the Feasibility Study. The Feasibility Study was designed to help evaluate the possibility of applying and implementing the good practices presented by foreign experts in our partner countries (Croatia and Serbia). The studies are attached to this Report (Annex VI).

The Project implementation process continued in Malmö/Revinge, Sweden, where Swedish partners organized the Project meeting/workshop on 3-4 February 2016 with the representatives of all Project partners.

The Guidelines containing best practices resulting from the workshops and assessed in the feasibility studies were prepared in March 2016. Their intention is to help other and future EU countries in their efforts to improve their own critical infrastructure protection. The Guidelines are attached to this Report (Annex VII).

The deadline for the mobile phone application (01/01/2016) was postponed and was finally presented at the International scientific Conference held in April 2016. The free mobile phone application is planned to be used not only during the Project but also in the follow-up.

The Conference preparations started well in advance in order for all the arrangements to be completed on time (hotel reservations, invitation letters, etc.). The papers to be presented at the Conference were selected by the Conference Program Committee and the Book of Proceedings was published after the Conference. The two-day Conference was held on April 11-12, 2016 in Split, Croatia with 105 participants coming from EU and non-EU countries. The Conference was the integration of the Project goals summing up all the efforts done throughout the Project and providing conclusions for the CIP follow-up strategy. The Conference report is attached (Annex VIII).

3.2. COMPARATIVE ANALYSIS

3.2.1. Initial and Current Time Schedule

All the deliverables were completed and delivered to Desk officers, mainly on time, but yet some of them needed postponement because of the scope of work and task complexity.

- *TASK A "Management and Reporting"*

The task was focused on coordinating and monitoring the Project progress and ensuring the achievement of the Project objectives as well as establishment of communication scheme between partners and delivery of reports to the European Commission.

The first deliverable was the **establishment of Management bodies** that NPRD and Project partners produced as part of Task assigned in Grant Agreement. The deadline was April 1, 2015 and nominations were delivered on March 26, 2015.

On May 1, 2015 we had the obligation of delivering the **Project plan** of Project implementation which was done on April 28, 2015.

The next deliverable was the **First progress report to the Commission on the technical and financial aspects of Project implementation** with deliverable date of July 1, 2015, which was sent to Desk officer on 30 June, 2015. We received comments which gave us better direction in further work on RECIPE 2015.

The Second progress report to the Commission on technical and financial aspects of Project implementation had deliverable date January 1, 2016 and was delivered on 30 December 2015.

Last deliverable of this Task will be this Final report inclusive with 30 August 2016 as deliverable date.

- *TASK B "Current State Assessment and Analysis"*

The deliverables of this Task were based on the analysis of the current state of critical infrastructure risk management at the partner countries national level – through panel discussions as the main activity of task which also helped to formulate national standpoints.

As part of the above mentioned Task, **Questionnaire was prepared and adapted to each partner country** (with date 01/04/2015) and was completed on March 26, 2015.

For the Questionnaire **evaluation report** we asked for the postponement of the deliverable. The deliverable date was **01/06/2015** but the Assessment Committee did not manage to finish it due to a large number of different data. A postponement of two weeks was requested (15th June), and it was sent on June 10, 2015, the version in the Croatian language, needed in order to produce national standpoints at the Panel discussion which was held on 16th and 17th of June. On 15th July, besides the already sent

Report in the Croatian language, we sent the translated analysis of national and EU sample of the Survey in the English language. With this, the "Questionnaire Data Analysis" was finalized, and it was conducted in accordance with Task B.

On August 28, 2015, we completed the **national standpoints reports** based on conclusions drawn from panel discussions in accordance with Task B and with given deliverable date of 01/09/2015. We delivered the Croatian and Serbian standpoints formed regarding critical infrastructure protection issues and the desired course of action. They were designed to serve as vital inputs for subsequent Project activities, among which joint workshops were planned for October 2015.

- **TASK C "*Exchange of Experiences and Best Practices*"**

The main guiding principle in this task is the fact that there are varying levels of critical infrastructure protection in relevant partner countries and the countries with developing or deficient CIP systems could profit from the achievements of the country boasting developed CIP system. The prime deliverables were the Feasibility studies conducted for assessing the implementation potential per country which was the basis for making Guidelines comprising best practices.

After **workshops** - held in Belgrade (13th October) and Zagreb (15th October) as Project Task C "Exchange of Experiences and Best Practices", we informed our Desk officers that they were very productive with information exchange among participants and acquired new knowledge. The next step for us was drafting the Workshop evaluation reports which were our obligation as a part of Task within deliverable date 15/11/2015 and which we sent on November 10, 2015.

Part of Task C which was predetermined in Grant Agreement of the Project was also performance of **Feasibility studies**. They needed to provide a selection of the best practices according to their implementation potential per country. As coordinators of the Project, NPRD consulted some experts experienced in conducting this kind of studies and suggested to the consortium Mr. Denis Čaleta, Ph.D., from The Institute of Corporative Security Studies ICS, Ljubljana on July 29, 2015. As all partners agreed, the first step in the Feasibility studies was subcontracting Mr. Čaleta, whereof Desk officers were informed on October 9, 2015. Finally, with additional customization and changes in the process which took some extra time of the planned deliverable date (1/2/2016), on March 16, 2016 "RECIPE 2015" Feasibility studies for the Republic of Serbia and the Republic of Croatia were performed, delivered and published on the RECIPE web site.

The following Project activity was publishing the **Guidelines** containing best practices in CIP field in the development of which we used the knowledge we obtained during joint workshops in Belgrade and Zagreb and the Feasibility Study. On February 19, 2016 a draft was delivered to the Project partners in order to validate the parts related to each partner countries. We also asked our Desk officer Ms. Biljana Zuber to distribute the Guidelines within the European Commission for comments and suggestions. Mr. Torben Fell (Policy Office European Commission, DG Migration and Home Affairs) gave us feedback with

some comments on ECI and informed us that the guidelines are very informative and they are offering interesting insights into CIP activities in the countries concerned. In general terms, as he said, "RECIPE 2015" aligns with two EC objectives: to disseminate best practices and foster engagement on CIP with countries neighboring the EU.

We waited until March 11 for comments from the EC and the approval of Desk officer. The Guidelines were published on RECIPE Web site on March 14, 2016, but due to technical aspects they were printed in the first half of June.

- ***TASK D "International Conference on critical infrastructure protection"***

The main activity of this task was International Scientific Conference that integrated the goals of the Project and summed up all the efforts done through the Project as well as providing conclusions for the follow-up strategy on CIP.

The date for publishing the **Book of proceedings** as deliverable for Task D was May 1, 2016. The activities for producing it started on April 22, and since the authors did not deliver all of them right on time (before the Conference) the first draft was produced on May 10, 2016. In the second half of May we posted the Book of proceedings on our Web site and it was released for printing in the first half of June.

The **Conference** was planned to take place by May 1, 2016 and it was held on April 11-12, 2016. Our Desk officer proposed and recommended some participants to add value to the Conference such as the Netherlands which has the presidency of the EU Council and has special interest on critical infrastructure protection. The representative of the European Commission was Mr. Alessandro Lazari, Ph.D. (European Reference Network for Critical Infrastructure Protection, Joint Research Centre) who gave us excellent presentation of the European dimension presenting the role of the Union Civil Protection Mechanism in strengthening infrastructure resilience.

The deadline for submitting the **Conference evaluation report** was June 1, 2016, and since on May 31 we were still working on the Conference evaluation report (waiting for inputs from panel moderators) we asked for a 15-day postponement on the deliverable. The report was sent on June 14.

Project follow-up strategy as planned activity had to define future cooperation modalities and solutions on the needs in the CI management system and was determined and delivered as specified, on June 1, 2016.

- ***TASK E "Dissemination of Project Results"***

The objective of this Task was to ensure the visibility of the Project tasks, actions and results.

Deliverable date for **Press release announcing the Project launch** as part of Task E was 01/04/2015 and NPRD and partners published the information about launching of Project "RECIPE 2015" right on time, already on January 28, 2015. NPRD published the press release on the web site, (links: http://www.duzs.hr/news.aspx?newsID=22163&pageID=144,http://www.duzs.hr/news.aspx?newsID=22

313&pageID=203), Faculty of Security Studies on their University site, (link: http://www.fb.bg.ac.rs/index.php?option=com_content&task=view&id=2712&Itemid=258), the same as University of Applied Sciences on their site (link: http://www.vvg.hr/index.php?option=com_content&view=article&id=1588:sredstva-iz-eu-fondova-za-projekte-vvg-a-i-duzs-a&catid=72:novosti&Itemid=34&lang=en).

Press releases were made in native languages.

In accordance with the task on 30/4/2015 we informed our Desk officers that we have **launched the Project web page** (visible at the following link: http://www.recipe2015.eu/) with the given deliverable date of 01/05/2015. Updating of the Web page was regularly done, following all events related to the Project. Thus, one of the main tasks of the Project was realized – the European visibility.

For the deliverable of a **free mobile phone application planned for** 1/1/2016 we asked for postponements of the deliverable due to the problems with the tender procedures. Also, we had some challenges related to agreements and contracts for the application, as well as defining the technical characteristics. As coordinator, NPRD assured the Desk officer that this postponement would not cause delay of some other deliverables important for finishing the Project on time. Regarding the development of test mobile application we gave a time limit to contracting companies for making the application by 3/4/2016 and completing the test run by 25/03/2016. A free mobile phone application was planned to be used not only during but also in the follow-up of the Project and we presented it at the Conference in April in Split.

At the Project partners level a Team for Promotion, Media Coverage and Protocol has been established. In this part the following activities were undertaken:

- media announcements of the start and end of the Project;
- ensuring the transparency of the project tasks, activities and results via web page and publishing of the contents on the web page during the entire project;
- ensuring media coverage of the workshops and final conference;
- coordination of invitations, arrival and work of the media representatives for the final Conference;
- ensuring contact persons for the media representatives in order to record statements, making reportages or other press forms;
- organization and coordination of participants in order to make reportage broadcast at the national television;
- producing the photo-documentation of the Conference;
- promotion of the Project results.

Apart from the official Project web page an overview of all the important information and activities that accompanied the Project were concurrently published also on all the official web sites, Facebook and Twitter profiles of the Project partners. Moreover, the Project was presented several times by Project

partners from Croatia and Serbia in various local and national television broadcasts. This is also one of the results of the Project in order to ensure the visibility at the local and national basis.

In addition, the report from the panel discussions figures at the website of the Belgrade-based Center for Risk Assessment and Crisis Management http://www.caruk.rs/panel-rasprava-analiza-stanja-i-potreba-u-nacionalnom-sistemu-zastite-kriticne-infrastrukture/

On the day of the completion of the Project all project partners published this news on their official websites as well as on the official Project website.

3.2.2. Planned and Used Resources

The financial activities related to RECIPE 2015 Project have been implemented under the Croatian Budget Act (Official Gazette No. 87/08, 136/12 and 15/15), International Accounting Standards, the requirements of the Agreement ECHO/SUB/2014/696006 and other external and internal rules and regulations governing financial activities. Pursuant to the above regulations, in 2015 and 2016 the plans were made in accordance with the foreseen.

NPRD, in its capacity of the Coordinator, coordinated the management of the allocated financial means. Out of the first instalment, amounting to EUR 183,904 (i.e. 60% of the total funding) received by the Commission, EUR 45,072.24 was communicated to the University of Belgrade, Faculty of Security Studies, the Republic of Serbia, EUR 29,900.15 to the University of Applied Sciences Velika Gorica, the Republic of Croatia, EUR 14,532.70 to the Swedish Civil Contingencies Agency and EUR 94,398.60 was held for Croatia.

Each Project partner prepared their financial plan in accordance with their individual obligations and they prepared their financial reports according to the prescribed financial forms. Any expense-related ambiguities or questions were addressed to the Commission by authorized persons in accordance with the arrangements made at the work meetings.

Procurement activities were executed in line with the Croatian Public Procurement Act (Official Gazette No. 90/11, 83/13, 143/13 and 13/14) and other external and internal rules and regulations governing the procurement activities. All objects of the procurement and the prescribed public procurement procedures were published on NPRD web pages as part of Public Procurement for 2015 and 2016. The procurement objects were determined according to the Accounting Plan as part of the Regulation on Budget Accounting and Accounting Plan (Official Gazette No. 114/10, 31/11 and 124/14). For all accomplished procedures and contracted expenses, the documentation was issued confirming the creation of financial obligation.

During the realization of the foreseen activities, some modifications in terms of harmonization with the realistic needs were required. Any changes and modifications to the Financial Plan and the Procurement Plan were recorded and made in order to suit the realistic needs and realistic financial possibilities while

still keeping in mind the necessary quality level of goods and services needed for unobstructed realization of the Project tasks. The financial reports with all the indicators prepared in accordance with the prescribed forms are attached (Annex IX).

3.2.3. Expected and Actual Results

The expected Project results were:

- *Facilitated exchange of knowledge, experiences and best practices among Member States and beyond*

In the frame of the three main Project objectives (public-private partnership in the field of CIP, establishment of the mechanism for sensitive information/data exchange in the CIP system, setting of preconditions for the establishment of national CI Centres), at two one-day national panel discussions (one in Zagreb, one in Belgrade) as well as two international workshops (Zagreb and Belgrade) and international scientific Conference, experts of different profiles, members of the scientific community and operators of critical infrastructure exchanged the knowledge, insight and experience in the field of risk, risk management and protection of critical infrastructure**.**

- *Enhanced stakeholder communication both at national and international level*

Project activities – national panel discussions, international workshops and international Conference which were a perfect opportunity to share best practices among relevant stakeholders for the benefit of future activities and real emergencies.

- *Strengthened mutual support and collaboration between all relevant public and private sector critical infrastructure protection partners*

During the Project activities (panel discussions, workshops, conference) relevant stakeholders - state bodies, CI operators, both public and private, and academic community came together and discussed the possibilities of further cooperation between the public and private sectors and the common benefits in the area of critical infrastructure protection, as well as on the role of academic community in this process. It was also agreed which recommendations will be submitted to the government regarding improvement of existing regulations or the adoption of appropriate regulations in the countries which do not yet have a system of public-private partnerships.

- Boosted scientific and research activity in the field of critical infrastructure risk management as an outcome of encouraged involvement of academic community in problem solving processes

Through the Project activities it was found and concluded that in all critical infrastructure risk management processes, it was necessary to intensively involve the scientific community and to use the results of scientific research in order to increase critical infrastructure resilience; stated includes education and training of stakeholders.

- Guidelines prepared intended to pave the way for the establishment of an optimal risk management system related to CIP in the Project partner countries (where missing)

One of the Project outcomes are Guidelines that are prepared on the basis of experiences and good practices of the Kingdom of Sweden and some other European countries with developed critical infrastructure protection system, taking into account the situation in the Republic of Croatia and the Republic of Serbia, 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 neighboring countries.

- Guidelines made available to the EC for further dissemination and use

The Guidelines are printed and available to the EC as well as to all participants in the critical infrastructure protection system in Croatia and neighboring countries. The Guidelines are also posted on the Project website so they are available to the public.

- Increased resilience and level of protection of European critical infrastructure resulting from improved coordination and cooperation between stakeholders and from the exchange of best practices

It is expected that the attainment of the Project objectives will increase the critical infrastructure resilience and thus raise the level of critical infrastructure safety; in this process coordination and cooperation between stakeholders and exchange of best practices play a crucial role.

- System approach assessment methodology for CIP established, taking into consideration cross-sectorial and cross border dimension of critical infrastructures

As result of the acquired knowledge during the Project in the Republic of Croatia there has been improvement of the system approach assessment methodology for CIP, taking into consideration cross-sectorial and cross border dimension of critical infrastructures. Since the Republic of Serbia is yet to create their own normative framework, all the knowledge acquired during the Project will be multiply meaningful and also specific for the indicated area.

- Defined follow-up strategy on CIP in the relevant countries

The Project has defined the continuity which will be held after the completion of the Project, defined as activities that will take place or continue in the Republic of Croatia and the Republic of Serbia.

- Assessed and defined needs for further education and training of public and private sectors in the related area (educational programs, exchange of experts)

Needs for further education and training, including exercises (curricula, manuals, textbooks, trainers) in the field of Critical Infrastructure Protection are assessed. Defined capacity building of public and private stakeholders is feasible and sustainable. There are capacities and resources for its implementation, including educational and scientific institutions, after the Project ends and it can be held continually.

- Increased awareness and knowledge based on disaster risks threatening infrastructure and disaster prevention

During all the activities in the Project as well as additional contacts with experts who participated or were recommended for contact through persons who participated in the activities and were contacted indirectly, there has been an increase in the awareness and knowledge about the risks that threaten CI and at the same time measures were discussed for the prevention of disasters in the CI area.

4. EVALUATION OF PROJECT MANAGEMENT / IMPLEMENTATION PROCESS

At the beginning of the project a comprehensive project team was formed and work tasks were assigned according to the following principle – three management teams (overall Project management, Administrative management and Financial management) and three committees (Assessment, Academic and Conference committee).

Communication among teams took place on a daily basis via e-mail and occasionally by phone. Every official event within the project was additionally used for the meetings of project partners. Since NPRD and VVG are located very close to each other and they cooperate within other projects, bilateral meetings of these partners were organized very often. Other partners within the project were then informed by e-mail about the conclusions of the meetings. Several times Skype video conferencing among partners was organized.

4.1. POSITIVE ASPECTS / OPPORTUNITIES

Each partner brought into the project previous institutional memory, knowledge, contacts and determined high-quality persons who would be involved in the project. A combination of partners coming from different backgrounds and bringing different perspectives into the project proved to be of high quality. Thus, NPRD, as coordinator within the CIP system being formed in the Republic of Croatia along with their own resources could bind in a certain way other bodies of government administration, regulatory agencies and potential national critical infrastructures with whom it has been working on these issues as well as in other fields. VVG and FB as primarily educational institutions dealing with the CIP area at the academic level brought into the project relevant knowledge about the models and methods of modern study of this issue. The MSB representatives, on the other hand, brought into the project the knowledge and experience of many years of dealing with these issues, the examples from practice and advice how to do certain things in the initial years of system formation.

4.2. INTERNAL AND EXTERNAL DIFFICULTIES ENCOUNTERED

Since this refers to project partners who have multiple experiences of participating and managing the international projects, as well as selected individuals to participate in the project, no challenges have been recorded during the project that might have influenced the realization of certain activities.

The only issue that needs to be better planned and further improved is the public procurement process that caused delays. As a lesson learned, we need to plan in advance and to include the people

conducting the procurements in all project activities from the project start (even in the project proposal preparing process).

4.3. PARTNERSHIP / CORE GROUP COOPERATION (as appropriate)

Positive spirit was present among partners during the entire period of the project duration. This has been evidenced by the proposals about joint continuation of the related activities listed in the Follow-up section of this report. Additionally, during the project the relationship has been expanded as well as the understanding about the possibility of future cooperation and the areas where cooperation would be required with the aim of building and maintaining the best possible CIP system in the countries in which the project has been implemented and to exchange knowledge and experiences into other countries.

4.4. COOPERATION WITH THE COMMISSION

The cooperation with the Commission is estimated as outstanding. Communication was based on the official correspondence via e-mail, but always prompt on both sides. As the manager of the project NPRD was in charge on behalf of project partners for direct communication with the Desk Officer designated by the Commission for this project. Also, the Desk Officer followed the project within the Commission and its bodies trying to find answers to questions raised by the project partners, and it was also very active in finding adequate experts who participated at the international scientific conference. In addition, the Desk Officer maintained constant visibility of the project implementation in the Commission and this resulted in the invitation to present the Project at the Civil Protection Committee meeting in Brussels on 18 May 2016. The participants were informed about the RECIPE 2015 Project through presentations of the implemented project activities, the expected and until then fulfilled tasks as well as the main objectives that span the entire project (public-private partnership in the area of CI protection; establishing a mechanism for the exchange of sensitive / classified data / information among the system stakeholders and creation of preconditions for the development and establishment of National critical infrastructure centers). The representative from the Netherlands gave feedback on how EC recognized “RECIPE 2015” as a valuable project, especially emphasizing the problems of public-private partnership noticed by the project consortium as an important item in improving the CI protection system. The officer for the policies and implementation (Policy officer) from DG ECHO, Mr. Bower, emphasized the presented fact that the project included the partner countries with different levels of CI protection and that thus the knowledge exchange allows the flow of recommendations and realization of opportunities to recognize potential supplements to the mechanisms of CI protection, thus proving the usefulness of the project. The impressions of the Civil Protection Committee members on the implementation of the project are exceptionally positive and it has been determined that the knowledge acquired by the project will provide a clearer perspective regarding levels of development of the CI protection system throughout EU, being thus of outstanding benefit in the efforts of the European Commission and

member countries for their balancing as well as certain contribution to the creation of the necessary consensus about the protection model of the European critical infrastructure. The project team received the final confirmation from DG BUDGET according to whose selection the "RECIPE 2015" Project was isolated as an example of a high-quality project and well spent EU means, and all this is the outcome of adequate visibility in the implementation of the activities of the project itself. In general, all the project partners agree in the assessment that the project has been excellently followed and supported by the Desk Officer.

During the Project implementation Desk Officer No. 1, Ms. Martina Topličanec nominated by the Commission was assigned to other duties and left the project monitoring, and his role was taken over by Desk Officer No. 2, Ms. Biljana Zuber.

4.5. COMMENTS ON THE EUROPEAN VALUE ADDED

The special value of the Project is the exchange of knowledge and experiences and the best practices among European Union member countries and those who tend to become ones. During the entire project numerous CIP experts from various parts of the European Union as well as the South-eastern European countries were included. This was especially visible during the international scientific conference on 11 and 12 April 2016 in Split attended by the experts and practitioners from the government bodies, regulatory agencies, critical infrastructure, academic communities, students from more than twenty countries from Europe and USA.

The results of the project collected and published in the deliverables and on the official web site of the project (www.recipe2015.eu) are very topical and useful. The materials will be of use primarily to the countries that are at the beginnings of forming the CIP system as well as to those that already have an established system in order to check the new ideas and practices achieved by the project partners. The project results will certainly represent a certain guide to all the interested in CIP and CIPR models as well as educational materials for the students since this area, no matter how well discussed, lacks high-quality materials, solutions and examples.

During the project, the representative of DG HOME, Mr. Torben Fell stated that he considered the project as extremely important and that its results will be used in cooperation with the third countries.

4.6. LESSONS LEARNED AND POSSIBLE IMPROVEMENTS

The main identified lesson from the project is that it is necessary to continue with the next project based on the results of the existing one. Why is this important? It is very difficult to achieve new solutions and due to many obligations specific attention is paid to a certain area. This project managed to mobilize experts and to draw attention not only in the countries of project implementation, but also wider, and

this has to be continued as long as there exists positive idea and willingness in the development of the CIP area.

Special recommendations are oriented towards the need of more frequent communication and meetings of the project partners since the best ideas and results have been achieved precisely in the immediate exchange of ideas and attitudes.

Stronger emphasis in the future should be on participation of the maximum number of end users into the very project. This has proven to be an extremely demanding task since from some only declarative support to the project has been obtained without actual participation.

5. ACTIVITIES

All the planned activities foreseen by the Project documentation (Agreement) have been carried out in all the countries of Project implementation in coordination with the Desk officer. The emphasis in performing the activities was on raising the awareness about the relevancy and importance of the respective topics, promotion of interagency cooperation and cooperation among the Project partners as well as including the experts from other EU member countries in the implementation of the Project.

5.1. COMPARISON BETWEEN INITIALLY PLANNED AND ACTUALLY IMPLEMENTED ACTIVITIES, INCLUDING MONITORING, EVALUATION AND DISSEMINATION

5.1.1. Panel discussion

The Project foresees the organization of panel discussions in the Republic of Croatia and the Republic of Serbia. In order to encourage the target groups to take part in both sessions, partners agreed to organize panel discussions during two consecutive days. Both Croatian and Serbian events were held on same dates (16 and 17 June 2015). Regarding topics the panel discussions were prepared on the basis of results of the Questionnaire that were done, sent for filling in, collected, analyzed prior to Panel discussions (these will be explained in detail in Item 6 of this Report).

The expected result was to collect high-quality and evidence-based inputs which would allow creation of a document defining national standpoints and addressing critical issues and emerging needs in the national CIP systems. The risk of encountering certain difficulties regarding all relevant stakeholders' involvement was planned to be mitigated with timely information about the Project objectives.

The panel discussions in the Republic of Croatia and in the Republic of Serbia were well prepared by the Project partners from these countries and carried out. In the Republic of Croatia the Panel discussion was held in the VVG premises. In the Republic of Serbia the Panel discussion was held at the Institute of International Politics and Economics, Belgrade. The Project visibility indicator and the interest of experts from various CI areas for the Project topics and the Project in general have been confirmed by the fact that the number of the interested parties was much larger than the initially planned number. Therefore, collaboration in organizational aspect in Croatia proved to be successful since 47 participants from 26 governmental, public and private organizations took part in the dynamic and lively discussions. The Panel discussions held in Serbia were attended by representatives of state bodies and relevant ministries of the Republic of Serbia in the area of CI operations and protection – 33 participants attended the first panel (16 June), 20 participants attended the second panel (17 June).

Additional visibility of both Panel discussions and the European dimension of implementing the entire project were realized by the announcement and publishing of the news and conclusions on the Project official website as well as on the websites, Facebook and Twitter profiles of the partners from Croatia and Serbia, and the TV broadcasts and in the University journal.

From the organizational and implementation aspect the analysis of the Project management after the realization of the Panel discussions showed that the preparation and monitoring of Panel discussions in Croatia and Serbia was successfully performed. The evaluation showed that apart from the interest of CI experts in this topic, a platform is necessary that will provide to everyone possibility of discussion and cooperation on the key topics. This is why the respective Project proved as precisely providing this opportunity and need in Croatia and Serbia. The very interest and commitment at Panel discussions proved that there is need for additional activities in promoting cooperation, exchange of experiences and possibility of acquiring new knowledge in the respective field.

The very conclusions and results of Panel discussions were formed in the national standpoints and disseminated to numerous receivers via different systems. These have been used, and we know this from feedback, as they contact the Project partners in this respect. Also, great value of the mentioned activity lies in the horizontal and vertical networking of various experts who are all important for the implementation of the activities in the field of strengthening the resilience and protection of CI.

5.1.2. Joint workshops

The action was planned as part of “Exchange of experience and best practices” Task and in application form was conceived as: discussion of national standpoints formed at Panel discussions in two workshops (organized one in Croatia, one in Serbia) intended to fill the gaps in CIP systems through the share of best practices mainly presented by the Swedish partners, but also participants/experts with well-developed, advanced systems from other Member States.

Expected results: share of the best practices, provided recommendations, raising awareness about more efficient solutions.

In the preparation phase the Project partners contacted all potential participants – experts from EU member countries, national CIP points and participants from Croatia (private sector, operators with the perspective of the actual application of CIP, participants from ministries competent for sectors of critical infrastructure).

Workshops were held in Belgrade (13 October) and Zagreb (15 October) and they were very productive and highly successful. All goals of the Workshop in Zagreb and Belgrade were fulfilled. We were satisfied with information transfer among participants and collected new cognitions. The Workshop Evaluation Reports are attached to this Final Report (Annexes IV and V), with this action implementation elaborated in details.

After delivering the Report, our Desk officer gave us feedback, acknowledging the quality of discussion on all the important issues related to CIP in the two countries. As there was a representative of Joint Research Centre (European Commission) present at both workshops, the importance of linking the activities in the workshop with the EU policy in CIP was also highlighted.

In conclusion, the Workshop justified the expectations, new knowledge was gained and experience was shared with numerous results, recommendations and good practices to implement on the national level.

5.1.3. International scientific conference

The Conference, as the main activity, was planned for integrating goals of the Project summing up all the efforts done throughout the Project and providing conclusions for the follow-up strategy on CIP. The two-day Conference was to cover the issues of CIP in general and on the main topics: 1. Public-private partnership in CIP; 2. Challenges and mechanisms for the exchange of sensitive information among the stakeholders of CIP system; 3. Setting preconditions for the development of national CIP Centers.

The expected results: providing recommendations by different experts on the establishment of an optimal CI risk management system, presenting academic approach to CIP.

The International Scientific Conference was held on April 11-12, 2016 in Split with a large range of participants – representatives of the scientific community, private and public sectors from partner countries, EU (the Netherlands, Greece, France, Slovenia, Hungary, Finland), non-EU countries (Bosnia and Herzegovina, Montenegro and Macedonia) and the United States of America, who presented their views on CIP. The Conference was split into three topical areas (panels) in line with above mentioned Project objectives. “RECIPE 2015” Conference highlighted the importance of many aspects, emphasizing the need for improvement on specific subjects such as raising awareness about the importance of CI protection to a satisfactory level, wider social perception, cooperation between public and civil sector, effective models of PPP, normative framework etc. Extensive Conference evaluation report is attached in Annex VII.

We are fully satisfied with the Conference realization, experts who participated, number of the total number of participants, media coverage as well as with the quality of presentations.

In the frame of Conference activities we had one day meeting right after the Conference in order to evaluate it and discuss future CIP modalities. It was concluded that the Conference fulfilled the cause, and the quality of the Conference was confirmed immediately afterwards with extremely positive feedback from the participants.

5.1.4. Follow-up strategy

The follow-up strategy was planned as the future goal of the Project summing up all the next steps needed to be done to provide a continuation of the current Project results and efforts.

The expected results: Project follow-up strategy determined in relation to the implementation of guidelines, future cooperation modalities and any other requirements in the protection of CI such as, for example, the need for further education and training of public and private stakeholders in the related area.

The Project has opened to all Project partners a perspective regarding the number of activities that need to be done in the future and that we, in the Republic of Croatia and the Republic of Serbia are at the start of the journey. In the Follow-up strategy we have recorded the basic direction indicators in which we should move in order to continue with the successful results and interest of all the active participants in the CIP process in the future as well. A detailed elaboration of the Follow-up strategy can be found in Item 8 of this Report.

It certainly has additional value at the EU level since numerous planned activities are complementary for all the countries dealing with constant arrangement of the CIP area.

6. PRESENTATION OF THE TECHNICAL RESULTS AND DELIVERABLES

The Project planned that for every activity there is a pre-activity and the result in the form of deliverables from the beginning to the end of the Project from the simpler to more complex achievements. Chronologically, after establishing the project management and assignment of concrete activities to Project teams, the first activity performed in the Republic of Croatia and in the Republic of Serbia was to produce a questionnaire. The questionnaires served as the basis for discussion at national workshops and the products of these were national standpoints. Next step was producing Feasibility studies that have provided selection of best practices according to their implementation potential per country which was also based on national standpoints and previous cognition gathered during project RECIPE. As highlight of the project, we have organized the conference which has produced Book of proceedings that brought together visions of experts on CIP. Along with Book of proceedings, we have published Guidelines which are containing best practice in CIP field and recommendations for its development made by using the knowledge we have obtained during joint workshops and the Feasibility Study. Final product and written deliverable of our project RECIPE was Project follow up strategy which as planned activity had to define future cooperation modalities and solutions on needs in the CI management system identified during implementation of the project.

The same as all activities in the Project were successfully realized, so also all deliverables were made on time and regarding content they are at the expected level. Further you will find a brief overview of each deliverable.

6.1. DESCRIPTION OF INDIVIDUAL DELIVERABLES, PURPOSE OF THE DELIVERABLE, EVALUATION OF THE DELIVERABLE, VALUE-ADDED – IN PARTICULAR EUROPEAN VALUE – ADDED AND TRANSFERABILITY – OF THE DELIVERABLE, DISSEMINATION

6.1.1. Questionnaire

The Project envisaged preparation and analysis of a questionnaire to be adapted to each respective country, where it would provide questions regarding current national CIP-related legislation, its positive aspects, downsides, and potentials for improvement. It was planned that the questionnaire be created by the Assessment Committee and its results would serve as the basis for panel discussions and as a stepping stone to build on other future activities. The Project members expected to get an overview of the current state of affairs regarding CIP issues, also striving to collect information of system deficiencies and needs for improvement. In order to avoid obstacles in implementing activity due to different

national organization structures, the questionnaire was to be adapted to individual country specificity (Republic of Croatia and the Republic of Serbia).

The final version of the Croatian questionnaire was sent by email to 70 addresses of the mentioned ministries, relevant EU and US institutions, and Project partners. After several repetitive emails, phone calls and personal contacts AB3 received 7 duly filled questionnaires and feedback from 17 participants. Invitees from EU member states had the highest response rate. At the dedicated meeting AB3 and the Project Coordinator discussed the methodology of analysis, and agreed on closer collaboration in data interpretation. Considering the high number of open questions and the nature of the topic, qualitative methodology including descriptive statistics, was chosen as the most appropriate. AB3 created a tailor-made database, developed list of codes for grouping similar answers, inserted collected data and drafted bilingual evaluation report (in Croatian and English) based on internal team's and Project Coordinator's inputs. The activity was implemented as scheduled.

FB prepared the questionnaire in the Serbian language and sent it to all relevant state institutions (over 20 Ministries, Directorates and Agencies), as well as to institutions in other Western Balkan countries (Montenegro, Bosnia and Herzegovina and Macedonia) in order to assess the current state of affairs related to CIP. This activity was performed between March and May 2015, due to slow response of certain institutions.

The activities of assessment and analysis were performed completely and at a satisfactory level from the methodological point of view. There were some difficulties in the questionnaire construction process since the Project includes many partners, which took additional time so there could be additional efforts in coordination. Another possible improvement in this part of assessment activities would be to include data and social research specialist in the beginning in order to define more precisely the goals, targeted population and research method. This would eventually bring more precise and complete data..

Due to open-type questions, the answers showed a large variation and inconsistency in perception and knowledge of the subject matter. Thus, there were some difficulties in their analysis. It seems that some of the participants were not motivated enough to provide precise answers and some of them did not understand the questions entirely. As expected, differences were noticed between examined countries' CIP politics and practice. Most of the national answers provided expected satisfactory results. However, there were some variations in national answers that were not expected but could be explained by the mentioned lack of motivation or understanding. Additional explanation could be that most of CIP aspects in Croatia have not yet been defined, so some answers are the logical result thereof. Furthermore, it should also be taken into consideration that information on identified critical infrastructure is largely classified and some of the respondents may have declined to answer the related questions or they gave a negative reply.

The obtained data fulfilled the expected goals and provided solid and useful baseline and a kick-off for the other followed activities such as panel discussions, workshops and final conference. The survey

offered initial data for unique guidelines for the critical infrastructure protection and its improvement at the regional level.

The results were presented on the national panel discussion held in Velika Gorica, Croatia (University of Applied Sciences VG) which stimulated significant amount of participants' reactions which entirely contributed to the general discussion. Learning of the presented results of the survey motivated some of present national CIP coordinators to revise their answers and to complete the questionnaire again. Feeling a moral obligation to enable this for the participants we decided to apply the questionnaire again to all of the ministries. Future comparison of the initial and final data are yet to be considered but it is not relevant for this Project as the fact that some of the motivational aspects could be improved by pointing out knowledge shortcomings and inconsistency in the knowledge of the responsible.

6.1.2. National standpoints

National standpoints are based on conclusions drawn from panel discussions in accordance with Task B „Current State Assessment and Analysis". Croatian and Serbian standpoints are formed regarding critical infrastructure protection issues and desired course of action. They served as vital inputs for subsequent Project activities, among which were joint workshops.

National standpoints are related to the analysis of the current national legislation and practice, their strengths and weaknesses, possibilities for their improvement and the analyses of regulations and practice in the field of identification and interdependencies of CI with regard to the requirements of the Directive 2008/114/EC.

The content of the National standpoints are as follows: Analysis of the current situation; Definition; Identification and legal regulation of CI in Republic of Croatia and Republic of Serbia; Public-private partnership in the CIP; Classified data sharing in the CIP system; Preconditions for the development of the National Critical Infrastructure Protection Centre.

Both National standpoints were made maximally concretely and correctly in accordance with the currently available data that could be collected and analyzed. A much bigger challenge was for the Project partners from the Republic of Serbia, who, lacking the CIP normative framework had to discuss much more at the hypothetical level and with more unknown variables.

The mentioned National standpoints have additional value at the EU level since it may be of interest for certain countries that still have not established their own CIP systems to see the complete overview of solutions and even new ideas from Croatia and Serbia. The added value is for the European Commission that may see and assess how a member country Croatia and an accession country Serbia have been developing this significant area. Also, the produced documents are of interest to the researchers and scientists, and besides, the colleagues from the USA have also shown interest in the mentioned documents.

Both documents in both countries have been delivered to the official institutions that are important factors of the CIP system. The information thereof was sent via network stations of the Project partners to the interested public and both documents were published on the official Project website.

6.1.3. Feasibility study

Feasibility Study is a set of measurable indicators that made it possible during the Project to make decisions related to national standpoints about which type of CIP system to propose. The purpose of the Feasibility Study is to compare several proposed models in order to obtain the result of the most efficient and effective one for complete functioning of the entire CIP system. Also, the Feasibility Study gives a proposal of an optimal and rationally structured National center for critical infrastructure protection, optimal, rational proposal of the model of sensitive data exchange and optimal, rational proposal of the relationship model of the public-private partnership.

It is precisely on the basis of the Feasibility Study that a decision has been made about further orientation of the National center for critical infrastructure protection. After the Project, the Study will be relevant for further development of the National center for critical infrastructure and these guidelines will be used to propose to the Government how to proceed regarding the CIP system and its improvement. Furthermore, the Study facilitates planning of further Projects and support of the development of the critical infrastructure protection system in the region.

The contents, structure, form and scope of this Study are entirely in compliance with the expectations of all the Project stakeholders, clearly showing that all the necessary elements have been included. First of all, various analyses have been included (socio-economic, cost-benefit, analysis of the NCCI organizational position, SWOT analysis, etc.) as well as assessment and evaluation that have been structured in detail and regarding contents, thus rendering the Study relevant, which means also adequate for its further use of the purpose of realizing the RECIPE Project as well as for its usage in the future.

The Feasibility Study has been developed on concrete countries (Republic of Croatia and Republic of Serbia) and as such cannot be applied to any other country since specific conditions of every country individually have been referred to, which is considered as extremely positive since in this way the knowledge on different systems of CIP are being expanded. However, it certainly is of value for the EU because due to the comparative overview of both mentioned countries, the EU has the possibility of comparing the condition in other European countries as well, even in countries that are not part of the EU, i.e. that are in the accession phase or those that would like to join the EU, and all this for the purpose of monitoring and improvement of the entire CIP system at the EU level.

The Feasibility Study was presented, i.e. disseminated at the RECIPE Conference in Split which was attended by the national coordinators who are persons in charge of the CIP in the Republic of Croatia

and they were informed about the result of the Project which provides and proposes the direction how to proceed in order to improve and enhance the critical infrastructure protection system.

The Feasibility Study will continue to be discussed in the future and it will continue to be used as the basic document for future Projects and planned activities in the sphere of improvement and enhancement of the CIP system.

6.1.4. Guidelines

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 neighboring 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 centers.

The Guidelines include the best knowledge that was acquired during the Project. We have looked at the practice and experience of the EU member states whose representatives participated actively in the Project, then at the solutions that have been applied in other countries all the way to the USA – this was realized through search of the websites, reading technical literature, and personal contacts with experts from these countries.

The Guidelines have a special value at the EU level since they represent a unique document which summarizes the best examples and suggestions of good solutions for the questions related to three main Project topics. This will certainly serve many member countries in order to see and compare their solutions and plans for the development of the CIP area. They represent added value for the researchers, students, and interested public.

This output was disseminated via printed Guidelines that were distributed among the Project participants, interested parties as well as published on the Project website.

6.1.5. Mobile application

One of the Project Recipe's deliverables carried out under the task Dissemination of Project Results was the development of the mobile application NWK Recipe (Recipe Network). The idea of creating such an application started with initial contacting potential partners where we were once again convinced how

poorly we were connected with other CIP stakeholders. As we started to develop the Project idea, we encountered the obstacles which would have been easier and faster to solve if we had a well-developed network of stakeholders.

The idea behind Recipe NWK mobile application is to compound a network of interested professionals involved in the protection of CI, providing us with information about their area of expertise and competences if we needed to contact them for business cooperation. Further development of the idea led us to enable the application for sharing the document, Project idea proposals, Project presentations and dissemination, events promotions, etc.

The funds allocated for the development of this mobile application were unfortunately not sufficient to realize all of the above for all operating systems in use, so we decided to develop a more complete application for a single operating system. We have selected Android operating system because of the greatest number of users.

The mobile application was designed, tested and presented at the Recipe Final Conference. The application will be promoted through the regular work of the partner institutions by experts from those institutions starting using all of the functionalities provided. It will also be promoted through the expansion of user network outside the Project partners' institutions.

The following step would be obtaining funds to make the application available for use on other mobile operating systems.

7. EVALUATION OF THE TECHNICAL RESULTS AND DELIVERABLES

7.1. GENERAL LESSONS LEARNT

Overall expected results of the Project are:

- Facilitated exchange of knowledge and experiences among countries;
- Higher level of awareness of risks that threaten the critical infrastructures;
- Larger knowledge base about the prevention against disasters;
- Improved communication among national and international stakeholders;
- Reinforced mutual support and cooperation among all relevant partners from public and private sector;
- Reinforced scientific and research activity in the area of risk management regarding critical infrastructures;
- Guidelines for the establishment of optimal risk management system of critical infrastructures in partner countries;
- Guidelines available to the European Commission for further dissemination and use;
- Improved resilience and level of protection of European critical infrastructures as result of enhanced coordination and cooperation among stakeholders;
- Established methodology of system protection assessment based on systemic approach;
- Defined long-term strategy about critical infrastructure management in the encompassed states;
- Defined requirements for further education and training of public and private sector (educational programs, exchange of experts).

During the Project the partner exchanged at workshops, panel discussions and visits to other countries the knowledge, experiences and best practices of their own countries, thus contributing to the realization of the above-mentioned expected results.

Through institutional cooperation in the Project the conclusion was reached that the countries fail to have a sufficiently developed protection of critical infrastructures at the national level since there is a lack of awareness both in public and in the leading structures of the countries. In order to change this, it is necessary to arouse the interest of the public, i.e. raise the awareness of the importance of critical infrastructure protection to a satisfactory level.

Also, apart from the Directive 2008/114/EC which speaks about the identification and naming of the European Critical Infrastructure as well as the strategy "***Cyber security Strategy of the European Union: an Open, Safe, and Secure* Cyberspace**" in which the concept of "resilience increase" from cyber-attack is mentioned, there is no common strategic plan, i.e. a document at the EU level that would provide the

key guidelines about the increase of the critical infrastructure resilience through mutual cooperation and exchange of best practices. The responsible parties shall have to write the mentioned strategic documents that would obligate the member countries and those that will become members to harmonize the protection and resilience of the critical infrastructure with the made strategic document.

The most important document of this Project is the "***Guidelines for Critical Infrastructures Resilience Evaluation"*** that showed the difference between the concepts of CIP and critical infrastructure resilience. ***Infrastructure protection*** is the ability to prevent or reduce the effect of an adverse event. ***Infrastructure resilience*** is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

The Project has determined that it is necessary to implement the resilience capacities that are intrinsic properties of infrastructure system in order for the infrastructure system to become resilient.

The resulting "***Guidelines for Critical Infrastructures Resilience Evaluation"*** from the RECIPE Project can serve to relevant, representative bodies during the writing of the strategic document about the increase of the critical infrastructures resilience at the EU level. Also, the Guidelines can be used for the dissemination of the very RECIPE Project.

We have learned in which way to approach the joint solving of problems. First of all, it is most important to identify the existence of the problem as soon as possible, in order to be able to intervene on time and thus prevent its further escalation, i.e. in order to eliminate the entire problem completely. Once the problem is identified, appropriate measures and actions are undertaken in order to influence it positively. Therefore, it is necessary to have appropriate tools that will manage to identify the problem on time as well as the instruments that, in case of a problem, will eliminate them in the most efficient and effective manner.

During the Project National Standpoints on the CIP have been developed and they show four main objectives and interests which are the following:

1 Development of CIP related legal and strategic framework (Republic of Serbia only, as the first beneficiary)
2 Public-private partnership in the area of CIP,
3 Establishment of the mechanism for the exchange of sensitive information/data among participants in the CIP system,
4 Establishment of preconditions for the development of national Centre for Critical Infrastructures.

Ad 1) Development of CIP related legal and strategic framework

A comprehensive and clear approach to the issue of CIP includes adoption of key documents in this field. Critical Infrastructure Protection Strategy would represent the most important strategic document with which basic directions of CIP would be established. Another option would be amendment of the existing relevant strategic documents (National Security Strategy, National Strategy for Protection and Rescue in Natural Disasters) so as to include the concepts of CI and CIP.

Apart from the Strategy, another key document will be the Law on Critical Infrastructure or Law on Critical Infrastructure Protection. This Law would establish the legal framework for defining, identification and determination of national and European CI. The Law would define the key CIP concepts (infrastructure, critical infrastructure, vital infrastructure, key infrastructure major, significant, threat, risks, hazards, vulnerability, consequence, protect, resilience, interdependency, prevention, mitigation, response, recovery) and also identify subjects of protection, competencies of state institutions, identification criteria, protection models and methods etc. Another option, as suggested by the relevant authorities would be the amendment to the draft Law on Natural and Other Disasters Risk Reduction and Emergency Management, which would include CI and CIP definitions and provisions. The new Law would be followed by bylaws that would give more details and practical solutions for CIP measures and tasks.

Once the Law (and the Strategy) is adopted the Government will identify relevant Ministries/Sectors, and the later the ministries/sectors will identify critical infrastructure under their jurisdiction. The CI identification process will be coordinated by the Expert Network/Intersectoral work group, coordinated by the Sector for Emergency Management of the Ministry of Interior.

The Law on CI and its bylaws will enable formal identification and prioritization of CI sectors and assets/facilities. First, the CI sectors will be identified and that task may be responsibility of National Forum for CI in which stakeholders from public and private sector will participate. Once the CI sectors are identified – and it will be suggested to reduce the number as much possible, due to the budget constraints (not more than ten) – identification of CI assets within particular sectors will be initiated. For those activities cooperation and partnership between public and private sector will be of utmost importance. The same goes for the prioritization of CI assets, which will be also done within sectors. Identification and prioritization will be done in accordance with the criteria presented in the bylaws to the Law on CI.

Ad 2) Public-private partnership in the area of critical infrastructures protection

Through the Project it has been learned that a cooperation of public and civil sector is necessary since its aim is to improve the realization of investment in the infrastructural projects or other types of operations because of which the public-private partnerships can be an efficient way of implementing the

obligations that ensure the realization of objectives of public policies connecting various forms of public and private resources.

In public-private partnership it is necessary to focus also on certain elements, i.e. guidelines for success and sustainability of cooperation for the purpose of implementing the objectives of resilience strengthening and protection of critical infrastructures, such as:

- Definition of roles and responsibilities;
- Application of resources;
- Openness for the development of capacities and changes;
- Realistic expectations.

It has also been learnt that the private sector is best familiar with the critical infrastructures requirements. Since the private sector in the western countries is the owner, i.e. manager of more than 80 percent of national critical infrastructures, it is understandable that it is precisely the private sector which is best familiar with their weaknesses and advantages, and it must strengthen the resilience and protection of critical infrastructures. The result is that the public sector requires the cooperation of the public and private sector in the mentioned field.

Furthermore, the Project has determined that the Republic of Croatia has to improve the normative framework of the activity of the public-private partnership in strengthening the resilience and protection of critical infrastructures to make it as clear and flexible as possible and open for new investments and maximal cooperation of the public and private sector. In the Republic of Serbia the Law on Public-Private Partnership should be amended to include provisions relevant to the situations in which the private partner is a CI owner or operator. However, this may be done only once the Law on CI or the amended Law on Natural and Other Disaster Risk Reduction and Emergency Management is adopted. The Project has shown that, for the maximal interrelation of the public and private sector, the existing legal framework has to be expanded in the following way:

- the area of critical infrastructures should become special subject of the Act on Public-Private Partnership;
- adjust the procedure of proposing and approving of the proposal of projects of public-private partnership, including the projects of public-private partnership of small value;
- include in the monitoring and control of public-private partnership projects the relevant bodies of government administration sector-authorized for single critical infrastructures.

Ad 3) Establishment of the mechanism for the exchange of sensitive information/data among participants in the critical infrastructures protection system

Since the critical infrastructures are of special significance for the state, because of the implementation of security critical infrastructures, the information system should satisfy certain requirements in order to

ensure its planned and expected security management. It has been learned by the Project that the information system, apart from two components that it has to satisfy, it has to ensure also certain conditions for the expected use of the information system.
The components are:

1. Organizational and technological level that ensures functional management of critical infrastructures;
2. The security level that ensures the satisfaction of security requirements, primarily in order to satisfy the requirements related to the classification of information used in the frame of critical infrastructures management.

The conditions are:

a) Implementation of information security management system;
b) Certification of the information security system;
c) Continuous verification of meeting the requirements of the Act on Information Security and/or HRN ISO/IES 27001:2014 standard;
d) Continuous education in order to raise the awareness of all the stakeholders related to information security of critical infrastructures;
e) Through education and training to train direct participants in critical infrastructures management for proper handling and implementation of information security requirements.

Ad 4) Establishment of preconditions for the development of the National Centre for Critical Infrastructures

The Project served to analyze which preconditions need to be realized in order to develop the National Centre for Critical Infrastructures. Various items were recognized that should be introduced/improved. These are tasks that should be performed by the persons in charge of critical infrastructure activities, improvement of normative framework, improvement of the existing and the development of new methodologies, development of criteria for the identification of the class of criticality and application of the necessary protection measures and the development of the model of the system of communication and insurance of information availability. In more detail, the following is meant:

Tasks that should be performed by the National Centre for Critical Infrastructure:

a) collection, analysis, and exchange of information among the stakeholders of protection / risk management of critical infrastructures;
b) proposing and writing of regulations in the field of critical infrastructures protection;

c) surveillance and directing of identification and producing of sector risk analyses of critical infrastructures;
d) surveillance and directing of risk analyses and security plans / plans for the continuation of the operation of the owner / manager of critical infrastructures, in cooperation with central bodies of state administration;
e) organization of education and training in the field of critical infrastructures protection in cooperation with other stakeholders of critical infrastructures protection;
f) establishment and functioning of the central point for planning, preparedness and response in emergencies in the area of critical infrastructures protection;
g) establishment and functioning of a contact point for the European critical infrastructure.

Improvement of normative framework in segments such as:

a) definition of critical infrastructure in the RS and designation in the RH;
b) place and role of security coordinators in relevant ministries;
c) opening space for appropriate incentive measures to those business subjects who will be recognised as national critical infrastructure.

Improvement of the existing and development of new methodologies:

a) improvement of Methodology for the development of risk analysis;
b) development of Methodology for risk management in compliance with the ISO 31000:2009 standard.

Development of criteria for the identification of the class of criticality and application of the necessary protection measures:

a) additional education of human resources in all sectors of critical infrastructures.

Development of the model of communication system and insurance of information availability:

a) building of a system of joint data and information flow;
b) building of a national database on critical infrastructures;
c) establishment of a Web-GIS browser on critical infrastructures.

7.2. STRENGTHS

The strengths resulting from the RECIPE Project represent an element which will certainly be of long-term benefit for all the Project stakeholders. The greatest strength is precisely the experience acquired by the Project partners, including other stakeholders, by implementing the Project and by further strengthening the partnership, thus creating the preconditions for further cooperation in the future Projects. Also, one of the greatest strengths of the Project is the acquiring of new knowledge additionally educating the Project stakeholders which will help them in the future when performing their regular

business activities, and certainly also for the new Projects. Furthermore, apart from a stronger partnership, new contacts have been established, new experiences exchanged as well as the best practices (visit to National Centre for Critical Infrastructure of the Hungary), which contributes mostly to the expansion of the existing as well as opening of new horizons. The Project stakeholders will be able to continue to deal actively and at a higher level with the topic of increasing the resilience of the CIP system in the sense of research, raising the awareness level and teaching certain target groups. And all this thanks to the strengths and the acquired knowledge while working on the RECIPE Project.

7.3. POSSIBLE CHALLENGES AND/OR IMPROVEMENTS TO BE TACKLED TROUGH FURTHER ACTION

With the RECIPE Project it has been determined that there are possible challenges and barriers that could be encountered after the Project. It refers to four dimensions of resilience system: from the lowest abstraction degree level (Logical and Physical) to the highest abstraction level (Cooperative).

Logical & physical dimension: Individuate the most advisable technologies today available for the cyber and physical protection. Considering the best technologies to be used for sector specific applications. How to address the ever-evolving threat and vulnerability landscape, with dynamic and continuously adapted technological solutions?
Personal dimension: How to define the Profile of the people in charge for CI's resilience? How possibly to certify the Resilience Skills of experts? Which should be the Training Program to prepare CI's resilient experts? In which way to motivate the CI personnel that is not security specific to take part in the overall challenge of security?
Organizational dimension: Accordingly, with a proposed general logical model, how to define at organizational level a Resilience Management System and how to implement it? How to individuate the people to be involved? How to define the responsibilities and at which level?
Cooperative dimension: How to promote the cooperation among different CI operators, both private and public? Who should have the responsibility of the initiative? Which is the state of the art and the best practices?

Furthermore, among the main challenges, i.e. barriers that may be encountered after the very Project "RECIPE", and refer to further development of the CIP system, is the political will. Because of other burning issues, namely, occupying the governing structures, i.e. because of insufficient political focus on the topic of CIP, a positive and sufficiently appropriate level of political will in the near future is not to be expected realistically. Since the politics holds in its hands the "key" to finances necessary for the development of the CIP system, its level of awareness about its necessity has to be raised, which would at the same time contribute to a possible discussion about the development of the CIP system which would be the initial phase when its development is in question. The condition of the political will reflects the condition of other factors necessary for the development of CIP system. Thus, for instance, with

insufficient level of political will to participate in the entire process, the private sector, which is of crucial importance for the functioning of the CIP system, will be even less interested in getting included in the system development.

7.4. RECOMMENDATIONS TO STAKEHOLDERS, PARTNERS, AUTHORITIES IN CHARGE, NATIONAL AND EU INSTITUTIONS

In order for the system to take on larger proportions of resilience and thus reduce the possible harmful impacts on it, it is first of all necessary to clearly conceive and define the concept of resilience in order to be able to develop maximally efficient CIP system that will be applicable in practice, i.e. in actual conditions. Therefore, and taught by the RECIPE Project, a development of the strategic document at the European level is proposed regarding CIP which will, among other things, clearly define all the concepts that are of crucial importance for complete understanding of the entire CIP system.

The identification of the critical business assets and the major threats that may occur on those assets, the estimation of the probability that those threats could occur and the evaluation of their impact (consequences on organization's capability to perform business activities) are cornerstone activities to design a safe and sound organization's protection system. In mission critical contexts is strongly recommended to consider not only the traditional, well-known threats, but also to explore the possible events and conditions (internal and external to the organization) that may engender unexpected negative consequences never considered before on the organization. Furthermore, considerations on the emerging threats scenario and the consequent updates of threat catalogue potentially affecting the organization should always be taken into account.

When speaking about "**Public-private partnership"**, it is necessary to say that in this segment there exists great potential and its fulfilment can contribute to more efficient and higher quality protection and rescue system. Public-private partnership, as a model of a relationship between public and private sector, is based on the identification and application of the benefits that the public and private sector can have from merging the means, as well as from expertise (knowledge), in order to improve and fulfil the requirements of the community. Through public-private partnership the private sector can direct its resources and skills into provision of assets and services that are according to tradition provided by government services. Thus, new quality can be created in the relationship between the government and the private sector through balanced distribution of tasks in the system. The partnership as such can combine the advantages of both sectors, harmonizing the social and public responsibility and efficient managing, financial possibilities and "entrepreneurial spirit" which are carried by the private sector. This may result in higher quality and more efficient protection of public interest in the field of critical infrastructure. However, without the habit of joint action, and above all joint readiness for cooperation, such models for the critical infrastructure protection cannot be adequately realised. Public-private

partnership is an extremely efficient tool for the cooperation in planning, coordination and communication.

By implementing the RECIPE Project it has been determined that it is necessary to take care of the policy of mutual assistance of the public-private partnership and it is proposed to produce an act at the national level that will stimulate public-private partnership. Its obligors will be precisely the stakeholders from both spheres, whether public or private economy, and by performing their own duties mentioned in the said act, they will jointly contribute to more efficient critical infrastructure protection.

In order to avoid manifesting the "profit motives" of private companies, as well as imposition of "bureaucratic" mindset of the public sector, it is important to focus on a broader goal to be achieved, and that is to strengthen the resilience and CIP with the awareness that the cooperation of the "public and private", in spite of potential aggravating factors, brings advantage such as, for instance, more efficient implementation. The public sector should tend to greater, more innovative and long-term financing of infrastructure Projects by the private sector. However, great attention is necessary to consider the interests of the private sector so as not to get the impression of one-way partnership.

When speaking about "**Handling sensitive information about national and European critical infrastructures"**, it has to be said that it is developing according to special regulations in the field of information security and international agreements. However, it has been determined in practice that the existing regulations are not implemented entirely so it is necessary to undertake additional activities in order to increase the efficiency and security in the exchange of sensitive information related to critical infrastructures.

The Project has determined that the existence and implementation of critical infrastructure security is based, among other things, also on the use of information system in all phases. Since critical infrastructures are of special significance for the government, it is obvious that also the information system has to satisfy certain requirements in order to ensure its planned and expected security management. Accordingly, the RECIPE Project suggests that the information system has to satisfy two components:

1) Organizational-technological level that ensures functional management of critical infrastructures;
2) Security level that ensures satisfaction of security requirements, primarily in order to satisfy the requirements related to the classification of information used as part of CI management.

Since information is one of the basic resources of each system, especially the information system that forms the basis for any activity with critical infrastructures, taught by the RECIPE Project, necessary prescribing of the frame and requirements that must be met in order to be functionally usable and satisfy the fulfilment of information features and classification requirements.

The RECIPE Project has determined that the satisfaction of the manipulation requirements by classified information is optimally achieved by implementation of the Information Security Management System

(ISMS) and this practice is proposed also in the future. In other words, implementation, certification, and supervision of ISMS only give satisfactory level of confidence in preservation of the security of information of critical infrastructures.

The establishment of the integral CI management system represents a long-term business and commitment of the Croatian Government, the competent body of government administration (NPRD – National Protection and Rescue Directorate), relevant ministries and all other stakeholders in this process. These are very responsible and continuous activities of national, security and economic interest. The implementation of the Act and bylaws requires hierarchically and functionally structured organization of the coordinators and executors of the implementation of tasks and control. Relevant Serbian institutions (Sector for Emergency Management of the Ministry of the Interior and Office of the National Security Council and Classified Information Protection), have also expressed the intent to develop the integrated CIP system in Serbia, once the legal framework is created.

To that end, and on the basis of all mentioned, the RECIPE Project has determined the proposal of national standpoints that it is necessary to establish the **National Centre for Critical Infrastructures**, as the central body of CI management in the Republic of Croatia that will have clearly and precisely defined tasks, responsibilities and accountability in the implementation of regulations in the field of critical infrastructures and to coordinate and ensure the functioning of all the stakeholders, vertically and horizontally. In Serbia, ideally, a similar Centre should be established, but it will need to be done in at least two phases. In the first phase, a Centre will not be able to answer to all CI related issues, but it should connect the business, research and government sectors by creating a National Forum or Experts Network comprised of CI experts from academic, institutional and corporate sectors., as an informal body. In the phase two, a formalized structure – Centre, may be established with the fully operational functionalities.

For the possible future Projects that will result from the RECIPE Project, and all the other future Projects, the following is specially recommended:

- Organizing of several sessions of the Project team discussing the previous part of the performed Project activities, discussing the activities that are in the process of implementation, and discussing those that follow in the near future;
- Coordination of partners in order to submit the reports continuously, for easier monitoring of the implementation of the Project as well as its more efficient implementation;
- Develop communication strategy that will precisely conceive and define the method in which certain activities are performed;
- Make a detailed plan of activities, who will perform which activity.

8. FOLLOW-UP

8.1. COMPARISON BETWEEN INITIAL AND CURRENT FOLLOW-UP MEASURES

The Project has defined the continuity that is to take place after the Project ends, i.e. the following activities that are to be held or continued in the RC and the RS:

A) *Development of CI and CIP related legal framework (Law on CI and its bylaws, amendment of the existing CI-related legal documents) – RS;*
B) *Implementation of the Guidelines that will suggest the best practice in particular systems of critical infrastructure protection - RC, RS;*
C) *Preserving the collaboration and connections between national and international stakeholders created during the Project;*
D) *Education and capacity building of public and private stakeholders in the field of Critical Infrastructure Protection;*
E) *Establishment of National Centre for Critical Infrastructure Protection with the aim of optimizing the critical infrastructure risk management;*
F) *Transfer and distribution of the "best practice" and knowledge gained during the Project to third countries;*
G) *Organization of workshops, conferences and similar activities on the topic of critical infrastructure protection;*
H) *Continuation of the free mobile app use after the Project ends.*

Ad A) Development of CI and CIP-related legal framework (Law on CI and its bylaws, amendment of the existing CI-related legal documents)

As the first beneficiary of the Project – RS lacks the legal framework (including the Law on CI that would include valid definition of the term CI and the roles and the responsibilities of the CIP stakeholders, as well as bylaws that would provide practical recommendations for the identification and the prioritization of CI sectors and assets). This is the key step to be taken for the sake of establishment of a functional and efficient CIP system. As a deliverable of the Project and a link to the Follow-up period, the Project Partner from RS – the Faculty of Security Studies (FB) shall provide the amendments to the draft Law on Risk Reduction and Emergency Management, based on the main outcomes of the Project activities and 'good practice' of the EU countries, to the Sector for Emergency Management of the Ministry of the Interior of RS (SEM) for their consideration. The amendments would include: definition of critical infrastructure and key related concepts (critical infrastructure protection, interdependency, resilience and organizational resilience etc), definition of duties and responsibilities in the field of CIP, including proposal of legal sanctions against subjects who fail to do so. The draft Law will substitute the existing

Law on Emergency Situations. As the following step FB may fully participate in developing the Bylaw on Identification Criteria for CI, based on the best practices available and with the support of other Project partners and EU experts who participated in the Project activities.
A risk for the successful implementation of this activity is the possibility that SEM may not be willing to accept the proposed document in its entirety, as the collaboration between academic and the state institutions (ministries, secretariats and agencies) is still insufficiently developed, and political reasons and some kind of power play are still more important than professional criteria and standards. The time framework for this activity would be three months (amendments to the Law), six months (Bylaw on CI Identification), maximum eighteen months adoption of the Law and the Bylaw.

Ad B) Implementation of Guidelines that will recommend the best practices, in particular Critical Infrastructure Protection systems – RC, RS

The activity *Implementation of Guidelines that will recommend the best practices, in particular Critical Infrastructure Protection systems* will be ideally implemented through the National Critical Infrastructure Centre in case it is established in both countries. In RC, for instance, the Centre could send the Guidelines to the state institution in charge of each of the 11 identified CI sectors, which these institutions would then forward to the subjects from their own sectors, identified as critical infrastructure. Taking into account the similarities between the two countries, a similar mechanism could be used in RS. However, it is not realistic to expect that this way of distribution and implementation of the (updated) Guidelines and other "best practices" may be achieved in the next 2-3 years.

Before the Centers are established the Guidelines could be distributed using the existing channels – NPRD in RC and SEM in RS, that would, in collaboration with the academic Project partners – VVG and FB and the state institutions representing the sectors identified (RC)/potentially identified (RS) as critical, work together on creating the shortlist of the CI to whom the Guidelines should be forwarded. Although the RC has identified CI sectors, the intra-sector identification of CI has not been performed yet due to the lack of a Bylaw on the Criteria for Critical Infrastructure Identification. This activity could be completed in a relatively short period (<1 year).

Ad C) Preserving the collaboration and connections between national and international stakeholders created during the Project

The activity *Preserving the collaboration and connections between national and international stakeholders created during the Project* is completely sustainable after the Project ends. The subjects in charge of it will be all Project partners - NPRD, FB, MSB and VVG, as well as other Project participants that were not part of the Project consortium (e.g. Institute for Corporative Security Studies - ICS, Republic of Slovenia).
During the Project, Project partners visited the Centre for Critical Infrastructure Protection in Budapest, Hungary, whilst the collaboration was established with the Greek Centre for Security Studies ("KEMEA"),

and Mr. Alessandro Lazari from the EU Joint Research Centre (JRC), who was also one of the final Conference panelists.
Similar conferences, panel discussions, workshops and potential joint Projects with all RECIPE Project participants may be easily organized in the future, thus strengthening the cooperation established during the Project. There are no obstacles for successful implementation of this activity and it can be continually implemented after the Project ends, both in long and short term.

Ad D) Education and capacity building of public and private stakeholders in the field of Critical Infrastructure Protection

The activity *Education and capacity building of public and private stakeholders in the field of Critical Infrastructure Protection* is feasible and sustainable. There are capacities and resources for its implementation in both RC and RS after the Project ends and it can be held continually. Among the capacities there are two academic institutions (FB and VVG) that can provide education in the field in question, NPRD and MSB that can establish working groups and through them organize workshops for separate sectors, which would provide motivation and a good source of information for public and private stakeholders.

The obstacle and a risk for successful implementation of this activity is the above-mentioned lack of identified critical infrastructure (in RS also lack of identified CI sectors), which also includes the lack of the necessary staff for whom the education, simulation exercises, training and capacity building activities would be organized.

Ad E) Establishment of National Centre for Critical Infrastructure Protection with the aim of optimizing critical infrastructure risk management

The activity *Establishment of National Centre for Critical Infrastructure Protection with the aim of optimizing the critical infrastructure risk management* is assessed as feasible in the Feasibility Study developed by the certified Institute for Corporative Security Studies – ICS from Slovenia. The Study confirms that the establishment of the National Centre is completely feasible: in RC as an inner organizational unit of the NPRD, in RS as an inner organizational unit or an added functionality of the Directorate for Risk and Emergency Management Projected in forthcoming legislation. However, the Project partners anticipate various obstacles to this activity – the most important being the lack of institutional support and low awareness of decision makers. Therefore, although deemed feasible, the implementation of this activity may be realistic only in a mid-term run (3-5 years).

Ad F) Transfer and distribution of the "best practices" and knowledge gained during the Project to third countries

The activity *Transfer and distribution of the "best practices" and the knowledge gained during the Project to third countries* is feasible for implementation by all Project partners with each partner focusing on particular target groups (e.g. NPRD – state bodies, FB and VVG to academic and professional community in their respective countries, etc.). The aim of this focused approach is to enable countries, EU or non-EU ones, especially those without developed critical infrastructure protection system, collect as much information as possible and thus facilitate the process of creation and development of the CIP system.
The know-how and best practices gained through the Project can be exchanged with the member countries in order to improve the CIP system, and it can also be transferred to third countries that will only initiate the process of development of CIP system (Bosnia and Herzegovina, Montenegro, Macedonia, etc.).

The main obstacle may be the low awareness level of the governing structures about the importance of the existence of an efficient and sustainable CIP system, especially in the countries such as RS where the CIP system is only to be developed. Due to this, the awareness raising activities such as panel discussions, workshops and the presence in the media are needed in order to motivate the stakeholders to participate in the initiation of the CIP system establishment.

Ad G) Organization of workshops, conferences and similar activities on the topic of critical infrastructure protection

The activity *Organization of workshops, conferences and similar activities on the topic of critical infrastructure protection* took place during the Project (panel discussions and workshops on the topic of critical infrastructure protection in Velika Gorica, Zagreb and Belgrade, as well as the international RECIPE 2015 conference in Split), at which all Project partners and prominent guests – worldwide experts in the CIP field – such as Mr. Alessandro Lazari on behalf of the Joint Research Centre took part.
In addition, during the Project, on the invitation of Col. Dr. Balázs Bognár – the main coordinator of the department for critical infrastructure and disaster management - the delegation comprised of the representatives of Project partners from RS and RC visited the Centre for Critical Infrastructure Protection in Budapest. The Project partners were introduced to the Hungarian best practices and got an insight into the Hungarian CIP system. Such activities may be also organized in continuity by Project partners and all other stakeholders that took part in the Project realization. The initiative for organizing those events should be on academic institutions (VVG and FB)

Ad H) Continuation of the free mobile app use after the Project ends

The activity *Continuation of the free mobile app use after the Project ends* will be done by the staff of the NPRD, for whom CIP represents a part of their regular work duties.

During the Project it was concluded that the activities should be systemized as short-term (1-2 years) and mid-term (2-3 years) ones, which need to be implemented for the sake of establishing a functional CIP system.

In order to successfully implement all the above mentioned activities it will be necessary:

- that the relevant stakeholders in the field of critical infrastructure protection continue with the efforts strengthened by the new knowledge gained during the Project;
- to set up educational programs in the field of CIP, including the exchange of experts;
- to include in the activities the persons trained and educated for critical infrastructure protection;
- to participate at international events dealing with the CIP-related issues;
- to participate in other Projects providing solutions to the problems and instigate further development of the CIP system;
- continuous building and expanding of the network of critical infrastructure protection stakeholders.

8.2. ADDITIONAL FOLLOW-UP APPROACHES

Institutional sustainability

The Faculty of Security Studies and the University of Applied Sciences Velika Gorica are academic institutions and thus able to work on the education and capacity building of the future CIP experts and professionals. The University of Velika Gorica is an institution of high education whose curriculum is, among other things, closely connected with the field of critical infrastructure (e.g. subjects like Critical Infrastructure, Critical Infrastructure Management, Risk Assessment, Corporate Risk and Security). Due to this, VVG as the center for CIP competencies will strengthen with its own staff the research activities in the field of critical infrastructure management in such a way that the teaching staff together with students will undertake research activities in the mentioned field. FB is the only state founded academic institution in RS that has recognized the field of CIP in comprehensive manner in its curriculum (subjects like Crisis Management, Civil Defense System, Civil Protection, Risk Management in Emergencies, Industrial Security and Protection, Management in Protection Systems, Corporative Security, Environmental Security, etc.) and its research activities (ANVIL Project within FP7 Program and RECIPE Project, as well as several national research Projects). Besides, FB offers postgraduate studies in the field of Crisis management, Emergency situations and Terrorism (Specialization) and is planning to launch master studies in Emergency management.

In addition, VVG offers education for the new and existing CI risk management and CI management staff. Furthermore, VVG will continue its practice of exchange of experts at its own educational programs with

relevant public and private institutions, with the aim of constant improvement of its educational program. In Serbia, FB will recommend national Projects in the field of CIP to the Ministry of Education, Science and Technological Development and work on the strengthening of competencies of young researchers, related to the EU initiatives for the systematic identification of emerging risks to the CI.

VVG and FB can coordinate workshops on the topic of CIP at which security coordinators, owners and operators of CI will participate, both from the public and private sectors, with the aim of raising awareness about the importance of critical infrastructure, permanent education on critical infrastructure (due to potential changes in the legal regulation) and motivation of all stakeholders for the joint cooperation.

Financial sustainability

VVG and FB have their own sources of income and the existing staff suitable for activities such as education, organization of workshops, conferences, etc. after the Project ends.

Political sustainability

The Project results, e.g. improvements in exchange of knowledge, experiences and good practices between member countries, candidates and third countries, and other results together with education activities can contribute for the state to develop a CIP system.
The University of Applied Sciences Velika Gorica will promote the need (via media, their own websites, official gazette, etc.) to develop a CIP system.

Apart from promoting the importance of the CIP in general public and academic and professional communities through the activities of its teaching staff (participation at conferences, workshops, seminars, interviews and press conference etc.) FB will also use its alumni service and lobbying through its ex-students and Ph.D. candidates who occupy important political and administrational positions in government ministries, agencies and other state bodies, for this issue to get the place it deserves on the public and political agenda.

Environmental sustainability

As there is no developed CIP system at this moment, it will be extremely important to monitor its development in order to prevent negative impact on the environment (for instance, the fall of a power line pole during dry summer months due to inadequate protection, which further triggers fire with enormous negative consequences to the environment).

ANNEXES

ANNEX I

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

Overall Project Management*

Project Manager: Robert Mikac

Deputy Project Manager: Petar Vitas

Members
Faculty of Security Studies: Zoran Kekovic
Swedish Civil Contingencies Agency: Clas Herbring
University of Applied Sciences Velika Gorica: Alen Stranjik

*Tasks:

- Coordinating and monitoring the project progress
- Ensuring the achievement of the project objectives
- Keeping track of deliverables and outcomes of the project

Administrative Management*

Administrative Manager Marijana Berket

Members
Faculty of Security Studies: Želimir Kešetović
Swedish Civil Contingencies Agency: Anna Rinne
University of Applied Sciences Velika Gorica: Ana Radman
NPRD: Ivana Cesarec

*Tasks:

- Establishing communication between the partners and with the EC
- Preparing the technical part of progress reports and final report
- Day-to-day administrative management
- Organization and scheduling project meetings, writing minutes and agendas
- Organization of panel discussions, workshops and conference

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

Financial Management*

Financial Manager:
Nataša Topić

Members
Faculty of Security Studies: Danijela Šušnjar
Swedish Civil Contingencies Agency: Anna Eriksson
University of Applied Sciences Velika Gorica: Vesna Valdec

*Tasks:

- Keeping track of costs, payments and budget plans
- Ensuring adherence to the rules for purchase and procurement
- Ensuring timely submission of financial documents of each project partner
- Preparing the financial part of progress reports and final report

Assessment Committee*

Chairman: Marko Toth

Member: Vladimir Jakovljević (Faculty of Security Studies)
Member: Maja Matijaš Filipović (NPRD)
Member: Clas Herbring (Swedish Civil Contingencies Agency)

*Tasks:

- Preparation of Analysis Questionnaire (Action B.1)
- Questionnaire Evaluation Report
- DUZS, FB, MSB and VVG

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

Academic Committee*

Chairman: Zoran Keković

Member: Jasmina Gačić (Faculty of Security Studies)
Member: Ivan Nađ (University of Applied Sciences Velika Gorica)
Member: Robert Mikac (NPRD)

*Tasks:

- **Feasibility studies –** representatives from national academic communities will conduct feasibility studies assessing best practices implementation applicability to Croatia's and Serbia's CIP system (Action C.2)
- **Guidelines** – best practices resulting from the workshops and assessed in Feasibility studies will be integrated and published in the Guidelines (Action C.3)
- FB and VVG
- Experts subcontracted 10.000 €

Conference Committee*

Chairman: Ivan Toth

Organizational	Programme
Member: Martina Mihalinčić, Alen Stranjik (University of Applied Sciences Velika Gorica)	Member: Ivan Nađ (University of Applied Sciences Velika Gorica)
Member: Igor Cvitanić (NPRD)	Member: Petar Vitas (NPRD)

*Tasks:

- Actions D.1, D.2 and D.3
- Organization of the conference
- Definition of the programme
- Selection of speakers and papers to be published in the Book of Proceedings
- Post conference evaluation

ANNEX II (1-3)

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

RECIPE Project – Questionnaire Analysis

One of the tasks of the RECIPE project is to conduct a survey through which we want to determine the method of identifying problems, as well as the formal and legal organization in the critical infrastructure protection. In addition, it is necessary to determine procedures and methods of implementing regulation in practice of states participating in the Project. A questionnaire has been developed for the purpose and its results, i.e. information obtained, besides indicating the state of the formal and legal organisation at the national level, will also point out the examples of good practice – effective procedures and methods of identifying and protecting critical infrastructure, as well as showing the areas that require improvements and corrections. Ultimately, this survey should offer unique guidelines for the critical infrastructure protection and its improvement at the regional level.

Information collection procedure

The Questionnaire is submitted to 9 ministries competent for 11 sectors of critical infrastructure and the University of Applied Sciences Velika Gorica. The National Protection and Rescue Directorate has also filled out the Questionnaire as the coordinator of all activities related to critical infrastructure in the Republic of Croatia and to facilitate comparison of the results with the results provided by other respondents.

At the international level, the questionnaire is submitted to 70 addresses, specifically to the national points of contact and to other representatives of Member State institutions competent for the critical infrastructure as well as to institutions in the United States of America.

Response of the Croatian part of the sample was 100 %, while 10 % of the international sample responded, however only European respondents had returned filled questionnaires.

Sample

The sample was prepared on a small, suitable sample of national central government bodies competent for critical infrastructure sectors and one higher-education institution whose curriculum also covers the issue of protection of critical infrastructure.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

The questionnaire was filled out by official persons delegated by the institutions included in the survey. Since it is a small population of institutions which are acquainted with issues of protection of critical infrastructure (a type of expert sample), instead of a general population. Taking an exceptional sensitivity of the subject matter of the survey from the point of view of national security into consideration, we find the justification for an analysis and conclusions based on such a small sample.

The primary objective and interest was to query the institutions on insights into the current state of policy and system of protection of critical infrastructure in the Republic of Croatia, therefore the results of this report present information provided by the Croatian sample separately.

Table 1. An overview of Croatian participants in the survey

Institution	Ownership
Ministry of Finance	government
Ministry of Economy	
Ministry of Culture	
Ministry of Maritime Affairs, Transport and Infrastructure	
Ministry of Agriculture	
Ministry of Interior	
Ministry of Environmental and Nature Protection	
Ministry of Health	
Ministry of Science, Education and Sport	
University of Applied Sciences Velika Gorica	private

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Results

1. Does Croatia have a national critical infrastructure protection policy?

One Croatian ministry did not provide any answer to the question (Figure 1) while other respondents claim that that there is a national critical infrastructure protection policy.

All respondents, except one, who confirmed that there is the national critical infrastructure protection policy in place indicated the act or regulation which regulates critical infrastructure protection (Figure 2) as the Critical Infrastructure Act (OG 56/13), and two ministries also specified the Regulation on methodology for analysis of critical infrastructure risks. Two ministries did not specify any legal document regulating critical infrastructure, including one ministry which previously claimed that there is no legislation pertaining to critical infrastructure protection, while one failed to provide any response, even though it previously claimed such regulation existed (Figure 2.).

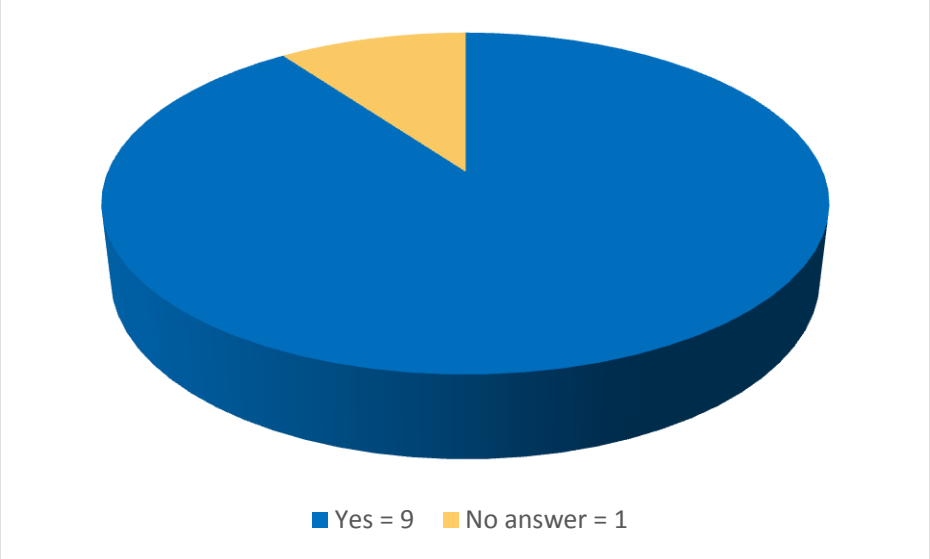


Figure 1. Reponses to the question "Does Croatia have a national critical infrastructure protection policy?" Response frequencies are shown (N=10).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

2. **If yes, under which Act/Regulation? (Pleas state title of the Act/Regulation)**

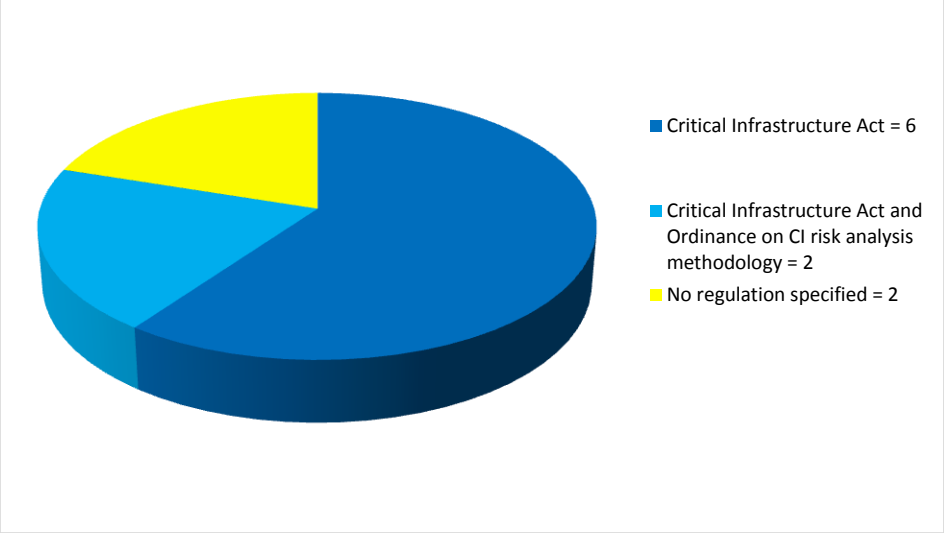


Figure 2. Responses to the question "If yes, under which Act/Regulation?" Response frequencies are shown (N=10).

3. **Is there a regulated, mandatory national surveillance regarding critical infrastructure protection in Croatia?**

Seven respondents declared that there is a regulated mandatory surveillance regarding critical infrastructure protection in Croatia. The University of Applied Sciences Velika Gorica claims that it is not the case in Croatia, while two ministries failed to provide an answer (Figure 3).

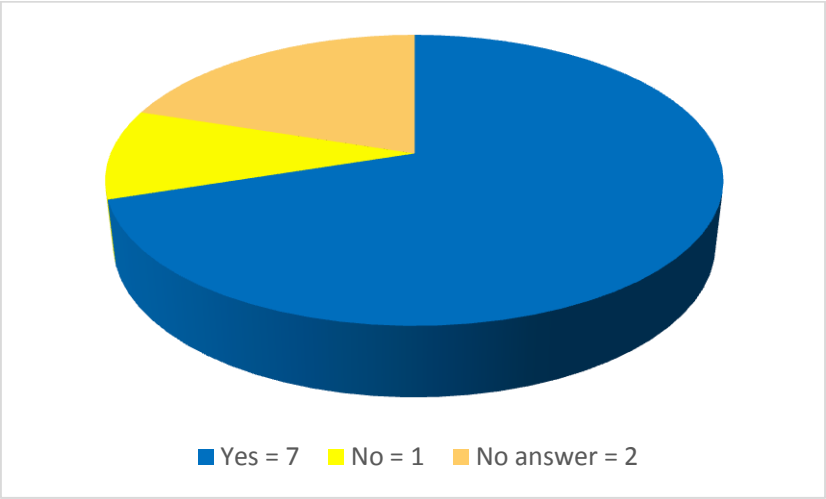


Figure 3. Responses to the question "Is there a regulated, mandatory national surveillance regarding critical infrastructure protection in Croatia?" Response frequencies are shown (N=10).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

4. Which areas are included in the aforementioned Act/Regulation?

Figure 4 shows that the areas most frequently specified by the respondents in relation to critical infrastructure protection legislation are: critical infrastructure sectors, threat and risk identification, critical infrastructure identification (own and European), and risk analysis / risk assessment. Critical infrastructure protection exercises, cross-cutting and sectoral criteria for identification, education and scientific research, public-private partnership and cooperation with the academic community, and finally Business Continuity Management were the least frequently selected options.

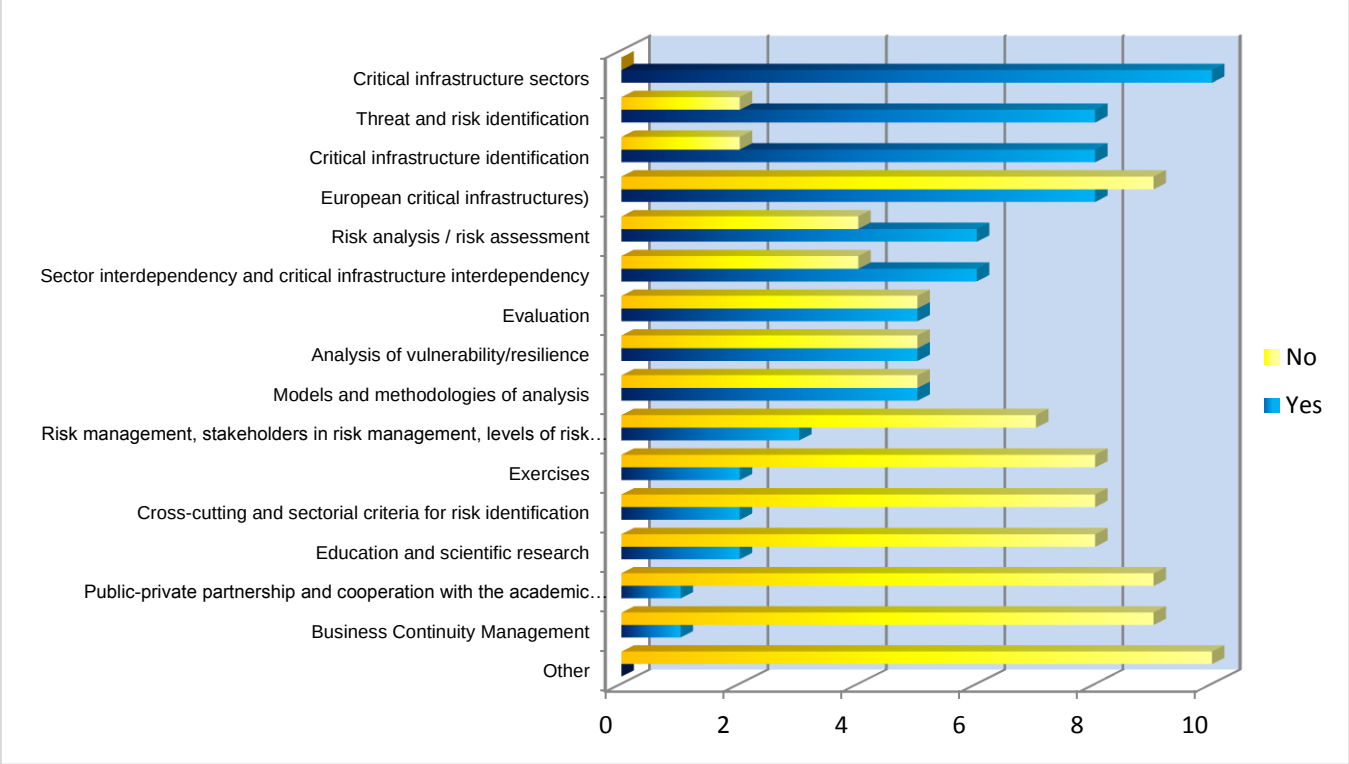


Figure 4. Responses to the question "Which areas are included in the aforementioned Act/Regulation?" Response frequencies are shown (N=10).

REMARK: Based on the above, it is clear that there is great discord and lack of knowledge which critical infrastructure elements are included in the legislation. It may be concluded that the critical infrastructure is well covered and defined by the legislation, as well as its protection, identification criteria, as well as methodology and tools for identification and assessment of critical infrastructure. On the other hand, there is poor implementation of the

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

act in practice, coordination among sectors, research, education and exercises in implementation of critical infrastructure protection. The above reveals another aspect since some of the representatives of the ministries who took part in "Risk analysis of critical infrastructure operation" seminar are still unable to recognise all areas included in the Critical Infrastructure Protection Act. The seminar was held at the University of Applied Sciences Velika Gorica in 2014 and it included provision of information on the Critical Infrastructure Protection Act.

5. **Which state body (bodies) is responsible for implementing the national critical infrastructure protection policy?**

The majority of the respondents correctly identified the National Protection and Rescue Directorate as the body responsible for implementation of the national critical infrastructure protection policy (a total of 7 respondents).

REMARK: Even though the responses are official because the questionnaires were filled out by persons appointed by the competent institutions, that does not mean they are correct. Responses provided by the National Protection and Rescue Directorate as the coordinator may be considered accurate, as well as responses by individual ministries which pertain to their particular sectors.

For instance, some ministries specified only themselves as competent while others gave non-specific responses such as "the ministries" which implies that all ministries are responsible or, for example, responses such as "central government body whose purview encompasses rescue and protection activities" which represents a very non-specific response even though it may be accepted as a correct one.

Even though all responses involving the National Protection and Rescue Directorate and/or own ministry and/or all the ministries may be considered correct to an extent, there is an impression that there is insufficient information on responsibility and obligations of individual respondents in implementation of the national policy on critical infrastructure protection. In any case, inaccuracy of the responses leads to a conclusion that coordination is needed among

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

the ministries in exchange of information and detailed familiarity with lines and areas of competence.

It is a fact that some ministries did not provide any remotely accurate response or that they gave the correct answer along with completely wrong one and it additionally points to the conclusion that there is a significant need for coordination of sectors involved with critical infrastructure protection, as well as further education, dissemination of information and cooperation among the sectors, especially in the field of exchange of information.

Responses by respondent are provided in Table 2.

Table 2. Responses to the question "Which state body (bodies) is responsible for implementing the national critical infrastructure protection policy?" Responses and response frequencies are shown (N=17).

Government body considered responsible for implementation of the national policy on critical infrastructure protection	Number of respondents who gave such response	Institution/respondent
National Protection and Rescue Directorate	7	Ministry of Finance Ministry of Economy Ministry of Culture Ministry of Maritime Affairs, Transport and Infrastructure Ministry of Interior Ministry of Health University of Applied Sciences Velika Gorica
Ministries	2	Ministry of Agriculture Ministry of Economy
Ministry of Economy	1	Ministry of Maritime Affairs, Transport and Infrastructure
Ministry of Maritime Affairs, Transport and Infrastructure	1	Ministry of Maritime Affairs, Transport and Infrastructure
Ministry of Environmental and Nature Protection	1	Ministry of Environmental and Nature Protection
Ministry of Health	1	Ministry of Health
Implementation bodies	1	Ministry of Agriculture
Central government body whose purview includes rescue and protection activities	1	Ministry of Science, Education and Sport
Government of the Republic of Croatia	1	Ministry of Agriculture
Other government institutions	1	Ministry of Maritime Affairs, Transport and Infrastructure

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

6. **Are the responsibilities for critical infrastructure protection divided in Croatia at the national, regional and local level?**

Figure 5 shows that the majority of the respondents deems that the responsibilities for the critical infrastructure within the country are distributed at the national level, while two of them deem them distributed at the national, regional and local levels. Two of the respondents did not provide an answer.

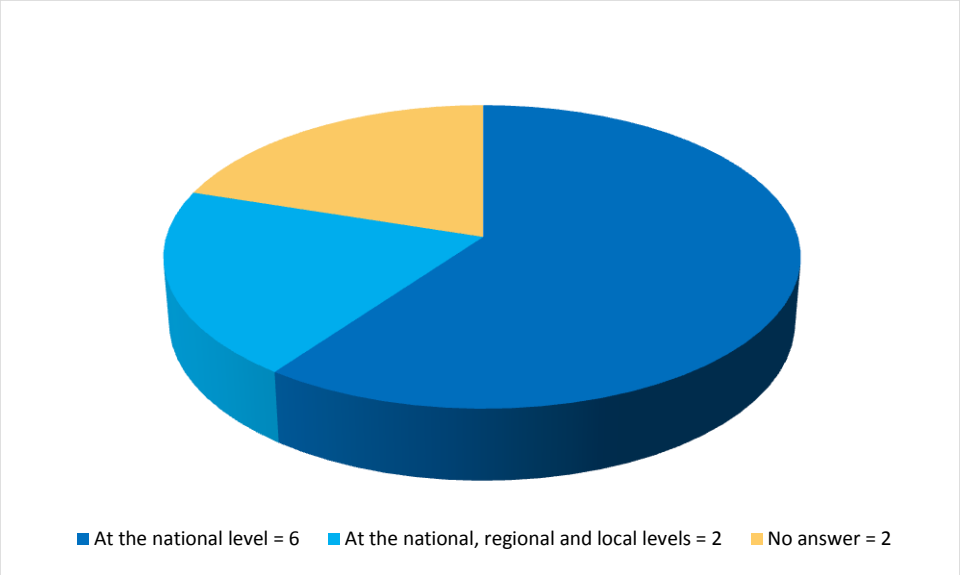


Figure 5. Responses to the question "Are the responsibilities for critical infrastructure protection divided in Croatia at the national, regional and local level?" Response frequencies are shown (N=10).

REMARK: The above points to the conclusion that the surveyed individuals are not well informed and that there is a mismatch in comprehension of responsibility for critical infrastructure protection.

7. **Has Croatia appointed a state body to coordinate activities related to implementing the national critical infrastructure policies?**

Figure 6 shows that all the respondents are acquainted with existence of a government body appointed to coordinate activities for implementation of national policy on critical infrastructure protection.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

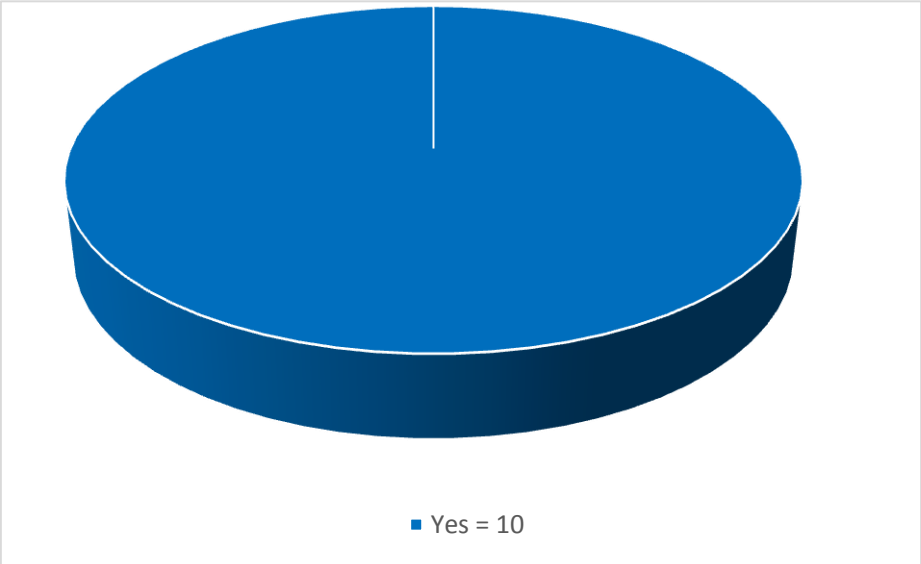


Figure 6. Response to the question "Has Croatia appointed a state body to coordinate activities related to implementing the national critical infrastructure policies?" Response frequencies are shown (N=10).

8. Has a platform or network for critical infrastructure protection at the national level for stakeholders been established?

A bit more than a half of the respondents (6) claim that a platform or network of stakeholders for critical infrastructure protection has been established, while one claims the opposite. Three did not respond.

Great differences exist in the responses.

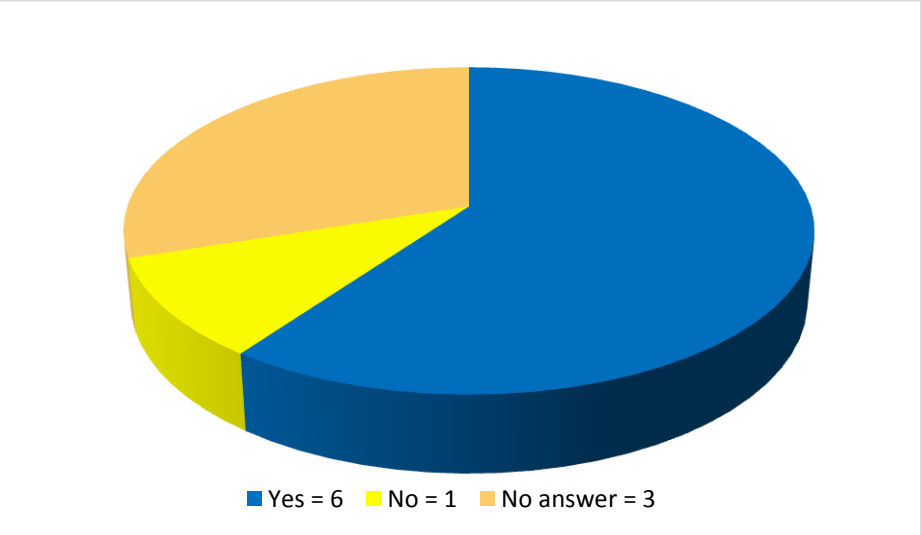


Figure 7. Response to the question Has a platform or network for CIP at the national level for stakeholders been established? Response frequencies are shown (N=10).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

9. Which critical infrastructure sectors have been identified in Croatia?

A half or more of the respondents did not specify individual sectors of the critical infrastructure. There are only five sectors which received the greatest number of mentions, and then only by one half of the sample. The responses by frequency are shown in Table 3 and Figure 8.

Table 3. Responses to the question "Which critical infrastructure sectors have been identified in Croatia?"

Specified critical infrastructure sector	Response frequency
Energy	5
Communication and information technologies	5
Transport	5
Finance	5
Healthcare	5
Water management	4
Food	4
National heritage and values	4
Public services	4
No sectors were specified	3
Production, transport and storage of hazardous substances	3
Science and education	1

The critical infrastructure has been determined in eleven sectors pursuant to a decision of the Government of the Republic of Croatia but only one ministry specified all eleven of them, two specified ten sectors each, one specified nine, while the other respondents specified up to two sectors (Table 4).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Table 4. Number of critical infrastructure sectors specified by institutions which had specified them

Number of critical infrastructure sectors specified	Institutions which had specified the sectors	Response frequency
11	Ministry of Science, Education and Sport	1
10	Ministry of Culture Ministry of Interior	2
9	Ministry of Economy	1
2	Ministry of Maritime Affairs, Transport and Infrastructure	1
1	Ministry of Finance Ministry of Health	2
0	University of Applied Sciences Velika Gorica Ministry of Agriculture Ministry of Environmental and Nature Protection	4

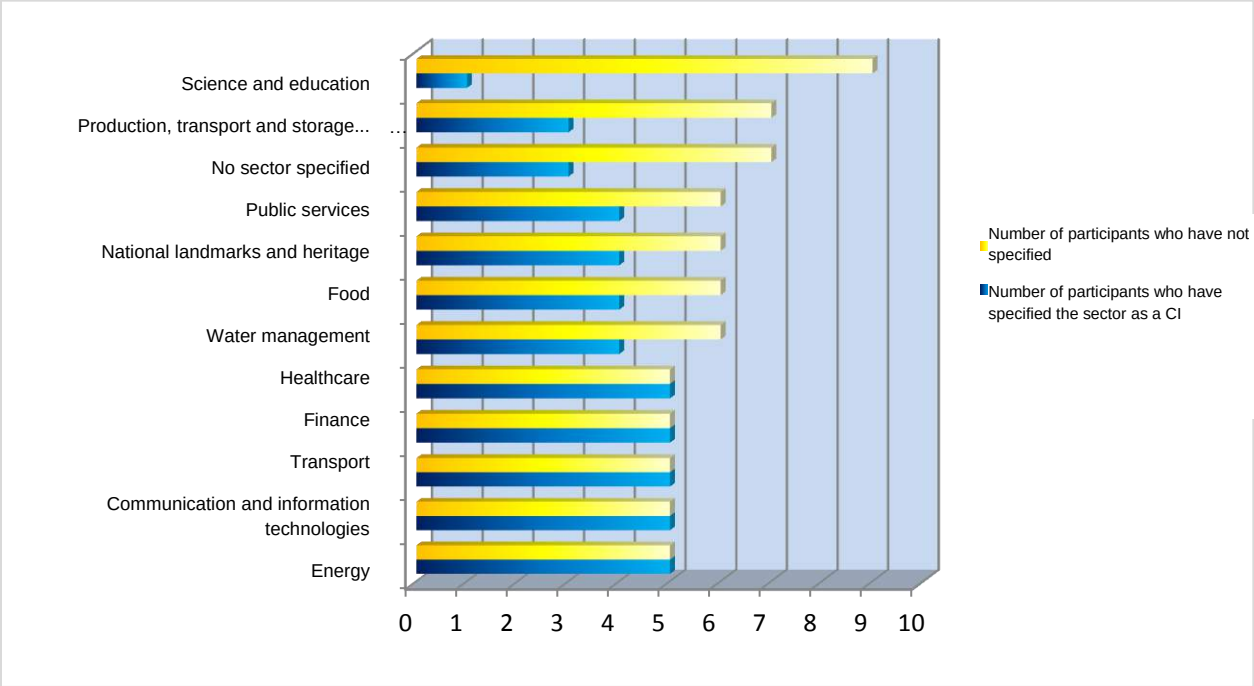


Figure 8. Responses to the question "Which critical infrastructure sectors have been identified in Croatia?" (N=10)

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

REMARK: In addition to indications relating to familiarity with regulations provided by these responses, a possible reason for incomplete responses to this question is a low motivation of the respondents to provide detailed questionnaire responses.

10. Have the sectoral analyses of risks and vulnerabilities been made?

Three respondents claim that an analysis of risks and vulnerabilities has been made in Croatia, while six claim otherwise. One responded did not give any answer. (Figure 9)

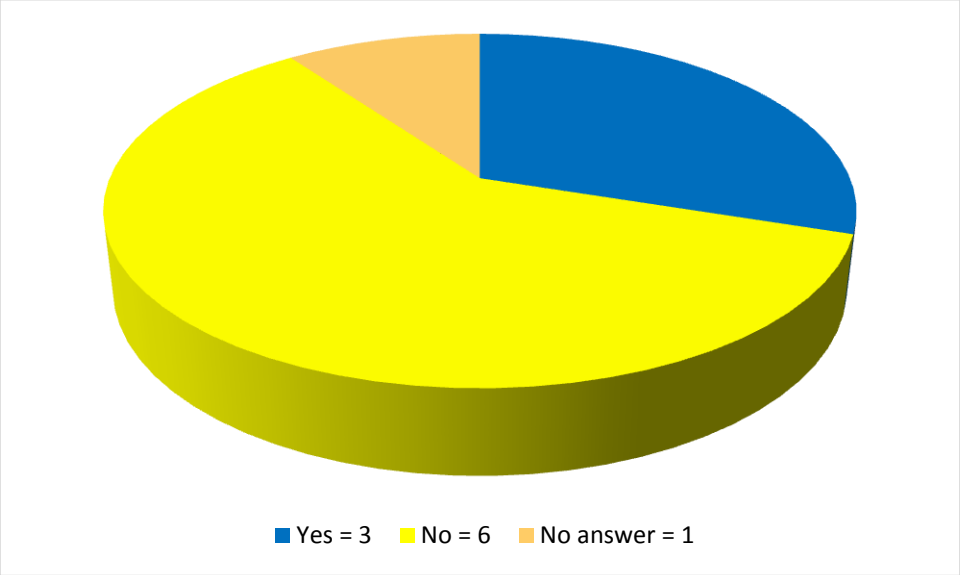


Figure 9. Responses to the question "Have the sectoral analyses of risks and vulnerabilities been made?" Response frequencies are shown (N=10).

11. Have the hazards and risks to the critical infrastructure in Croatia been identified?

Three respondents claim that an analysis of hazards and risks to the infrastructure has been made; five think the opposite, while two gave no answers. (Figure 10)

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

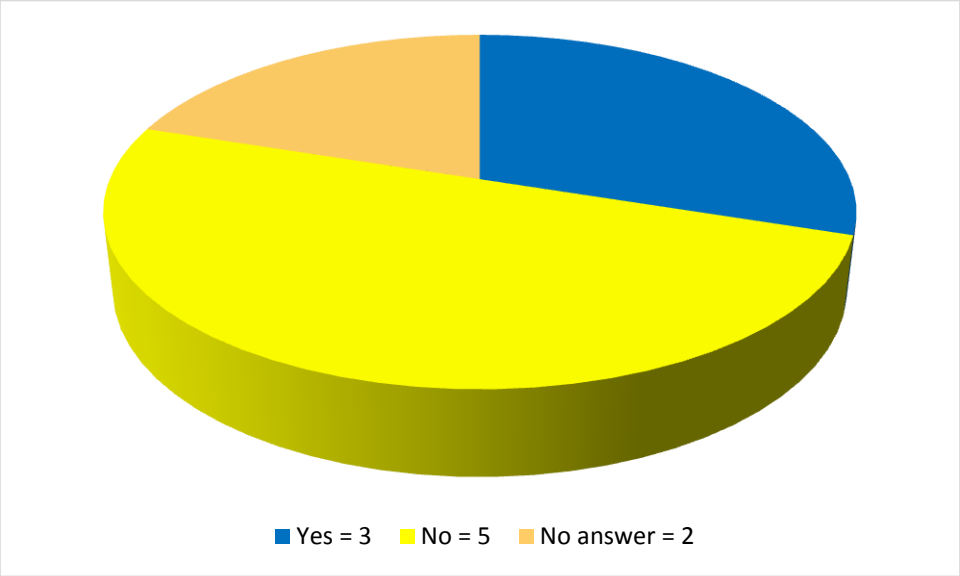


Figure 10. Responses to the question "Have the hazards and risks to the critical infrastructure in Croatia been identified?". Response frequencies are shown (N=10).

If yes, please state which hazards and risks.

Responses to the question by respondents' institution are provided in Table 5

REMARK: The single adequate answer was given by the University of Applied Sciences Velika Gorica – that the identified hazards and risks to the critical infrastructure are "anthropogenous threats, technical-technological threats and natural threats". The answer given by the Ministry of Health indicates that the Ministry is dealing with some aspects of critical infrastructure protection within its own purview even though the answer to this question itself is irrelevant.

Table 5. Response to the question "Which hazards and risks are identified in Croatia?"

Institution	Response	Number of institutions which provided an answer
University of Applied Sciences Velika Gorica	Anthropogenous threats Technical-technological threats	1

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Ministry of Health	Natural threats Structural security Non-structural security Functional security	1
Ministry of Agriculture Ministry of Economy Ministry of Culture Ministry of Science, Education and Sport Ministry of Finance Ministry of Maritime Affairs, Transport and Infrastructure Ministry of Environmental and Nature Protection Ministry of Interior	Nothing specified, or a very general and non-specific answer, or specific risks and threats are not specified	8

12. In the management process, has each critical infrastructure sector adopted the all-hazard approach and developed sector specific plans?

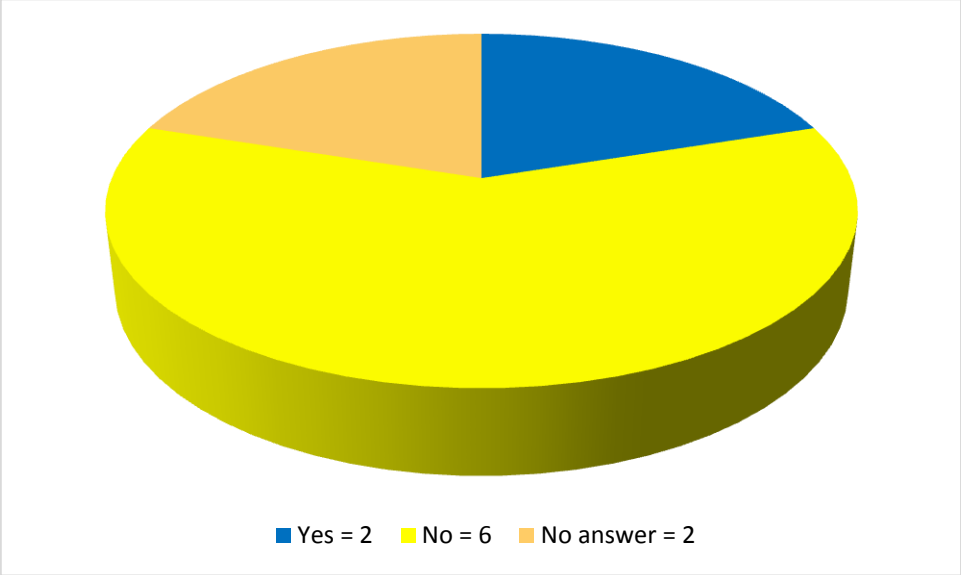


Figure 11. Response to the question "In the management process, has each critical infrastructure sector adopted the all-hazard approach and developed sector specific plans?" Response frequencies are shown (N=10).

REMARK: An example of non-specific responses: "Qualitative methods shall be used".

An example of irrelevant responses: "Not harmonised, equal".

It is suspected that this question was not completely clearly presented and explained. Since relevant ministers have not adopted any decision on the all-hazard approach in the risk

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

analysis, "no" can actually be treated as a correct response. Even though competence of individual ministries for critical infrastructure protection is limited to individual sectors, all risks should nonetheless be taken into account including other sectors outside their competence.

13. Which methodologies and which software models are used in Croatia for risk analysis and analysis of critical infrastructure interdependency?

Table 6. Response to the question "Which methodologies and which software models are used in Croatia for risk analysis and analysis of critical infrastructure interdependency?"

Institution	Response	Number of institutions which provided an answer
Ministry of Finance Ministry of Economy Ministry of Culture Ministry of Maritime Affairs, Transport and Infrastructure Ministry of Agriculture Ministry of Interior Ministry of Environmental and Nature Protection	No response, do not know, irrelevant or non-specific answers	7
University of Applied Sciences Velika Gorica	IISO 31000 and ISO 22301	1
Ministry of Health	World Health Organization methodology	1
Ministry of Science, Education and Sport	Ordinance on methodology for critical infrastructure operation risk analysis.	1

14. Do government institutions in Croatia cooperate with the scientific-research institutions, private companies (i.e. universities, institutes etc.) with the aim of developing models and methodologies for critical infrastructure risk management? If yes, with which ones?

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Most of the respondents (6) stated that there is cooperation of government institutions with scientific institutes with the aim of developing models and methodologies for critical infrastructure risk management (Figure 12), while two respondents responded negatively and two gave no answer.

REMARK: The aforementioned cooperation actually does not exist, but it is possible that some of the respondents mistook the "Risk analysis of critical infrastructure operation" seminar held at the University of Applied Sciences Velika Gorica in 2014 as an example of such cooperation. That may also be concluded from the responses to the question regarding institutions with which the cooperation has been established considering that the University of Applied Sciences Velika Gorica may be perceived as a privately-owned university and scientific-research institution.

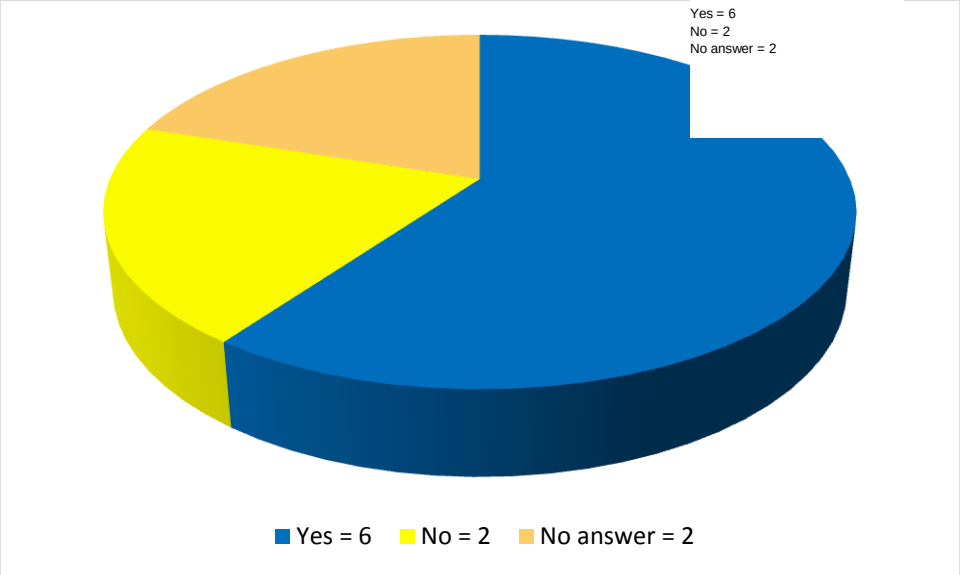


Figure 12. Response to the question "Do government institutions in Croatia cooperate with the scientific-research institutions, private companies (i.e. universities, institutes etc.) with the aim of developing models and methodologies for critical infrastructure risk management?" Response frequencies are shown (N=10).

The most of the respondents (4) stated that the cooperation has been established with universities, three said that it has been established with private enterprises, and two claimed it is in place with scientific and research institutes (Figure 12). "Other" category encompasses "not known" and "public enterprises" responses.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

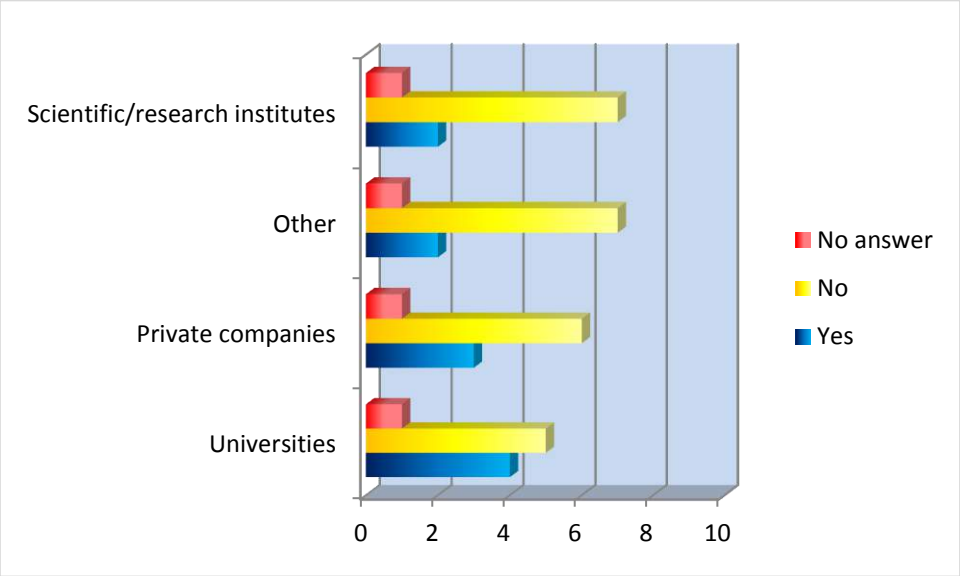


Figure 13. Response to the question "Which institutions do government institutions in Croatia cooperate with?". Response frequencies are shown (N=10).

REMARK: There are three stakeholders in development of the models and methodologies for critical infrastructure risk management: central government administration bodies, scientific-research institutions, and owners and managers of critical infrastructure. However, the cooperation has yet to be established.

The provided answers indicate the need for better information and coordination of government bodies tasked with critical infrastructure protection in respect of cooperation of public and private sectors, i.e. achieving and enhancing awareness and motivation for its establishment.

15. Has Croatia developed any guidelines/directives/manuals for critical infrastructure evaluation and risk management?

CLARIFICATION: With exceptions of two institutions which gave no answer and two which responded negatively, the respondents indicated that guidelines/directives/manuals for critical infrastructure evaluation and risk management have been developed in their country. (Figure 14)

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

REMARK: It is important to point out that such guidelines/directives/manuals for critical infrastructure evaluation have not yet been developed in the Republic of Croatia, except for the Ordinance on methodology for critical infrastructure risk analysis developed and adopted by the National Protection and Rescue Directorate. It is possible that some of the teaching materials distributed at the seminar held by University of Applied Sciences Velika Gorica have been misinterpreted as such instructions, but it was not an official government-approved document.

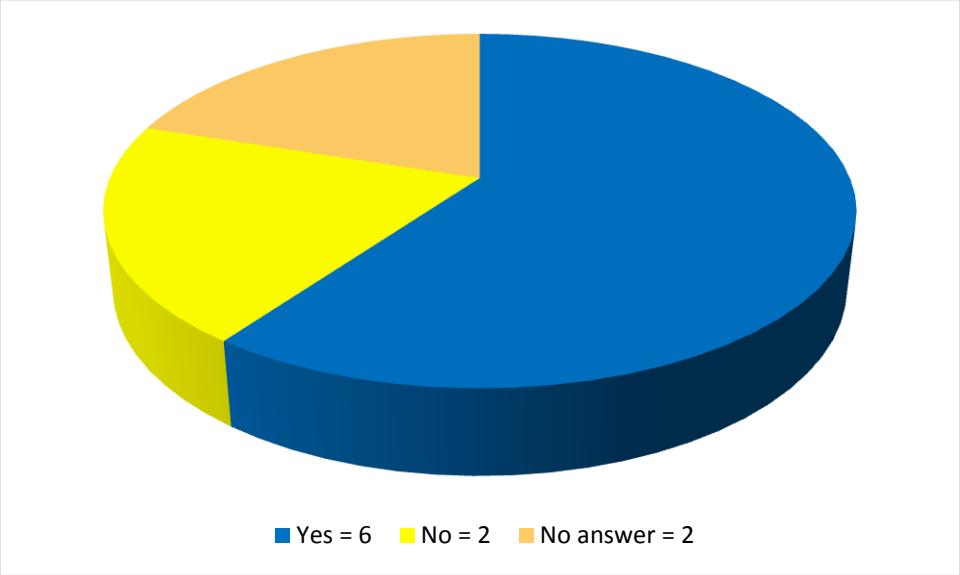


Figure 14. Response to the question "Has Croatia developed any guidelines/directives/manuals for critical infrastructure evaluation and risk management?" Response frequencies are shown (N=10).

16. Which international standards for critical infrastructure risk management and business continuity are being used in Croatia?

REMARK: Individual responses shown in Table 7 indicate a large diversity of level of information possessed by the respondents who provided answers

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Table 7. Response to the question "Which international standards for critical infrastructure risk management and business continuity are being used in Croatia?"

Institution/respondent	Response	Number of statements
Ministry of Finance Ministry of Economy Ministry of Culture Ministry of Agriculture Ministry of Interior Ministry of Environmental and Nature Protection	No answer on not specified	6
University of Applied Sciences Velika Gorica Ministry of Maritime Affairs, Transport and Infrastructure	ISO 31000 and ISO 22301	2
Ministry of Science, Education and Sport	ISO 31000	1
Ministry of Health	ISO 22301	1

17. Is risk management a part of business strategy for legal entities, i.e. the owners and operators of infrastructures in Croatia? Please state which international norms are being implemented in this process.

REMARK: The answers are uniformly distributed in all categories. Nonetheless, it is clear that only three respondents (Ministry of Science, Education and Sport, Ministry of Culture and Ministry of Maritime Affairs, Transport and Infrastructure) correctly claimed that the risk management is a part of business strategy of legal entities – infrastructure managers and owners. On the other hand, responses of the majority of the respondents still point to varying levels of information on the above possessed within this area since four of them gave negative replies, and three failed to provide any answer at all. (Figure 15)

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Figure 15. Response to the question "Is risk management a part of business strategy for legal entities, i.e. the owners/operators of infrastructures?" Response frequencies are shown (N=10).

The international norms implemented in the process, according to statements by the respondents, are shown in Table 8. However, we can observe that only two respondents provided a specific norm.

REMARK: It is clear that the more specific questions are the fewer respondents provided or knew the answers.

Table 8. Responses to the question "Which international norms are being implemented in risk management?" with a review of institutions to which the respondents who provided answers belong.

Institution/respondent	Response	Number of statements
University of Applied Sciences Velika Gorica	ISO 31000	1
Ministry of Health	World Health Organization norm	1
Ministry of Finance Ministry of Economy Ministry of Culture Ministry of Agriculture Ministry of Interior Ministry of Environmental and Nature Protection Ministry of Maritime Affairs, Transport and Infrastructure Ministry of Science, Education and Sport	No answer	8

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

18. Is Business Continuity Management a part of business strategy for legal entities, i.e. the owners and operators of infrastructures in Croatia?

Six (6) respondents who participated in the survey gave no answer, while two stated that Business Continuity Management is not a part of legal entities' business strategies. There are only two affirmative answers (Ministry of Maritime Affairs, Transport and Infrastructure and, and Ministry of Health). (Figure 16)

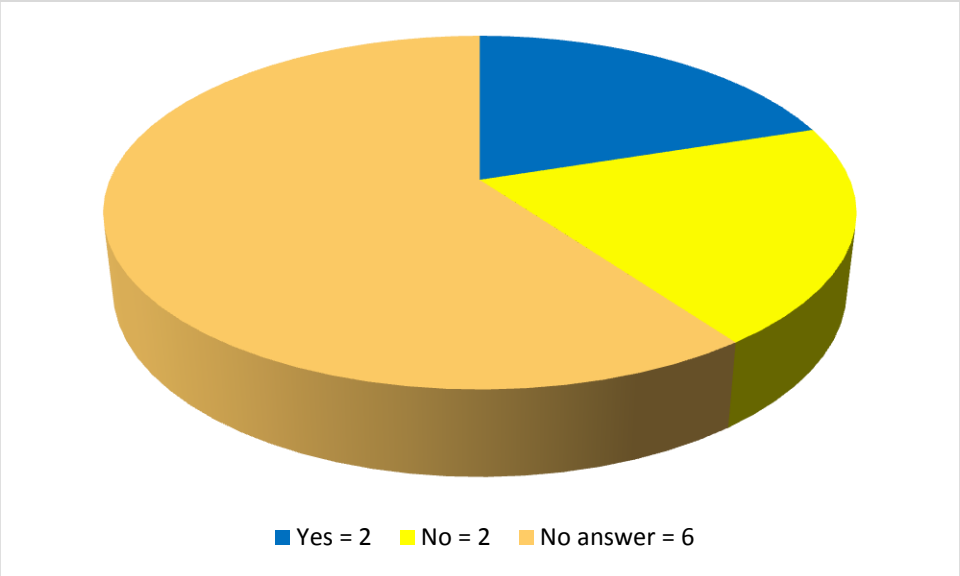


Figure 16. Response to the question "Is Business Continuity Management a part of business strategy for legal entities, i.e. the owners and operators of infrastructures in Croatia?" Response frequencies are shown (N=10).

19. Do public and private sectors cooperate in critical infrastructure risk management in Croatia?

According to Figure 17, it is clear that a greater number of respondents is not clear if there is a cooperation between private and public sectors in critical infrastructure risk management (4 provided no replies and 3 denied there is one). Three claimed that such cooperation exists (University of Applied Sciences Velika Gorica, Ministry of Economy, and Ministry of Science, Education and Sport).

REMARK: The information points to the need to enhance cooperation between private and public sectors and establish it at multiple levels to create a network of cooperating institutions.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Two respondents (University of Applied Sciences Velika Gorica and Ministry of Economy) provided descriptions of the above cooperation and assessed the cooperation as moderately satisfactory. The above information is shown in Table 9.

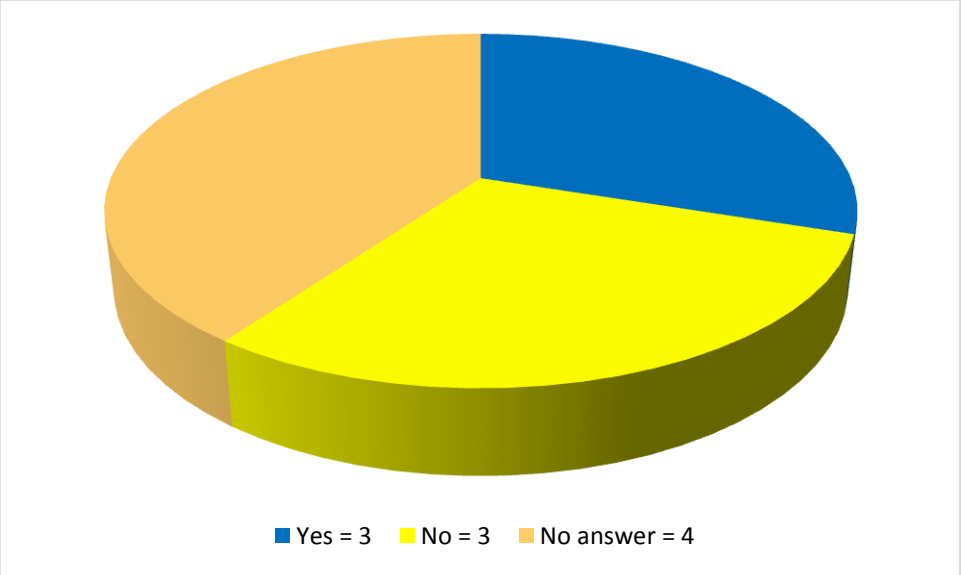


Figure 17. Response to the question "Do public and private sectors cooperate in critical infrastructure risk management in Croatia?" Response frequencies are shown (N=10).

Table 9. Description of cooperation between public and private sectors cooperate in establishment of critical infrastructure risk management in Croatia

Institution/respondent	Description of cooperation	Assessment of cooperation	Suggestions for improvements
University of Applied Sciences in Velika Gorica	In preventive activities and advice required regarding introduction of protection systems and in cases of increased threats	**Moderate**	Cooperation between public and private sectors is necessary in development of an assessment of threat to critical infrastructure. In absence of that cooperation, the assessment may not be prepared properly, especially in cases of possible security threats to property.
Ministry of Economy	Development of analyses and estimates		Define equal measurements at the national level

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

20. How you evaluate the critical infrastructure protection and management system in Croatia.

The respondents are requested to evaluate the critical infrastructure protection and management system. The received replies are provided in Table 10.

The evaluation scale contained three grades: "low", "moderate", and "high".

Only a half of the respondents rated the system: three of them assessed it as "moderate" and two as "low". (Figure 18)

An example of irrelevant description of the cooperation: "National Protection and Rescue Directorate should assume full responsibility for implementation and supervision of implementation of provisions of legislation or hand over its competence to others."

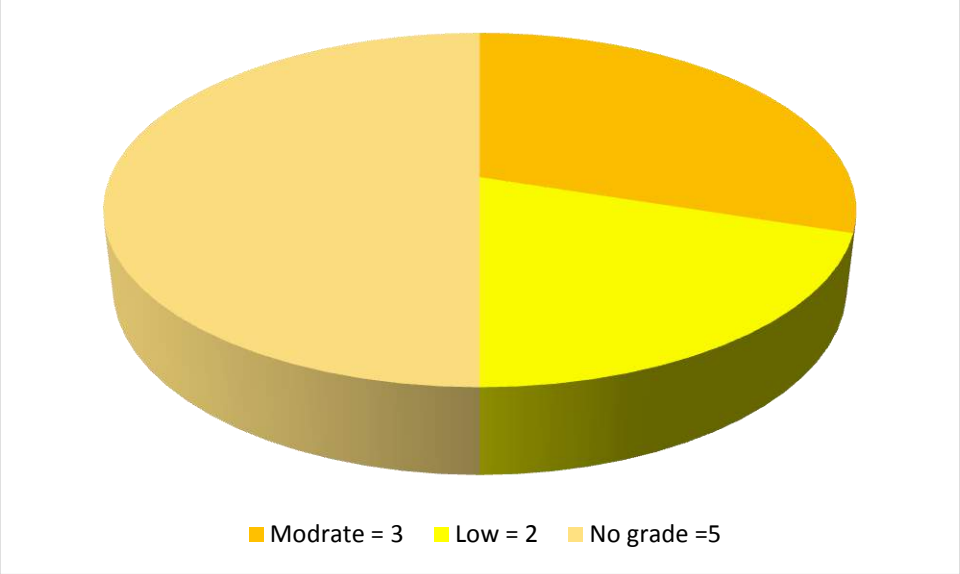


Figure 18. Distribution of the critical infrastructure protection and management system evaluation grades considering the part of the sample which provided a grade.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Table 10. Evaluation of the critical infrastructure protection and management system in Croatia

Institution/respondent	Description of cooperation	Response frequency	Own assessment of the system
University of Applied Sciences Velika Gorica Ministry of Science, Education and Sport Ministry of Finance Ministry of Interior	Identification of critical infrastructure in progress	2	No evaluation grade (5)
Ministry of Culture Ministry of Maritime Affairs, Transport and Infrastructure Ministry of Environmental and Nature Protection	No answer or an irrelevant description	5	Low (2)
Ministry of Health	It is a business process which we currently strive to integrate in daily work routine	1	Moderate (3)
Ministry of Economy Ministry of Agriculture	It is not sufficiently developed	2	

21. Has Croatia identified the European critical infrastructures:

a) On its territory?

b) On another country's territory?

No affirmative answers were given in response to questions on identification of European critical infrastructure in one's own territory (Figure 19) and in territories of another country (Figure 20). Most of the respondents (7) gave a negative answer to the question on identification of European critical infrastructure in one's own territory, otherwise no reply was received. In response to the question on identification of European critical infrastructure in other country's territory, 6 respondents gave no answer, and 4 respondents replied negatively.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

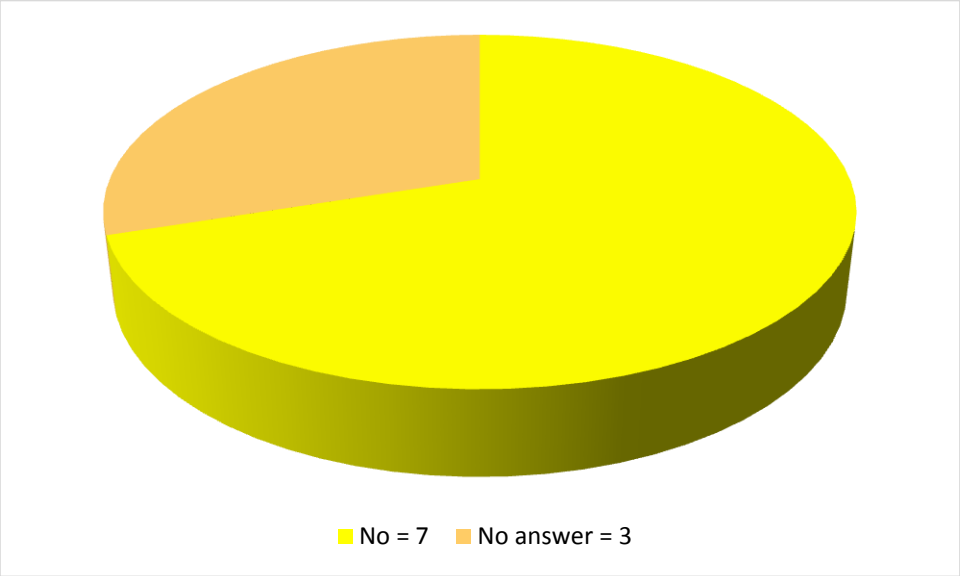


Figure 19. Response to the question "Has Croatia identified the European critical infrastructures in its own territory?" Response frequencies are shown (N=10).

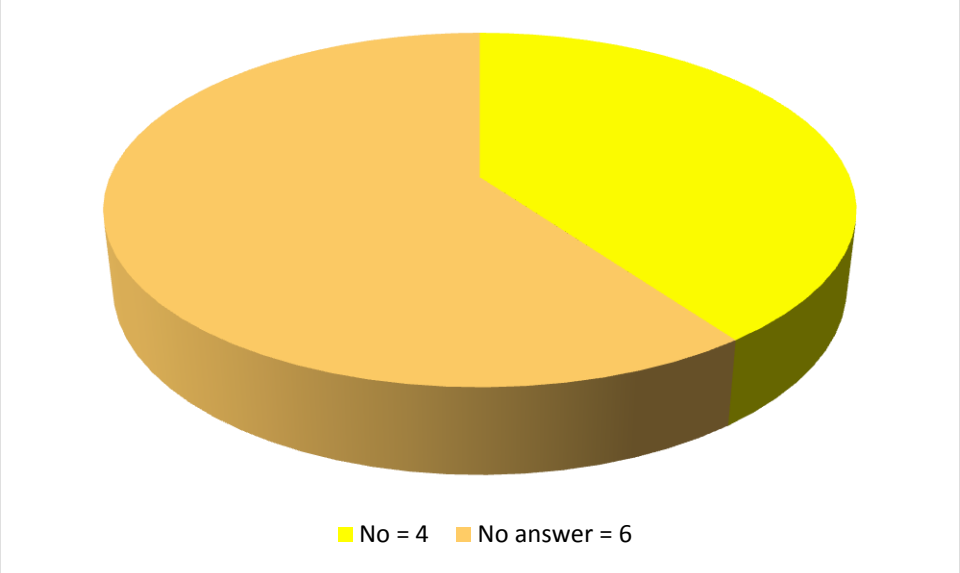


Figure 20. Response to the question "Has Croatia identified the European critical infrastructures in another country's territory?" Response frequencies are shown (N=10).

a) and b) If yes, please state from which sector and to what extent has the European critical infrastructure been identified in your state's territory or in territories of other countries?

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

22. If your country has identified the European critical infrastructures, please state what methodologies and criteria were used?

None of the 10 respondents provided any answer to questions a) and b) or to question 22.

23. Describe and assess the cooperation of your country with countries sharing the same identified European critical infrastructure.

Two of the respondents provided an assessment of international cooperation of countries who share the same European critical infrastructure, and only one ministry provided a description of the cooperation (Table 11).

The responses are irrelevant, since there are no identified European critical infrastructure at this point in the territory of Croatia, or Croatian ones in the territory of other Member States.

Table 11. Description of cooperation of the Republic of Croatia with countries sharing the same identified European critical infrastructure.

Institution	Response	Own assessment of the cooperation
Ministry of Health Ministry of Environmental and Nature Protection	We currently cooperate in the field of CBRN accidents within the framework of global and European safety of health through state institutions	Moderate

24. Is there any national funding for critical infrastructure protection in Croatia (non-EU funding)?

Six of the responded did not answer the question (Figure 21), while four of them correctly replied that there is no funding.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

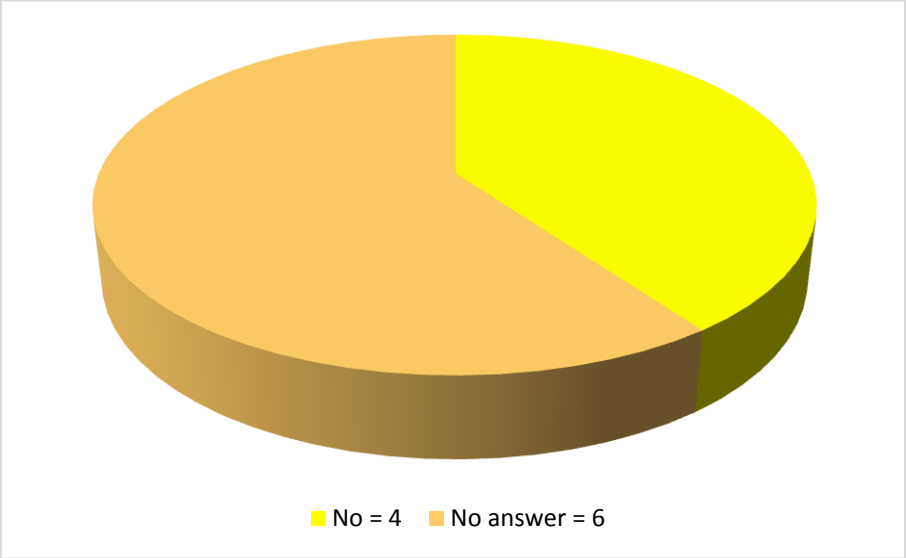


Figure 21. Response to the question "Is there any national funding for critical infrastructure protection in Croatia (non-EU funding)?" Response frequencies are shown (N=10).

25. Is there a possibility for cooperation in critical infrastructure protection on the regional level?

REMARK: There is a certain degree of interest for cooperation in critical infrastructure protection at a regional level since 6 of the respondents declared that there is a possibility for it (Figure 22). Negative (2) and missing (2) answers may be somewhat justified by the fact that current legislative framework does not allow it.

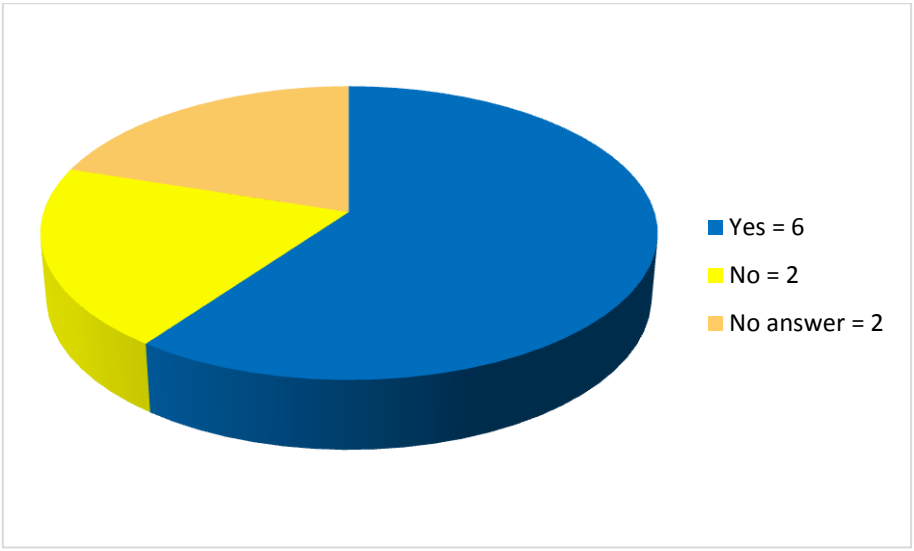


Figure 22. Response to the question "Is there a possibility for cooperation in critical infrastructure protection on the regional level of CIP?" Response frequencies are shown (N=10).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Descriptions of possibilities for the cooperation at a regional level are provided in Table 12.

Table 12. Description of possible cooperation in critical infrastructure protection at a regional level

Institution	Response	Response frequency
Ministry of Health	CBRN (in the field of cross-border accidents)	1
Ministry of Economy	The same principle as applied at the national level	1
Ministry of Agriculture	In identification of possible threats to critical infrastructure where the critical infrastructure is in the vicinity of a specific country or related to the same country	1
Ministry of Culture	Harmonisation of plans	1
University of Applied Sciences Velika Gorica Ministry of Finance Ministry of Interior Ministry of Maritime Affairs, Transport and Infrastructure Ministry of Environmental and Nature Protection Ministry of Science, Education and Sport	No answer	6

26. Are stimulating mechanisms (such as premiums and other benefits) used by insurance companies for critical infrastructure protection systems that implement security measures against disaster risks?

Five of the respondents did not answer this question, two replied affirmatively, and two denied existence of such mechanisms. (Figure 23)

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

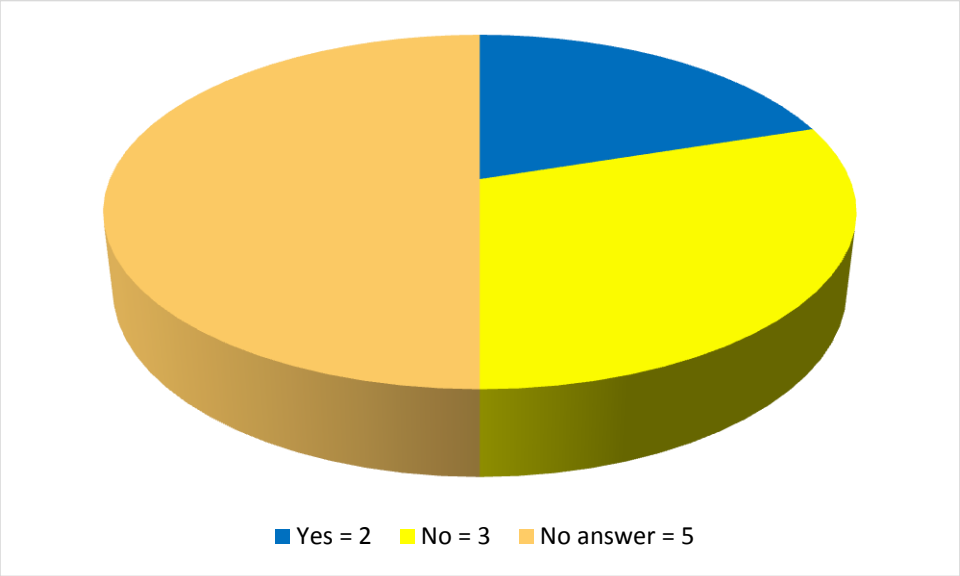


Figure 23. Response to the question "Are stimulating mechanisms (such as premiums and other benefits) used by insurance companies for critical infrastructure protection systems that implement security measures against disaster risks?" Response frequencies are shown (N=10).

REMARK:

The Ministry of Agriculture provided a description of such a mechanism:
"Assets are generally insured against potential threats. However, owners/managers avoid insurance of a part of the assets due to high premiums. Therefore, the assets are insured generally in accordance with legal requirements applicable to the owner/manager."

27. Are the policies of cost-benefit analysis of special measures for disaster risk reduction applied as resilience metrics?

No affirmative answers to this question were received, seven failed to reply and three returned negative replies. (Figure 24)

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

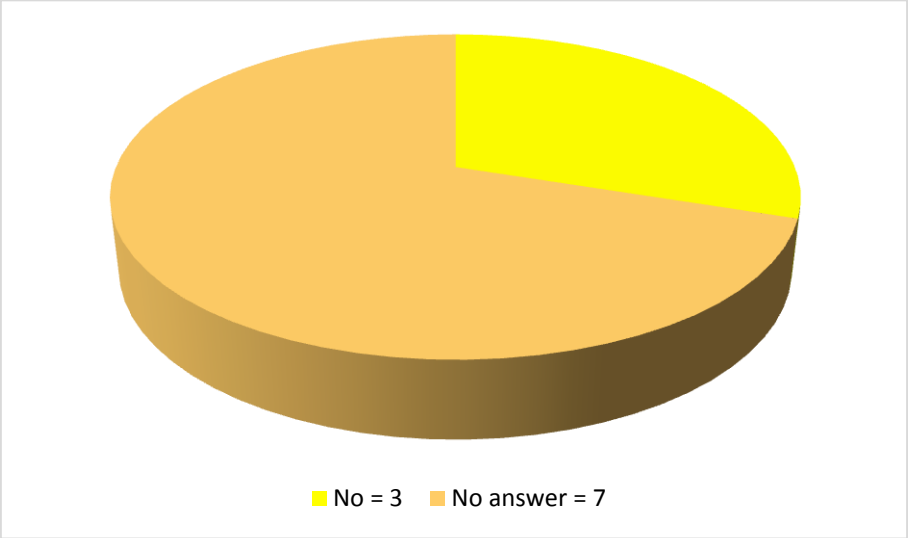


Figure 24. Response to the question "Are the policies of cost-benefit analysis of special measures for disaster risk reduction applied as resilience metrics?" Response frequencies are shown (N=10).

28. Are education and scientific research programmes in the field of critical infrastructure protection integrated into the higher education system?

A minority of three respondents declared that there are educational and scientific research programmes in the field of critical infrastructure protection within the higher education system, while other replied that there is none (2), or gave no answer (5). (Figure 25)

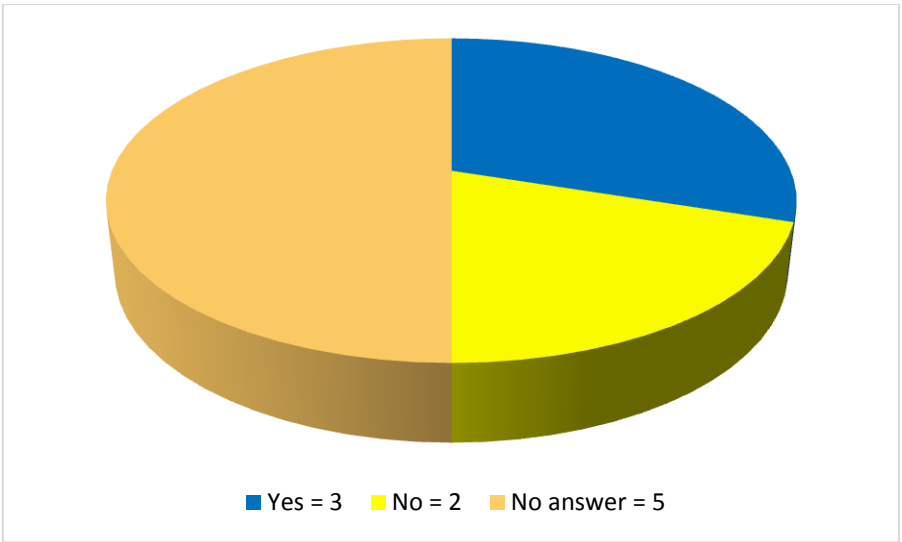


Figure 25. Response to the question "Are education and scientific research programmes in the field of critical infrastructure protection integrated into the higher education system?" Response frequencies are shown (N=10).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

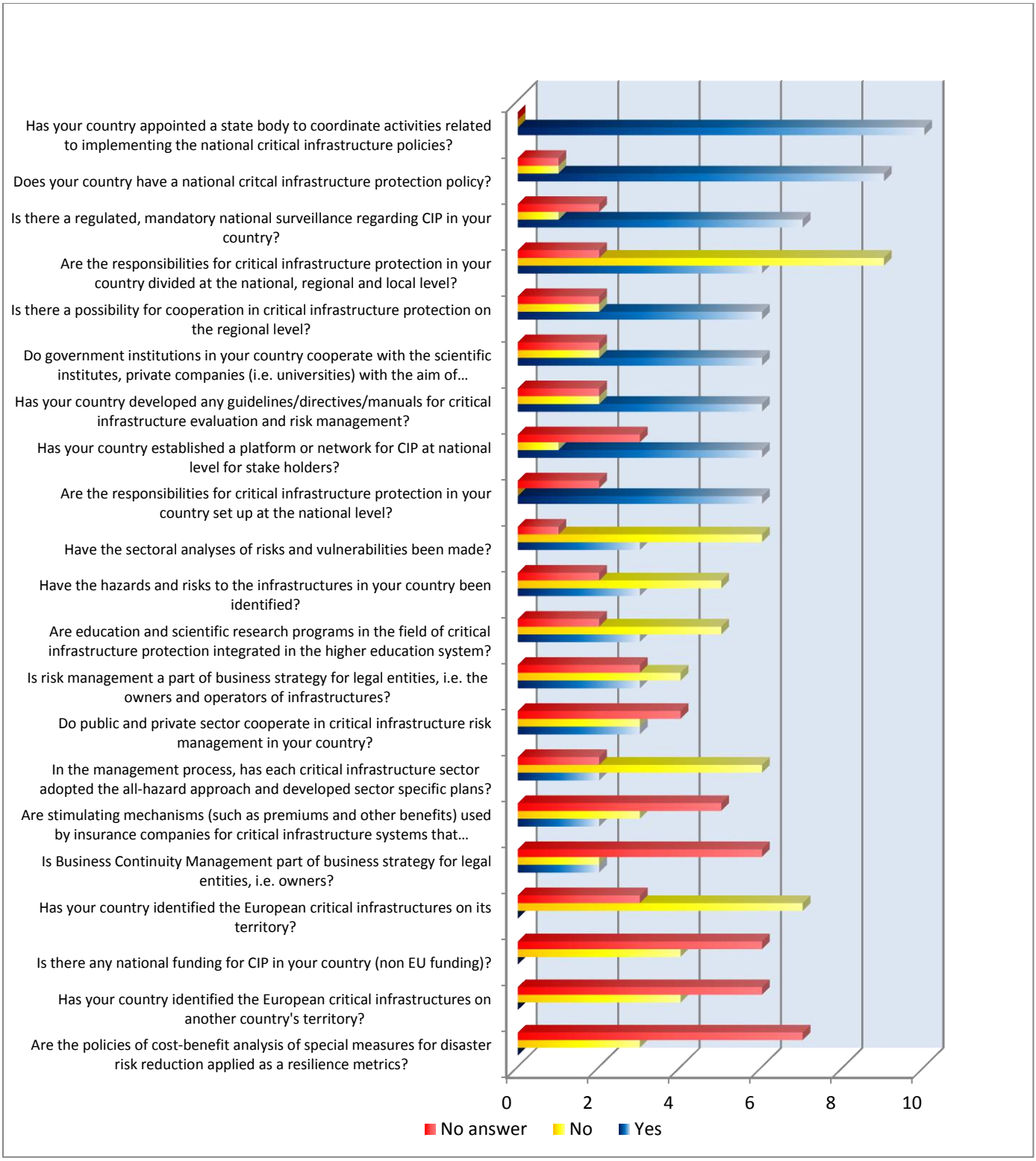


Figure 26. An overview of answers to all questions which could have been answered by a "yes" or "no" follows – sorted by the number of "yes" answers

CURRENT STATE ANALYSIS QUESTIONNAIRE SERBIA

Resilience of Critical Infrastructure Protection in Europe (RECIPE)

Financed under European Union Civil Protection Mechanism projects on Preparedness and Prevention projects in civil protection and marine pollution 2014

Humanitarian Aid
and Civil Protection
ECHO/SUB/2014/69600

1. CONTENTS

ACRONYMS AND ABBREVIATIONS 3
2. INTRODUCTION 4
2.1 Information collection procedure 4
3. RESULTS 6
3.1 Does your ministry/department have a critical infrastructure protection policy? 6
3.2 Is there a regulated, mandatory national surveillance regarding CIP in your ministry/department? 8
3.3 Is the legal regulative regarding CIP in line with the EU norms (EC Directive) regarding CIP? 9
3.4 Which of the following areas are included in the aforementioned Act/Regulation? 10
3.5 Which body (bodies) are responsible for implementing the national critical infrastructure protection policies in your ministry/department? 12
3.6 How are the responsibilities for CIP divided in your ministry/department? 13
3.7 Has your ministry/department appointed a body to coordinate activities related to implementing the national critical infrastructure policies? 14
3.8 Has your ministry/department established a platform or network for CIP at the national level for stake holders? 15
3.9 Which critical infrastructure sectors have been identified in your ministry/department? 16
3.10 Have the hazards and risks to the infrastructures in your ministry/department been identified? 17
3.11 Have the vulnerability and risk analyses to the infrastructures in your ministry been performed? 18
3.12 In the management process, has each critical infrastructure sector adopted the all-hazard approach and developed sector specific plans? 19
3.13 Which methodologies and which software models are used in for risk analysis and analysis of critical infrastructure interdependency? 20
3.14 Does your ministry/department cooperate with other institutions with the aim of developing models and methodologies for critical infrastructure risk management? 21

3.15 Has your ministry/department developed any guidelines / directives / manuals for critical infrastructure evaluation and risk management? 22

3.16 Which international standards for critical infrastructure risk management and business continuity are being used in your ministry/department? 23

3.17 Is risk management a part of business strategy for legal entities, i.e. the owners and operators of infrastructures within the scope of your ministry/sector? 24

3.18 Is Business Continuity Management part of business strategy for legal entities, i.e. owners of the process of critical infrastructure under the jurisdiction of your ministry/department? 25

3.19 Do public and private sector cooperate in critical infrastructure risk management under the jurisdiction of your ministry/department? 26

3.20 Please evaluate the system for management and protection of critical infrastructures under the jurisdiction of their ministry/department. 26

3.21 Has your ministry/sector has the authority to identify the European critical infrastructures? 27

3.22 Is there any national funding for CIP in your ministry/department (non-EU funding)? .28

3.23 Whether the security policy of the critical infrastructure owners is aligned with the legal regulations in the field of the CIP? 29

3.24 Is there a possibility for cooperation in critical infrastructure protection on the regional level? 30

3.25 Are stimulating mechanisms (such as premiums and other benefits) used by insurance companies for critical infrastructure systems that implement security measures against disaster risks? 31

3.26 Are the policies of cost-benefit analysis of special measures for disaster risk reduction applied as resilience metrics? 32

3.27 Are education and scientific research programs in the field of critical infrastructure protection integrated into the higher education system? 32

4. ANSWERS OF THE RESPONDENTS FROM THE COUNTRIES IN REGION 33

ACRONYMS AND ABBREVIATIONS

BIH	Bosnia and Herzegovina
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CMC	Crisis Management Centre (Macedonia).
DUZS	National Protection and Rescue Directorate – Republic of Croatia
GIS	Geographic Information System
ISPS Code	The International Ship and Port Facility Security
MAEP	Ministry of Agriculture and Environmental Protection
MCTI	Ministry of Construction, Transport and Infrastructure (Inland Waterway Transport and Navigation Security Sector).
MES	Cabinet of the Minister for Emergency Situations
MI	Ministry of Interior
MS	Ministry of Security (BiH);
MSB	Swedish Civil Contingencies Agency
MTC	Ministry of Transport and Communications (BiH);
RECIPE	Resilience of Critical Infrastructure Protection in Europe
RS	Republic of Serbia
SEVESO	Seveso-Directive (Directive 82/501/EEC); Seveso-II (Directive 96/82/EC); Seveso-III (Directive 2012/18/EU)
SOLAS	The International Convention for the Safety of Life at Sea
VVG	University of Applied Sciences, Velika Gorica, Republic of Croatia
ФБ	Faculty of Security Studies, University of Belgrade, Republic of Serbia

2. INTRODUCTION

Our survey, a part of the international project RECIPE (Resilience of Critical Infrastructure Protection in Europe), covered one project participant state (Serbia) and three neighbouring countries of the Region (Bosnia and Herzegovina, Montenegro and Macedonia).

The aim of the survey was to identify normative-legal aspects of organization of critical infrastructure protection (hereinafter CIP) and the most important practical problems in this field.

In accordance with the planned survey goals, the questionnaire with 29 questions, mostly of closed type, grouped in several sections:

- legal framework and practice of CIP of the Republic of Serbia;
- vulnerability assessment and threat identification of the critical infrastructure (hereinafter CI) of the Republic of Serbia;
- applicability of the existing methods and analyses for the CI risk assessment;
- interdependency analysis of CI in the Republic of Serbia;
- establishment of procedural strategies for improvement of cooperation and communication between national subjects (state sector, private sector and academic community), and between relevant subjects on international level;
- future modalities of efficient exchange of experience and transfer of knowledge between relevant subjects and definition of mechanisms for exchange of sensitive information.

2.1 Information collection procedure

After the preparation, creation and printing of the questionnaires, the survey was conducted in the period April - May 2015. The final sample consists of 14 questionnaires, of which 9 were completed by the national institutions from Serbia, and 5 from the neighbouring countries in the region.

National institutions from Serbia that sent the completed questionnaires are:

- Ministry of Mining and Energy (Sector for Power Engineering, Sector for oil and gas, Sector for geology and mines);
- Ministry of Construction, Transport and Infrastructure (Inland Waterway Transport and Navigation Security Sector, Sector for Railways and Intermodal Transport);
- Ministry of Agriculture and Environmental Protection (Department of Planning and Management in the Environment – Division for Major Chemical Accidents);
- Ministry of the Interior (Sector for Emergency Management);

- Cabinet of the Minister for Emergency Situations;
- Institute of Public Health of Serbia „Batut“.

The other national institutions that received the questionnaire but did not send the required information are: Ministry of Defence, Ministry of Foreign Affairs, Ministry of Culture and Information, Ministry of Finance, Ministry of Economy, Ministry of Health, Ministry of Public Administration and Local Self-Government, National Bank of Serbia, Government Office for Reconstruction and Flood Relief, and Republic Institute of Public Health Dr Milan Jovanovic Batut.

National institutions from the countries in the region that submitted the completed questionnaires are:

Bosnia and Herzegovina

- Ministry of Transport and Communications
- Ministry of Security

Montenegro

- Ministry of Interior (Directorate for Emergency Situations)

Macedonia

- Protection and Rescue Directorate
- Crisis Management Centre

3. RESULTS

3.1 Does your ministry/department have a critical infrastructure protection policy?

To the question does your ministry/department have a critical infrastructure protection policy a negative answer was given by the majority of respondents (n=8 or 88,8%) (Diagram 1). The exception was the Ministry of Construction, Transport and Infrastructure (Inland Waterway Transport and Navigation Security Sector) in which the CIP policy is regulated by the Law on Sea ("Official Gazette RS, no. 87/11, 104/13 i 18/15) and the Law on Navigation and Ports on Inland Waters ("Official Gazette RS", no. 73//10, 121/12 i 18/15).

The respondent from the Ministry of Agriculture and Environment Protection (Department of Planning and Management in the Environment – Division for Major Chemical Accidents) answered that there was no CIP policy in that ministry, but added the following comment: The Law on Environment Protection ("Official Gazette RS", no. 135/04, 36/09, 36/09 – other law and 72/09 – other law) and bylaws brought on the basis of that Law, as well as on the Law on Confirmation of the Convention on the Transboundary Effects of Industrial Accidents (Official Gazette RS, no. 42/09), regulate the field of the major chemical accident protection. The Law on Environment Protection and its bylaws partially transposed the SEVESO Directive on Control of Major-Accident Hazards including dangerous substances. The subjects of these regulations are SEVESO infrastructures/complexes, some of which may enter the definition of „critical infrastructure" within the Energy sector.

Besides that, the respondent from the Ministry of the Interior (Sector for Emergency Management) gave the following comment: CIP is not regulated by any law, nor is processed in the Law on Emergency Situations („Official Gazette RS", no. 111/09). The only regulation which mentions CI is the Guideline on the Methodology for Vulnerability Assessment and Emergency Plans Development, brought by the Minister in charge on October 5th, 2012 (Official Gazette RS, no.96/12). In this guideline, in the chapter dealing with the creation of vulnerability assessment, the field of the Critical Infrastructure Assessment from the Standpoint of Vulnerability to Natural Disasters and Other Accidents. By creation of the National Vulnerability Assessment to Natural Disasters and Other Accidents the CI objects and installations will be identified and assessed the vulnerability and adverse effects on their functioning, as well as the consequences of a potential disruption to their performance in certain key activities. The Action Plan for the Implementation of the Chapter 24 is being developed, in the part related to the creation of the legal framework for CI identification and protection in the Republic of Serbia.

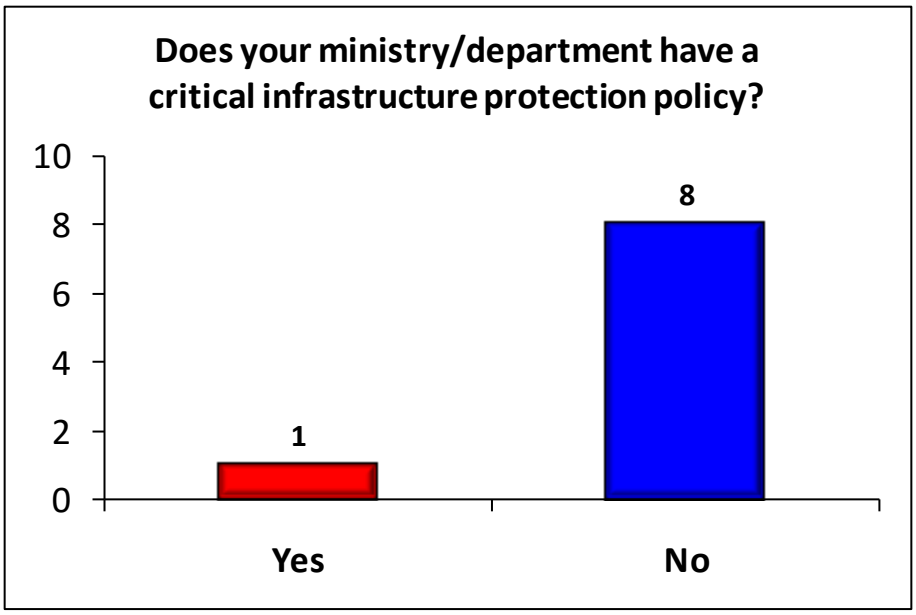


Diagram 1. Overview of results about the existence of CIP policies

3.2 Is there a regulated, mandatory national surveillance regarding CIP in your ministry/department?

The clear majority of respondents answered that ***there is no regulated, mandatory national surveillance regarding CIP in their ministry/sector*** (n=8 or 88,8%). Again, the exception is Ministry of Construction, Transport and Infrastructure, where within the Department for Water Transport and Security of Navigation, according to the answer of one respondent, there is normatively regulated, mandatory national surveillance regarding CIP (Diagram 2).

A respondent from the Ministry of Agriculture and Environment Protection answered that there is no a regulated, mandatory national surveillance regarding CIP, but added that the Law on Environment Protection and the Law on Confirmation of the Convention on the Transboundary Effects of Industrial Accidents regulate the field of inspection surveillance of SEVESO installations/complexes and the control of its implementation.

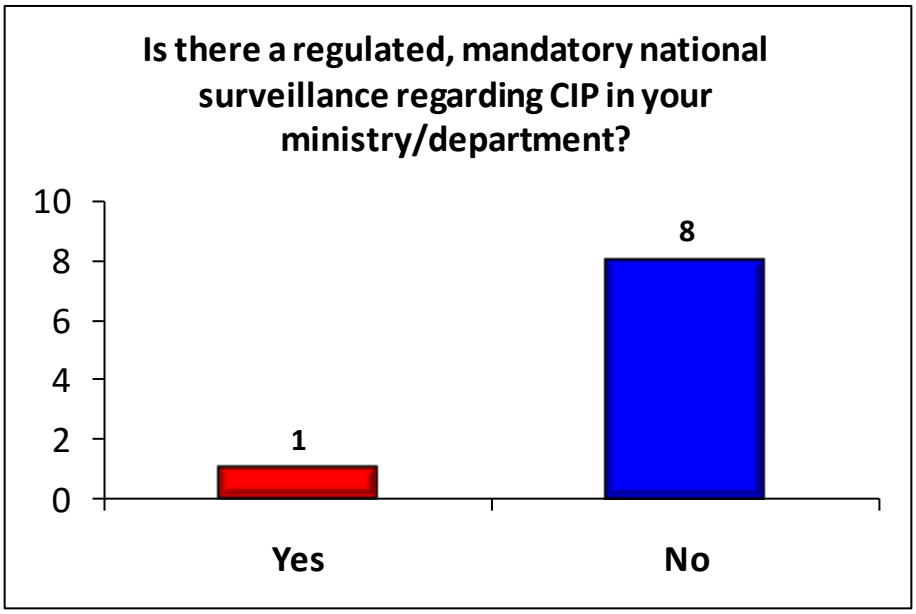


Diagram 2. Overview of results of mandatory national surveillance regarding CIP

3.3 Is the legal regulative regarding CIP in line with the EU norms (EC Directive) regarding CIP?

All respondents answered that national legal regulation regarding CIP is not in line with the EU norms (EC Directive) (Table 1). On the other hand, the respondent from the Ministry of Agriculture and Environment Protection commented that the Law on Environment Protection and its bylaws partially transpose the SEVESO directive on Control of Major-Accident Hazards Including Dangerous Substances.

Does the legal regulation regarding CIP conform with the EU norms (Directive EC) regarding CIP?	Number of respondents	%
Yes	0	0,0
No	9	100,0
Total	9	100,0

Table 1. Overview of results on conformity of national legal regulations regarding CIP with the EU norms (EC Directive) regarding CIP

3.4 Which of the following areas are included in the aforementioned Act/Regulation?

To the question ***which areas are included in the aforementioned Act/Regulation*** the majority of the respondents did not answer (n=5 or 55,5%), whilst some respondents think that the future act/regulation should contain particular areas (Table 2).

Besides that, the respondent from the Ministry of Agriculture and Environment Protection (Department of Planning and Management in the Environment – Division for Major Chemical Accidents) commented that an operator of a SEVESO installation/complex has the duty to create the Security Report and the Accident Protection Plan, in which he has to prove that he manages the risk of major chemical accident through a defined system of security management, to perform the threat identification (including the identification of external causes of chemical accidents, e.g. accidents on local SEVESO complexes, natural disasters, electricity cuts, terrorism etc.), model the effects of the worst case scenario of chemical accidents (with the theoretical foundation given as a maximum capacity of the dangerous substances and the failure of technical prevention measures), to estimate potential consequences of those accidents, to implement of necessary preventive measures on the complex he is in charge of, to plan the response to a possible chemical accident and, for the accidents with capacity to cross the border of complex, to provide the information to the local authorities for the creation of External accident protection plans, which are constituents of Prevention and Rescue Plans in Emergency Situations, on the basis of the Law on Emergency Situations.

Area	MAEP	MI	MES.	MCTI
Hazard and Risk Identification		x	x	
Critical Infrastructure Sectors		x	x	
Critical Infrastructure Identification		x	x	x
Risk Assessment and Analysis		x	x	
Vulnerability/Resilience Analysis		x	x	
Sector interdependency and critical infrastructure interdependency				
Models and methodologies of analysis			x	
Evaluation			x	

Cross-cutting and sectorial criteria for risk identification and risk analysis				
Risk management, stakeholders in risk management, levels of risk management				
Public-private partnership and cooperation with the academic community				
Business Continuity Management				
Exercises				
European critical infrastructures				
Education and scientific research			x	
Other	x			

Table 2. Overview of results stating which areas should be included in the aforementioned act/regulation

Legend: *MAEP – Ministry of Agriculture and Environmental Protection; MI – Ministry of Interior; MES – Cabinet of the Minister for Emergency Situations; MCTI – Ministry of Construction, Transport and Infrastructure (Inland Waterway Transport and Navigation Security Sector).*

3.5 Which body (bodies) are responsible for implementing the national critical infrastructure protection policies in your ministry/department?

To the question ***which body (bodies) are responsible for implementing the critical infrastructure protection policies in your Ministry/department*** majority of responders answered that it is not regulated (n=6 or 66,6%), whilst the respondent from the Ministry of Agriculture and Environment Protection did not respond to this question, and the respondent from the Cabinet of the Minister for Emergency Situations mentioned Ministry of the Interior (Sector for Emergency Management) as a responsible body.

The respondent from the Ministry of the Interior explained his answer in the following way: Risk Management Directorate within the Sector for Emergency Management is in charge of the creation of the National vulnerability assessment, so it will be also in charge for unification of results and opinions of the relevant ministries in charge of CI identification, which will be represented in the CI vulnerability assessment. In that sense, vulnerability assessment of CI objects in the following areas will be taken into account:

- electrical energy production and distribution (hydro and coal fuelled power plants, transmission lines, transformer substations);
- production and supply of fuels (refineries, oil deposits, gas storages and storages of oil derivatives, oil and gas pipelines);
- Telecommunications (transmission lines, fixed and mobile telephony, telephone exchanges);
- Production and supply of potable water (water springs and factories, distributional centres);
- Production and supply of food (food production plants); Health Protection (health protection institutions and objects);
- material and cultural goods (museums, theatres, cultural historical monuments) and National Parks.

After the creation and adoption of the Vulnerability assessment, the Sector for Emergency Management (Office for Civil Protection) will together with relevant ministries, organizations and other relevant legal entities begin with creation of the National rescue and protection plan, which will contain separate rescue and protection plans of people and material goods related to threats and hazards identified in the Vulnerability assessment (floods, earthquakes, forest fires, epidemics etc.). In those plans a particular attention will be paid to the CIP regarding all hazards.

3.6 How are the responsibilities for CIP divided in your ministry/department?

Answers to the question ***How are the responsibilities for CIP divided in Your ministry/department*** are given in the Table 3.

The respondents from the Ministry of Mining and Energy think that the following organizations are responsible for CI security and protection:

- Sector for geology and mines (companies involved in the exploitation of coal for supply of coal fired power stations);
- Oil and gas sector (energy subjects).

The respondent from the Public Health Institute „Batut“ stated that the responsibility is essentially divided among all levels, but that the monitoring and reporting mechanisms have not been formally established. The respondent from the MI stated that after identification and creation of the CI regulations, the responsible sides for the CIP at all levels will be also defined.

Division of responsibilities for CIP in the ministries/departments	Number of respondents	Presence %
No answer	1	11,1
Not regulated	1	11,1
At the national level only	2	22,2
At the national and regional level	1	11,1
At the national, regional and local level	0	0,0
Other	4	44,5
Total	9	100,0

Table 3. Overview of results on division of responsibility for the CIP e

3.7 Has your ministry/department appointed a body to coordinate activities related to implementing the national critical infrastructure policies?

To the question ***„Has your ministry/department appointed a body to coordinate activities related to implementing the national critical infrastructure policies?"*** the negative answer was given by the majority of respondents (n=7 or 77,7%). The respondent from the Ministry of Agriculture and Environment Protection did not answer this question, whilst the Cabinet of the Minister for Emergency Situations named the coordination body, but the respondent did not state its name (Diagram 3).

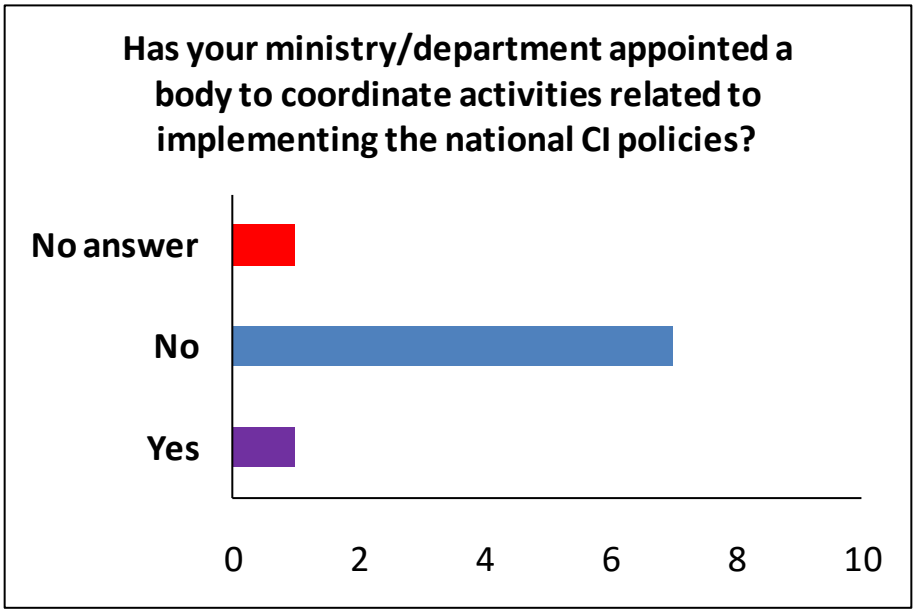


Diagram 3. Overview of results on appointment of bodies for coordination of activities related to implementing the national critical infrastructure protection policies

3.8 Has your ministry/department established a platform or network for CIP at the national level for stake holders?

The majority of respondents answered that ***their ministry/department has not established a platform or network for CIP at the national level for stake holders*** (n=7 or 77,7%). The respondent from the Ministry of Agriculture and Environment Protection did not answer this question, whilst the Ministry of Construction, Transport and Infrastructure (the Sector for Water Transport and Navigation Security) has established a platform or network for CIP for stakeholders, but the respondent did not mention its name (Diagram 4).

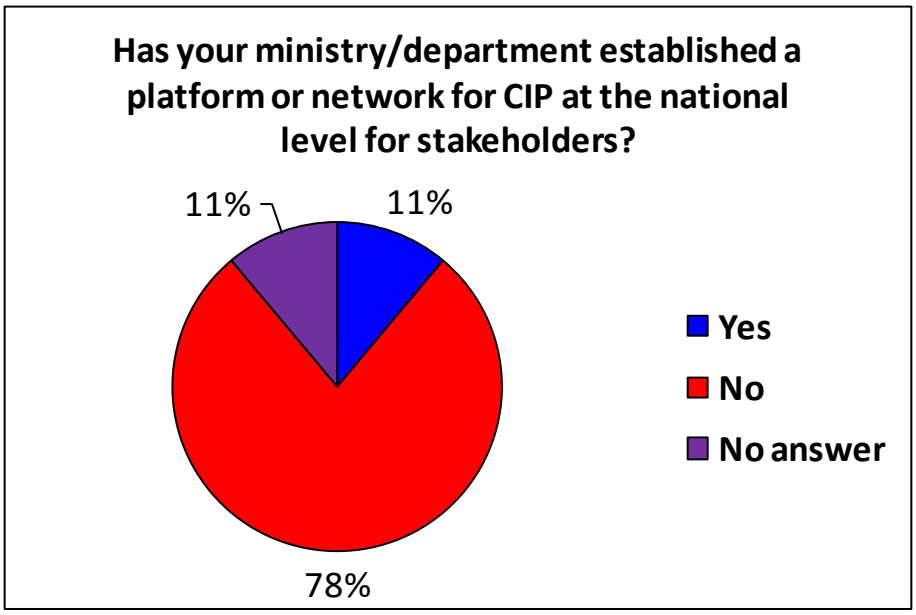


Diagram 4. Overview of results on established platforms or networks for stakeholders

3.9 Which critical infrastructure sectors have been identified in your ministry/department?

Four respondents did not give an answer to the question ***Which critical infrastructure sectors have been identified in your ministry/department?***, whilst two respondents said that it was not regulated.

Some ministries identified the following CI: ships, objects of navigation security and ports, shipyards (Inland Waterway Transport and Navigation Security Sector of the Ministry of Construction, Transport and Infrastructure); and Hydroelectric Power Plant „Đerdap“ (Cabinet of the Minister for Emergency Situations).

The respondent from the Ministry of Agriculture and Environment Protection (Department of Planning and Management in the Environment – Division for Major Chemical Accidents) stated that this ministry, in line with regulative, maintains the Registry of facilities on the basis of the submitted documents, in which 53 SEVESO „lower order“ facilities / complexes, and 44 SEVESO „higher order“ facilities / complexes were identified (some of these facilities / complexes can be identified as CI).

3.10 Have the hazards and risks to the infrastructures in your ministry/department been identified?

Majority of respondents answered that ***their ministry/department has not identified hazards and risks to their critical infrastructures*** (n=7 or 77,7%), whilst the Cabinet of the Minister for Emergency Situations identified landslides and escarpments.

The respondent from the Ministry of Agriculture and Environment Protection stated that operators are due to identify hazards in SEVESO facilities/complexes within the Security Reports, which encompasses identification of critical points, i.e. points in process or in facilities that represent the weakest links or potential sources of hazard from the aspect of accident formation.

Within the identification process, human factor is particularly analysed as a potential source of accident. During the identification of critical points, all segments of technological processes are checked, as well as all parts of facilities, machinery, transport vehicles and equipment, and then critical points on facilities, machinery and equipment are marked and defined, as well as the causes that can trigger disruptions or failures leading to chemical accident. This includes the following analyses: technical and technological specificities and shortcomings in production, transport and storage; specificity of physicochemical properties of dangerous substances; possible failures of components and materials due to deterioration of equipment and interruption of energy supplies; external sources of hazard (extreme temperatures, wind, rainfall and floods, fires, earthquakes and landslides); activities of neighbouring operators; and analysis of previous accidents.

3.11 Have the vulnerability and risk analyses to the infrastructures in your ministry been performed?

A negative answer by the majority of the respondents was given to the question ***Have the vulnerability and risk analyses to the infrastructures in your ministry been performed?*** (Diagram 5).

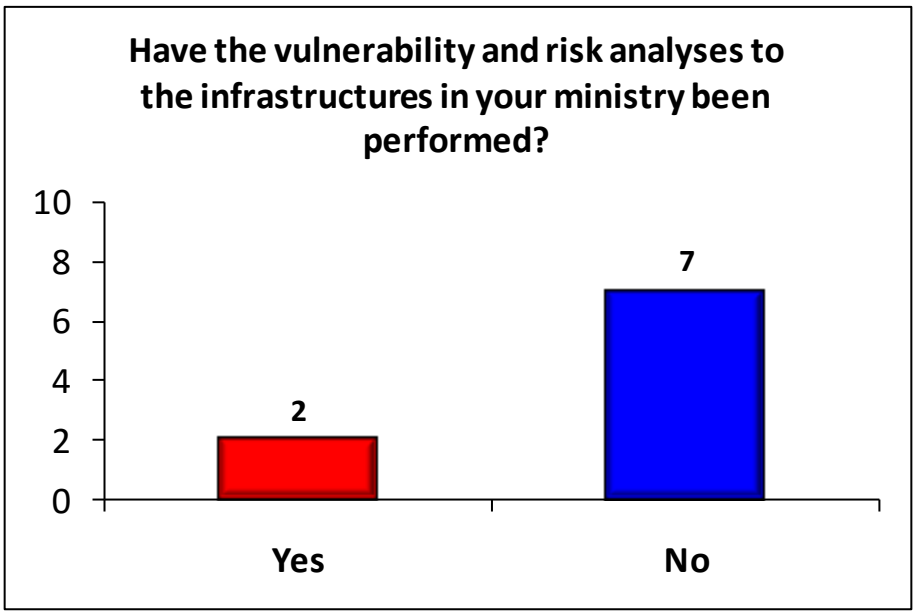


Diagram 5. Overview of results on performed vulnerability and risk analyses to the CI

CI vulnerability and risk analyses were performed in the Cabinet of the Minister for Emergency Situations, and in the Ministry of Agriculture and Environment Protection (Department of Planning and Management in the Environment – Division for Major Chemical Accidents) where in accordance with the aforementioned regulations, during the course of creation of the Security Report operators must perform consequence analysis for SEVESO „higher order" facilities/complexes, which comprises modelling of effects, vulnerability analysis, determination of the potential accident level and risk assessment (Diagram 5).

3.12 In the management process, has each critical infrastructure sector adopted the all-hazard approach and developed sector specific plans?

The majority of respondents (n=6 or 66,6%) answered that ***in the management process, not each critical infrastructure sector adopted the all-hazard approach and has not developed sector specific plans***, whilst only the respondent from the Cabinet of the Minister for Emergency Situations did not answer this questions.

Within the Ministry of Construction, Transport and Infrastructure (Inland Waterway Transport and Navigation Security Sector) the law provides the duties of Directorate for Inland Waterways, port operators, ship-owners and shipyards.

The respondent from the Ministry of Agriculture and Environment Protection (Department of Planning and Management in the Environment – Division for Major Chemical Accidents) stated that for the sake of security management, the operators have duty to create the Security Management System. This system the operator needs to define and implement in order to fulfil previously defined goals and business policies.

3.13 Which methodologies and which software models are used in for risk analysis and analysis of critical infrastructure interdependency?

The answer to the question about ***which methodologies and which software models are used in for risk analysis and analysis of critical infrastructure interdependency*** did not give four respondents, whilst one respondent answered that this problem is not regulated. The remaining four respondents stated the following methodologies and software models that are used in their ministries/departments for risk analysis and analysis of critical infrastructure interdependency:

- ArcGIS software for assessment of landslides, escarpments and erosion, creation of geology hazard and risk maps, as well as for the data related to the exploitation fields (Ministry of Mining and Energy, Sector for Geology and Mines);
- Rule book on the content of the accident prevention policy and content and methodology of creation of The Security report and Accident protection plan Ministry of Agriculture and Environment Protection (Department of Planning and Management in the Environment – Division for Major Chemical Accidents);
- Instruction on methodology for creation of vulnerability assessment and rescue and protection plans (Ministry of Interior);
- Risk Assessment Methodology (Cabinet of the Minister for Emergency Situations).

3.14 Does your ministry/department cooperate with other institutions with the aim of developing models and methodologies for critical infrastructure risk management?

To the question **does your ministry/department cooperate with other institutions with the aim of developing models and methodologies for critical infrastructure risk management**? five respondents answered "yes" and four respondents answered "no" (Diagram 6).

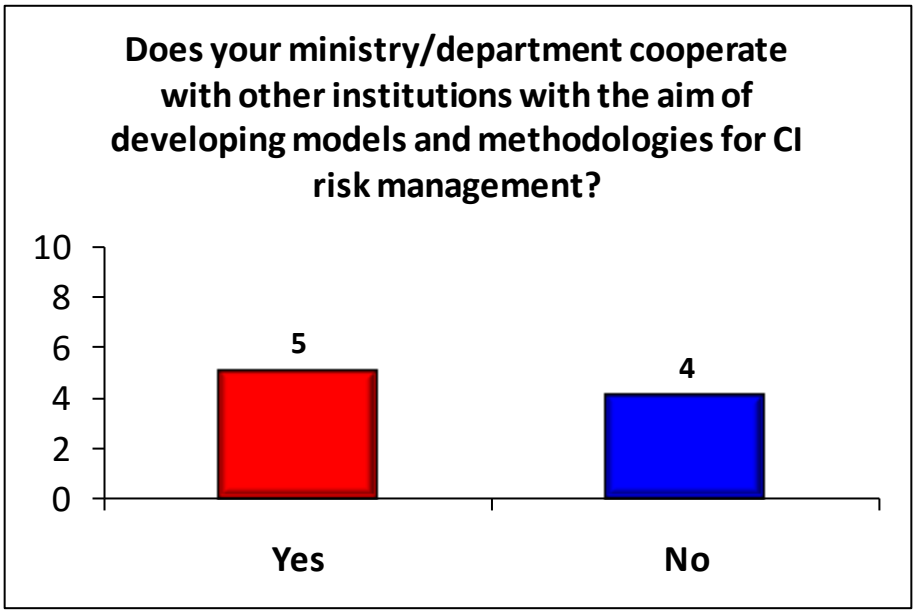


Diagram 6. Overview of results on cooperation of ministries/departments and other institutions

Ministry of Mining and Energy in cooperation with Faculty of Mining and Geology, University of Belgrade and Sector for Emergency Management of the Ministry of the Interior developed a methodology for geology hazard and risk assessment.

Ministry of the Interior (Sector for Emergency Management) has an established cooperation with scientific institutes and universities, as well as with other ministries, organizations and big technical systems.

Ministry of Agriculture and Environment Protection (Department of Planning and Management in the Environment – Division for Major Chemical Accidents) has an established cooperation with scientific institutes and universities.

3.15 Has your ministry/department developed any guidelines / directives / manuals for critical infrastructure evaluation and risk management?

To the question ***Has your ministry/sector developed any guidelines/directives/manuals for critical infrastructure evaluation and risk management?*** the majority of respondents gave a negative answer (n = 8 or 88,8%).

The respondent from the Cabinet of the Minister for Emergency Situations gave positive answer to this question, but he has not stated any concrete guidelines/directives/manuals developed by the Minister (Diagram 7).

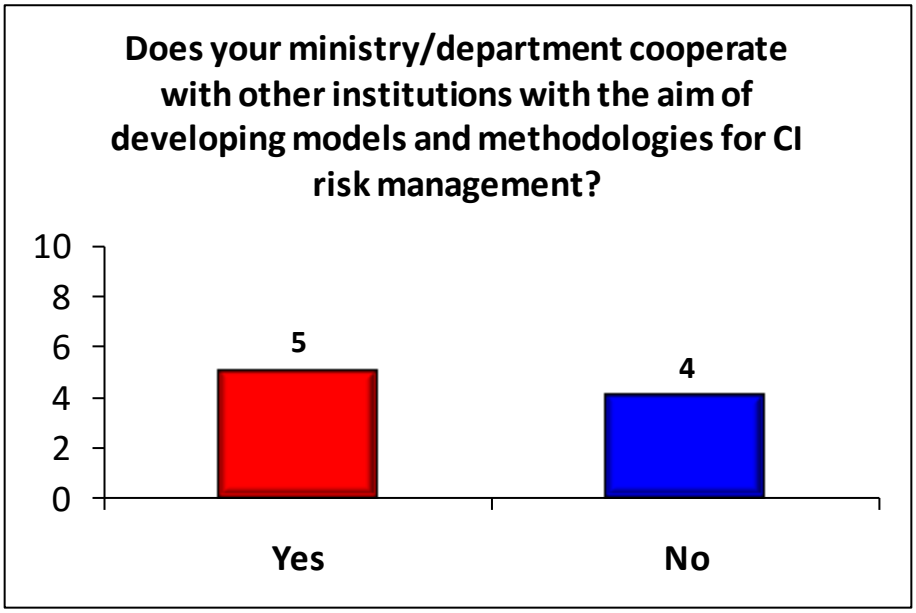


Diagram 7. Overview of results on developed guidelines/directives/manuals for critical infrastructure evaluation and risk management

3.16 Which international standards for critical infrastructure risk management and business continuity are being used in your ministry/department?

Six respondents did not respond the question: ***Which international standards for critical infrastructure risk management and business continuity are being used in your ministry/department?*** (n = 6 or 66,6%), whilst the respondent from the Ministry of Mining and Energy (Sector for Power Engineering) stated that this field is not regulated.

The respondent from the Cabinet of the Minister for Emergency Situations mentioned the *Safe Land Project*, and the respondent from the Ministry of Construction, Transport and Infrastructure (Inland Waterway Transport and Navigation Security Sector) asserted that this field is regulated by an international agreement – The International Convention for the Safety of Life at Sea (SOLAS) and The International Ship and Port Facility Security (ISPS Code).

3.17 Is risk management a part of business strategy for legal entities, i.e. the owners and operators of infrastructures within the scope of your ministry/sector?

Five respondents (55,5%) gave a negative answer to the question ***Is risk management a part of business strategy for legal entities, i.e. the owners and operators of infrastructures within the scope of your ministry/sector?***, whilst 2 respondents gave the positive answer – from Ministry of Agriculture and Environment Protection (Department of Planning and Management in the Environment –Division for Major Chemical Accidents) and the Ministry of Construction, Transport and Infrastructure (Inland Waterway Transport and Navigation Security Sector), who stated that those are Danube Commission Recommendations on Security of Shipping on Danube. The respondent from the Sector for Emergency Management (Ministry of Interior) did not respond to this question, whilst the respondent from the Institute for the Public Health of Serbia „Batut" answered that he had no information regarding that question (Diagram 8) .

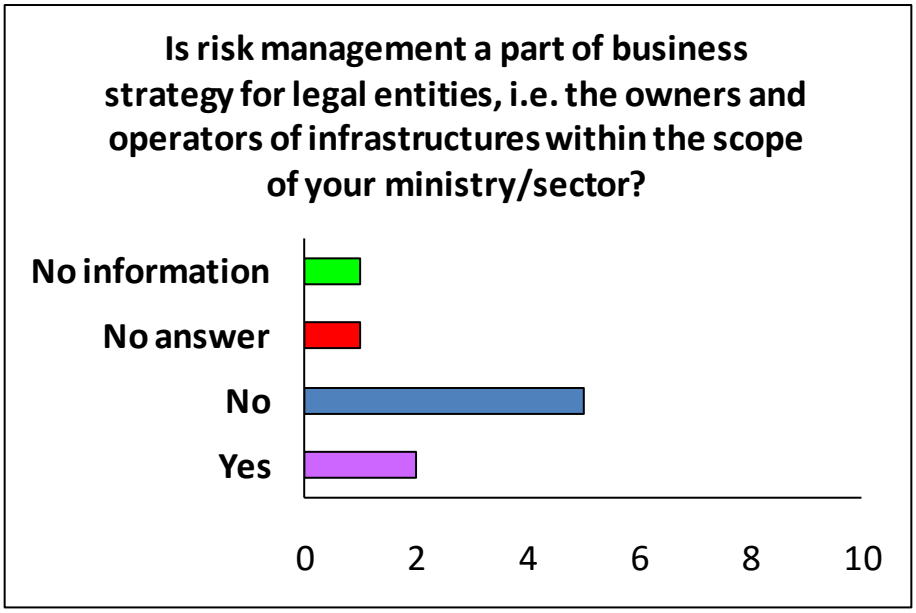


Diagram 8. Overview of results on risk management as a part of business strategy

3.18 Is Business Continuity Management part of business strategy for legal entities, i.e. owners of the process of critical infrastructure under the jurisdiction of your ministry/department?

The majority of respondents (n = 5 or 55,5%) gave a negative answer to the question ***Is Business Continuity Management part of business strategy for legal entities, i.e. owners of the process of critical infrastructure under the jurisdiction of your ministry/department***. The respondent from the from the Institute for the Public Health of Serbia „Batut“ answered that he had no information regarding that question, while the positive answer was given by two respondents (Cabinet of Minister for Emergency Situations, Ministry of Construction, Transport and Infrastructure - Inland Waterway Transport and Navigation Security Sector), and the respondent from the Ministry of the Interior (Sector for Emergency Management) did not answer to this question (Diagram 9).

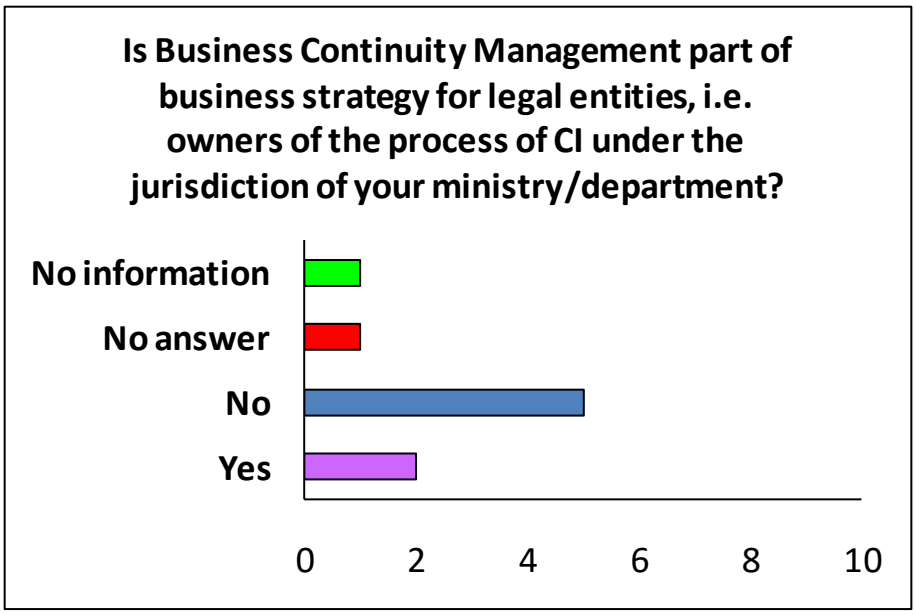


Diagram 9. Results on Business Continuity Management as a part of business strategy

3.19 Do public and private sector cooperate in critical infrastructure risk management under the jurisdiction of your ministry/department?

A negative answer to the question ***Do public and private sector cooperate in critical infrastructure risk management under the jurisdiction of your ministry/department?*** gave 5 respondents (55,5%).

The respondents who gave the positive answer to this question and evaluated that cooperation in risk management come from the following institutions:

- Ministry of Agriculture and Environment Protection (cooperation level is moderate);
- Institute for the Public Health of Serbia „Batut“ (cooperation level is low);
- Cabinet of Minister for Emergency Situations (cooperation level is low);
- Ministry of Construction, Transport and Infrastructure - Inland Waterway Transport and Navigation Security Sector (cooperation level is moderate).

3.20 Please evaluate the system for management and protection of critical infrastructures under the jurisdiction of their ministry/department.

The request ***to evaluate the system for management and protection of critical infrastructures under the jurisdiction of their ministry/department*** was not answered by 4 respondents (44,4%), whilst the respondent from the Ministry of Mining and Energy (Sector for Power Engineering) answered that the mentioned system in their sector is not regulated.

The system for management and protection of critical infrastructures was evaluated by the respondents from the following institutions:

- Ministry of Agriculture and Environment Protection (Moderate);
- Institute for the Public Health of Serbia „Batut“ (low);
- Ministry of Construction, Transport and Infrastructure - Inland Waterway Transport and Navigation Security Sector (moderate);
- Ministry of Construction, Transport and Infrastructure - Sector for Railways and Intermodal Transport (moderate).

3.21 Has your ministry/sector has the authority to identify the European critical infrastructures?

Five respondents (55,5%) gave a negative answer to the question ***Has your ministry/sector has the authority to identify the European critical infrastructures?.***

One respondent did not have information related to this question (Sector for Power Engineering, Ministry of Mining and Energy), whilst another respondent from the same ministry but different sector (Sector for Geology and Mines) did not answer this question (Diagram 10).

The respondent from the Cabinet of the Minister for Emergency Situations responded that their Cabinet has the abovementioned authority, but solely on its territory.

The respondent from the Ministry of Construction, Transport and Infrastructure (Sector for Water Transport and Navigation Security) stated that they have that authority over international waterways (Danube and Sava rivers).

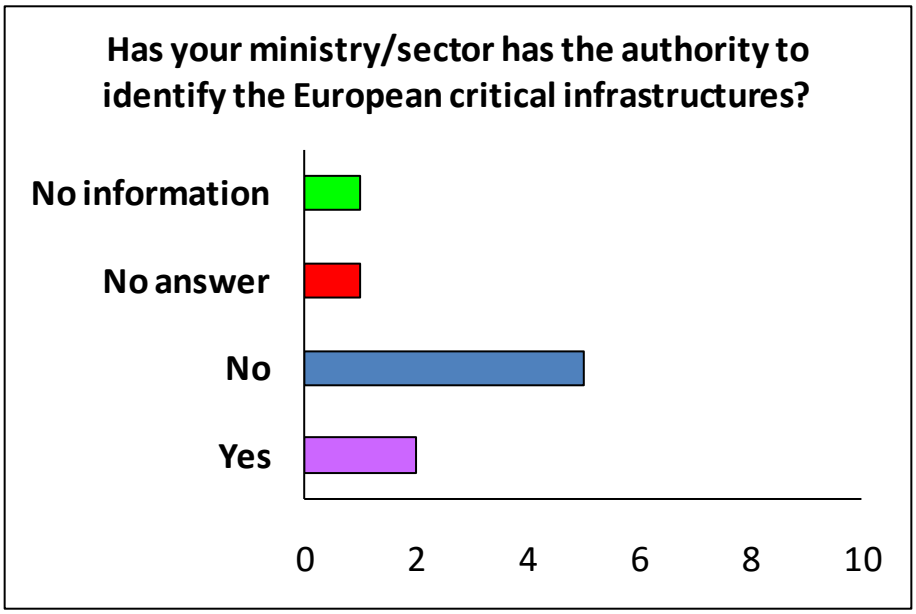


Diagram 10. Overview of Results on authority to identify the European CI

3.22 Is there any national funding for CIP in your ministry/department (non-EU funding)?

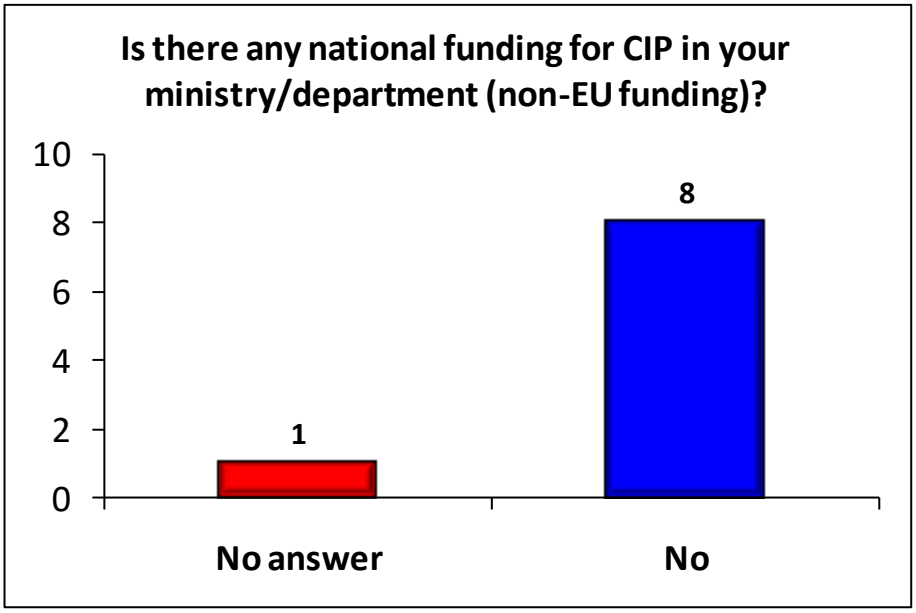


Diagram 11.

3.23 Whether the security policy of the critical infrastructure owners is aligned with the legal regulations in the field of the CIP?

To the question ***whether the security policy of the critical infrastructure owners is aligned with the legal regulations in the field of the CIP*** the answer did not give 5 respondents (55,5%).

The affirmative answer to this question was given by the respondent from the Ministry of Agriculture and Environment Protection (Sector for Environment Planning and Management – Department for Major Chemical Accidents Protection), who stated that the policy of the prevention of major chemical accidents, defined by operators of SEVESO facilities/complexes, is in accordance with the legal acts in the field of chemical accidents protection. Also, the affirmative answer was given by the respondent from the Ministry of Construction, Transport and Infrastructure (Inland Waterway Transport and Navigation Security Sector), who wrote that the legal solutions defined the duties that have to be observed.

The answer of the respondent from the Ministry of Mining and Energy (Sector for Power Engineering) was that this security policy is not regulated, whilst the respondent from the Cabinet of the Minister for Emergency Situations answered negatively.

3.24 Is there a possibility for cooperation in critical infrastructure protection on the regional level?

The question ***Is there a possibility for cooperation in critical infrastructure protection on the regional level?*** was affirmatively answered by 5 (55,5%) respondents, without précising which forms of cooperation they consider the most important. The respondent from the Ministry of Construction, Transport and Infrastructure (Department for Railways and Intermodal Transport) thinks that there is no such possibility. An answer to this question was not given by two respondents – Ministry of Mining and Energy (Sector for Geology and Mining) and the Ministry of Agriculture and Environment Protection, whilst the respondent from the Ministry of Mining and Energy (Sector for Power Engineering) was not sufficiently informed about the possibility for aforementioned cooperation (Diagram 12).

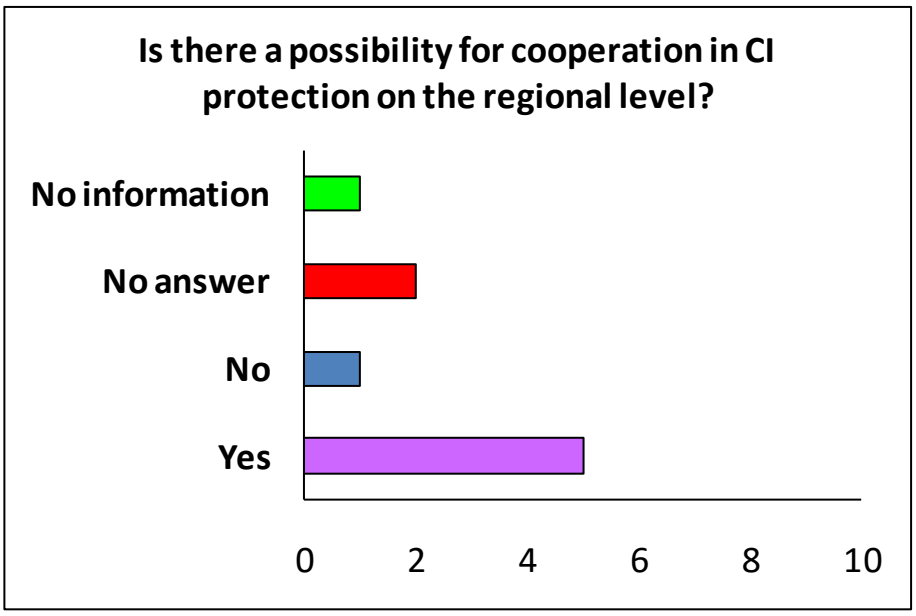


Diagram 12. A possibility for cooperation in CIP on the regional level

3.25 Are stimulating mechanisms (such as premiums and other benefits) used by insurance companies for critical infrastructure systems that implement security measures against disaster risks?

The answers to the question ***are stimulating mechanisms (such as premiums and other benefits) used by insurance companies for critical infrastructure systems that implement security measures against disaster risks***? are given in the Table 4. Four respondents (44,4%) answered negatively, whilst three respondents (33,3%) did not have that information.

Ministry/Department	No	No answer	No information
MME/Sector for Power Engineering			X
MME/Sector for oil and gas	X		
MME/Sector for geology and mines		X	
MCTI/ Inland Waterway Transport and Navigation Security Sector	x		
MCTI/ Department for Railways and Intermodal Transport	x		
MAEP/Sector for Environment Planning and Management			X
MI/ Sector for Emergency Management	x		
Cabinet of Minister for Emergency Situations		x	
Institute of Public Health of Serbia „Batut“			X

Table 4. Overview of results on implementation of stimulating mechanisms (premiums and other benefits)

3.26 Are the policies of cost-benefit analysis of special measures for disaster risk reduction applied as resilience metrics?

The majority of respondents answered negatively (n=6 or 66,6%) the question ***Are the policies of cost-benefit analysis of special measures for disaster risk reduction applied as resilience metrics?*** The respondents from the Ministry of Mining and Energy (Sector for Power Engineering) and Institute of Public Health of Serbia „Batut“ did not have information about this question, whilst the respondent from the Ministry of Mining and Energy (Sector for Mining and Geology) did not answer this question.

3.27 Are education and scientific research programs in the field of critical infrastructure protection integrated into the higher education system?

The answer „yes“ to the question ***Are education and scientific research programs in the field of critical infrastructure protection integrated into the higher education system?*** gave four respondents (44,4%) from the following institutions: Ministry of Mining and Energy (Sector for Mining and Geology, Sector for Oil and Gas), Institute of Public Health of Serbia „Batut“, Ministry of Construction, Transport and Infrastructure (Inland Waterway Transport and Navigation Security Sector).

The negative answers were given by the respondent from the Ministry of the Interior (Sector for Emergency Management) and the Ministry of Construction, Transport and Infrastructure (Department for Railways and Intermodal Transport). The answer that they do not have information was given by the respondents from two ministries (Mining and Energy -Sector for Power Engineering, Ministry of Agriculture and Environment Protection), whilst the respondent from the Cabinet of Minister for Emergency Situations did not answer this question.

4. ANSWERS OF THE RESPONDENTS FROM THE COUNTRIES IN REGION

The question ***Does your ministry/department have a national critical infrastructure protection policy*** was affirmatively answered by 3 respondents – BiH (Ministry of Security) and Macedonia (Directorate for Protection and Rescue, Crisis Management centre), whilst two respondents answered negatively – BiH (Ministry of Communications and Transport) and Montenegro (Directorate for Emergency Situations) (Table 5).

According to the respondent from the Ministry of Security (BiH) – in line with the decentralized system of public government the adoption of the document called „the policy of critical infrastructure protection" is under the jurisdiction of the entities, whilst the Ministry of Transport and Communications of Bosnia and Herzegovina is in charge of the coordination of its activities on the state level. From the operative aspect of the Ministry of Security, the CIP policy elements are integrated in the Plan of Protection and Rescue from Natural and Other Disasters, whose creation is mandatory in accordance with the Framework Law on Protection and Rescue from Natural and Other Disasters in Bosnia and Herzegovina.

Country/Institution	Yes	No
BiH / Ministry of Security	X	
BiH / Ministry of Communications and Transport		x
Montenegro / Directorate for Emergency Situations		x
Macedonia / Directorate for Protection and Rescue	X	
Macedonia / Crisis Management Centre	x	

Table 5. Overview of results of existence of CIP policies

The respondent from the Protection and Rescue Directorate (Macedonia) explained that the Law on Protection and Rescue regulates a general duty of all existing public and private entities for implementation of protection and rescue measures from natural and technological disasters. This means that each subject must have a vulnerability assessment document and the protection and rescue plan. Critical Infrastructure as such is not mentioned. Currently, the Law on Critical Infrastructure Protection is in the procedure, which should transpose the EU CIP directive.

The respondent from the Crisis Management Centre (Macedonia), mentioned the Government Direction as the main document, without explaining its details and content.

Four respondents gave a negative answer to the question ***Is there a regulated, mandatory national surveillance regarding CIP in your ministry/department?***

The positive answer to this question was given only by the respondent from the Protection and Rescue Directorate (Macedonia), who stated that the Direction has the Department for the Inspection Surveillance, in which 28 inspectors are employed, who control the protection and rescue measures in all subjects, including those who are in theory representatives of critical infrastructure. Prevention in these subjects is already included during the construction phase of those capacities, when the Direction issues a separate opinion for the applicability of protection and rescue measures in the object that is being constructed. In addition, the Directorate issues opinions during the adoption of urbanistic plans for implementation of protection and rescue measures.

The question ***if the legal regulative regarding CIP is in line with the EU norms (EC Directive) regarding CIP*** was negatively answered by four respondents, while the respondent from the Ministry of Security (BiH) answered that he supposes they are in line, but that he does not have sufficient information that would corroborate it, taking into account the decentralized system.

The question ***Which of the following areas are included in the aforementioned Act/Regulation*** (15 activities offered and the possibility that respondents add other activities) was not answered by respondents from the Directorate for Emergency Situations (Montenegro) and Protection and Rescue Directorate (Macedonia), whilst some respondents had the opinion that a future regulation/act should contain particular areas (Table 6).

The respondent from the Ministry of Transport and Communications (BiH) stated that there is no normatively regulated state act, given the structure of the state, but that on the lower levels of governance (entities, cantons, municipalities) there are acts that regulate CIP. In addition, each public company, within its organizational scheme, has a separate unit for protection of its own infrastructure, which includes certain areas mentioned in the Table 6.

Area	MTC (BiH)	MS (BiH)	CMC (Macedonia)
Threat and risk identification	x	x	X
Critical infrastructure sectors	x	x	

Critical infrastructure identification	x	x	X
Risk analysis / risk assessment	x	x	X
Analysis of vulnerability/resilience	x	x	X
Sector interdependency and critical infrastructure interdependency	x		X
Models and methodologies of analysis	x	x	
Evaluation	x	x	
Cross-cutting and sectorial criteria for risk identification and risk analysis	x		
Risk management, stakeholders in risk management, levels of risk management	x	x	X
Public-private partnership and cooperation with the academic community		x	
Business Continuity Management			
Exercises	x	x	
European critical infrastructures	x		
Education and scientific research	x	x	
Other			

Table 6. Overview of results on which areas should be included in the aforementioned act/regulation

Legend: MTC – Ministry of Transport and Communications (BiH); MS - Ministry of Security (BiH); CMC – Crisis Management Centre (Macedonia).

To the question ***Which body (bodies) are responsible for implementing the national critical infrastructure protection policies in your ministry/sector?*** the majority of respondents answered that it is not regulated in their ministry/sector (n=4). The respondent from the Ministry of Security (BiH) gave the positive answer and mentioned the following bodies: Coordinative Body of BiH for Protection and Rescue and Protection and the Sector for Protection and Rescue.

Although the respondent from the Protection and Rescue Directorate (Macedonia) gave a negative answer, he particularly mentioned that currently several ministries are in charge of critical infrastructure protection, and that such confusing situation would be resolved by adoption of the singular law.

The question ***Are the responsibilities for critical infrastructure protection divided in your ministry/department at the national, regional and local level?*** was negatively answered by the respondents from the Protection and Rescue Directorate and Crisis Management Centre (Macedonia).

According to the respondent from the Ministry of Transport and Communications (BiH) that responsibility is divided at the regional and local level, whilst the respondent from the Directorate for Emergency Situations (Montenegro) responded that this question is not regulated.

The respondent from the Ministry of Security stated that BiH is a decentralized country and that all activities are being performed in accordance with the system of governance at all levels (national, entity, cantonal, District of Brcko, local).

All five respondents answered negatively to the question ***Has your ministry/department appointed a body to coordinate activities related to implementing the national critical infrastructure policies?,*** with the respondent from the Ministry of Security (BiH) pointed out that the appointment of the mentioned coordination body is not under jurisdiction of his ministry.

All five respondents answered negatively to the question Has your ministry/department established a platform or network for CIP at the national level for stake holders?, with the respondent from the Ministry of Security (BiH) pointed out that the appointment of the mentioned coordination body is not under jurisdiction of his ministry.

To the question ***which critical infrastructure sectors have been identified in your ministry/sector*** the respondents gave the following answers:

- Ministry of Transport and Communications (BiH) – the critical infrastructure was identified during the creation of the Vulnerability assessment of BiH to Natural and Other Disasters led by the Ministry of Security of BiH;
- Ministry of Security (BiH) – through the work of the existing police agencies at the state level the jurisdiction for protection of objects in which BiH institutions and international diplomatic representative offices are located;
- Directorate for Emergency Situations (Montenegro) – has not identified any critical infrastructures;
- Protection and Rescue Directorate (Macedonia) – there is a certain categorization of objects in accordance with the Law on Construction (I, II, III category) which envisages what sort of documentation is needed for construction of a particular object (for instance, category I represent the most important and most complex projects, where some connection with the critical infrastructure can be made). Besides that, the same respondent stressed the fact that

the Ministry of Defence has the list of companies that are of special importance in the case of war;

- Crisis Management Centre (Macedonia) – an integral part of vulnerability assessment is the identification of critical infrastructure at the local and national level, which comprises systems or subsystems (energy, oil and gas pipelines, water supply etc.) and particular critical infrastructure objects (on the basis of the singular Nomenclature).

To the question ***Have the hazards and risks to the infrastructures in your ministry/department been identified?,*** a negative answer was only given by the respondent from the Directorate for Emergency Situations (Montenegro).

The respondent from the Ministry of Transport and Communications (BiH) stated that the identification of hazards and risks is present in the document Protection and Rescue Plan, also led by the Ministry of Security of BiH.

The respondent from the Ministry of Security (BiH) stated the natural and anthropogenic accidents, threats to public order and peace, as well as terrorist activities.

The respondent from the Protection and Rescue Directorate (Macedonia) stated that his Direction performs only identification, analyses and evaluations of natural and technological hazards and risks, whilst the respondent from the Crisis Management Centre (Macedonia) stated that hazards and risks for infrastructures are a constituent part of Hazard profiles of local and national assessments, but he did not precise which hazards and risks were identified.

The question ***Have vulnerability and risk analyses for critical infrastructure been performed?*** was negatively answered by the respondent from the Directorate for Emergency Situations (Montenegro) and Crisis Management Centre (Macedonia), whilst three remaining respondents gave a positive answer.

The question ***In the management process, has each critical infrastructure sector adopted the all-hazard approach and developed sector specific plans*** was positively answered only by the respondent from the Ministry of Security (BiH), who said that this approach is applied at the national level, adding that he does not dispose with precise information regarding the activities at the lower levels.

The answer to the question ***Which methodologies and which software models are used*** was not provided only by the respondent from the Ministry of Transport and Communications (BiH), whilst the respondent from the Directorate for Emergency Situations (Montenegro) responded that in his Department no software models are used. The remaining three respondents mentioned the following methodologies and software models used in their ministries/sectors for risk analysis and analysis of critical infrastructure interdependencies:

- The own methodology based on the national legislation and international methodologies treating this area, also coordination of activities of all state institutions (Ministry of Security - BiH);
- Methodology for risk assessment and content of the protection and rescue plans from 2006. With the help from DEMA (Danish Emergency Management Agency) during 2010 a manual for risks based on dimensioning was created, but currently no software for risk assessment and analysis is used (Protection and Rescue Directorate(Macedonia);
- Methodology for creation of vulnerability assessment of municipalities and the Republic to all hazards and risks. Besides that, software applications for Cataloguing of Critical Infrastructure and Geographic Informational System (GIS) for spatial analysis and mapping are used (Crisis Management Centre - Macedonia);

To the question ***Does your ministry/department cooperate with the scientific institutes, private companies (i.e. universities) with the aim of developing models and methodologies for critical infrastructure risk management*** 3 respondents gave a negative answer – from the Ministry of Communication and Transport (BiH), Directorate for Emergency Situations (Montenegro) and Direction for Protection and Rescue (Macedonia).

The respondent from the Ministry of Security (BiH) stated that his ministry cooperates with scientific institutes, universities and private companies, whilst the respondent from the Crisis Management Centre (Macedonia) asserted that his sector cooperates with scientific-research institutes, insurance sector and international organizations.

Most respondents gave negative answer (n=4) to the question ***Has your ministry/department developed any guidelines/directives/manuals for critical infrastructure evaluation and risk management,*** apart from the respondent from the Ministry of Security (BiH) who gave the positive answer.

Three respondents did not answer the question ***which international standards for critical infrastructure risk management and business continuity are being used in your ministry/department***, whilst the respondent from the Crisis Management Centre (Macedonia) said that he has no information about this question. The EU Directive of Critical Infrastructure Protection is used by the Ministry of Security (BiH).

Risk management is a part of business strategy of legal entities, i.e. the owners and operators of infrastructures in the areas under the jurisdiction of institutions from Macedonia (Direction for protection and rescue, Crisis Management Centre). On the other hand, it does not come under the jurisdiction of the BiH institutions (Ministry of Communications and Transport, Ministry of Security) and Montenegro (Directorate for Emergency Situations).

All respondents stated that **Business Continuity Management as a part of business strategy for legal entities, i.e. owners** is not in the jurisdiction of their ministries/departments.

A negative answer to the question ***Do public and private sector cooperate in critical infrastructure risk management in the areas under the jurisdiction of your ministry/department*** gave two respondents. The respondents who gave positive answers come from the following institutions: Ministry of Security – BiH (moderate level of cooperation), Protection and Rescue Directorate– Macedonia (moderate level of cooperation), Crisis Management Centre (moderate level of cooperation). In addition, the respondent from the Ministry of Security (BiH) thinks that the changes in the legal regulations are necessary for the improvement of the critical infrastructure management and protection system.

The evaluations of CI management and protection systems in the jurisdiction of their ministry/department are as follows:

- *low* (Ministry of Communication and Transport – BiH, Directorate for Emergency Situations – Montenegro, Protection and Rescue Directorate– Macedonia);
- *moderate* (Ministry of Security – BiH, Crisis Management Centre – Macedonia).

The respondents from BiH stated that the State should define critical infrastructure in its strategic documents and in accordance with them do everything that is covered with this questionnaire. They also think that in order to improve the CI management and protection system the changes legal regulations are needed.

All respondents answered that their ministry/department is not empowered to identify European critical infrastructure, neither on their own territory, nor on the territory of another country. Therefore, no respondents answered the following question – which methodologies and criteria are applied.

The request to ***describe the cooperation of their respective ministry/department with ministries/departments of the countries sharing the same identified European critical infrastructure*** was answered by only two respondents (Directorate for Emergency Situations – Montenegro, Protection and Rescue Directorate- Macedonia), who evaluated this cooperation to be at the „low level".

The question ***Is there any national funding for CIP in your ministry/department (non-EU funding)?*** was negatively answered by three respondents – Ministry of Security and Ministry of Transport and Communications (BiH) and Protection and Rescue Directorate(Macedonia). The respondent from the Directorate for Emergency Situations (Montenegro) did not answer this question, whilst the respondent from the Crisis Management Centre (Macedonia) answered that he had no information about national funding.

The question ***whether the security policy of the critical infrastructure owners is aligned with the legal regulations in the field of the CIP*** was affirmatively answered only by the respondent from the Ministry of Security (BiH), who mentioned the EU Directive on Critical Infrastructure Protection. A negative answer was given by two respondents (Ministry of Transport and Communications – BiH, Protection and Rescue Directorate- Macedonia). The respondent from the Directorate for Emergency Situations

(Montenegro) did not answer this question; whilst the respondent from the Crisis Management Centre (Macedonia) answered that he had no information about this issue.

All respondents answered that ***there is a possibility for cooperation in CIP at the regional level.*** The forms of cooperation the respondents suggested as the most important ones are:

- development of joint plans with the aim of undertaking preventive actions against previously identified threats (Ministry of Transport and Communications - BiH);
- exchange of knowledge, information and experience (Ministry of Security- BiH);
- harmonization of standards, regional atlas of CI, early warning system and the academic cooperation (Direction for Protection and Rescue - Macedonia);
- joint activities on identification of cross border/regional CI and assessment of key hazards (Crisis Management Centre - Macedonia).

The majority of respondents did not have sufficient information regarding the question ***Are stimulating mechanisms (such as premiums and other benefits) used by insurance companies for critical infrastructure systems that implement security measures against disaster risks?,*** whilst the respondent from the Ministry of Transport and Communications (BiH) answered negatively, and the respondent from the Directorate for Emergency Situations (Montenegro) did not answer this question.

The respondent from the Directorate for Emergency Situations (Montenegro) did not answer the question ***Are the policies of cost-benefit analysis of special measures for disaster risk reduction applied as resilience metrics?,*** whilst all other respondents answered negatively.

The question ***Are education and scientific research programs in the field of critical infrastructure protection integrated into the higher education system?*** was affirmatively answered by two respondents (Ministry of Transport and Communications – BiH, Crisis Management Centre - Macedonia). The respondent from the Ministry of Security (BiH) stated that he did not have information, and two respondents did not answer this question (Directorate for Emergency Situations – Montenegro, Protection and Rescue Directorate- Macedonia).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

RECIPE 2015 Questionnaire Data Analysis

One of the tasks of the "RECIPE 2015" Project is to conduct a survey through which we want to determine the method of identifying problems, as well as the formal and legal organization in the critical infrastructure protection. In addition, it is necessary to determine procedures and methods of implementing regulation in practice of states participating in the Project. A questionnaire has been developed for the purpose and its results, i.e. information obtained, besides indicating the state of the formal and legal organization at the national level, will also point out the examples of good practice – effective procedures and methods of identifying and protecting critical infrastructure, as well as showing the areas that require improvements and corrections. Ultimately, this survey should offer unique guidelines for the critical infrastructure protection and its improvement at the regional level.

Information collection procedure

At the international level, the questionnaire is submitted to 70 addresses, to the national points of contact and to other representatives of Member State institutions competent for the critical infrastructure as well as to institutions in the United States of America.

The response was 10 %, and only those questionnaires submitted to European addresses were returned.

Sample

The questionnaire was filled out by official persons delegated by the institutions included in the survey. Since it is a small population of institutions which are acquainted with issues of protection of critical infrastructure (a type of expert sample), instead of a general population. Taking an exceptional sensitivity of the subject matter of the survey from the point of view of national security into consideration, we find the justification for an analysis and conclusions based on such a small sample.

The following is an analysis of the European part of the sample. Criteria results of the questionnaire used for a comparison, provided for Croatia by the National Protection and

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Rescue Directorate, are not shown within the European sample, but are reviewed and compared with it in the accompanying text.

Table 1. Overview of European participants in the survey

Country	Institution	Ownership
Belgium	Federal Service of Home Affairs, Directorate Crisis Centre	government
Czech Republic	Ministry of interior - DG FRS	
Denmark	Emergency Management Agency	
Slovenia	Ministarstvo za obrambo	
Spain	The National Centre for Critical Infrastructure Protection	
Sweden	The Swedish Civil Contingencies Agency, MSB	
Hungary	National Directorate General for Disaster Management, Ministry of Interior	

Results

1. **Does your country have a national critical infrastructure protection policy?**

Only Denmark provided a negative reply to the question (Figure 1) while the other respondents claim that there are national critical infrastructure protection policies and every one of them specifies their own versions – similar to the Croatia's Critical Infrastructure Act (Official Gazette 56/13).

REMARK: Croatia is aligned with the most of the respondent countries which have formal, legally established policy for protection of national critical infrastructure. Unfortunately, a formally established policy does not always equate its implementation in practice. At the same time, it is a relatively new legislation, therefore its implementation in Croatia is in a developmental stage. Further analysis presented herein shall demonstrate that Croatia is not an isolated case. We are inclined to conclude that critical infrastructure protection is, in a formal definition, still seeking good practice established by only a handful of countries (like Sweden) by now.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

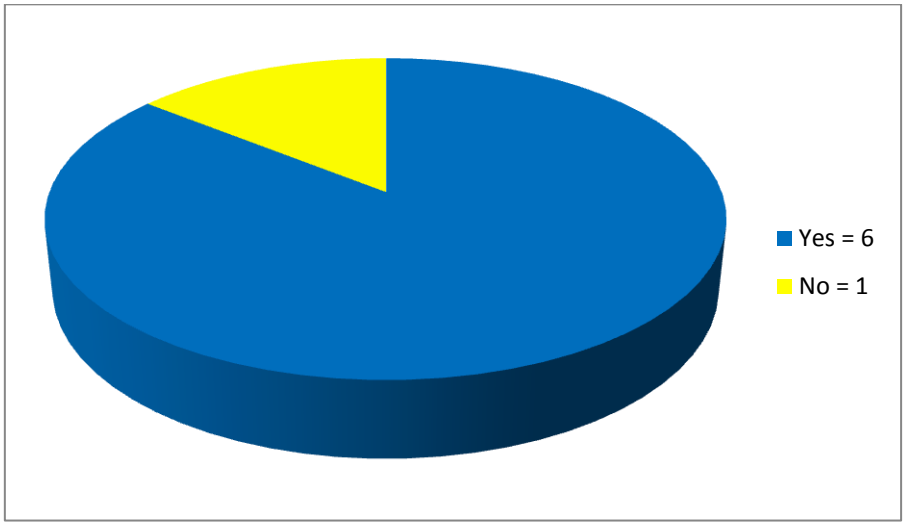


Figure 1. Reponses to the question "Does your country have a national critical infrastructure protection policy?" Response frequencies are shown (*N=7*).

2. If yes, under which Act/Regulation? (Pleas state title of the Act/Regulation)

Considering specific legal variations of different European countries, we have not specified identified legislation or regulations for each country individually. Instead, we indicate in Figure 2 that six countries specified a particular regulation or legislation determining their national critical infrastructure protection policies. Following the above question, it is clear that only Denmark has not identified such regulation or legislation because it has not enacted one yet.

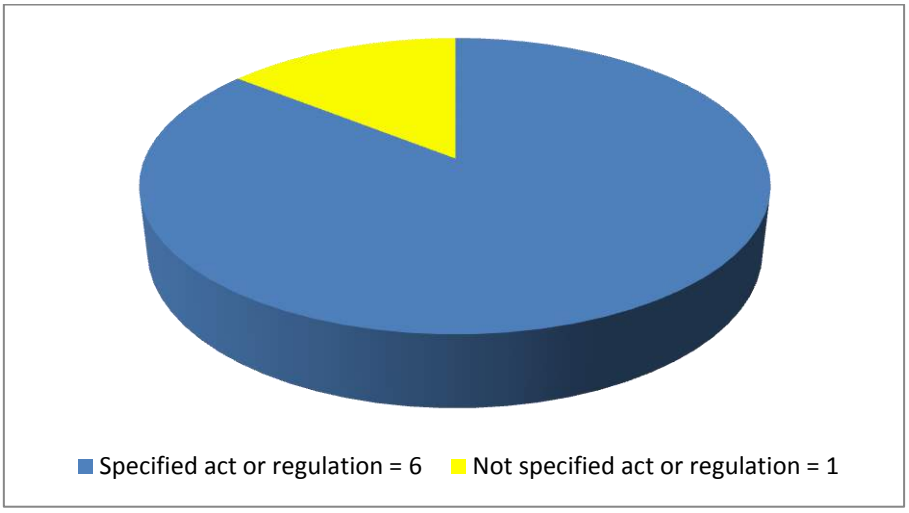


Figure 2. Responses to the question "If yes, under which Act/Regulation?" Response frequencies are shown (*N=7*).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

3. Is there a regulated, mandatory national surveillance regarding critical infrastructure protection in your country?

Four countries replied that there is a regulated mandatory surveillance regarding critical infrastructure protection there (Figure 3). Those countries are: Belgium, Czech Republic, Hungary and Spain.

Croatia may be added to the group, because it assigned that task to the National Protection and Rescue Directorate.

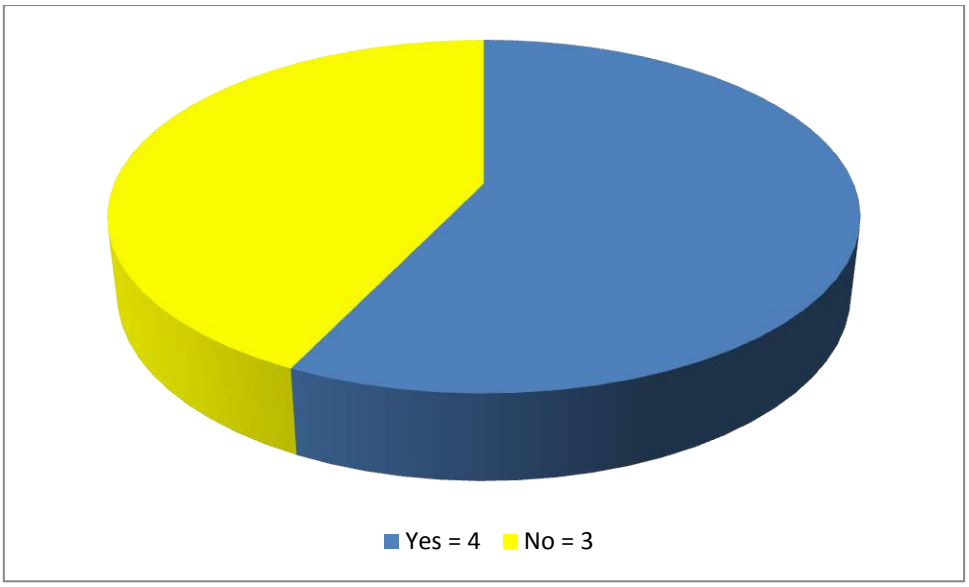


Figure 3. Reponses to the question "Is there a regulated, mandatory national surveillance regarding critical infrastructure protection in your country?" Response frequencies are shown (N=7).

4. Which areas are included in the aforementioned Act/Regulation?

Figure 4 shows that the areas most frequently included in the legislation and regulations related to critical infrastructure protection in the surveyed European countries are: critical infrastructure sectors, threat and risk identification, critical infrastructure identification, as well as risk analysis / risk assessment.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

The least included ones are sector interdependence and interdependence of critical infrastructure, education and scientific research, business continuity, as well as critical infrastructure analysis methodology and models.

REMARK:

The following is included in the Croatia's Critical Infrastructures Act:

- Threat and risk identification,
- Risk analysis / risk assessment,
- Critical infrastructure identification,
- Critical infrastructure sectors,
- Sector interdependence and interdependence of critical infrastructure,
- Cross-cutting and sectoral criteria for risk identification and risk analysis.

Therefore we observed that there are large differences between the existing legislation and regulations in individual European countries in terms of critical infrastructure. Even though it may be concluded that critical infrastructure, as well as its protection, identification criteria, as well as methodology and tools for identification and assessment of the critical infrastructure, is legally well covered and defined in Croatia, it is still not addressed in the fields of practical implementation of the legislation, coordination among sectors, research, education and critical infrastructure protection implementation exercises, therefore those are the areas in need of work and consideration of possible future amendments of the legislation.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

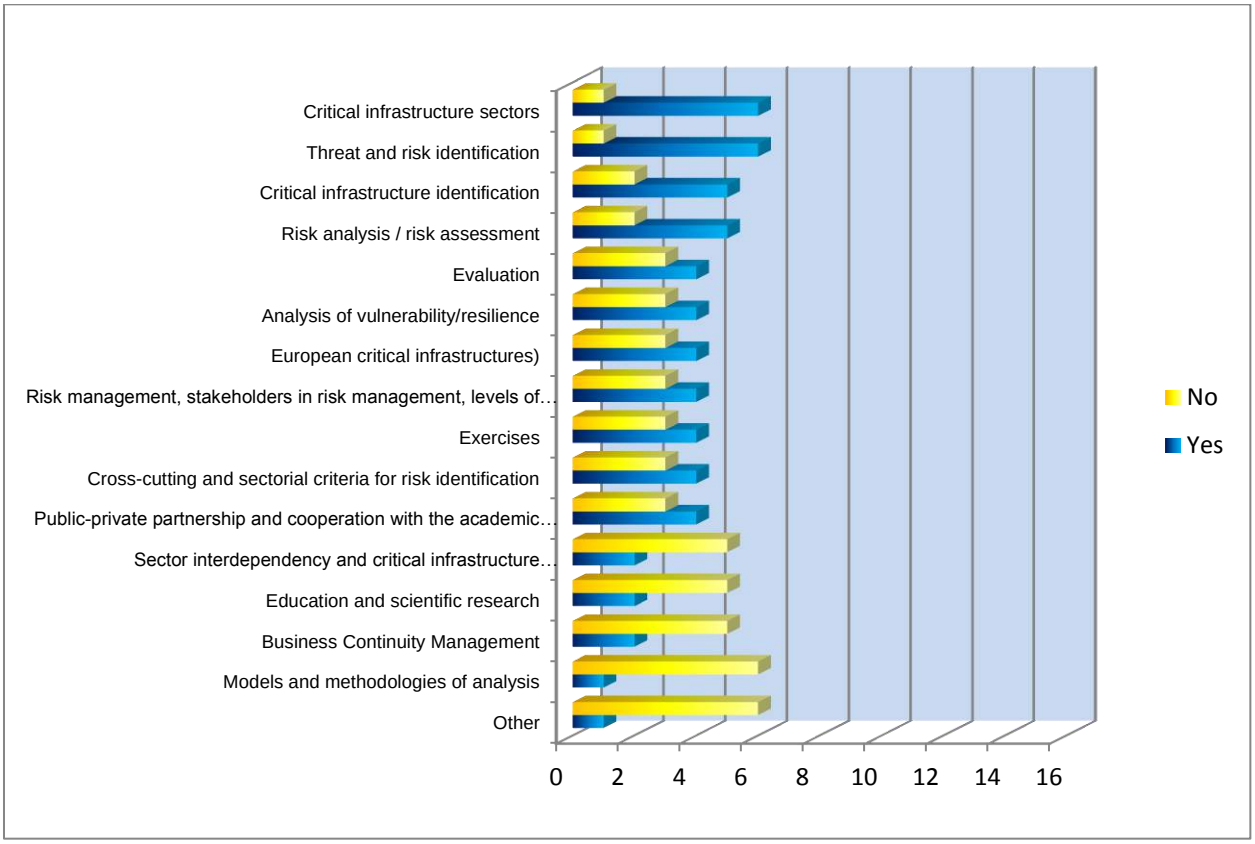


Figure 4. Responses to the question "Which areas are included in the aforementioned Act/Regulation?" Response frequencies are shown (N=7).

5. Which state body (bodies) is responsible for implementing the national critical infrastructure protection policy?

As expected, there are significant differences among the countries in terms of responsibility of individual government bodies for implementation of critical infrastructure protection policies (Table 2).

REMARK: It should be noted that even though the responses are official because the questionnaires were filled out by persons appointed by the competent institutions, that does not mean they are correct.

Nonetheless, several types of responsible bodies may be observed in the European sample, including Croatia:

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

1. Existing government bodies and services appointed to implement critical infrastructure protection policies: Croatia, Belgium, Sweden, Spain and Hungary,
2. All government bodies whose area of competence contains identified critical infrastructure sectors: Belgium, Croatia, Czech Republic, Slovenia, Sweden and Denmark.

Considering diversity of competent bodies and the lines of competence of individual countries, this information is considered useful to start an analysis of the existing competence models and seek a proposed universal competence model.

Existence of various types of competent government bodies as well as differences in authority and hierarchy of competences led us to a conclusion that coordination is necessary between individual government bodies regarding exchange of information and accurate knowledge of lines and areas of competence both on national and international levels.

Table 2. Responses to the question "Which state body (bodies) is responsible for implementing the national critical infrastructure protection policy?" Responses and response frequencies are shown (N=7).

Government body considered responsible for implementation of the national policy on critical infrastructure protection	Country
Government of the Republic of Croatia **National Protection and Rescue Directorate** **Central government administration bodies**	**Croatia**
Federal Public Service of Home Affairs: Crisis Centre Sectoral authorities	Belgium
Ministry of Interior Ministry of Transport Ministry of Industry and Trade Ministry of Finance Ministry of Labor and Social Affair Ministry of Health Ministry of Agriculture	Czech Republic

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Ministry of Environment National Security Authority Czech National Bank Administration of State Material Reserves National Institute for Nuclear, Chemical and Biological Protection	
Ministry of Defense Cross-sectoral coordination group for harmonization of preparations for critical infrastructure protection	Slovenia
Civil Contingencies Agency in corporation with national Regional and local authorities.	Sweden
There is no national critical infrastructure protection policy Each sector is responsible	Denmark
State police Civil Guard[1]	Spain
Ministry of Interior	Hungary

6. Are the responsibilities for critical infrastructure protection divided in your country at the national, regional and local level?

Figure 5 indicates that most of the surveyed institutions (four) claims that responsibilities for critical infrastructure in the country are distributed at national, regional and local levels, while three of them claim that those are distributed at the national level.

Countries where the responsibility for the critical infrastructure is divided at the national, regional and local levels are:

- Denmark,
- Hungary,
- Spain,
- Sweden.

[1] Military units performing police duties, gendarmerie

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

While countries where the responsibility for the critical infrastructure is divided at the national level only are:

- Belgium,
- Czech Republic,
- Slovenia.

Even though Figure 4 does not include it, Croatia also belongs to the latter group.

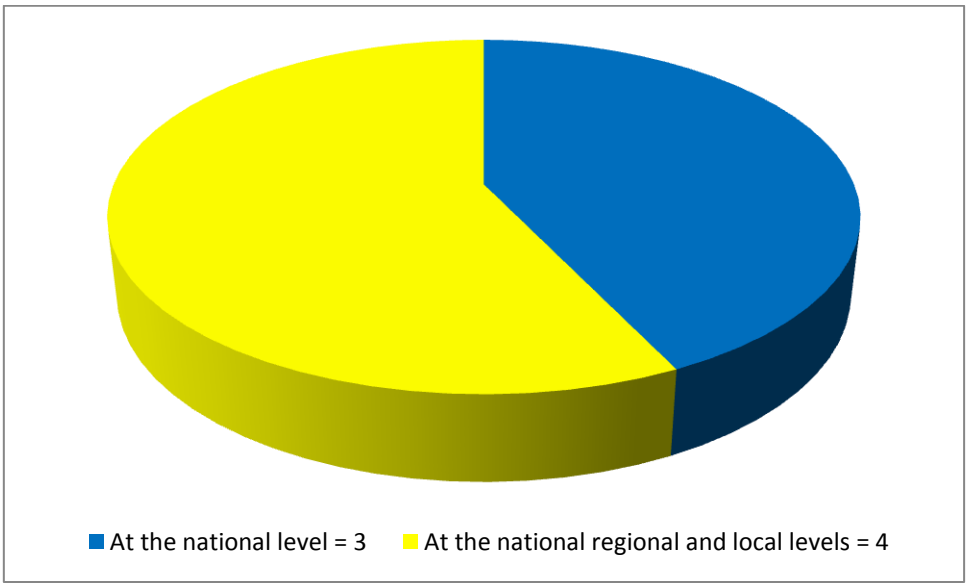


Figure 4. Responses to the question "Are the responsibilities for critical infrastructure protection divided in your country at the national, regional and local level?" Response frequencies are shown (N=7).

7. **Has your country appointed a state body to coordinate activities related to implementing the national critical infrastructure policies?**

All the countries stated that there is a government body appointed to coordinate activities for implementation of national critical infrastructure protection policies.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

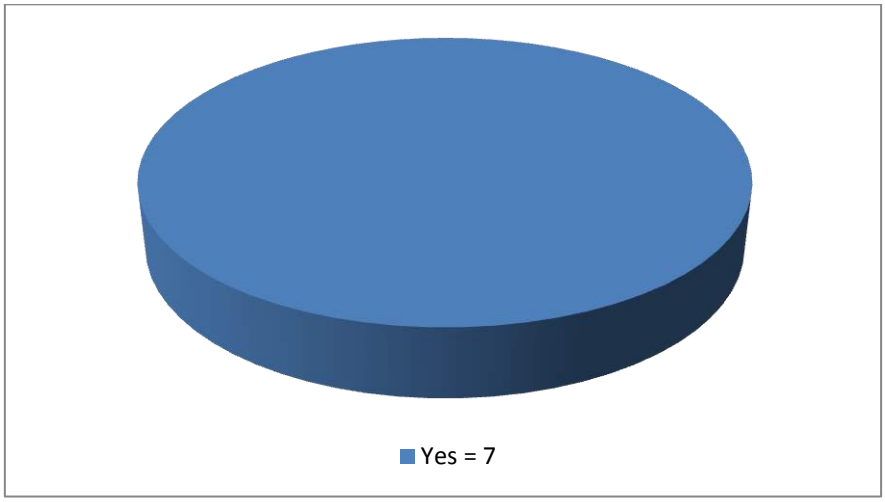


Figure 5. Response to the question "Has your country appointed a state body to coordinate activities related to implementing the national critical infrastructure policies?" Response frequencies are shown (N=7).

8. Has your country established a platform or network for critical infrastructure protection at the national level for stakeholders?

The platform or a network of stakeholders has been established in only two countries: in Belgium and in Spain. Croatia would fall into that group too, even though it is not shown in Figure 6. Denmark provided no answer, while the other countries claimed that the platform or network of stakeholders for critical infrastructure protection has not been established at the national level.

Figure 6. Response to the question "Has your country appointed a state body to coordinate activities related to implementing the national critical infrastructure policies?" Response frequencies are shown (N=7).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

9. Which critical infrastructure sectors have been identified in your country?

Table 3 presents answers provided by seven surveyed European countries, with Croatia included for comparison. The greatest degree of overlapping in the identified critical infrastructure sectors (specified by seven out of eight countries) is recorded in the following sectors:

- Energy,
- Communication and information technologies,
- Transport,
- Finance.

The following sectors were specified by six countries:

- Healthcare,
- Water management (however there are significant variations in comprehension of this sector – including potable water and waste water disposal in some cases, but potable water only elsewhere),
- Food.

Administration is also noteworthy with four mentions, while three lists included: Defense, protection and security in the broadest terms, since those represent a large number of related but not completely identical sectors.

REMARK: It should be pointed out that the respondents who filled out the questionnaires on behalf of government institutions (survey participants) may not have provided accurate and completely correct responses, therefore it is possible that there are even greater overlaps of the sectors among the countries.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Table 3. Responses to the question "Which critical infrastructure sectors have been identified in your country?"

Critical infrastructure sector	DEN[2]	CRO	SWE	ESP	CZE	SLO	BEL	HUN	Total
Energy	+	+	+		+	+	+	+	7
Communication and information technologies	+	+	+	+	+	+	+		7
Transport	+	+	+	+	+	+	+		7
Finance	+	+	+	+	+	+	+		7
Healthcare	+	+	+	+	+	+			6
Water management	+[3]	+		+[4]	+	+[5]		+	6
Food	+	+	+	+	+[6]	+			6
Administration			+	+	+		+		4
Defense, protection and security	+[7]		+					+	3
Public services		+			+				2
Science and education	+	+							2
Production, transport and storage of hazardous substances		+							1
National heritage and values		+							1
Chemical industry				+					1
Research laboratories				+					1
Nuclear industry				+					1
Industry and trade			+						1
Regional technical services			+						1
Environmental protection						+			1
Line of competence	+								1

[2] Not official
[3] Water and waste water separately
[4] Water, drinking and waste water separately
[5] Potable water supply only
[6] and agriculture
[7] Including intelligence services

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Agriculture								+	1
Civil defense	+								1
Social security/Social issues	+		+						2
Meteorology	+								1
Crisis management	+								1
Foreign (external) services	+								1
Total number of specified sectors	**15**	**11**	**11**	**10**	**9**	**8**	**5**	**4**	

Pursuant to a decision by the Government of the Republic of Croatia, critical infrastructure has been determined in eleven sectors, and the following seven critical infrastructure sectors exhibit the greatest overlaps with the remaining surveyed countries.

- Energy,
- Communication and information technologies,
- Transport,
- Finance,
- Healthcare,
- Water management,
- Food.

In comparison with the other surveyed countries, Croatia as well as Sweden have the greatest number of critical infrastructure sectors. However, the above only applies if one assumes that the other countries have provided correct and accurate replies and if one takes into consideration that Denmark is only considering fifteen foregoing sectors (but there is a high probability that the total number shall be lower than fifteen).

It is also interesting that there is a divergence between the countries in sectors which should logically be the same, but we are inclined to attribute it to cultural differences. For instance, the water management sector includes the following separate alternatives:

- Water and waste water separately,
- Water, drinking and waste water separately,
- Potable water supply only.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

10. Have the sectoral analyses of risks and vulnerabilities been made?

Sectoral risk and vulnerability analyses were performed in six out of seven surveyed countries (Figure 7). Czech Republic is the only one which has not performed the analyses, just like Croatia.

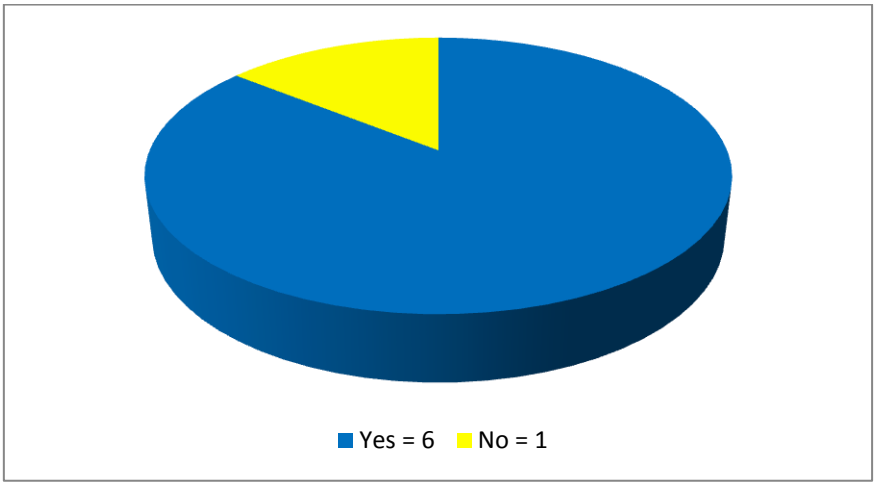


Figure 7. Responses to the question "Have the sectoral analyses of risks and vulnerabilities been made?" Response frequencies are shown (N=7).

11. Have the hazards and risks to the infrastructures in your country been identified?

Five countries claim that infrastructure hazards and risks analyses were performed, while Hungary stated that it was not done, just as in Croatia. Denmark provided no answer (Figure 8).

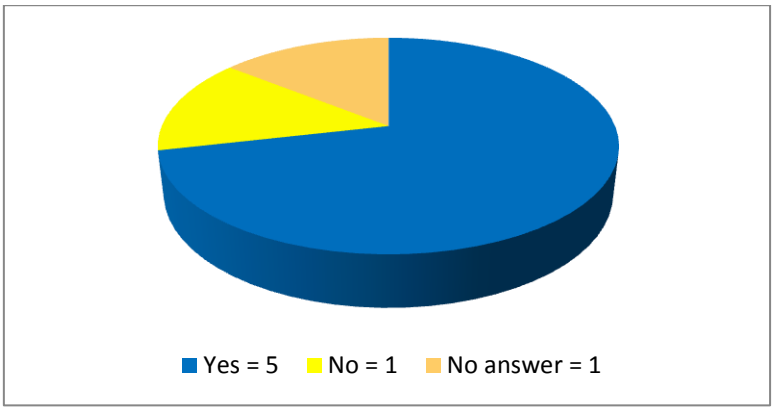


Figure 8. Response to the question "Have the hazards and risks to the infrastructures in your country been identified?" Response frequencies are shown (N=7).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

If yes, please state which hazards and risks.

Responses to the question, by country, are shown in Table 4. It is observed that the replies range from very specific ones such as those provided by Sweden and Slovenia, to very general ones as in case of Belgium.

Table 4. Response to the question "Which hazards and risks are identified in your country?"

Country	Response	Number of institutions which provided an answer
Belgium Czech Republic	Anthropogenous threats Technical-technological threats[8] Natural threats	2
Sweden	Scenarios: Sunstorm, Mudflow, Sulfur fog, Widespread disruption to GNSS, Disruption to food supply A dam failure, A prolonged heat wave Violent riots, Pandemic by influenza, Terrorist attack Nuclear accident	1
Slovenia	E.g. Interdependence of critical infrastructure sectors Information-communication support Supply of energy sources The risks of disruption after an identified incident (short-term, continuous…) Defining ways of exceeding incidents	1
Croatia Hungary	Not identified	2
Denmark Spain	Non-specified response or no response	2

[8] Czech Republic did not specify the technical-technological threats

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

12. In the management process, has each critical infrastructure sector adopted the all-hazard approach and developed sector specific plans?

The above is confirmed by six countries while Slovenia gave a negative response, which also applies to Croatia. (Figure 9)

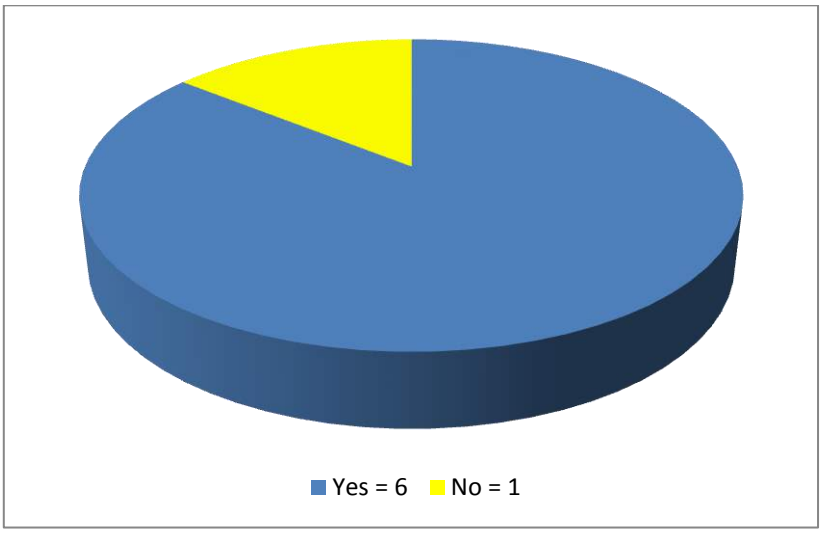


Figure 9. Response to the question "In the management process, has each critical infrastructure sector adopted the all-hazard approach and developed sector specific plans?" Response frequencies are shown (N=7).

13. Which methodologies and which software models are used in your country for risk analysis and analysis of critical infrastructure interdependency?

According to diversity of responses presented in Table 5, it is concluded that the practice is not uniform at the European level, and efforts should be invested towards development of methodology and models for analysis of risks and interdependencies of critical infrastructure. In individual sectors such as Production, transmission and distribution of electrical power, indicated by Czech Republic, there is a specific methodology and models, but not all the sectors are covered.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Table 5. Response to the question "Which methodologies and which software models are used in your country for risk analysis and analysis of critical infrastructure interdependency?"

Institution	Response	Number of institutions which provided an answer
Denmark Hungary	No answer	2
Slovenia Belgium	None	2
Spain	**Any established international system**	1
Sweden	**Various risk and vulnerability analysis tools are available. There is no special tool to identify critical infrastructure or vital social functions.** There however an ongoing work, based on the action plan, to develop tools and methods to support the actors in the work with CIP /PVSF	1
Czech Republic	**Methodology to ensure critical infrastructure protection in the field of production, transmission and distribution of electrical power**	1
Croatia	Ordinance on methodology for critical infrastructure operation risk analysis – risk analysis development guidelines – is in effect. Models/software packages are not prescribed or provided in the guidelines. At this time, the ministries do not have appropriate software at their disposal.	1

14. Do government institutions in your country cooperate with the scientific-research institutions, private companies (i.e. universities, institutes etc.) with the aim of developing models and methodologies for critical infrastructure risk management? If yes, with which ones?

Most of the countries (five) stated that there is cooperation of government institutions with scientific institutes with the aim of developing models and methodologies for critical infrastructure risk management (Figure 10). Two (Slovenia and Belgium) indicate that such cooperation does not exist.

REMARK: The foregoing cooperation does not exist in Croatia either.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

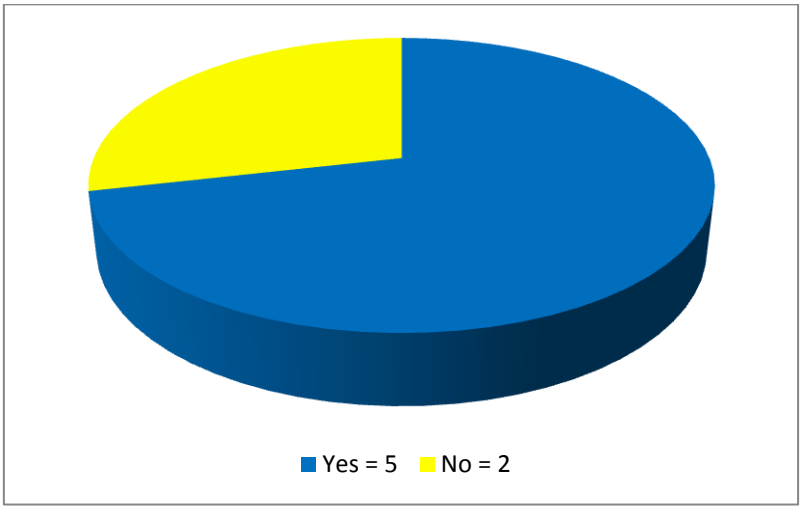


Figure 10. Response to the question "Do government institutions in your country cooperate with the scientific-research institutions, private companies (i.e. universities, institutes etc.) with the aim of developing models and methodologies for critical infrastructure risk management?" Response frequencies are shown (N=7).

The most of the respondents (five) stated that the cooperation has been established with universities, three said that it has been established with research institutes as well, and two indicated private companies (Figure 12).

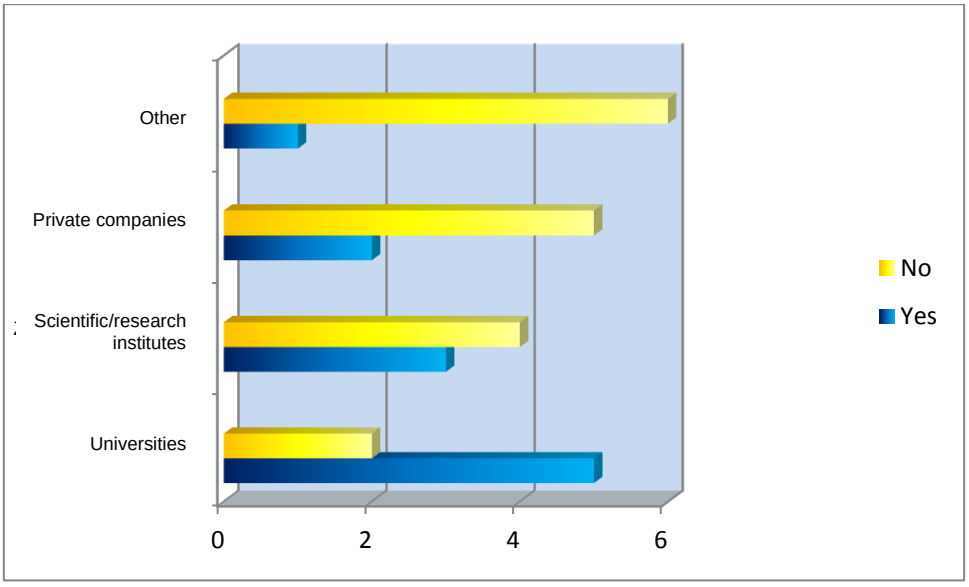


Figure 12. Response to the question "Which institutions do government institutions in your country cooperate with?" Response frequencies are shown (N=7).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

15. Has your country developed any guidelines/directives/manuals for critical infrastructure evaluation and risk management?

Two countries which stated that they have developed guidelines/directives/manuals for assessment of critical infrastructure and risk management are Belgium and Spain. The remaining five do not have them (Figure 11).

REMARK: Such guidelines/directives/manuals for critical infrastructure evaluation have not yet been developed in the Republic of Croatia, except for the Ordinance on methodology for critical infrastructure risk analysis developed and adopted by the National Protection and Rescue Directorate, and Croatia might be added to the latter group.

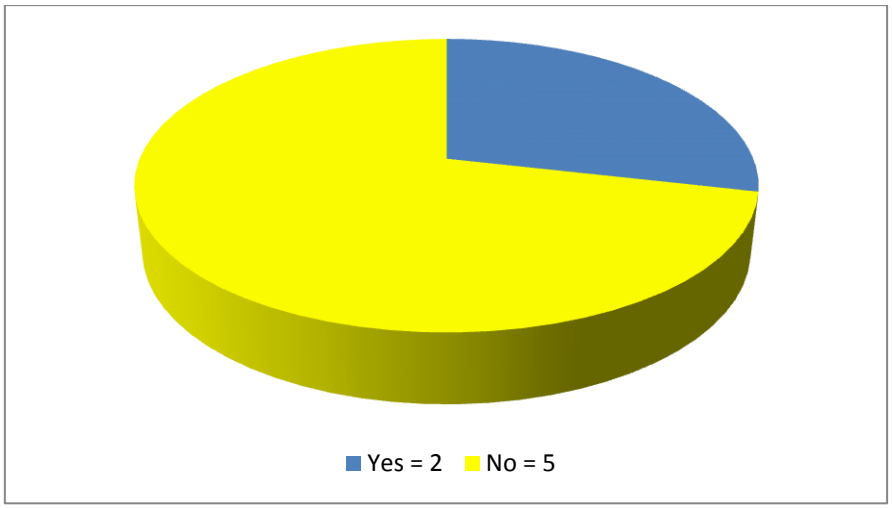


Figure 11. Response to the question "Has your country developed any guidelines/directives/manuals for critical infrastructure evaluation and risk management?" Response frequencies are shown (N=7).

16. Which international standards for critical infrastructure risk management and business continuity are being used in your country?

Individual replies are presented in Table 6. Czech Republic, Sweden and Croatia stated that they use specific ISO standards for critical infrastructure risk management and business continuity, however Czech Republic did not specify them. The other five countries did not specify anything, and the group includes Belgium which explicitly specified that no international standards are used for the stated purpose

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Table 6. Response to the question "Which international standards for critical infrastructure risk management and business continuity are being used in your country?"

Country	Response		Number of statements
Denmark Spain Hungary Slovenia Belgium	No answer on not specified		5
Czech Republic		Not specified individually	1
Sweden	ISO standards	ISO 31000 ISO 31010 ISO 22313	1
Croatia	ISO standards	ISO 31000 ISO 31010 ISO 22301	1

17. Is risk management a part of business strategy for legal entities, i.e. the owners and operators of infrastructures in your country? Please state which international norms are being implemented in this process.

All countries except Belgium confirmed that risk management is a part of business strategies of legal entities – managers and owners of infrastructure in the country (Figure 12), and the same is true for Croatia.

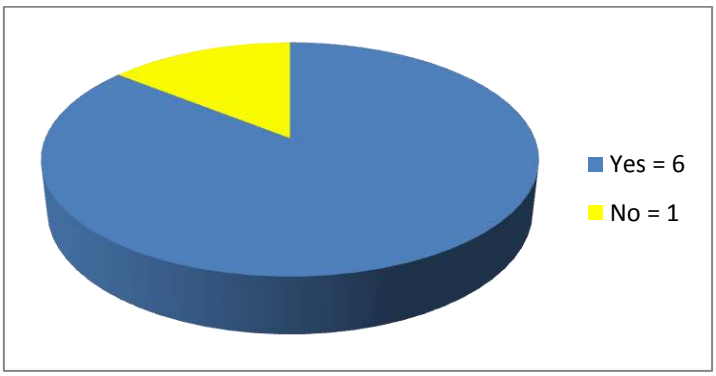


Figure 12. Response to the question "Is risk management a part of business strategy for legal entities, i.e. the owners/operators of infrastructures in your country?" Response frequencies are shown (N=7).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

REMARK: International norms implemented in the risk management process are not specified by most of the countries which responded affirmatively. Slovenia and Sweden are exceptions to that. Slovenia provided a somewhat more elaborated reply which is paraphrased herein with a note that many of the above ones have not been officially included in critical infrastructure protection by now. Instead they are an obligation of legal entities/owners/managers of critical infrastructure to ensure business continuity for a longer period of time. Future integration and inclusion of these regulations into critical infrastructure protection is under consideration.

In its response, Slovenia specified the following:

1. European Union standards and regulations
2. Special regulations applicable to individual sectors of critical infrastructure:
   E.g. communication and information support sector: CEN, CENELEC, ETSI, ITU, IEC (accepted by European organizations);
   E.g. field of air transport: European Commission regulations, ICAO guidelines.
   E.g. environmental protection area: SEVESO directive,
3. Principles, guidelines and standards applicable to risk management:
   SIST ISO 31000;
   SIST ISO 31010:2011.

Sweden also specified that implementation of risk management into the existing system for critical infrastructure protection is in progress and that the national objective is to include all identified critical infrastructure into the security management system by 2020. In the process, pillars of the system are:

1. Risk management,
2. Business continuity management,
3. Ability to act, whereby participants are provided motivation to use it actively and to use international norms.

Use of specific norms in Croatia depends on specific nature of individual sectors and security areas where they must act.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

18. Is Business Continuity Management a part of business strategy for legal entities, i.e. the owners and operators of critical infrastructure in your country?

All surveyed countries claimed that Business Continuity Management is a part of business strategy for legal entities, i.e. the owners and operators of critical infrastructure in their country.

REMARK: In Croatia, finance and information and communication technology sectors have adopted a business continuity management process within their own business strategy, while information relevant for other sectors is not known.

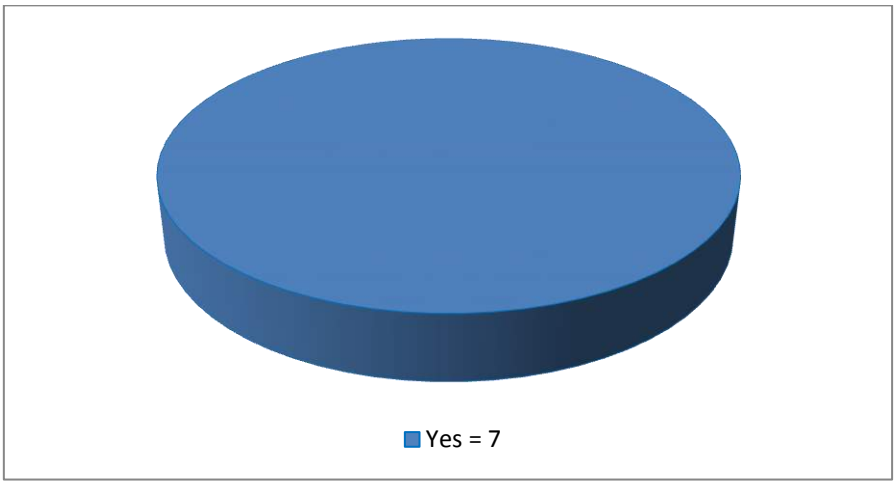


Figure 13. Response to the question "Is Business Continuity Management a part of business strategy for legal entities, i.e. the owners and operators of infrastructures in your country?" Response frequencies are shown (N=7).

19. Do public and private sectors cooperate in critical infrastructure risk management in Croatia?

Figure 14 clearly shows that public and private sectors cooperate in management of critical infrastructure risks in each surveyed country.

REMARK: Unfortunately, such cooperation is not established in Croatia. Based on examples of cooperation in the surveyed European countries, a need to establish the cooperation in the Republic of Croatia as well is observed. The following Table 8 contains a description of such

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

cooperation in individual European countries and an assessment of the same along with improvement proposals.

An answer provided by Hungary may be singled out as an example of good practice: "All identified elements of critical infrastructure have a safety coordinator[9] whose task is to establish a permanent contact between the main executive coordinator[10] and the National administration for disaster management[11]." Since such cooperation is missing in Croatia, the Hungarian example could be used as a guideline how to commence public-private cooperation in critical infrastructure risk management

In addition, the respondents were asked to assess the cooperation on a three-grade scale: "low", "moderate" and "high".

Even though Hungary provided the most detailed description of the above cooperation, it assumes a critical point of view and assesses the cooperation as moderate, which may point to some practical problems in application of formalized and institutionalized cooperation within the system. In that case, it is useful to establish cooperation and exchange of experience with Hungary in search of practical solutions.

Sweden, as a partner in "RECIPE 2015" project, expressed even greater degree of self-criticism than Hungary, assessing cooperation between public and private sectors in critical infrastructure risk management as low, even though the cooperation was described as "fruitful". Using the above reply (provided in full in Table 7), it is possible to interpret that the government institutions (public sector) bears responsibility for coordination and inclusion of private sector in implementation of "strategies and action plans for key social functions".

Furthermore, Sweden also made a proposal for improvement of the cooperation, and its opinion is shared by Slovenia as well. It is necessary to apply a legal definition to the public-private cooperation, clarify roles, responsibilities and requirements of involved parties and harmonize it with legal standards.

[9] Security Liaison Officer).
[10] Chief Executive Officer
[11] National Directorate General for Disaster Management (NDGDM)

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

We think that Croatia shares similar problems, in addition to the fact that public-private partnerships have not been established in critical infrastructure protection, and the above is seen as good guidelines to achieve the foregoing cooperation.

We find it interesting that the countries which awarded higher grades to the public-private cooperation did not provide detailed descriptions of the cooperation, even though Spain pointed out problems similar to those described by Sweden.

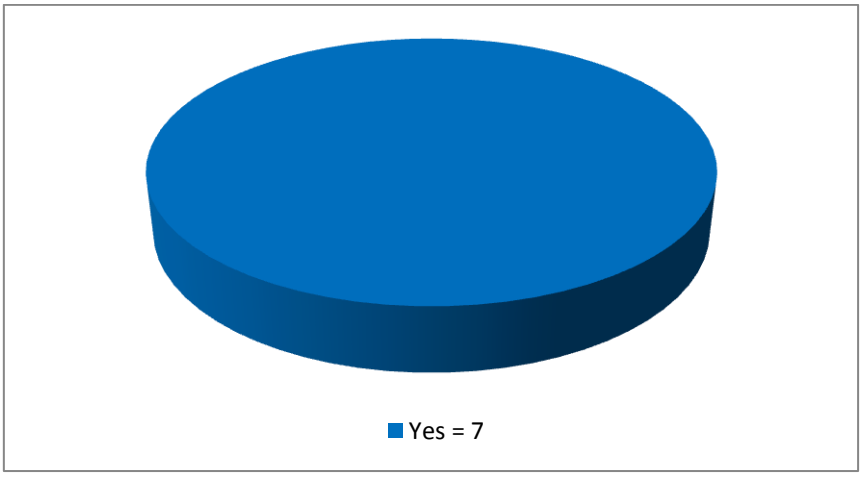


Figure 14. Response to the question "Do public and private sectors cooperate in critical infrastructure risk management in your country?" Response frequencies are shown (N=7).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Table 7. Description and assessment of cooperation between public and private sectors cooperate in establishment of critical infrastructure risk management in individual European countries

Country	Description of cooperation	Assessment of cooperation	Suggestions for improvements
Slovenia	The cooperation takes place in the field of legislation. There are examples of public-private partnerships.	Low	Legally define the public-private cooperation, clarify roles, responsibilities and requirements of involved parties and harmonize it with legal standards.
Sweden	In the course of development of strategies and action plans for key social functions, the private and public sectors achieved fruitful cooperation. The private sector participates in implementation of the action plans in future activities.		
Hungary	All identified elements of critical infrastructure have security coordinators[12]tasked with establishment of permanent contacts between the main executive coordinator [13] and the State administration for disaster management[14].	Moderate	
Czech Republic	Exchange of information and mutual cooperation.		
Denmark	There are various examples		
Spain	The cooperation takes place with guidance and coordination from the Ministry of Interior through various strategic plans	High	
Belgium	The private and public sectors exchange and discuss risk analyses.		

20. How you evaluate the critical infrastructure protection and management system in your country.

The respondents are requested to verbally evaluate the critical infrastructure protection and management system in their country. Received replies are presented in Table 8, as well as individual evaluations by country on a scale consisting of three grades (low, moderate and high).

[12] Security Liaison Officer).
[13] Chief Executive Officer
[14]National Directorate General for Disaster Management (NDGDM)

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Table 8. Evaluation of the critical infrastructure protection and management system in European countries.

Country	Response	System evaluation	Suggestions for improvements
Slovenia	We are in an initial stage of establishment of legislation in the field of critical infrastructure protection and we are still developing the system	Low	Legally define the public-private cooperation, clarify roles, responsibilities and requirements of involved parties and harmonize it with legal standards.
Sweden	The system is built upon cooperation and free will. Work on public sectors risk and vulnerability analysis is the basis for the evaluation. The analyses provide an insight into state of the critical infrastructure on all levels of the society. Following evaluation of implementation of the action plans, we will perform their implementation as well as work on systematic security. The similar situation exists in respect of a risk assessment on the national level.		
Hungary	Based on EU regulations and it is parallel to EU standards	Moderate	
Czech Republic			
Belgium	Positive	High	Legally define the public-private cooperation, clarify roles, responsibilities and requirements of involved parties and harmonize it with legal standards.
Spain	Classified		
Denmark	No answer		

REMARK: The responses reveal that the countries which provided the most comprehensive answers were the most critical in evaluation of their own systems: Slovenia, Sweden and Hungary. Conversely, the highest grades were awarded by the countries which provided short answers or no replies at all. Disregarding those which did not provide any description of their systems, we may conclude that the system is legally regulated in Hungary alone. Proposals submitted by Slovenia, Sweden and Belgium are identical, aiming at improving the critical infrastructure protection through the need for legal defining of public-private cooperation, clarification of roles, responsibilities and requirements of involved parties and harmonization with legal standards.

In Croatia, before the Critical Infrastructure Act was enacted, this area was regulated and addressed only in the context of protection of structures of special interest for the national defense, in accordance with the Defense Act. On the other hand, this area was standardized

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

through the Protection and Rescue Act, which prescribed an obligation for local and regional self-government units to develop an assessment of threats and protection and rescue plans in their areas through subordinate legislation. An integral part of those planning documents is an assessment of threats to critical infrastructure and a plan for its protection, but only in the context of protection and rescue.

21. Has your country identified the European critical infrastructures:

a) On its territory?

b) On another country's territory?

In response to the questions regarding identification of European critical infrastructure on one's own territory (Figure 15), two countries (Spain and Czech Republic) stated that they had identified European critical infrastructure. Czech Republic stated that it was also done in the territory of other countries, while others did not do so (Figure 16). Belgium gave no answer regarding identification of critical infrastructure in its own territory or in territories of other countries.

REMARK: It should be taken into consideration that information on identified critical infrastructure is largely classified and some of the respondents may have declined to answer that question or they gave a negative reply.

Croatia is still in the process of identification of its own and European infrastructure.

Figure 15. Response to the question "Has your country identified the European critical infrastructures in its own territory?" Response frequencies are shown (N=7).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Figure 16. Response to the question "Has your country identified the European critical infrastructures in another country's territory?" Response frequencies are shown (N=7).

a) and b) If yes, please state from which sector and to what extent has the European critical infrastructure been identified in your state's territory or in territories of other countries?

Only Czech Republic stated that it had identified critical infrastructure in the field of energy both in its own and in other country's territory. Belgium and Spain strictly specified that the information is classified, while other countries did not give an answer.

22. If your country has identified the European critical infrastructures, please state what methodologies and criteria were used?

In the course of identification, Czech Republic used COUNCIL DIRECTIVE 2008/114/EC method. Other respondents provided no answer.

23. Describe and assess the cooperation of your country with countries sharing the same identified European critical infrastructure.

Five countries did not provide any description of cooperation with countries with which they share European critical infrastructure, while some of them refused to answer claiming that the information is confidential. Table 9 contains descriptions of the cooperation and evaluations.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

REMARK: Croatia has not yet achieved that type of cooperation.

Table 9. Description of cooperation of the Republic of Croatia with countries sharing the same identified European critical infrastructure.

Country	Description of cooperation	Assessment of cooperation
Belgium	Confidential information	No evaluation grade
Sweden Denmark Slovenia	No answer	Moderate
Hungary	Insignificant prior to identification of European critical infrastructure	Low
Spain	Confidential information	High
Czech Republic	Close cooperation, Signing of protocols	

24. Is there any national funding for critical infrastructure protection in your country (non-EU funding)?

Two countries gave no response to the question (Figure 17), and three replied that there is no such funding system – which applies to Croatia as well. Denmark and Sweden have national systems to fund critical infrastructure protection outside EU funds.

Figure 17. Response to the question "Is there any national funding for critical infrastructure protection in your country (non-EU funding)?" Response frequencies are shown (N=7).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

25. Is there a possibility for cooperation in critical infrastructure protection on the regional level in your country?

There is an interest for cooperation in critical infrastructure protection at a regional level expressed by the majority, i.e. five countries, since six respondents declared that there is a possibility for it (Figure 18) while Slovenia and Hungary deem there is none.

REMARK: Present legal framework in Croatia does not permit it.

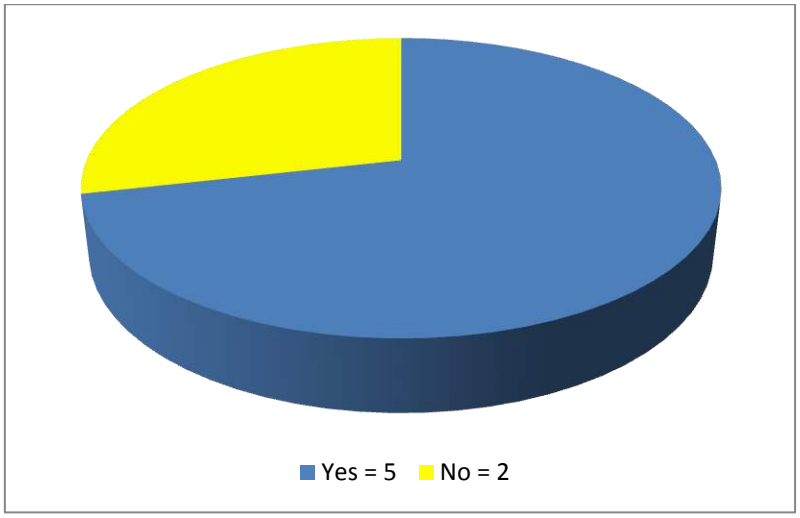


Figure 18. Response to the question "Is there a possibility for cooperation in critical infrastructure protection on the regional level?" Response frequencies are shown (N=7).

Descriptions of possibilities for the cooperation at a regional level were not provided.

26. Are stimulating mechanisms (such as premiums and other benefits) used by insurance companies for critical infrastructure protection systems that implement security measures against disaster risks?

Denmark did not answer this question, while other countries denied existence of such mechanisms. Sweden is an exception where such stimulating mechanisms exist (Figure 19).

REMARK: Some forms of such mechanisms also exist in Croatia.

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

Figure 19. Response to the question "Are stimulating mechanisms (such as premiums and other benefits) used by insurance companies for critical infrastructure protection systems that implement security measures against disaster risks?" Response frequencies are shown (N=7).

27. Are the policies of cost-benefit analysis of special measures for disaster risk reduction applied as resilience metrics?

No affirmative answer was provided to this question (Figure 20), and the same applies to Croatia.

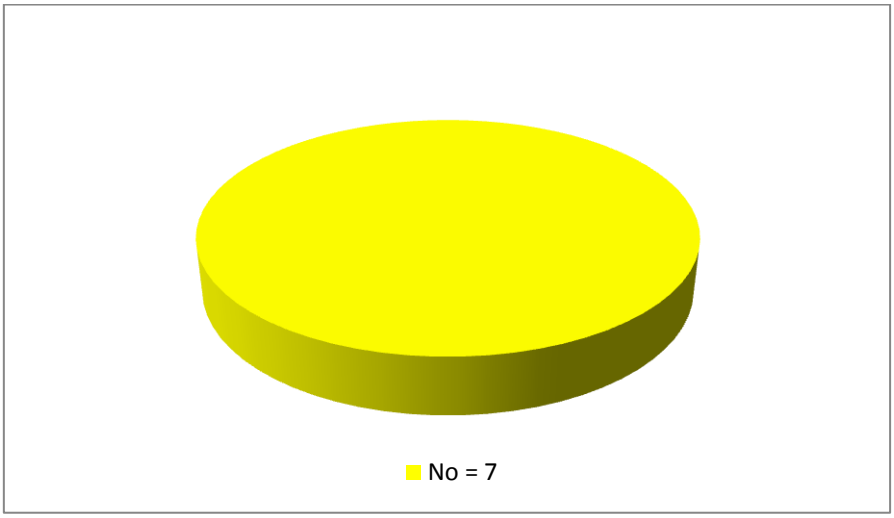


Figure 20. Responses to the question "Are the policies of cost-benefit analysis of special measures for disaster risk reduction applied as resilience metrics?" Response frequencies are shown (N=7).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

28. Are education and scientific research programmes in the field of critical infrastructure protection integrated into the higher education system?

Education and scientific research programmes in the field of critical infrastructure protection are integrated into the higher education system of four countries. Those countries are: Slovenia, Sweden, Spain and Denmark. (Figure 21).

REMARK: In Croatia, that field became a part of curriculum at a handful of higher-education institutions only, but scientific research is not currently publicly available.

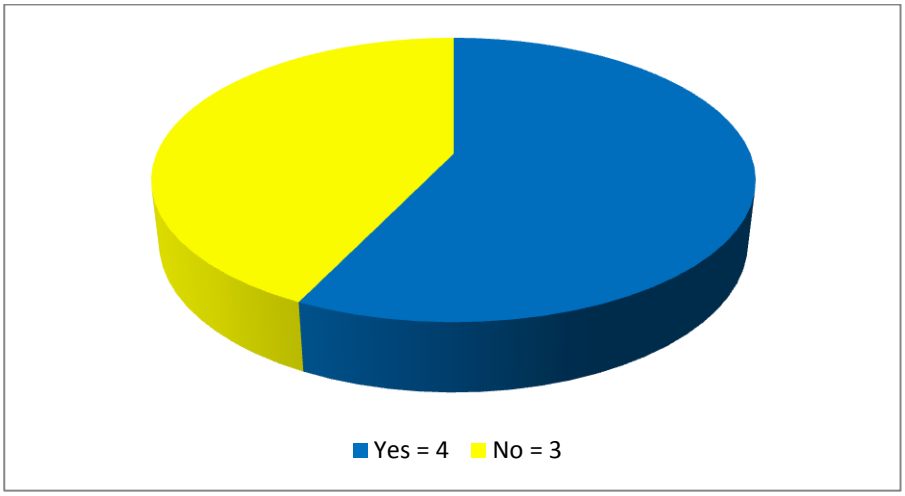


Figure 21. Response to the question "Are education and scientific research programmes in the field of critical infrastructure protection integrated into the higher education system?" Response frequencies are shown (N=7).

Co-financed by the EU
Civil Protection Financial Instrument
ECHO/SUB/2014/696006

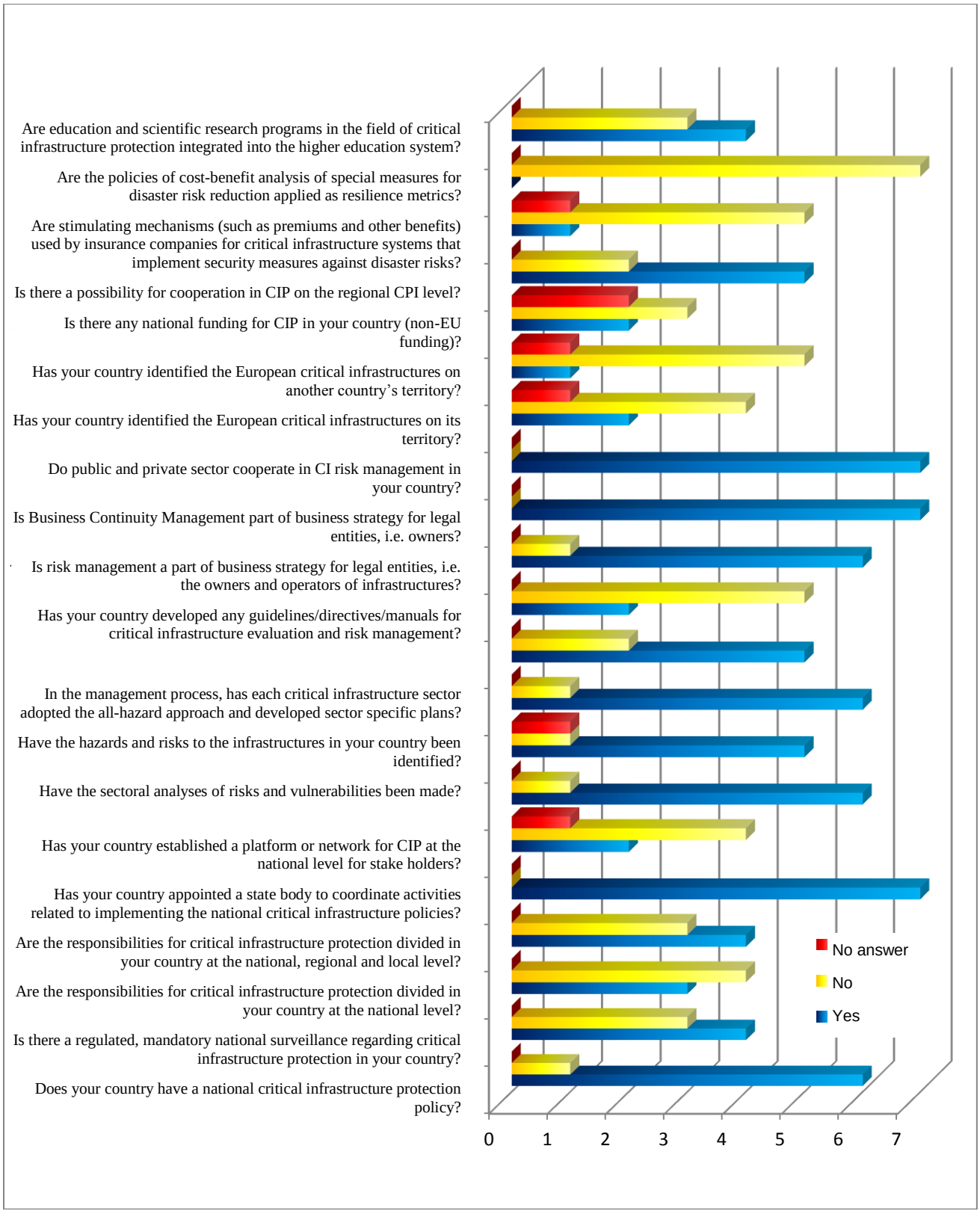


Figure 24. An overview of answers to all questions which could have been answered by a "yes" or "no" follows – sorted by the number of "yes" answers.

ANNEX III (1-2)

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 2

1. PROJECT SUMMARY 3
2. PURPOSE AND OBJECTIVES OF THE PROJECT 4
3. ANALYSIS OF THE EXISTING SITUATION 8
4. PUBLIC-PRIVATE PARTNERSHIPS IN THE FIELD OF CRITICAL INFRASTRUCTURE PROTECTION 10
5. ESTABLISHMENT OF MECHANISMS FOR EXCHANGE OF SENSITIVE INFORMATION/DATA AMONG PARTICIPANTS IN THE CRITICAL INFRASTRUCTURE PROTECTION SYSTEM 18
6. ESTABLISHMENT OF PRECONDITIONS FOR DEVELOPMENT OF A NATIONAL CENTRE FOR CRITICAL INFRASTRUCTURES 22

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

NATIONAL STANDPOINTS PROPOSAL

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

Project is funded by the Directorate-General for Humanitarian Aid and Civil Protection (ECHO), 2014.

Date of update: August 27. 2015.

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

CONTENTS

ABBREVIATIONS ..... **Error! Bookmark not defined.**

1. PROJECT DESCRIPTION ..... **Error! Bookmark not defined.**
2. PROJECT PURPOSE AND OBJECTIVES ..... **Error! Bookmark not defined.**
3. ANALYSIS OF THE CURRENT SITUATION 7
4. DEFINITION, IDENTIFICATION AND LEGAL REGULATION OF CRITICAL INFRASTRUCTURE IN THE REPUBLIC OF SERBIA 9
5. PUBLIC PRIVATE PARTNERSHIPS IN PROTECTING CRITICAL INFRASTRUCTURE 11
6. CLASSIFIED DATA SHARING IN THE CRITICAL INFRASTRUCTURE PROTECTION SYSTEM ..... **Error! Bookmark not defined.**
7. PRECONDITIONS FOR THE DEVELOPMENT OF THE NATIONAL CENTRE FOR CRITICAL INFRASTRUCTURE 27
8. CONCLUSION ..... **Error! Bookmark not defined.**

ABBREVIATIONS

CI	Critical Infrastructure
CoESS	Confederation of European Private Security Services
EU	European Union
EC	European Commission
FB	Faculty of Security Studies, University of Belgrade
NCCI	National Centre for Critical Infrastructure
RECIPE	Resilience of Critical Infrastructure Protection in Europe

1. PROJECT DESCRIPTION

Project Coordinator: National Protection and Rescue Directorate, Republic of Croatia (DUZS),

Project Partners:

- Faculty of Security Studies, University of Belgrade (FB), Republic of Serbia
- University of Applied Studies Velika Gorica (VVG), Republic of Croatia
- Swedish Civil Contingencies Agency (MMB), Kingdom of Sweden

Area of Implementation:

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

Project Aim: Strengthening the resilience of critical infrastructure protection systems both at national and European level by filling the gaps in the management and protection of critical infrastructure.

Source of co-funding: European Committee - Directorate-General for Humanitarian Aid and Civil Protection (DG ECHO http://ec.europa.eu/echo/).
In line with the Agreement of Funding, 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.

Project Duration: 01.01.2015. - 30.06.2016.

2. PROJECT PURPOSE AND OBJECTIVES

Failure in functioning of basic support systems of our society such as energy, traffic, transport, healthcare, financial and telecommunications, and shortage of necessities such as food and water contain the possibility of a massive adverse impact on:

- ✓ Welfare of population and environment,
- ✓ Functioning of industry and economy,
- ✓ Freedom and capacity of governments to respond and act.

The field of Critical Infrastructure Protection (hereinafter CIP) is among the EU key priorities. From the EU aspect, CI is 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]

The Republic of Croatia in 2013 adopted the following CIP related legislation: Law on Critical Infrastructure, Rulebook on methodology for risk assessment for critical infrastructure operations, and Decision on designation of sectors from which central state administration bodies identify national critical infrastructure and CI sector sequence list.[2]

In May 2014, the Consortium composed of partners from the Republic of Serbia, Republic of Croatia and Kingdom of Sweden, participated at the European Commission call for proposals for projects in the field of civil protection and marine pollution, with the proposal on the topic of critical infrastructure protection - „Resilience of Critical Infrastructure Protection in Europe“ (RECIPE).

The Project is implemented in the Republic of Croatia, Republic of Serbia and Kingdom of Sweden, with the Consortium partners being: National Protection and Rescue Directorate, Republic of Croatia (project coordinator), University of Velika Gorica, Faculty of Security Studies of the University of Belgrade, and Swedish Civil Contingencies Agency. The project has started on January 1st 2015, and will end on June 30th 2016. The Project website is www.recipe2015.eu

---

1 Article 2. Council Directive 2008/114/EC of December 8.2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (SL L 345/75, 23.12.2008.).

2 Law on Critical Infrastructure of the Republic of Croatia (Official Gazette RH, 56/13); Rulebook on methodology for risk assessment for critical infrastructure operations (Official Gazette RH, 128/13); Decision on designation of sectors from which central state administration bodies identify national critical infrastructure and CI sector sequence list (Official Gazette RH, 108/13).

Given that CI is the backbone of the development of contemporary society, 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 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 European CI.

The aim of the RECIPE project is to facilitate establishment of a platform for exchange of experience and 'best practice' between experts and countries that are on different levels of development of CIP.

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

The project's main objective is development of several applicable and efficient models for:

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

Project approach and expected results

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

- ✓ Panel discussions,
- ✓ Joint workshops,
- ✓ International scientific conference,
- ✓ Follow up strategy.

Since the project start date, four one-day panel discussions were organized – two in Belgrade and two in Zagreb. The results of panels are National Standpoints documents related to the analysis of current national legislation and practice, their strengths and weaknesses, possibilities for their improvement and the analyses of regulations and practice in the field of identification and interdependencies of CI with regard to the requirements of the Directive 2008/114/EC.

National Standpoints will be the basic document for international stakeholders participating at the ***joint workshops*** where they will exchange their experiences and best practices. The results of joint workshops will be used for *Instructions/Guidelines* for better and more efficient management of CI.

International conference will integrate all the results of the efforts throughout the project and provide conclusions for the follow-up strategy on CIP in general and on the following topics in particular: public-private partnership in the field of CIP; mechanisms of classified information/data exchange in the CIP system; setting of preconditions for the establishment of National CI Centres.

The Follow-up strategy will define future cooperation models on any other needs in the CI management system (e.g. training etc.).

Expected results of the project:

- ✓ Facilitated exchange of knowledge, experiences and best practices among Member States and beyond,
- ✓ Increased awareness of and knowledge base on disaster risks threatening critical infrastructure and disaster prevention,
- ✓ Enhanced stakeholder communication both at national and international level,
- ✓ Strengthened mutual support and collaboration between all relevant public and private sector partners,
- ✓ Boosted scientific and research activity in the field of critical infrastructure risk management,
- ✓ Guidelines for the establishment of an optimal risk management system related to CIP in the project partner countries,
- ✓ Guidelines made available to the EC for further dissemination and use;
- ✓ Increased resilience and level of protection of European critical infrastructure resulting from improved coordination and cooperation between stakeholders and from the exchange of best practices,
- ✓ Assessment methodology for CIP established based on the system approach,
- ✓ Defined long-term follow-up strategy on CIP in the project partner countries,
- ✓ Assessed and defined needs for further education and training of public and private sectors in the related area (educational programmes, exchange of experts).

3. ANALYSIS OF THE CURRENT SITUATION

The concept of 'Critical Infrastructure' has only recently appeared in Serbia, for the first time in 2011, in the Regulation on the Content and Methodology for the Development of Protection and Rescue Plans in Emergency Situations (Official Gazette of RS, No. 8/2011). The Article 8 of the Regulation highlights the assessment of CI from the standpoint of natural disasters and other major accidents. However, neither this nor any other document gives a definition of the concept.

Furthermore, 'Guideline on Methodology for Preparation of Vulnerability Assessment and the Protection and Rescue Plans in a State of Emergency' (The Official Gazette of RS No. 96/12), establishes criteria for the assessment of ten CI sectors with regard to their vulnerability to natural disasters and other accidents. Although the methodology contains the most comprehensive approach to the CIP in the national legislation, it is focused on identifying sources of threats and particularly on the consequences that a disturbance or interruption of the facility operation has on the economy and ecology. However, this methodology does not include 'all-hazard approach', nor the measures for improving resilience that could reduce the adverse effects of natural and other disasters on the infrastructure, including the cascade effects caused by interdependencies.

There is a particular need to develop models and methods for improvement of resilience of CI system in order to improve its capacity to minimize the consequences. It is necessary to define criteria for the identification of potential threats/hazards and generation of hazards and interdependencies tailored to different CI sectors in line with international, European and national standards.

Therefore, the first step in the regulation of this field would be to adopt the Law on Critical Infrastructure, thus establishing the legal framework for definition, identification and protection of national and European CI. After the adoption of the Law, it will be necessary to develop and adopt the bylaws that would provide practical solutions and criteria for identification of CI sectors and systems.

It should be added that the identification of CI will not start from scratch, as some existing legal acts give a solid starting point. In particular, the Law on Defence ("Off. Gazette of RS", no. 116/2007, 88/2009, 88/2009 - ot. Law 104/2009 - other. Law 10 / 2015) with its related bylaws should be observed. The Law refers mainly to the defence industry of Serbia, but also to other industrial and infrastructure objects, which during war, state of emergency or mobilization of the Serbian Army primarily provide the services and operations stipulated by the Ministry of Defence.

Other laws, bylaws and strategic documents relevant for the CIP are: the Law on Emergency Situations ('Official Gazette of RS' no.111/2009), National Strategy of Protection and Rescue in

Emergency Situations ('Official Gazette of RS', no. 86/2011), Law on Private Security ('Official Gazette of RS', no. 104/2013), Law on Environmental Protection ('Off. Gazette of RS', no. 135/2004, 36/2009, 36 / 2009 – other law 72/2009 and 43/2011 - Decision), Data Secrecy Law ("Off. Gazette of RS", no.104/2009), Law on Planning and Construction ("Off. Gazette " no.72/2009), Law on Water (Official Gazette. Gazette no.30/10, 93/12), and other relevant documents.

In the following steps it will be necessary to prioritize the identified CI sectors and regulate the aspects of the CIP that have shown to be particularly problematic in the European and global practice – public-private partnership (PPP) and exchange of classified information.

4. DEFINITION, IDENTIFICATION AND LEGAL REGULATION OF THE FIELD OF CRITICAL INFRASTRUCTURE IN THE REPUBLIC OF SERBIA

Based on the international experience and 'good practice', the partners agree that the definition of critical infrastructure and its content cannot be identical in each and every country, therefore its definition and content should be determined at the national level.

Therefore, in order to be sure about the content and the boundaries of the CI concept, it is crucial to adopt the Law on Critical Infrastructure. The Law would establish a regulatory framework for defining, identifying, and protecting national and European CI in Serbia. In addition, its bylaws should provide practical solutions and criteria for the identification and prioritization of CI.

The adoption of the Law on CI (or CIP) is among the obligations of the Republic of Serbia in the process of EU accession. The Action Plan for Chapter 24 for the EU accession recognizes the Ministry of Internal Affairs of the Republic of Serbia as the authority responsible for the future Law. Within the Ministry of 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 a national CIP policy.

The future Law on CI, but also other laws relevant to the CI should contain the provisions of the European Directive on the Protection of Critical Infrastructure (Directive 2008/114 / EC). In this regard, it is necessary to make amendments in the CIP related parts of the National Strategy for Protection and Rescue in the Emergency Situations and in the Law on Emergency Situations. For effective CIP and comprehensive legal regulation of this area it will be necessary to implement the existing Data Secrecy Law, which, according to some experts, exists only on paper. In addition, the Law on Information Security (the work on its draft commenced more than three years ago), the Regulation on Encryption and Cyber Security Strategy should also be adopted.

During the identification of CI sectors and facilities it would be desirable to start from international, or at least from the regional level. While many developed countries identified over ten CI sectors (including the Republic of Croatia - eleven sectors identified), it is suggested that lawmakers in Serbia should be realistic and not make a list of sectors that is too broad, taking into account the limited state budget, due to which not all identified sectors and belonging facilities could be protected in an optimal manner. The next step would be to identify CI facilities at lower levels, in addition to regional and national. CI facilities can also be identified at the city, local, and even at the sectoral level. Preliminary identification and classification of CI facilities may be done even before the law is adopted, provided the criteria and departmental sector analysis are defined.

The following infrastructure sectors appear in almost all countries with the developed CIP policies and can be used for creation of a wider list of CI sectors in Serbia:

- Energy (production, transmission, distribution and storage of energy supplies (oil and gas) and electricity)
- Information and communication technologies (electronic communication, data transmission, information systems, audio and multimedia services)
- Transport (road, rail, air, water)
- Health (hospitals, pharmaceutical industry)
- Water (drinking water supply, dams, wastewater treatment, water protection)
- Food (production, food supply, food security, commodity stocks)
- Finance (banking, stock exchanges, investment, insurance and payment systems) and
- Public services (preservation of public order, protection and rescue, emergency medical assistance).

Various ministries, sectors and departments have different criteria and classification of objects and facilities under their jurisdiction. The Law on Defence provides the definition of facilities that are of special importance for the national defence: large technical and technological systems; facilities in which products of importance for defence purposes are produced, stored or kept, or facilities that provide service for defence purposes; buildings occupied by public authorities and legal entities of special importance for the national defence, as well as certain infrastructure facilities. The Plan of Defence mentions hundreds of technical and technological systems, with the respective plans of defence, whilst the Instruction on Creation of Plans of Defence from 2013 provides a methodology for identification of those technical and technological. Therefore, it is possible that future CIP plans will be included in plans of defence. In addition to the Law on Defence and Plans of Defence, the following bylaws are also relevant for future identification and classification of CI in Serbia:

- Decision on Types of Investment Facilities and Spatial and Urban Plans of Importance for National Defence ("Off. Gazette FRY", no. 39/95).
- Decision on Facilities of Particular Importance for National Defence ("Off. Gazette of RS", no. 112/2008)
- Decision on Identification of Large Technical Systems Important for National Defence ("Off. Gazette of RS", No.41 / 2014 and 35/2015)
- Decision on Identification of Products and Services of Special Importance for the National Defence of the Republic of Serbia ("Off. Gazette of RS", no.58 / 2008);

The abovementioned documents primarily refer to defence industry in Serbia, as well as other industrial and infrastructure facilities that in time of war or state of emergency, as well as during the mobilization of the Army of Serbia primarily provide those services determined by the Ministry of Defence.

Another relevant law for the identification of CI is the Law on Planning and Construction, and its associated plans: Spatial Plan of the RS, followed by regional and local plans. Particularly

important are the spatial plans of special purpose areas, which almost completely coincide with critical infrastructures.

Conclusion

As the first step towards establishment of an efficient protection and resilience CI system, the legal regulation of this field is of key importance. First of all, it is necessary to adopt the Law on CI and its bylaws that will more precisely regulate the particular challenges such as the identification of CI sectors, identification of CI facilities in specific sectors, classification and prioritization of identified CI, public-private partnerships and the exchange of classified information. This procedure will not start from scratch as the existing legal framework provides a solid base for the inclusion of certain provisions in the new law and accompanying bylaws. The term „critical infrastructure "should be included in the existing relevant laws and bylaws, which will further need to be harmonized with the Law on CIP when it comes into force.

5. PUBLIC-PRIVATE PARTNERSHIP IN PROTECTING CRITICAL INFRASTRUCTURE

Abstract

The aim of the proposal is to establish a platform for public-private partnership in the field of the critical infrastructure protection and resilience that will provide the logic and principles for the following: the concept of cooperation; projects; security; creation of a new and improvement of existing legal and normative framework; identification of critical infrastructure; prioritization of vital critical infrastructure; development of programs and tools for achievement and improvement of resilience and security.

Public-private partnership (hereinafter - PPP) is among the key factors of the CIP process. In the majority of developed countries around 80% of CI is privately owned. Although for Serbia and the Western Balkans region precise figures do not exist, that percentage is undoubtedly lower. However, the increase of the percentage of privately owned CI facilities is expected, taking into account global trends of market liberalization. According to the Communication from the European Commission on the principles of the PPP "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. At the same time, PPPs are interesting vehicles for the long-term structural development of infrastructures and services, bringing together distinct advantages of the private sector and the public sector, respectively."[3]

In the contemporary "risk society", where we are exposed to an increasing number of security threats and challenges - from climate change to organized crime and terrorism - the cooperation, including the exchange of knowledge and experiences between the private and public sectors is crucial. The state and state "institutions of force" do not always have sufficient capacity for meeting the security needs of society, which is especially noticeable in the field of protection. Indeed, PPP appears to be the mechanism of choice for cooperation between the factors that may impact the efficient resolution of security challenges. PPP as a model of relations between the public and private sectors is established on the premises of recognizing the benefits for both public and private sector from the pooling of resources and expertise (knowledge), for the purpose of meeting community needs. This partnership combines the expertise, resources and strengths of both sectors, harmonizes social and public accountability and effective management of the public sector with financial capabilities and the "entrepreneurial spirit" inherent to the

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 November 2009 - Mobilising private and public investment for recovery and long term structural change: developing Public Private Partnerships [COM(2009) 615 final – Not published in the Official Journal].

private sector. This may result in better and more efficient protection of public interest in the field of CIP. Therefore, the priority should be given to those joint initiatives of the public and business sectors in which each entity contributes with specific resources and cooperates in the planning and decision-making process.

Certainly, one should take into account that in PPP there must be some differences in the "approach" to the concept of cooperation between the partners. For example, private companies will often manifest "profit motives“, whilst the public sector can impose "bureaucratic" thinking and decision making thus demotivating the other side. In order to overcome potential differences, it is important to concentrate on wider picture. If it is correctly designed and implemented, PPP can bring palpable benefits in terms of helping governments to finance infrastructure investments in a more efficient manner, as scarce resources may be channelled to other national priorities (e.g. meeting the basic needs of citizens in the fields of education, health care) with better value for money.

According to the “Best Practice” analysed, PPP should meet the following criteria: open dialogue between the responsible public authorities and service providers of private security, clear guidelines on the role of each partner, clear legal and contractual framework, regular assessments and the necessary corrections and improvements when and where necessary. In addition, the interaction must exist within the framework of specifically established and formally bound joint structures.

In order to meet these criteria and optimize the effectiveness of the partnership between the public and the private security sector in CIP arena, it is vital that each partner fully understands its role, responsibilities and limitations. The Confederation of European Security Services (CoESS) believes that due to the lack of knowledge of these elements, the partnership between the public and private sectors in the field of CIP across Europe is still underdeveloped and far from reaching its maximum potential.

It should be added that, when considering policy cooperation with private security companies in the field of CIP, the necessary attention should be paid to the quality of service. CoESS therefore recommends that national regulations concerning private security services include provisions on special licenses or authorizations for the CIP services. This can be achieved through additional licensing and setting of work criteria for private security companies or through compulsory special training programs for the staff of private security in this field.

It should be stressed that the private security sector in Serbia is very active and a proponent of the large number of initiatives on the adoption and improvement of legislation and national standards.

Private security sector companies are engaged in the CIP projects through the process of public procurement. It is essential that private security sector reaches a certain level of competence for such operations, as is necessary in the case of state security institutions - the army and police. It was noted that major problems arise in the process of public procurement of private security

services, since the only criterion is the lowest available price, even though the EU Directive provides clear guidelines that mandatory criteria are the most economically advantageous tender, and the competitive dialogue. As the price of private security services in Serbia is the lowest in Europe, the quality of services is questionable if the cheapest offer is chosen. This can have serious consequences for the CIP, since many of CI facilities are protected by companies characterized by a low level of service quality, personnel training, equipment and others.

The National Security Strategy of the Republic of Serbia and the public-private partnership

The National Security Strategy of the Republic of Serbia identifies PPPs as a matter of a huge importance to the national security. "An important prerequisite for achieving and improving protection of life and property of citizens, human and minority rights is the cooperation of state bodies with the entities from the field of private security and other institutions, local governments, professional associations, churches and religious communities, the media, minority communities, civil society organizations and citizens, thus developing relationships of trust, building and strengthening security and solving security problems."[4]

The National Security Strategy of the Republic of Serbia also addresses the issue of private security companies by stating that: "Along with government and other bodies and institutions, the entities in the field of private security services have increasing responsibility for the implementation of internal security policy, whose activities include security protection of individuals, objects and other material goods not covered by the protection of the competent state authorities. Of particular importance is that the social activities of the entities in the field of private security are entirely normatively and doctrinally regulated."[5]

Law on Public-Private Partnership and Critical Infrastructure

It is to be expected that certain provisions of the future Law on CI will be based on the Law on Public-Private Partnership, adopted in 2011 ("Official Gazette of the RS" no. 88/2011). Certainly, the Law on PPP does not recognize the term 'critical infrastructure", due to non-existent legislation on CI. However, it is clear that many facilities and services of public interest mentioned in this Law will enter the framework of the prospective Law on CI and future bylaws and regulations in this area.

According to this law, the PPP is a long-term cooperation between a public and a private partner for the purposes of providing financing, construction, reconstruction, management or maintenance of infrastructure and other facilities of public interest and provision of services, of

[4] National Security Strategy of the Republic of Serbia, p.27.
[5] Ibid, p.26

public interest, which may be contractual or institutional (Article 7) The period for which the public contract is concluded may not be less than five, nor more than fifty years (Article 18).

Article 4 of the Law defines public partner as one or more public bodies, or a legal person who according to this law is in charge of approving the concession, which enters into a public contract with the private partner or the SPV, or one or more public bodies that are linked with the private partner through membership in some joint enterprise.

The private partner is defined as a natural or legal person, national or foreign, with local or foreign share or without it, or a consortium of one or more such natural and legal persons which have been selected in a public procurement procedure or concession granting procedure and which have signed with the public partner a public contract, or which is establishing for that purpose an SPV, or which is establishing with the public partner a joint enterprise.

It is interesting to note that Article 3 states that the Law does not apply to PPPs if the subject of that partnership was the use of a public telecommunications network or the provision of telecommunications services. Paragraph 2 of the same article also points out non-application of the law in the event that the establishment of such PPP would require enabling access to the information whose disclosure would endanger the security of the Republic of Serbia

Article 5 of the Law sets out Principle on environmental protection as one of the basic principles for conclusion of public contracts. According to the Article 6 **The principle of environmental protection** includes the principles defined by the law regulating environmental protection, such as: the principle of integrity, the principle of prevention and precaution, the principle of preservation of natural values, sustainable development, the polluter-pays principle and other.

The private partner has an obligation to take over from the public partner the design, construction or reconstruction of public infrastructure or a facility of public interest, as well as the maintenance of public infrastructure or provision of services of public interest including one or more of the following obligations: financing, management and maintenance, for the purpose of providing services of public interest to final beneficiaries from within the competences of the public partner, or for the purpose of ensuring the necessary preconditions for the public partner for the provision of services of public interest within his competences, or provision of services of public interest from within the competences of the public partner to the final beneficiaries

Also, each partner is to undertake responsibility for the risk which it can better manage or which it can affect, or risks are divided in a balanced manner, all for the purpose or ensuring optimal risk management for the duration of the PPP project, with the use of management, technical, financial and innovative capacities of the private partner, and by improved exchange of skills and knowledge between the public and the private partners.

The concept of ‘concession’ which regulates relations in various infrastructure sectors will surely be relevant for the PPPs in the field of CI. According to this Law, the concession is a PPP with

the elements of concession in which a public contract regulates the commercial use of natural resources or assets in general use which are publicly owned or the performance of an activity of public interest which the competent authority transfers to a national or foreign person, for a specific period of time, under specially prescribed conditions, against the payment of a concession fee by the private or the public partner, with the private partner bearing the risk associated with the commercial use of the subject of concession. (Article 10)

Among other things, the concession may be given for exploration and exploitation of mineral resources and other geological resources, in the area of energy, for construction and maintenance of ports, public roads, public transport, airports, railways, health care, etc. (Article 11). It should be noted that not all areas of public interest are explicitly mentioned in the Law, so some of them remain open to interpretation. The concession granting authority may be the Government of the Republic of Serbia, the Government of an autonomous province, the local assembly or a public company. (Article 13) As far as the private partner, participant in the award of a public contract may be any domestic or foreign natural or legal person (Article 14).

According to the Law, the state PPP Commission gives professional assistance in the implementation of PPP projects and concessions. The chairman of the Commission's is the representative of the Ministry of Economy and Regional Development, whilst his deputy is a representative of the Ministry of finance (Article 65). The Commission, as the most important state body for the approval of PPP projects determines whether the project proposal is in the public interest and whether it is submitted by a public body. As the Commission is composed of representatives of various ministries, under whose competencies are areas that will belong to future CI sectors - such as the Ministries of energy, transport, mining, etc., their representatives will be directly involved in projects related to CI belonging to their competencies.

The Commission for PPP in the Security Sector, organized within the Serbian Chamber of Commerce, is identified as an important subject in the CIP related PPP projects. Its members are representatives of private security associations and companies, representatives of ministries with an interest to cooperate with private security sector, representatives of the academic community and various citizen associations (NGOs).

National and International Standards

Some provisions of international and national standards give an insight into the "good practice" of PPP. For instance, draft ISO 22397 Standard (Societal security - Public private partnership - Guidelines for establishing partnership agreements among organizations) from 2012 mentions critical values of the assets and disruptive events.

According to this draft, the first parameters for the establishment of a partnership agreement are the identification and classification of common critical assets, as well as the identification and evaluation of potentially disruptive events. It is proposed that these activities are executed in accordance with the guidelines of ISO 31000: 2010 (Risk Management). For the same purpose, in

Serbia the national standard SRPS A.L2.003 2010, Social security - Risk Assessment in the Protection of Persons, Property and Business (Official Gazette of RS, no. 92/2010) can be used.

When identifying critical assets, the parties should provide a comprehensive list of all relevant resources, and also identify any vulnerable targets. Information about critical assets (facilities, systems, equipment, services, processes, people, etc.) should be made in accordance with the mission, confidentiality and expectations set out in the partnership agreement. Analysis and prioritization of identified assets can be a useful input for the next phase of classification.

During the classification process the contracting parties should jointly establish a list of identified critical assets. The contracting parties should also define the method of evaluation, which may include the correlation between the protected assets. The level of detail of mathematical modelling should be determined by the expectations of the parties. Audit and 'field' evaluation can also be used to gain insight on particular assets and/or for the validation of previous criticality assessments.

Identification of disruptive events involves identification and description of the sources of risk, and the potential consequences for the identified critical assets. Risk identification must be comprehensive and should include interdependencies, cascade and cumulative effects, but also consider the consequences of events when risk sources are not recorded. In the case of complex partnership agreements with more contracting parties, stakeholders and assets, the parties should consider multiple causes and scenarios, and pay special attention to potential correlations between sources of risks and interdependencies.

Recommendations

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

After it is clearly defined what we understand under CI protection and resilience, and what it needs to achieve, it will be necessary to devise a strategy for its implementation and to provide the political will to implement its objectives. The following step is to raise awareness among all stakeholders, especially between the CI owners and operators of. 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:

1. The development of standards and exchange of best practice

2. Promotion of education and training

3. Promotion of research and development

4. Exchange of information

During the project, the Faculty of Security Studies, as the Project beneficiary in the Republic of Serbia, will ensure the participation of representatives from relevant ministries, agencies, sectors and other state bodies, as well as representatives of the most important economic entities (potentially identified as CI facilities), professional and academic community, Serbian Association of Corporate Security Managers, the Association of Private Security Managers within the Chamber of Commerce of Serbia, the Commission for Public-Private Partnerships and numerous other stakeholders to discuss and propose the optimal concept of cooperation.

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

Although PPP is not the ideal model for all infrastructure projects, it is necessary to consider a joint action wherever possible and mutually justified. Construction of missing CI capacities, maintaining and improving the resilience of the existing ones, and the CIP, is 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 sector interest, in order to avoid the impression of unidirectional partnerships.

PPP 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. To this purpose we propose the following: conclusion of long-term projects by public sector; joint public and private funding; involvement of the private sector in the responsibilities of the public sector (procurement, construction, management, maintenance, etc.); creation of risk and responsibilities sharing models during the course of the partnership.[6]

In Serbia, currently there is an initiative to include private security companies in the TETRA protected communication network, set within the 112 Service, which is also being implemented.[7]

During the course of the Project, FB will organize meetings and discussions on potential models of cooperation between the most important stakeholders in this field, and it will also collect and analyse the best available practice and models for their implementation.

Establishment and improvement of normative framework with the view to 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 ground for further action, new ideas and

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

[7] In all EU countries, 112 is the contact number of emergency services (ambulance, firefighters and police). The calls are free of charge and the number is accessible 24/7.

models of implementation of legal regulations. In addition, normative framework should provide a stimulative approach for new investments and creation of new values.

First of all, we refer to the adoption of Law on Critical Infrastructure that will regulate this field, as well as to bylaws pertaining to this law. Furthermore, we refer 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 CI protection and resilience, and also regulate PPP in this field.

In the process of establishing the normative framework for a new framework, the lawmaker most frequently takes over the *acquis communitaire* (in the EU context) and opens a public discussion with all stakeholders. As the preparation and adoption of Law on Critical Infrastructure (an obligation of the Republic of Serbia in the process of accession to the EU) is announced for 2016, an important part will be dedicated to the regulation of PPP in CIP. FB will broaden the public discussion with the aim of obtaining high quality proposals for the improvement of the normative framework, in order to make it clear, flexible and open for new investments, as well as for the bigger and better cooperation between public and private sector.

Identification and prioritization of CI using the mechanism of PPP

After the CI related law and bylaws are adopted and the CI sectors and facilities identified, the following step will be the 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 CI sectors and facilities and the experience of countries that have already adopted this paradigm, it is concluded that it would be impracticable to equally protect and build resilience of all CI facilities. Private actors, primarily the owners and operators of the privately owned CIs can provide a valuable contribution to this process.

Project partners will collect and share the best international practice with all stakeholders and ensure the platform for establishment of PPP in the field of CIP.

Development of programs and tools for building and improvement of CI protection and resilience using PPP

First and the foremost, CIP includes prevention and risk assessment of CIs. On the other hand, resilience signifies the ability of a system to reduce efficiently both the magnitude and duration of the deviation from targeted system-performance levels.[8] As it is a complex concept that requires holistic approach, PPP is a very convenient tool for strengthening its resilience.

[8] Biringer B, Vugrin E and Drake Warren, *Critical Infrastructure System Security and Resiliency*, CRC Press, Boca Raton, 2013, p.107

During the course of the project, national partners will perform the necessary research in order to connect knowledge and experience, and consequently recommend programs and tools for building and improvement of critical infrastructure protection and resilience using PPP.

Conclusion

FB will continuously work on updating and reviewing of this document in coordination with all stakeholders.

This chapter intends to create national standpoints on PPP in CI protection and resilience and to exchange the best practice regarding: the concept of cooperation; projects; security; improvement of normative framework; prioritization of vital CI; development of programs and tools for building and improvement of CI protection and resilience.

Literature

Strategies and Laws

Narodna Skupština Republike Srbije (2009) *Strategija nacionalne bezbednosti Republike Srbije*, dostupno na: http://www.kombeg.org.rs/Slike/CeBezbednost/statika/Strategija%20nacionalne%20bezbednosti%20Republike%20Srbije.pdf , (accessed July 2, 2015.).

Narodna Skupština Republike Srbije (2011) *Zakon o javno-privatnom partnerstvu i koncesijama*, dostupno na: http://www.paragraf.rs/propisi/zakon_o_javno_privatnom_partnerstvu_i_koncesijama.html , (accessed July 2, 2015.).

Standards

ISO 31000 Risk management – Principles and guidelines on implementation

ISO/IEC 31010 Risk management – Risk assessment techniques

ISO/CD 3 22397 Societal security — Guidelines for establishing partnering arrangements

ISO/TC 223 N 337 Societal security - Public private partnership — Guidelines for establishing partnership agreements among organizations

SRPS A.L2.002:2008, Društvena bezbednost – Usluge privatnog obezbeđenja – Zahtevi i uputstvo za ocenjivanje usaglašenosti, Službeni glasnik RS, br.07/2009.

SRPS A.L2.003:2010, Društvena bezbednost – Procena rizika u zaštiti lica,imovine i poslovanja. Službeni glasnik RS, br. 92/2010.

EU Documents

Critical Infrastructure, *Security and protection, The Public - Private opportunity*, CoESS, B-1780 Wemmel, Belgija, May 2012

Risk Management Capability Assessment Guidelines (ECommisison notice, 2014)

European Commission (2009) Mobilising private and public investment for recovery and long term structural change: developing Public Private Partnerships.

Research papers

Auzzir Z.A. et al. (2014) *Public-private partnerships (PPP) in disaster management in developing countries: a conceptual framework,* http://www.sciencedirect.com/science/article/pii/S2212567114010065, (pristupljeno 24. jula 2015.).

Biringer B, Vugrin E and Drake Warren (2013), *Critical Infrastructure System Security and Resiliency*, CRC Press, Boca Raton.

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, (pristupljeno 24. jula 2015.).

Heammerli, B. i Renda, A. (2010) *Protecting Critical Infrastructure in the EU*, Brussels: Centre for European Policy Studies, http://www.ceps.eu/ceps/dld/4061/pdf (pristupljeno 5. februara 2014.).

Keković, Z., Savić, S., Komazec, N., Milošević, M., Jovanović, D. (2010) *Procena rizika u zaštiti lica, imovine i poslovanja,* Centar za analizu rizika i upravljanje krizama, Beograd

6. CLASSIFIED SHARING IN THE CRITICAL INFRASTRURCTURE PROTECTION SYSTEM

Thanks to the first security incidents in cyber space it was noticed that computer systems and networks represent a huge source of risk to information and, indirectly, to individual, corporate, national, regional and global security. Due to the continuous process of informatization of the population and progressive automatization of the critical infrastructure and services, the significance of information security has increased. This concept has become a central element of the national security policies of all technologically developed countries, and also of regional and global security policies. Many experts have concluded that "security, economy, standard of living and, quite possibly, the very existence of industrialized countries depend on" electricity, telecommunications and computers ... which are, in addition to traditional physical threats, exposed to new cyber threats."

Therefore, the information is the main entity exposed to the security threats from the arsenal of information warfare. Three aspects of information can be compromised: privacy, integrity and availability. In addition, the total infrastructure in charge of transmission of data and information and their storage is exposed to threats and risks.

Disruption of normal operation of information systems in the modern society can have severe consequences in all spheres of social life. The consequences can be even fatal, if critical information infrastructure, such as systems for control of land and air transport, hydro-dams, nuclear power plants, security and health services, or even systems for electricity distribution, is compromised. After the 9/11 terrorist attacks, the issue of security of cyber space and the protection of critical information infrastructures has come in the focus in developed countries. The focus on these issues, according to some analysts, was the result of fear of the US administration of possible "boomerang effect", i.e. as an understanding that the Internet for terrorists constituted the tool for planning and implementing attacks. Heightened perception of the possibility of transferring terrorism threat to the cyber space, but also of other forms of information warfare that may cause material damage to the state and its citizens, jeopardize defence systems, negatively impact human rights, health and life, put the possibility of creating a safe information space high on the agenda of regional and international organizations.

In the growing number of discussions on CIP, the information infrastructure receives special attention. Over the years various measures for prevention and response to possible incidents, caused by technical failures, natural disasters or intentional destructive acts were developed. The growing dependence of systems on information infrastructure represents an additional risk, given that it permeates all other systems and imposes them its own vulnerabilities. A typical example of the permeation can be shown in the example of control systems - specialized computers and technologies

that are used in many industries and infrastructure services for the monitoring and control of the most sensitive processes. In the electricity industry, for example, control systems manage and control the generation, transmission and distribution of electricity. In the gas distribution the monitoring of the flow of gas in the pipelines is performed from remote locations. In water distribution such systems control the water level in wells and reservoirs, the pumps, the level of water quality and the presence of chemical additives.

Nowadays the information base, control systems and means of communication are interconnected at the global level. This situation has its "Achilles heel" as the most advanced technological party may, at the same time, be the most vulnerable one, or if adequately protected, the most dangerous one. The rapid entry of "information conflicts" into the civil and corporate sphere is a serious problem for managers responsible for the safety and security of the information infrastructure. Management structure at the corporate-economic level should be aware of the broad scope of potential attacks, including espionage, organized crime, perceptual battle, as well as attacks by hackers and groups sponsored by a state or business competitors. The concept of managing security risks in the information space in terms of national security, however, requires harmonization of national legislation with the existing international standards.

The Republic of Serbia is lagging behind many EU countries, as well as behind another participant in this project, the Republic of Croatia, which passed the Law on Critical Infrastructure in 2013 (Official Gazette No. 56/13), and the Data Protection Law, which clearly defined the problem of sensitive information. The problems that our country face 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 unclear role of the Ministry for Construction, Transport and Infrastructure, lack of skilled personnel in the Ministry to deal with the CI issues, the lack of permanent education of managers in the field of CI and in the field of information protection, the lack of awareness of people in charge of the CI 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 recognition of importance of secret data, sensitive information and their protection is reflected in the Data Secrecy Law ("Off. Gazette of RS", no. 104/2009). This Law regulates the single system of determination and protection of secret data of interest for national security and public safety, defence, internal and foreign affairs of the Republic of Serbia; protection of foreign classified data; access to classified data and their declassification; competence of authorities and oversight of the implementation of this Law, as well as accountability for non-implementation of obligations arising from this Law, and other issues of importance for data secrecy protection. The Law provides definitions of various concepts: data of interest for the

Republic of Serbia, classified data, foreign classified data, document, classification of data, determining the level of secrecy 'top secret', 'secret', 'confidential' or 'restricted, security clearance, damage, classified data controller, data user, security risk and protection measures. According to the Law Data that can be classified as secret shall be any data of interest for the Republic of Serbia, whose disclosure to an unauthorised person would result in damage, if the need to protect the interest of the Republic of Serbia prevails over the interest to have free access to information of public importance. The data from paragraph 1 of the Article 8 are particularly relevant to: 1. national security of the Republic of Serbia, public safety, or defence, foreign, security and intelligence affairs of public authorities; 2. relations between the Republic of Serbia and other countries, international organisations and other international entities; 3 systems, equipment, projects, plans and structures in connection with the data from items 1) and 2) of this paragraph; 4. scientific, research, technological, economic and financial affairs in connection with the data from items 1) and 2) of this paragraph.

Data classification is performed by authorized persons under the conditions and in the manner prescribed by the Law. The Article 9 mentions the following authorized persons: 1. the President of the National Assembly; 2. the President of the Republic; 3. the Prime Minister; 4. the head of a public authority; 5. elected, appointed or nominated public authority officials, authorised to classify data by law or regulation adopted under law, or authorised in writing by the head of a public authority; 6.persons employed by a public authority, who have been authorised in writing for data classification by the head of the public authority. The authorised persons from paragraph 2 items 5) and 6) of this Article may not delegate their authority to other persons. The authorised persons classify data during their creation, i.e. when the public authority begins to perform an activity resulting in the creation of classified data. As an exception to paragraph 1 of this Article, an authorised person may also classify data subsequently, upon fulfilling the criteria established by this Law.

In classifying data, an authorised person assesses possible damage to the interest of the Republic of Serbia. A person employed by or performing certain tasks for a public authority is obliged, within his/her tasks or powers, to inform an authorised person of any data that can be classified as secret. A document containing classified data is marked with: 1. a classification level; 2. the manner in which it is to be declassified; 3. details on the authorised person; 4 details on the public authority. The Government prescribes the manner and procedure of marking the level of classification, i.e. the document. The data from Article 8 of the Law are assigned one of the following levels of classification: 1. "TOP SECRET", which is assigned with a view to preventing irreparable grave damage to the interests of the Republic of Serbia; 2. "SECRET", which is assigned with a view to preventing grave damage to the interests of the Republic of Serbia; 3. "CONFIDENTIAL", which is assigned with a view to preventing damage to the interests of the Republic of Serbia; 4 "RESTRICTED", which is assigned with a view to preventing damage to the operation or performance of tasks and activities of the public authority which defined them. In determining the level of data classification, only the levels of

classification from paragraph 1 of this Article may be applied. The Government defines more detailed criteria for determining the "TOP SECRET" and "SECRET" levels of classification, upon obtaining an opinion of the National Security Council. The Government defines more detailed criteria for determining the "CONFIDENTIAL"and "RESTRICTED"levels of classification, at the proposal of the competent minister or the head of a public authority.

According to the Law, a public authority establishes a system of procedures and measures to protect classified data according to the following criteria: 1. the level of classification; 2. the nature of the document containing classified data; 3. classified data security threat assessment. A public authority applies general and special protection measures under law and regulations adopted under law, with a view to protecting classified data in its possession. General measures for the protection of classified data include: 1. determining the classification level; 2. assessing classified data security threat ; 3. establishing the manner of using and handling classified data; 4. designating a person responsible for keeping, using, exchanging and other forms of classified data processing; 5 designating a classified data controller, including his security clearance depending on the classification level; 6. determining special zones, buildings and premises intended for classified data and foreign classified data protection; 7. classified data handling control; 8. measures for the physical and technical protection of classified data, including the installation and set-up of technical means of protection, determination of a security zone and protection outside that zone; 9. protection measures for information and telecommunication systems; 10. crypto protection measures; 11. protection regime for jobs and formation posts, under any internal acts on job classification and systematisation; 12. establishing special educational and training programmes required for the protection of classified data and foreign classified data; 13. other general measures prescribed by law. With a view to efficiently implementing general measures for classified data protection from Article 32 of the Law, special measures for classified data protection can be brought under a Government act.

Classified data are kept in such a manner that only authorised users are allowed access to these data. Classified data may be transmitted and delivered outside the premises of a public authority only in compliance with the prescribed security measures and procedures ensuring that classified data could be received only by a person who has a certificate for access to classified data and is entitled to receive them.

In transmitting and delivering classified data outside the premises of a public authority, security procedures and measures are determined according to the classification level assigned to such data, under law and in compliance with any regulation adopted under law. The application of the prescribed measures of crypto protection is mandatory in transmitting and delivering classified data over telecommunication and information systems. In transmitting and delivering classified data from paragraphs 3 and 4 of this Article, crypto protection measures are implemented under law. When an official, employee or a person performing specific tasks in a public authority, learns of any loss, theft, damage, destruction or unauthorised disclosure of classified data or

foreign classified data, he/she shall inform the authorised person of a public authority thereof without delay.

In addition, the Law regulates the access to classified data, procedure for issuing certificate or permission to natural, legal and foreign persons, control and oversight (the role of the National Security Council in particular), punitive, transitional and final provisions.

Bearing in mind that data and information are among the most important resources with which societies dispose, and that without them the elementary areas of everyday life would be impossible to maintain, it is necessary to adopt a holistic and multidimensional approach to the problem of storing and protection of classified data in public and private sector. The first assumption in their protection is timely prevention of their exposure and abuse.

Suggestions and Conclusions

1. With a view to establish 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 of 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 intersectorial 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”.

7. PRECONDITIONS FOR DEVELOPMENT OF THE NATIONAL CI CENTRE

One of the main institutional preconditions for the establishment of an efficient CIP system is the development of a National CI Centre (NCIC) that would, among other tasks, coordinate the CIP activities taking into account important issues discussed above: PPP and classified data exchange.

As the Republic of Croatia has an established CIP system, the model and proposal for the establishment of the NCIC developed by our project partners from Croatia deserves to be mentioned. According to this proposal the establishment of NCIC will be the task for the Government of the Republic of Croatia, DUZS and other stakeholders. The NCIC should have clearly defined tasks, competencies and responsibilities for implementation of the regulations in the field of CI, as well as for the coordination and improvement of cooperation of all participants. DUZS and VVG propose two models for its establishment. According to the first model, the NCIC may be established either within the DUZS as an independent sector, as a service within the Civil Protection Sector, or as a department within the Service for Prevention, Planning and Analytics of the Civil Protection Sector. The second model proposes the intersectoral establishment of the NCIC as a separate agency of the Croatian Government.

Regarding its functionalities, NCIC would be in charge of: 1. creation of the holistic concept of the CIP, 2. review, harmonization and improvement of the relevant legal framework, 3. oversight of the implementation of the legal framework.

Some of the important short-term NCIC activities shall be: 1. creation of sectoral and intersectoral measures for identification of criticality levels, 3. definition of protection measures to be implemented depending on the identified criticality level, 3. implementation of the procedures for identification of a criticality level.

Regardless of its future structure, NCIC will perform its duties through the CIP Committee (intersectoral working group). The Committee members will have the role of security coordinators for CI. The main task of the committee would be the verification of documentation and procedures created by the NCIC. Such approach implies that NCIC has the mandate for the engagement of relevant professional institutions and experts with the purpose of creation of CIP related documents and procedures. The work of the committee would not require significant additional funds. On the other hand, for creation of the mentioned documents and procedures NCIC should obtain necessary financial means from the state budget.

RECIPE project partners agree that functionalities of NCIC both in Serbia and in Croatia should be clearly defined as the first step, as afterwards it would be easier to decide whether it should be established within an existing institution or as an independent body. The partners agree that NCIC must have both consulting and research aspect. Instead of simple information collection and distribution, the Centre needs to have capacities for their analysis, as well as capacities for oversight over the implementation of the Law on CI at the national level. As a good example and

potential model for the future NCICs in the region, the partners recommend the UK Centre for Protection of National Infrastructure http://www.cpni.gov.uk/ .

8. CONCLUSION

In the Republic of Serbia, the process of identification, prioritization, protection, resilience and legal regulation of the field of CI is at the very beginning. RECIPE project intends to provide assistance to the lawmakers and relevant state bodies to regulate this field in an easier and more efficient manner, through consultations and exchange of experience and good practice with the partners from the EU member states.

The creation and adoption of the Law on Critical Infrastructure is announced for 2016, and the results of the RECIPE project will be taken into account during the writing of its draft. Certainly, the existing problems and challenges will not be resolved with passing of this law. The CI sectors and facilities identification and prioritization, adoption of methodologies for the CI risk assessment, PPP in the field of CIP, exchange of classified data, as well as prospective establishment of the National Critical Infrastructure Centre are the main, but not the only challenges that lawmakers, CI owners and operators and other stakeholders in Serbia will face in the coming period. These challenges may be overcome by passing of the bylaws, adoption of amendments and harmonization of other relevant laws (e.g. Data Secrecy Law, Law on Public-Private Partnership, Law on Defence etc.), by education and raising awareness of CI owners and operators, by adoption and implementation of national and international standards and improved cooperation with academic institutions.

The project partners argue that CI sectors should be identified as 'narrowly' as possible, as the national capacities and state budgets are limited. For instance, the Republic of Croatia has identified eleven CI sectors, which is, in opinion of Croatian experts, too many for efficient protection. Consequently, the process of prioritization has caused much disagreement between CI owners and operators on one side, and lawmakers on another. On the other hand, the Directive 114/2008/EC identifies only two European CI sectors – energy and transport, which is arguably a too narrow classification to be applied for the national CI sectors. Therefore, a balanced solution between these two approaches should be found.

The establishment of PPP mechanism in the CI protection and resilience arena is of particular importance, as during the process of liberalization more CI facilities will pass into private ownership, whilst private security sector plays an increasingly important role. Long-term arrangements of private security companies in the contracts related to CIP and legal regulations on mandatory protection of facilities that private CI owners and operators must comply with are the key points of this issue.

The question of classified data sharing in the CIP system is a complex one and will need to be considered carefully by all stakeholders. An efficient and secure system of sensitive and classified data exchange needs to be established, with the accent on the 'horizontal' approach (exchange of data between sectors and CI systems), in comparison with the 'vertical' one, which is still prevalent, but is not quick and efficient enough. Furthermore, the provisions on the exchange of classified/sensitive data need to be incorporated in the future Law on Information Security, Regulation on Encryption Protection, and in the Cyber Security Strategy.

For purpose of the efficient implementation of the future Law on CI, as well as for collection, processing and analyses of the CIP related data, the partners propose establishment of National Critical Infrastructure Centre, modelled after the UK Centre for Protection of National Infrastructure. In Serbia, this centre could function either within the Sector for Emergency Management, as an independent organizational unit of the Ministry of Interior, or even as an independent Government agency.

This National Standpoints draft document on CI protection and resilience in the Republic of Serbia was submitted for review to all relevant stakeholders for comments and possible amendments. The final version in English language is submitted to the donor, i.e. European Commission, and will be used as the material for joint workshops at which the participants will exchange experience and good practice, which should consequently result with Guidelines/Instructions for better and more efficient CI management.

ANNEX IV

RECIPE 2015 SERBIA WORKSHOP EVALUATION REPORT

A. INTRODUCTION

The joint workshop of project partners, Serbian and international CIP experts was held on 13th of October 2015. in Belgrade, Republic of Serbia, at the premises of the Institute for International Politics and Economic. The aforementioned activity within the RECIPE 2015 project framework was marked as Task ID „C“, Task Title „Exchange of Experiences and Best Practices“, Action C.1.

At the workshop the following participants were present:

Representatives of the Project coordinator – National Protection and Rescue Directorate (DUZS):

Mr. Robert Mikac

Ms. Maja Matijaš Filipović

Ms. Ivana Cesarec

Ms. Kristina Mulić

Ms. Andreja Zrilić

Project Partners:

Faculty of Security Studies (FB):

Mr. Zoran Keković

Mr. Želimir Kešetovic

Ms. Jasmina Gačić

Mr. Vladimir Ninković

Ms. Mirjana Stekić

Veleučilište Velika Gorica (VVG):

Mr. Alen Stranjik

Mr. Ivan Nađ

Mr. Nenad Petrović

Mr. Marko Toth

Swedish Civil Contingencies Agency (MSB):

Ms. Therese Wikström

International experts:

Mr. Hannu Hernesniemi and Ms. Katri Liekkilä (National Emergency Supply Agency), Finland

Mr. Marc van der Velde (Ministry of Security and Justice), the Netherlands

Mr. Denis Čaleta (Institute for Corporate Security Studies) (ICS), Slovenia

Mr. Sandro Bologna (Association of Critical Infrastructure Experts), Italy

Mr. Alessandro Lazari, Joint Research Centre, European Commission

Mr. Zdenko Adelsberger, (Bluefield ltd.) - Croatia

Mr. Marjan Marjanović (Security Guard ltd.) – Montenegro

Mr. Miro Miskin (M:Tel) – Bosnia and Herzegovina

Participants from Serbia

Mr. Marko Blagojević (Director of the Government Office for Redevelopment and Flood Relief)

Mr. Goran Matić (Director of the Government Office of the National Security Council and Classified Information Protection)

Mr. Momčilo Milinović (Faculty of Mechanical Engineering)

Mr. Ozren Džigurski and Mr. Aleksandar Vukalović (members of the EU accession negotiating groups for the chapters 10, 24 and 31)

The aim of the workshop was to discuss Serbian 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 through the exchange of experience and best practice presented by the international experts. The particular attention was on the presentation of the state and development of the Kingdom of Sweden CIP system.

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

The discussion was aimed at the four main goals of the project relevant for Serbia:

1. Definition, identification and the legal regulation of the field of CI in Serbia
2. Establishment of the public-private partnership in the CIP system,
3. Establishment of the mechanisms for exchange of sensitive information/data between participants in the CIP system,

4. Setting of preconditions for the development of the National Critical Infrastructure Centre.

B. Analysis of the current situation in the Republic of Serbia

The field of Critical infrastructure is still not legally regulated in the Republic of Serbia. Therefore, the first step in the regulation of this field would be to adopt the Law on Critical Infrastructure in line with the requirements of the Directive 2008/114/ EC, thus establishing the legal framework for definition, identification and protection of national and European CI. After the adoption of the Law, it will be necessary to develop and adopt the bylaws that would provide practical solutions and criteria for identification of CI sectors and systems.

It should be added that the identification of CI will not start from scratch, as some existing legal acts give a solid starting point. In particular, the Law on Defence ("Off. Gazette of RS", no. 116/2007, 88/2009, 88/2009 - ot. Law 104/2009 - other. Law 10 / 2015) with its related bylaws should be observed. The Law refers mainly to the defence industry of Serbia, but also to other industrial and infrastructure objects, which during war, state of emergency or mobilization of the Serbian Army primarily provide the services and operations stipulated by the Ministry of Defence.

In the following steps it will be necessary to prioritize the identified CI sectors and regulate the aspects of the CIP that have shown to be particularly problematic in the European and global practice – public-private partnership (PPP) and exchange of classified information.

Key questions and issues discussed: Insight in the legal framework of the countries from which the international experts came from, and the potential to include some of their recommendations in the future Serbian CI legal framework; the international (EU) experiences related to the identification of critical infrastructure sectors and facilities at the various levels (national, regional or local) .

C. National Standpoints of the Republic of Serbia – overview

C.1. Definition, identification and legal regulation of the field of critical infrastructure in the Republic of Serbia

In order to be sure about the content and the boundaries of the CI concept, it is crucial to adopt the Law on Critical Infrastructure. The Law would establish a regulatory framework for defining, identifying, and protecting national and European CI in Serbia. In addition, its

bylaws should provide practical solutions and criteria for the identification and prioritization of CI.

The adoption of the Law on CI (or CIP) is among the obligations of the Republic of Serbia in the process of EU accession. The Action Plan for Chapter 24 for the EU accession recognizes the Ministry of Internal Affairs of the Republic of Serbia as the authority responsible for the future Law. Within the Ministry of 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 a national CIP policy.

The future Law on CI, but also other laws relevant to the CI should contain the provisions of the European Directive on the Protection of Critical Infrastructure (Directive 2008/114 / EC). In this regard, it is necessary to make amendments in the CIP related parts of the National Strategy for Protection and Rescue in the Emergency Situations and in the Law on Emergency Situations. For effective CIP and comprehensive legal regulation of this area it will be necessary to implement the existing Data Secrecy Law, which, according to some experts, exists only on paper. In addition, the Law on Information Security (the work on its draft commenced more than three years ago), the Regulation on Encryption and Cyber Security Strategy should also be adopted.

During the identification of CI sectors and facilities it would be desirable to start from international, or at least from the regional level. While many developed countries identified over ten CI sectors (including the Republic of Croatia - eleven sectors identified), it is suggested that lawmakers in Serbia should be realistic and not make a list of sectors that is too broad, taking into account the limited state budget, due to which not all identified sectors and belonging facilities could be protected in an optimal manner. The next step would be to identify CI facilities at lower levels, in addition to regional and national. CI facilities can also be identified at the city, local, and even at the sectoral level. Preliminary identification and classification of CI facilities may be done even before the law is adopted, provided the criteria and departmental sector analysis are defined.

Key questions for discussion: How are CI sectors identified in different EU countries? Are CI facilities identified only at the national level or also at the lower (regional, local) levels? Do all countries have Law on CI, or can it be regulated by strategic documents?

C.2. Public-private partnership in the field of CI resilience strengthening and protection

As the project goal in this field we identified 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.

Public-private partnership (hereinafter - PPP) is among the key factors of the CIP process. In the majority of developed countries around 80% of CI is privately owned. Although for Serbia and the Western Balkans region precise figures do not exist, that percentage is undoubtedly lower. However, the increase of the percentage of privately owned CI facilities is expected, taking into account global trends of market liberalization. In line with this conclusion, we suggested the following:

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 widen the existing legal framework related to the PPP with the following provisions:
   - the concept of critical infrastructrue should be incorporated in the Law on Public-Private Partnership, as well as the concept of PPP should be incorporated in the future Law on Critical Infrastructure;
   - Adjust the procedure of submission and approval of PPP project proposals, including small value PPPs in the CI field;
   - Involve the state bodies (in particular the State PPP Commission, comprised of representatives of various ministries, including those that will be certainly identified as CI sectors) in the monitoring and control of PPP CI related projects.
2. Taking into account the large number of CI sectors and facilities and the experience of countries that have already adopted this paradigm, it is concluded that it would be impracticable to equally protect and build resilience of all CI facilities. Private actors, primarily the owners and operators of the privately owned CIs can provide a valuable contribution to this process.

Key questions for discussion: How is the CI related PPP established in their respective countries? Is the framework formal or informal? Are there any limits to PPPs, considering the profit-driven approach of private sector?

C.3. Establishment of the mechanisms for sharing of sensitive information within the CIP system

In Serbia, the sharing and treating of sensitive and classified information is performed in accordance with the Data Secrecy Law ("Off. Gazette of RS", no. 104/2009). However, The problems that our country face 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 unclear role of the Ministry for Construction, Transport and Infrastructure, lack of skilled personnel in the Ministry to deal

with the CI issues, the lack of permanent education of managers in the field of CI and in the field of information protection, the lack of awareness of people in charge of the CI 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.

In the National Standpoints document the following suggestions are offered for overcoming the abovementioned shortcomings:

1. With a view to establish 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 of 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 intersectorial 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".

Key questions for discussion: Which CI related information should be classified? What are the best technical and ICT solutions that are implemented in the EU countries? How to encourage the participation of the private sector in the sharing of information? How can public sector support the private sector with a view to creation and development of mutual trust in this process?

C.4. Preconditions for setting up of national critical infrastructure centre

Even though the Serbian partners agree about the need of setting up the National CI or CIP centre, they conclude that it is the step that may be taken only once the previous preconditions are successfully implemented. Such conclusion was reflected in the general lack of debate among the Serbian participants at the panel discussions about this issue, as the discussion was focused at the previously presented concepts.

However, some general recommendations are given. As for its functionalities the project partners agreed that NCIC should be in charge of: 1. creation of the holistic concept of the CIP, 2. review, harmonization and improvement of the relevant legal framework, 3. oversight of the implementation of the legal framework.

RECIPE project partners agree that functionalities of NCIC both in Serbia and in Croatia should be clearly defined as the first step, as afterwards it would be easier to decide whether it should be established within an existing institution or as an independent body. The partners agree that NCIC must have both consulting and research aspect. Instead of simple information

collection and distribution, the Centre needs to have capacities for their analysis, as well as capacities for oversight over the implementation of the Law on CI at the national level. As a good example and potential model for the future NCICs in the region, the partners recommend the UK Centre for Protection of National Infrastructure

Key questions for discussion: Which are suggested minimal functions of the Centre? What are the models available for organizational positioning of the Centre within the state administration?

D. Discussion

D.1. Legal framework, criticality, threat and risk assessment – identification and prioritization of critical infrastructure

The participants agreed that the future Law (or the strategy, as some EU countries do not have particular laws on CI) on Critical Infrastructure in Serbia needs to be carefully designed as there are many bad examples in Europe. The most important thing will be to know who is in charge, i.e. who the „front desk" for the CI issues is. It should be born in mind that, taking into account the economic situation in Serbia and its need to attract foreign investments, overregulating should be avoided.

In the existing legislation in Serbia, for instance in the field of Emergency management, the principle of subsidiarity and decentralization is adopted, however many municipalities are very poor so the decentralization remains a fiction, especially during disasters and disaster recovery. In addition, there are big differences in the level of development among Serbian regions, thus they may response in a different manner. The draft Law on Minimization of Risk of Natural and Other Disasters and Emergency Management provides that competent ministries, regional and local authorities in charge of infrastructure facilities and systems of national, regional and local importance are obliged to create plans of risk minimization, critical infrastructure protection and resilience.

There are still not enough CIP arrangements on the EU level, it is mostly done on bilateral case (e.g. Finland has procurement arrangements with Estonia and Latvia, so that Finland can store oil in those countries).

There are varying experiences among the EU countries, related to the identification of CI sectors and facilities. For instance, in Sweden and the Netherlands the CI sectors (called Vital Societal Functions in Sweden) and assets are identified on local, regional and national level, whereas in Italy there has not been official CI identification and the main focus is on cyber security.

Similar differences can be observed in the field of threat, vulnerability and the risk assessment. The threats should be constantly monitored as they change, as CI assets are also continuously changing and adapting to changes. They also depend on other CIs and extend

cross borders of national states. Sweden implements 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 on national level, followed with 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.

Swedish Government commissioned the Swedish Civil Contingencies Agency, MSB, to produce a unified national strategy for the protection of vital societal functions, which was reported in 2011. The strategy was produced in collaboration with several governmental agencies, county administrative boards, municipalities, and county councils. Representatives from the private sector who own, operate or manage large parts of the vital societal functions have participated in this collaboration and process. Apart from the Strategy, the Action plan is also existing. The objective for the action plan is to concretize the strategy by initiating measures and activities that create conditions that allow for all VSF & CI to have implemented systematic safety work into their operations locally, regionally and nationally by 2020. The aim is to create a resilient society with an improved ability in VSF & CI to withstand and recover from serious disruptions.

Emergency management and work on the protection of VSF & CI is based on responsibility and cooperation between entities at different levels and in different societal areas of responsibility. The target audience for the action plan includes all entities that own or operate VSF & CI, i.e. municipalities, county councils, county administrative boards, national authorities and private sector operators.

However, the actors are experiencing difficulties in identifying VSF on different levels. FOI, Swedish Defence Research Agency, has on behalf of MSB recently conducted a study in which a number of other countries work with criteria for identifying critical infrastructure on national level. The study will be used in the continued work with criteria for national VSF. Prioritization of the facilities is done within sectors and not by the government.

In the Netherlands, the National Coordinator for Security and Counterterrorism (NCTV) identifies threats, risks and strengthens the resilience and protection of vital interests and critical infrastructure. There is no Law on Critical Infrastructure, but there are quantification criteria for criticality of infrastructure, something that is yet to be done in, for instance, Sweden. Thirteen CI sectors have been identified, which is a very high number. Criteria for criticality assessment are: economic, physical and societal impact. Dependencies between sectors and potential cascading effects must be analyzed as well, as some sectors are more interconnected than others, i.e. electricity.

In Finland National Security Strategy determines vital functions (eleven in total) which then translate into critical infrastructure, similar to Sweden.

In Italy the Directive 2008/114 was implemented in 2011 with the Law on European Critical Infrastructure adopted in 2011, but the identification of European CIs is still not finished. The focus is on Cyber Security with the 2013 Prime Minister's Decree containing strategic guidelines for the national cyberspace protection and ICT security. The Decree intends to establish the architecture, but it is considered as too complex and confusing, with various overlapping responsibilities between ministries etc. There are two important strategic documents: National Strategic Framework for Cyber Security and The National Plan for Cyberspace Protection and ICT Security, containing concrete applications of the strategic guidelines.

D.2. Public-private partnership in the function of critical infrastructure protection and resilience

.

In Serbia, 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 Western Balkans 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 PPPs. Strategic management in companies needs to take into account the privatization trends in 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, also, has been the source of disasters in the region and globally.

Big 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 an additional problem. In addition, in some important companies and facilities (energy sector) corporate security is lowly positioned on the organizational ladder, and not recognized as important by top-management, thus does not have a say in the decision making process.

In the process of risk management PPP may encounter further obstacles, as the private owners and operators often have different perception. The state needs to define the „skeleton of basic threats/hazards" for which the CI operators will be in charge of. For complex threats the state

institutions should be engaged. The state can offer tax incentives for companies that perform security activities well.

Several examples from the EU practice were mentioned by the foreign participants. For instance, in Romania, a Serbia's neighboring country, potential private owners and operators need to notify the government about their future ownership or management of identified CI facilities, and government has two months to give its approval. In France, CI assets (the French term is vital infrastructure) are narrowed down to a number that can be protected in a satifsying manner, and then public and private sectors work together on their protection.

In Finland there are over two thousand prioritized companies with around one thousand CI experts who work together with the state institutions on their protection.
From the common experience CI operators and owners are difficult to engage. Top-down is not the best approach for PPP, as the companies will perceive it as an overregulation.

Some countries by law oblige the operators to state how they engage security companies. Private companies want to implement their business driven decisions and keep secrecy about as many information as possible. In the Netherlands, despite of the nonexistence of the Law on Critical Infrastructures, the cooperation between participants of the system is very good and is based on the principle of "networks and trust". It is based on the premises that there are win-win situations for both sides: "win" situation for government being the knowledge sharing and policy support (policies, strategies, laws), "win" situation for private sector – high degree of protection and profit. National risk assessments (NRA) are in some countries done very thoroughly, but the (private) operators have to be involved in the decision making process.

PPP can be a funnel through which results of research and development projects and activities can reach operators and owners. The EU produces a lot of research in the security field and it's difficult for everything to be implemented, so experimental capabilities are also very important for projects. National government needs to ensure that operator acts in line with the best available knowledge.

D.3. Establishment of the mechanism for sensitive information exchange in the critical infrastructure protection system

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 sharing of sensitive/classified data is regulated by the Data Secrecy Law which is not often 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.

In Croatian legislation all information related to the CI is classified, which creates a number of problems. The exchange of information can go through systems and secret channels, but which data will enter it, especially in cases involving PPP, remains unknown. According to the Croatian Law sensitive data are those data about CI that are denominated as classified in accordance with the law. In order to obtain access to it, both private and public sector personnel require security certificate, for which the procedure is very long. So, the problem arises when somebody needs to transfer the information to somebody who does not have the certificate.

In the EU security clearance is relied upon, as well as upon the security liaison officer confirmation. The classification needs to exist 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 manner. In Finland, Sweden and in the Netherlands some companies mark information with colors – "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. Netherlands' experience says that in sectors and facilities there should be designated persons in charge of information exchange and which will remain in the position for a long time, as the trust takes time to be developed.

D.4. Preconditions for the development of the national critical infrastructure centre

For Serbia, an important milestone in this regard will be the reorganization of the Office for Redevelopment and Flood Relief as the Directorate for Risk Management and Emergency Situations, which will provide support for all CIP related efforts by both private and public stakeholders.

It is believed that the establishment of a national CI centre will need to be done in at least two phases. In the first phase, a centre will not be able to answer to all CI related issues, but it should connect the business, research and government sectors. In the phase two, the wanted outcomes may be attained. There is a valuable experience from the UK and Poland, which can be used for deciding what functionalities and what organizational position in the system should be adopted.

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

E. Conclusions and recommendations for the Republic of Serbia

As the first beneficiary of the RECIPE project, Republic of Serbia is just making the first steps in the establishment of the critical infrastruction protection and resilience system. Thanks to the project partners from the Republic of Croatia and Kingdom of Sweden, but also to other international participants from Finland, Italy and the Netherlands, Serbian experts from both the private and public sector, as well as participants from Bosnia and Herzegovina and Montenegro had an opportunity to discuss the issues pertaining to the three main objectives of the RECIPE Project – public-private partnership, sharing of sensitive information and establishment of a national critical infrastructure center, but also to the education and standards implementation. The workshop showed that all these areas are mutually complementary and need to be observed as a whole.

As the results of the RECIPE project will be incorporated in the future Serbian legislation of the field of critical infrastructure, the information gathered from the presentations and discussion will be of invaluable importance. Hence, we can state that the workshops, both in Belgrade and in Zagreb have completely fulfilled the expected outcomes written in the RECIPE project „Grant Agreement". The best practice has been shared with the project partners and experts from the Republic of Serbia, the recommendations were provided and awareness on efficient solutions and existing models raised. Therefore, we can expect that Serbian legislation and solutions for the CIP system will carefully analyse various models for identification of CI sectors and assets, risk management, education of CIP experts, establishment of PPP projects, exchange of sensitive information and, potentially, for establishment of a national CI center.

Due to the poor economic situation of the Republic of Serbia, overregulation of the CI field may be a step in the wrong direction, as it would discourage the foreign investment in the CI assets. Awareness raising and benefits for the private sector would be a better approach which would encourage the private owners and operators to invest in protection and fully adhere to the standards.

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 to

the lack of SOPs and protocols. The trust between private and public sector will take time to be established, and it can be particularly problematic in cases where CI assets are in foreign ownership.

The newly established Directorate for Risk Management and Emergency Situations will at the beginning deal with all issues pertaining to CIP, but in the future this role may be taken by a separate National CI Centre. The models for the establishment of the Centre will be developed, and consequently compared and evaluated in the Feasibility study.

The Serbian project partners, Faculty of Security Studies, University of Belgrade, regard the RECIPE Joint Workshop in Belgrade as a successul event that fulfilled all expectations. Together with the results and deliverables of the previous activities, the results of the Joint Workshop will be used for legislation, PPP, sensitive information sharing and a critical infrastructure centre models which will be further evaluated in the Feasibility study, conducted within the RECIPE project.

Based on the „Grant Agreementa RECIPE 2015“, Task ID „C“, Task Title „Exchange of experience and best practice“, Action C.1., the Project Partner Faculty of Security Studies, is in charge of the writing of „Workshop Evaluation Report“ for the Joint Workshop in Belgrade.

Authors:
Dr. Zoran Keković
Dr. Želimir Kešetović
Vladimir Ninković

ANNEX V

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

RECIPE 2015 CROATIA WORKSHOP EVALUATION REPORT

A. Introduction

A joint workshop by the project partners and Croatian and foreign experts in the field of critical infrastructures (CI), was held on 15 October 2015, in Zagreb, the Republic of Croatia. The aforementioned activity within the RECIPE 2015 project is marked under Task ID "C", Task Title "Exchange of Experiences and Best Practices", Action C.1.

The workshop was attended by the following participants:

Representatives of the project coordinator – the National Protection and Rescue Directorate (NPRD): Robert Mikac; Maja Matijaš Filipović; Ivana Cesarec; Igor Cvitanić; Marijana Berket; Andreja Zrilić.

On behalf of project partners: **University of Applied Sciences Velika Gorica:** Ivan Toth; Alen Stranjik; Ivan Nađ; Nenad Petrović; Marko Toth. **University of Belgrade, Faculty of Security Studies:** Zoran Keković; Želimir Kešetović; Vladimir Ninković; Ivica Đorđević. **Swedish Civil Contingencies Agency:** Anna Rinne; Therese Wikström.

Experts from EU member coutries: Hannu Hernesniemi; Katri Liekkilä (National Emergency Supply Agency), Finland; Marc van der Velde (Ministry of Security and Justice), the Kingdom of the Netherlands; Bognár Balázs (National Directorate General for Disaster Management), Hungary; Denis Čaleta (Institute for Corporative Security Studies), Slovenia; Alessandro Lazari, Joint Research Centre, European Commission.

Participants from Croatia: Dražen Ljubić and Zvonimir Grubišić (Information System Security Bureau); Sandro Šegedin (Ministry of the Interior) - security critical infrastructure coordinator; Damir Matejčić (Ministry of Agriculture) - security critical infrastructure coordinator; Zdenko Adelsberger, (Bluefield d.o.o.) – project consultant; Mladen Ružman (HEP d.d.); Boris Čavrak – expert in the field of energetics.

The project-based aim of the workshop was to discuss Croatian national standpoints formed at the national panel discussion in order to fill certain voids in the critical infrastructure system through the exchange of experience and good practices presented by the foreign experts. Special attention was to be paid to the current state and development of the critical infrastructure protection system of the Kingdom of Sweden.

The expected results of the workshop 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.

B. Analysis of the existing situation in the Republic of Croatia

During 2013, the Republic of Croatia enacted the Critical Infrastructures Act, Ordinance on methodology for critical infrastructure operation risk analysis and Decision on determination of eleven (11) 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 as the system coordinator 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 (defined by the Act), 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 Act also stipulates that central government administration bodies appoint a security critical infrastructure coordinator and his deputy for each critical infrastructure sector in its purview, while owners/managers of critical infrastructures are required to 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 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, even though the deadlines given in the Act passed. Therefore, the critical infrastructure protection and management system in the Republic of Croatia is in an initial stage of its development.

Key questions and areas which needed to be discussed during the workshop related to the following: Insight into the normative framework of countries from which foreign experts came and can the present normative framework of the Republic of Croatia successfully meet the current challenges in the critical infrastructure protection and strengthening of their resilience? What are the experiences in implementation and effectiveness of solutions that include the identification and determination of critical infrastructures at the local, regional and national level, compared to Croatian legislature which prescribes the identification and determination of critical infrastructures solely at the national level?

C. National standpoints of the Republic of Croatia – cross-section

C.1. Public-private partnerships in the field of strengthening of resilience and critical infrastructure protection

The objective of the project in this area is to establish a platform for public-private partnership which shall provide logic and principles for the following areas of interest: cooperation concept, projects, security and improvements to the normative framework.

Based on the conclusions in the National standpoints, the public-private partnership imposes itself as one of significant principles of the strengthening of resilience and protection of critical infrastructures. Accordingly, to achieve the most effective application of benefits of such interaction between the public and private sector, the following considerations need to be applied:

1. Considering the significance of critical infrastructures for the national and public security and for the stability and functioning of the state, it is necessary to broaden the existing legislative (normative) framework in the area of public-private partnership, namely:
   - The area of critical infrastructures should be a part of the Public-Private Partnership Act, and public-private partnership should be a part of the Act on Critical Infrastructures;
   - The procedure of submission and approval of public private projects, including small value public private partnerships, should be adapted in the area of critical infrastructures.
   - Competent government administration bodies having sectoral competence for individual critical infrastructures should be included in monitoring and supervision of public private partnership projects.
2. State administration body competent for coordination of critical infrastructures risk management activities, in cooperation with government administration bodies having competence in sectors of the critical infrastructures and owners/managers of the critical infrastructures, develops a plan and proposal of public-private partners projects

whose objective is to increase resilience/security of those critical infrastructures, following the prioritisation of the critical infrastructures.

3. When planning public-private partnership projects whose objective is to increase resilience and protect critical infrastructures, the possibility to use European structural and investment funds should be taken into consideration, especially in the part pertaining to public-private partnerships.

Key questions to which we wanted answers were: How to establish the mentioned partnership in the observed countries? Is the framework of the mentioned formal or informal? Having in mind that the private sector is primarily profit-oriented, in what way does the public sector suggest areas of cooperation and in which areas?

C.2. Establishment of mechanisms for exchange of sensitive information/data among participants in the critical infrastructure protection system

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. It is therefore necessary to undertake additional activities in order to increase efficacy and security in exchange of information related to critical infrastructures.

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

In the course of its activities carried out to date, the RECIPE project has recognised the following needs:

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

Based on the aforementioned, the conclusions of the national standpoints are that it is necessary for the following to be performed:

1. Implementation of the Information Security Management System for all owners and operators of critical infrastructures.

2. In order to establish the efficient information management in the area of critical infrastructures management and harmonisation of procedures for the exchange of that information among stakeholders, it is necessary to develop a model of efficient information management in the area of critical infrastructures management.
3. Establishment of a cross-sectoral working group of representatives of central state 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 Point 2.
4. Security critical infrastructure coordinators and advisors for information security of central state 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 Act on Information Security) to the owner of the data/information.
5. The security coordinators and advisors for information security of competent central state 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 Act on Information Security.
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.

Key questions in this part, relevant to the enhancement of the system in the Republic of Croatia, referred to: Which information/data is necessary to be marked with levels of sensitivity in the exchange among the shareholders of the critical infrastructure system? Which technical and IT solutions are applied in countries that workshop participants come from? How can the willingness of the representatives of private sector in the exchange of sensitive information be ensured? What benefits does the public sector offer or can offer to the private sector for the purpose of building and developing mutual relations and trust in this process?

C.3. Establishment of preconditions for development of the national Centre for critical infrastructures

In the summary of this section, the authors have decided to emphasise the need to develop a conceptual model of comprehensive protection and management of critical infrastructures in the Republic of Croatia whose central point will be the National Centre for Critical Infrastructures. The project needs to define prerequisites for establishment and development of the Centre 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.

The panel discussions showed that there are several possible models of establishing the stated Centre in the Republic of Croatia, for instance:

- National Centre for Critical Infrastructures as an organisational unit in the NPRD,
- National Centre for Critical Infrastructures as an organisational unit in another central state administration body,
- National Centre for Critical Infrastructures organised within services and offices of the Government of the Republic of Croatia,
- National Centre for Critical Infrastructures as an independent state administration body.

Within the RECIPE project, it was recognised that the Centre for Critical Infrastructures should be tasked with the following:

a) Gathering, analysis and exchange of information among shareholders 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.
b) Proposing and drafting regulations in the area of critical infrastructure protection.
c) Supervising 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 state government administration bodies
e) Organising education and exercises in the area of critical infrastructure protection, in cooperation with other shareholders in critical infrastructure protection.
f) Establishing and functioning of a central point for planning, preparedness and responses in emergencies in the area of critical infrastructure protection.
g) Coordinating and monitoring public-private partnerships projects in the area of critical infrastructure protection.
h) Establishing and functioning of the contact point for European critical infrastructure.

In this section the following conclusions are determined, which the project partners from the Republic of Croatia need to elaborate further and search for solutions which can be implemented:

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 personnel.
3. Suggest necessary 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.

Key questions significant for the further development of the model of the National Centre for Critical Infrastructures are: What is the recommended minimum of the functionality of the Centre? Even though we are aware of the differences between countries, what are the recommendations for the organisational placement of the Centre within the structure of the state administration? Should the establishing of the Centre be approached in phases or should we seek a single solution?

D. Discussion on the main project aims based on the presentations of foreign experts conducted

D.1. Normative framework in strengthening of resilience and protection of critical infrastructures - discussion

All workshop 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 shareholders of the system. It was noted that certain countries such as the Republic of Slovenia and the Kingdom of the Netherlands do not have an Act on Critical Infrastructures, but they have certain critical infrastructure sectors, identified and designated critical infrastructures, with the properly organised system of their protection. The example of the Republic of Italy shows that they do not have a clearly defined national normative framework for determining national critical infrastructures, but – on the other hand – they have legal provisions which envisage the identification, determination and protection of European critical infrastructures.

The need has already been recognised for the Republic of Croatia, and the discussions during the project and the workshop have 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 already in this phase of implementation enabled the Croatian representatives to gain new insights, best practices, and the course of development of the critical infrastructure area outside of Croatia. Certain important notions such as public-private partnerships in the critical infrastructure protection and the area of national IT critical infrastructures 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 in the beginning of October 2015, incorporating knowledge and experience gained also during the RECIPE project.

Although the Republic of Croatia is successfully building the strategic and normative framework in the area of critical infrastructures, the challenge of implementing the stipulated provisions in practice has been recognised. Therefore, the added value of the RECIPE project is that it enabled the exchange of opinions among experts in the area - how and in what way can certain challenges be overcome, how to restart activities that stopped and how to additionally encourage those activities that are in progress. During the joint workshop in Belgrade and in Zagreb, representatives of the Republic of Croatia heard and received more information about a variety of practical solutions, some of which will definitely be built in the system of strengthening the security and resilience of critical infrastructure.

For establishing a normative framework, it is important to consider the space and time context, the mission and vision of each country, serving as a basis for setting up organisational implementation models. As the presentations of all foreign experts started with the overview and aims of public and national security systems and continued towards to project goals, it is necessary to emphasize certain sections of the presentations by the representatives of the Kingdom of Sweden (project partner) and pay special attention to the overview of the development of the critical infrastructure protection system in the Kingdom of Sweden.

The Swedish emergency preparedness system is based on the principle of duty and responsibility of everyone for their activities and the need for mutual cooperation in order to minimise vulnerabilities and increase capacities for action during emergencies. The area of

our interest, based on the overview of the situation in the Kingdom of Sweden, has proven to be narrower, in relation to the situation which is in Sweden considered more broadly and more comprehensively than in the Republic of Croatia and in most other countries of workshop participants. Accepting such an approach represents added value within the project. Their area of interest and activity is based on protecting 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, globalisation, privatisation, efficiency, timeliness etc.) are taken into account when considering challenges. Such a broad picture and consideration of the areas of interest is most definitely wider than the current discourse in the Republic of Croatia and will serve as a signpost, indicating the direction that needs to be taken in the future, once the conditions are 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 prioritisation of sectors has been determined. This is the area in which the Republic of Croatia in the continuation of cooperation during the project can gain valuable experience and implement them in the medium term in its own critical infrastructure protection system.

The workshop proceeded to present and explain the relationship among the social sector, vital social functions and critical infrastructures. The aforementioned presents a good and logically well set up system of conceptual and organisational units. During the workshop, it sparked great interest of all participants, which is exactly the added value of the RECIPE project – exchange of experiences and best practices, not only among project partners, but also among all interested experts, countries and European Union as a whole.

The action plan in the stated area contains the time component for the implementation of key programme processes which need to be realised by 2020. The two main processes are: “Measures for knowledge enhancement” and “Activities for the implementation of systematic safety”. Both processes have sub-processes or pillars in the implementation. “Measures for knowledge enhancement” contains: “Grounds and regulations”; “Research”; “Training/education”; “Exercises”. “Activities for the implementation of systematic safety” contains: “Sector plans”; “Experience feedback”; “Robust procurements”; “Components of a systematic safety work”; “Criteria for national critical infrastructure”. The stated structure is the result of the long-term successful work of the critical infrastructure experts in the Kingdom of Sweden and presents a very interesting model for the Republic of Croatia. Given the time available during the workshop, certain pillars were discussed to a larger extent (such as “Training/education”; “Exercises”; “Experience feedback”; “Criteria for national critical

infrastructure") and the continuation of cooperation in the exchange of knowledge and experience in this area was agreed.

The final segment of the presentations by the representatives of the Kingdom of Sweden related to the identification of vital social functions through risk and vulnerability analysis and to the presentation of a case study involving the "Styrel" company, responsible for the "management of electricity". The stated segment also aroused great interest of all participants of the workshop and provided guidelines on how to continue developing the system of strengthening of resilience and protection of critical infrastructures in the Republic of Croatia.

D.2. Public-private partnerships in the field of strengthening of resilience and critical infrastructure protection - discussion

Swedish experience in cooperation within public-private partnership is good, but with certain challenges on both sides. Croatian representatives are particularly interested in the aforementioned and will devote special attention to this during the planned visit to the Kingdom of Sweden. In Finland, there are more than two thousand prioritised companies in the system. Considering the fact that there are around a thousand experts on critical infrastructures, the Finnish concept is based on the "seven sectors and pull system". The section relating to the developed model of financing activities for the needs of the critical infrastructure protection system was particularly important. The Kingdom of the Netherlands does not have the Act on Critical Infrastructures, but they function very successfully even without it. They have been determined 13 sectors in which it is possible to identify and determine national critical infrastructures, and they have prescribed the quantification of criteria for determining critical infrastructures. This is something that project partners from the Kingdom of Sweden and the Republic of Croatia, who work on the aforementioned, have yet to do. The Dutch experience is ultimately very significant to all project partners. Despite the nonexistence of the Act on Critical Infrastructures, the cooperation among the shareholders of the system is very good and is carried out on the principle "networks and trust" (basic principle is "win-win situation"). Hungary has ten critical infrastructure sectors, half of which have been analysed. Within them, a little over a hundred facilities, networks or systems which represent the national critical infrastructure have been identified and designated.

During the presentations of the experiences of European countries, the successful French model of public-private partnership in the area of strengthening of resilience and critical infrastructure protection was mentioned, as well as the activities of the European Commission which are carried out in the stated area.

For the basis for the development and attracting the private sector as an interested partner in this area, it is recommended that the cooperation be built on the platform of "Business

continuity planning", because the key question from the position of the private sector is: what is the direct benefit from the partnership for them. Several very concrete suggestions were given about the direction that the public sector should take in order to stimulate the interest of the private sector for the joint cooperation, such as: provision of knowledge, experience and guidance; explanations of and enhancements of elements of the information system and risk and threat warning system; advising on standardisation and best equipment according to information available to the public sector from the cooperation with other countries, international organisations 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 standardised questionnaires to private companies; and offers for joint education, trainings and exercises.

D.3. Establishment of mechanisms for exchange of sensitive information/data among participants in the critical infrastructure protection system - discussion

The discussion was very dynamic and productive. Many different opinions were stated, some of which will be very important for further development of this area in the Republic of Croatia. The questions were raised whether there is a need in the Republic of Croatia to establish an information network for the exchange of sensitive information among shareholders of the system due to a series of facts which are not immediately apparent when thinking about something like that, such as: accreditation of such network, the issues of industrial security, the manners in which information circulate among all shareholders etc. These questions are important particularly because there are countries which, despite the existence of the information networks, still use the official letter mail exchange system. In this part it was noted that a country like the Republic of Croatia which starts the setting up of all functionalities of the system should first consider the format of the information that they want shared, paying less attention to the confidentiality levels of these information. It was also noted that the ISO international standards in the area of the exchange of sensitive information are currently being developed globally, and it is necessary to consider how much of that can be applied in each country. During the discussion, opinions were expressed that the protection of sensitive information, significant for the issues of public and national security, is mostly addressed. On the other hand, the need to protect business information, in which the business sector is particularly interested, is not emphasised enough. Within this context, it was pointed out that the Republic of Hungary owns special software for the exchange of sensitive information among all shareholders of the system.

D.4. Establishment of preconditions for development of the national Centre for critical infrastructures - discussion

Representative from the Republic of Hungary presented the functioning of the National centre for critical infrastructures and invited project partners to visit the Centre in Budapest, in order to be able to provide a better insight into Hungarian solutions and the direction their system is taking. Project partners thanked the representative for the invitation and will accept it, primarily because such cooperation presents added value of this project.

Workshop participants exchanged their views on the best location for the National centre for critical infrastructures.

E. Workshop conclusion and recommendations for the Republic of Croatia

All significant changes require time, 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 on it.

Workshops that took place in Zagreb and in Belgrade 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.

In this phase of the project it is visible that the normative framework of the Republic of Croatia does not suffice for considering and dealing with all challenges that are present / yet to come. In this respect, the presentations and discussions during the workshop fully met the expected results from the "Grant Agreement of the RECIPE project" in particular: "best practices shared", "recommendations provided", "awareness on more efficient solutions raised". The amendments, further development and harmonisation of the normative framework are on-going tasks of the holder of the authority and responsibility within the system, rendering the experience gained at the workshop very important.

It also needs to be noted that, because of the contacts, cooperation and joint activities of the project partners and invited foreign experts, representatives of the Republic of Croatia received additional confirmation of the validity of the current drafts and proposals in the area of quantifying criteria for identifying national critical infrastructures, as well as for identifying the first national critical infrastructures. The stated activities will be implemented over the course of the RECIPE project, which we already at this stage consider to be of great assistance for the Republic of Croatia, and a success.

With regards 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 will try to strengthen the legal provisions of the critical infrastructure area in the Public-Private Partnership Act, as well as the public-private partnership in the Act 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 shareholders 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 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 was adopted to investigate the possibility of using "HITRONet" communication network, which serves to connect different public law 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 the 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 organisational approaches in the National standpoints of the Republic of Croatia, two were deemed as the most appropriate ones during the workshop: Centre as a body of the Government of the Republic of Croatia, and the Centre as an organisational unit within the NPRD. Both proposals will be elaborated in more detail in order to serve as foundation for the development of models and their comparison in the Feasibility study which is an important part of the RECIPE project. 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.

In conclusion, the workshop in Zagreb fulfilled all its goals and justified the participants' expectations. All participants gained new knowledge, saw best practice and successful solutions in other countries, shared experience on different problems in the implementation of

certain parts and in so doing gained valuable insight into which challenges require specific attention.

Croatian project representatives from the National Protection and Rescue Directorate and the University of Applied Sciences Velika Gorica deem the workshop highly successful.

Based on the "Grant Agreement RECIPE 2015" under Task ID "C", Task Title "Exchange of experience and best practice", Action C.1., Project coordinator, the National Protection and Rescue Directorate, is responsible for writing the "Workshop Evaluation Report" from the joint workshop which took place in the Republic of Croatia.

Drafted by:	**Agreed by:**	**Approved by:**
Maja Matijaš Filipović Ivana Cesarec RECIPE Project Assistants	Robert Mikac RECIPE Project Manager	Jadran Perinić, PhD Director General of the NPRD

ANNEX VI (1-2)

FEASIBILITY STUDY OF THE MODEL OF CRITICAL INFRASTRUCTURE PROTECTION IN THE REPUBLIC OF CROATIA

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

Project is funded by the Directorate-General for Humanitarian Aid and Civil Protection (ECHO), 2014.

Dr. Denis Čaleta, Aljoša Kandžič

Institute for Corporative Security Studies, ICS-Ljubljana

Date: 13. JANUARY 2016

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

CONTENTS

PROJECT SUMMARY ……. 3

1 INTRODUCTION ……..... 5

1.1 The purpose of the study and expected results…… 7

1.2 Methodology ……..... 8

1.3 Development of the national centre for critical infrastructure of the Republic of Croatia …… 9

1.4 National and EU legal framework in the project specific area……. 10

1.5 Compliance of the project/project goals with strategic documents and strategic objectives of the Republic of Croatia and with EU documents …… 11

1.6 Socio-economic cost-benefit analysis ……... 14

2 ANALYSIS OF SOLUTION/MODELS FOR THE REPUBLIC OF CROATIA ……..... 16

2.1 Proposal of NCCI model …….. 16

3 ANALYSIS OF THE BASIC BUSINESS PROCESSES IN THE NCCI…… 26

4 ESTABLISHING A SYSTEM OF SENSITIVEDATA EXCHANGE IN CRITICAL INFRASTRUCTURE PROTECTION ……... 46

5 A MODEL OF PUBLIC-PRIVATE PARTNERSHIP IN CRITICAL INFRASTRUCTURE PROTECTION…… 51

6 ANALYSIS OF PROPOSED RESOURCES NECESSARY FOR IMPLEMENTING PROPOSED SOLUTIONS IN THE PROJECT AND FINANCIAL ANALYSIS……. 58

7 RESULTS AND CONCLUSION …… 60

PROJECT SUMMARY

The drafters of the study of RECIPE 2015 project have, in accordance with the objectives and planned results, prepared a proposal of the model of critical infrastructure management in the Republic of Croatia. The barycentre of the model is focused on three key areas, namely the establishment of the National Center on critical infrastructure, the establishment of a system for key information exchange and the model of public-private partnership in critical infrastructure protection. The three main areas are set out in detail by the processes and sub-processes that are planned for the realisation of the main objective. Through the feasibility study, we evaluated in details whether the planned processes and tasks are feasible regarding the legal-formal environment and other factors of influence. Each process has been analysed through SWOT analysis and evaluated through the positive and negative factors that could affect the likelihood of its practical implementation. The analysis also contains in all parts an indicative financial assessment of the feasibility of the project. In the conclusion of the feasibility study, all proposals that will make the feasibility of the set project easier are presented.

The methodological framework of the feasibility study of the proposed model to establish a system of critical infrastructure protection of the Republic of Croatia is based on an interdisciplinary approach of assessment of the proposed model. Through various methods, among which we highlight the methods of analysis, synthesis, deduction and induction and the historical method, the suggested solutions of the model of the establishment of critical infrastructure management in the Republic of Croatia were evaluated. The analysis of the individual components of the key processes in the field of critical infrastructure has also allowed a set of indicators that may serve to the operators in the later practice as a proper basis and assistance in the evaluation of the implementation of the proposed model into the direct practical social environment. Through the method of expertise we have, with the involvement of all of the above methods provided, taken into consideration also the direct good practices and years of experience in setting up systems of critical infrastructure protection in the various projects within individual countries in transition in the region.

The feasibility study of the foreseen model of critical infrastructure protection in the Republic of Croatia points to the fact that it can be implemented in all the foreseen steps. Structurally

the study needs to be concretised in some parts in more detail. This will of course be affected by the decision of the competent decision-makers on which suggested solutions they will decide. Below, the mentioned solutions will be concretised and further analysed from all angles. The biggest shortcoming of the proposed model is an estimate of the financial resources that will be necessary to provide for the realisation of the proposed. This is partly understandable because at this stage the model defines different solutions, which will be with the appropriate choice of one of the proposed options later also concretised, including the foreseen resources.

NCCI will in any event constitute a breaking point that will, by taking the right decisions and actions, represent an important step towards the relevant systemic regulation of CI protection. The proper functioning of NCCI will provide a suitable platform for guidance, assistance, exchange of good practices, counselling and control over the measures taken at different levels of the system of CI protection. This support offered by the NCCI on the one hand to the strategic management (the Government of the Republic of Croatia and the Paliament Republic of Croatia with its committees) in the public sector, as well as to the operators of CI in the private sector, will bring added value, which will be reflected in the quality of decisions, a better understanding of the situation and issues, a higher level of awareness and, finally, in the increased financial resources to ensure the effective functioning of the system of CI protection.

In the information age of rapid and secure transmission of data, the awareness of the strategic structures in the public and private sphere will play an important role also in establishing a system for the exchange of key information in the field of CI. All three main objectives which have been set in the RECIPE 2015 project are closely intertwined, and are in its implementation in a strong relationship of interdependence. It is necessary to strive to the greatest use of existing information facilities available to the state administration in the field of classified information protection, and to systemic upgrading of a specific part of the software and hardware to the existing IT backbone.

It is difficult to assess whether the well-functioning model of public-private partnership is a need or the result of a properly functioning system of CI protection. By recognising that an increasing proportion of CI passes into private ownership, a good cooperation between the public and private environment will play an even more important role in the future. A proper awareness of strategic leadership in both systems should result in pursuit of common objectives in the direction of positive factors that are brought about by such cooperation. In an era of scarce resources, working on major projects is the only one possible. Participation in

joint projects, including in the framework of EU resources, however, will further strengthen this cooperation and put it on stronger foundations of good practices and experiences gained in this process.

The political will and determination to establish and systematically regulate this important area of critical infrastructure in the Republic of Croatia remains the main factor for the realisation of the solutions of RECIPE 2015 project. In the end it is necessary to clearly define that the Republic of Croatia has laid solid foundations of the system of CI protection. The legal framework and the role that, brought about in this context by NPRD with the national coordinator for CI, delivers positive results. The RECIPE 2015 project is a good opportunity and gives the right bases to upgrade the system for CI protection. The Republic of Croatia will thus become an example of good practice, which will be applied to other countries in the region, especially the candidates for accession to the EU.

1 INTRODUCTION

The creation of an appropriate system of critical infrastructure protection constitutes an extremely demanding task for any country. Critical infrastructure 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. The complexity of the security environment and threats that arise for the functioning of this infrastructure put the state, its bodies and operators themselves in front of an extremely challenging task. 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 has occured in the EU as a term in the last twenty years. Terrorist threats, cyber-risk and natural disasters have set the need for continuity of critical infrastructure in the high priorities of the state regulation. Of course, it is necessary to realise that the system approaches of regulating that area are different from country to country. This diversity of 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 Croatia belongs to the group of countries where the organisation of the state and legal order stems from the European

continental tradition. In this context, the state represents a very important and central place for the regulation of relationships in terms of the authorities and responsibilities of the institutions for regulating individual social processes. Managing and ensuring the continuity of critical infrastructure certainly belongs among them. Certainly it cannot be said that the Republic of Croatia has no 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 a 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 the Republic of Croatia has no experience in the field of the protection of key facilities, institutions and processes that are today terminologically defined as critical infrastructure. In this work not only in the Republic of Croatia, but in the majority of transition countries it has always come mainly to inadequate understanding of the term critical infrastructure and the process itself, which it brings together in its 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 in the direction of a market economy, in the extent of stakeholders that are important for the effective operation of the system of critical infrastructure, private capital appeared, which through the ownership in companies which manage critical infrastructure is becoming one of the key factors. This represents that one additional moment, which is crucial for the perception of changes in the situation from the system which operated 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 stakeholders understand the positive aspects of the regulation of the system of critical infrastructure protection, and are from this point ready to invest the necessary efforts and other resources in building this system.

In this stage of development in the Republic of Croatia, the level of awareness and understanding of the importance of uninterrupted operation of critical infrastructure and of the process itself covered by critical infrastructure, is a necessary factor as a relatively new concept in social relations. However, it should be emphasised immediately that the Republic of Croatia has made significant and important steps in the field of critical infrastructure protection among the countries in the region. The country adopted the Law on the protection of critical infrastructure, which provides an adequate legal basis for the development of comprehensive and systemic approaches of critical infrastructure protection. Of course, the adopted law is by itself not a sufficient guarantee for the success of the system of critical inftrastructure. The practical implementation of its provisions is of particular importance. A wider social perception is also important that the critical infrastructure protection and the ensurance of its continuous operation is an important goal not only in the narrow domain of individual state agencies or operators of critical infrastructure, but it is the task of the whole spectrum of different institutions, in both public and private environments. For the construction of such an approach there is a need to ensure a strong and functioning public-private partnership.

It is precisely because of the complexity of critical infrastructure protection in this context necessary to highlight the importance of coordination. This arrangement requires both procedural as well as an organisational dimension, which is reflected through the appropriate involvement of the National Centre for Critical Infrastructure into the structure of state administration. However, this alone is not enough, because the mentioned institution should constitute a central place in the Republic of Croatia, which will, in addition to the organisational and coordination requirements, implement also an appropriate environment for the exchange of good practices and experiences. This will substantially contribute to strengthening the system of public-private partnership between state institutions and operators of critical infrastructure, which in the majority result from the economic environment. A well organised system of the exchange of senstitive information relevant to the effective critical infrastructure protection certainly represents an upgrade of this process. The current solution, when the State National Protection and Rescue Directorate (NPRD hereinafter) was determined for the central state institution, has not proved to be entirely appropriate. The decision was more and less bureaucratic without appropriate additional resources (personnel, financial and organizational). Some important changes should be implemented in the low and additional resources should be put in NPRD. For this reason the implementation of project

RECIPE 2015 solutions will upgrade role and position NPRD as a central state institution for critical infrastructure protection.

1.1 The purpose of the study and expected results

The drafters of the study have in accordance with the objectives and the intended results prepared a proposal of a model of managing critical infrastructure in the Republic of Croatia. The center of gravity is focused on three key areas, namely the establishment of the National Center for Critical Infrastructure, the establishment of a system for the exchange of key information and the model of public-private partnership in protecting critical infrastructure. The three main areas are hereinafter set out in detail by the processes and sub-processes that are planned for the realisation of the main objective. Through the feasibility study we will evaluate in detail whether the planned processes and the tasks resulting are feasible regarding the legal-formal environment and other factors of influence. Each process will be analysed through SWOT analysis and evaluated through the positive and negative factors that could affect the likelihood of its practical implementation. The analysis will in all parts include also the financial assessment of the feasibility of the project. In the conclusion of the feasibility study, the proposals that will enable an easier implementatuion of the project will be presented.

1.2 Methodology

The methodological framework of the feasibility study of the proposed model to establish a system of critical infrastructure protection of the Republic of Croatia is based on an interdisciplinary approach of assessment of the proposed model. Through the method of deduction, we checked the proposed solutions according to the wider social processes. In the following part the method of induction was used, in which a concrete solution was analysed in the direction of placing conclusions and their impact for a further understanding and the response of the wider social environment, especially the institutions of the state and operators of critical infrastructure, to the proposed concrete solutions.

By the method of analysis, we dissected the individual components of the proposed model and analysed the individual processes and factors. The analysis of the individual components of the key processes in the field of critical infrastructure has also allowed to set certain indicators that can, in practice, later serve the operators as a proper basis and help in the evaluation of

the implementation of the proposed model into the direct practical social environment. By the method of synthesis we then ensured that all the essential findings of the individual parts of the process were combined into a whole and evaluated from the perspective of the feasibility and effectiveness of the overall operation of the proposed model. Of course, in the feasibility study, we could not avoid the comparative historical method, since the historical dimension of the development of each company is one of the key determinants to understand the situation and the consequences of the company's development in the Republic of Croatia and of course the current regulation of relations in the field of critical infrastructure protection.

Through the method of expertise we have, with the involvement of all of the above methods, also considered the direct good practices and our own years of experience in setting up systems of critical infrastructure protection in the various projects within individual countries in transition in the region.

1.3 Development of the national centre for critical infrastructure of the Republic of Croatia

In the introduction, it should be noted that the establishment of the model of the public-private partnership is a key dimension for the success of establishing a comprehensive and effective system of critical infrastructure protection in each country but also in the Republic of Croatia. Without establishing this cooperation all attempts are doomed to low-level performance, and often non-systemic measures which bring their increase of the need to the resources invested. The result of such an approach through clearly established experiences in several cases is lower than expected. However, an analysis of this system will be specifically made in the third part of this study.

The next fact, which is very important in the introduction of the analysis of this part of the model, is the role of the state. The state represents the central point in any system and the motor in ensuring an effective system of critical infrastructure protection. The state's biggest interest is, in fact, that critical infrastructure, irrespective of which ownership structure the organisation that manages critical infrastructure is currently in, operates continuously, thus ensuring the smooth functioning of the community. From this perspective, it is necessary to put the understanding of the situation and the measures into raising of awareness and proper understanding of the importance of critical infrastructure in the strategic management of the state and its institutions. The proposed model of "top-bottom" approach is the most appropriate at this time, as the country has to take with its organisational levers significant

legal and substantive steps for the final establishment of an effective model of critical infrastructure protection. This 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 determining the criteria for determining critical infrastructure in specific sectors. In the comparative practice, because of the different views, understanding of the importance of critical infrastructure, and not least because of partial interests of individual organisations and also state institutions (ministries), here came the biggest tensions that accompanied by inadequate management of this process endangered the functioning of the entire system of critical infrastructure protection in the country. This position could bring about significant delays in the development of a system of critical infrastructure protection, which had the effect of undermining the normal functioning of the wider community, which was in the situations of the need of continuous operation of critical infrastructure directly affected.

The drafters of the Croatian model have derived from the current regulatory frameworks that are in the Republic of Croatia arranged at a fairly high level. The Republic of Croatia has adopted the Act on Critical Infrastructure that directly identifies indicative activities and responsibilities of each stakeholder in the field of critical infrastructure protection.

1.4 National and EU legal framework in the project specific area

In the introduction to the analysis of the legal framework it is necessary to emphasise that the Republic of Croatia has at this moment with its legal framework, which consists largely of the Act on Critical Infrastructure (Official Gazette No. 56/2013) and the later adopted Decision on the determination of sectors from which the central government bodies identify national critical infrastructure and lists the order of the critical infrastructure sectors (Official Gazette No. 108/2013) and The Ordinance on methodology for critical infrastructure operation risk analysis (Official Gazette No. 128/2013), adopted all the essential provisions foreseen by the Community acquis contained in the Council Directive 2008/114/EC of 8 December 2008.

The aforementioned Act regulates the rights, authority and obligation of the Government of the Republic of Croatia, the National Protection and Rescue Directorate and the central state administration bodies (ministries), 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. National Standpoints of the Republic of Croatia, p. 7).

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 (Ibidem, p.7). In principle, this is also an appropriate legal solution, but in practice it has shown that NPRD, due to the structural organisation and the lack of specific resources, is unable to fully perform all of the tasks defined in the Act on Critical Infrastructure. In the provided solutions of this study, two models are proposed to the forefront, which in their basis, primarily due to the organisational placement of the National Centre for Critical Infrastructure (NCCI), derive from the different legal positions and needs. The fact is that any system of critical infrastructure requires a central coordinating institution which brings together all the necessary processes in the field of critical infrastructure protection. The model No. 1 that NCCI becomes an internal organisational unit of NPRD, in its essence requires minimal corrections of the current legislation. With certain bases, all the necessary tasks and relationships are later defined by a regulation (decree) for the smooth functioning of NCCI. The proposed model No. 3, where NCCI would become an independent Government agency directly subordinate to the Government of the Republic of Croatia, presents a major interference with the legislative framework. However, we will discuss the positive and negative aspects and the necessary extent of amendments to legislation in a concrete analysis of the model of establishing NCCI.

In each case, it can be seen through the analysis of the legal sources and in particular their implementation in practice that the legal provisions are not fully implemented. That is the factor which is essential when it comes to adaptability of the whole system to the particular needs and requirements of the national and international environment.

1.5 Compliance of the project goals with strategic documents and strategic objectives of the Republic of Croatia and with EU documents

The RECIPE 2015 project has in its implementation phase defined the basic objectives and results which will be further compared with the implemented proposal for a project model for the management of critical infrastructure in the Republic of Croatia.

Overall expected results of the project are (RECIPE 2015 National standpoints of the Republic of Croatia, 2015: p. 8)**:**

1. Easier exchange of knowledge and experience between countries
2. Increased awareness of risks threatening critical infrastructures
3. Increased disaster event prevention knowledge base
4. Improved communication among national and international stakeholders
5. Strengthened mutual support and cooperation among all relevant public and private sector partners
6. Increased scientific and research activity in the field of critical infrastructures risk management
7. Guidelines for establishment of optimal critical infrastructures risk management systems in partner states
8. The guidelines are made available to the European Commission for further dissemination and use.
9. Increased resilience and level of protection of European critical infrastructures as a result of improved coordination and cooperation among the stakeholders
10. Established methodology for assessment of system protection based on a systematic approach
11. Defined long-term strategy for critical infrastructures management in the encompassed states
12. Defined needs for further education and training of public and private sectors (education programmes, exchange of professionals).

In a detailed analysis of the proposed model of operating of critical infrastructure of the Republic of Croatia and with regard to all the preparatory workshops, it can with certainty be stated that the above conclusions and the study itself have ensured the achievement of most of the set goals. The goals 1-9 were directly included in the presented solutions and conclusions of the RECIPE 2015 project up to this point. The entire project was primarily intended for the participating countries that through the proposed solutions and feasibility analysis of the mentioned solutions provide raising the quality of the systemic approach of the critical

infrastructure protection. Of course, it is necessary to recognise that interdependence is one of the very important factors of European critical infrastructure. This means that each country, in addition to national factors that can be posed by the risks for the continuous operation of critical infrastructure, is directly fastened with a specific part of critical infrastructure to the wider international arena. From this perspective, the importance of fulfillment of the set goals is all the more important since the Republic of Croatia through the proposed model gets a good basis for systemic improvement of critical infrastructure protection. With their approach and implementation of the proposed model in the practical solutions it can provide an example of good practice for all the countries that have not yet adequately regulated and established their own national models of critical infrastructure. With the establishment of these solutions it represents a pilot case for the countries of the region, which are currently candidates for entering the European Union.

The Republic of Croatia has also in its strategic documents stated that through the various levers of national security mechanisms it ensures the implementation of its national interests, and above all the establishment of a secure environment for its development. The strategy of the national security is currently in the phase of re-defining the strategic factors of ensuring the national security. The area of critical infrastructure protection management will in any case have to be re-installed among the important areas. The importance of critical infrastructure protection is evident also from other legal and strategic documents that are directly or indirectly tied to the area of critical infrastructure. The most important statutory provision at a strategic level is certainly the Act on Critical Infrastructure. It needs to be stressed, though, that the Republic of Croatia has some difficulty with a direct implementation of the accepted legal solutions into practice. In certain parts, the area of law differs from the direct practice and deficient implementation processes.

This is a factor that is characteristic of most countries in transition, which include the Republic of Croatia. There are several reasons for this, the most exposed mainly the one that adaptation to acquis has required very extensive adaptations, which were otherwise defined by changes in legal solutions, but there was not enough experiences and resources for the full implementation of the statutory system requirements. This is understandable for this point of view. An important factor can certainly be found in political culture and direct awareness of the importance of critical infrastructure for the smooth functioning of the wider community. Strategic management of companies and the ruling policy make the proper operation of critical infrastructure, in a 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 are realised in the important part. A well-functioning system of critical infrastructure in the Republic of Croatia, its resistance of operation to exposed security risks provides the continuity of operation, which is a key moment and the expectation of the citizens of the Republic of Croatia, as well as the international environment in which it is involved. The model specifically highlights the need for the establishment of a central coordination point for managing systematic coordinated activities for critical infrastructure protection, which would be with the realisation of the proposed model managed by NCCI with close coordination with operators of CI. This moment is represented by one of the fundamental factors for the realisation of the objectives, which are related to the exchange of experience and the latest knowledge and its transmission to other countries within the EU. The strategic objective of the Republic of Croatia is that it wants to play an important role in the region, especially in the field of mentoring the other candidate countries. The above exposed factor of the effective coordination in the central institution is in harmony with these strategic goals of the Republic of Croatia.

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 in the later period the functioning of critical infrastructure protection. In making a strategic and legislative frameworks in the Republic of Croatia, 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 also at the level of critical infrastructure operators themselves. This is an important basis for the establishment of long-term trust among all partners in the process of critical infrastructure protection in the Republic of Croatia. Whether at this time it is necessary to change the provisions of the Act on public-private partnership, we believe that the problem is more at the level of understanding and implementation of these solutions rather than the inadequacy of the legislative basis. In this context, we need to understand and take into account also the system of public procurement, which is a very important factor, especially in that part of critical infrastructure, where operators of critical infrastructure are public organisations.

1.6 Socio-economic cost-benefit analysis

The analysed critical infrastructure management model in the Republic of Croatia through the social economic dimension of the analysis is very important for a proper understanding of the

importance of the continuity of the functioning of critical infrastructure. This is essential for the smooth functioning of the wider social community and especially its vital processes and organisational components. The complexity of the security environment puts the modern society increasingly in front of the fact of the need for an appropriate and comprehensive approach to the management of safety risks. If in this context we are talking about critical infrastructure and the need for its continuity, this fact becomes all the more important. When it comes to safety, especially if we are talking about such an important segment, such as critical infrastructure, we cannot directly take a rough economic and cost-benefit analysis as a base. This was until recently the main basis for the development of the neo-liberal concept of development of the society, where at minimum input we try to ensure maximum profits. In such an important field, such as the continuity of critical infrastructure, it is necessary to assess the necessary input in relation to the optimal solutions and results. Although the proposed model does not directly define the necessary financial resources for the realisation of the above processes in the field of the establishment of the National Center of critical infrastructure, an appropriate public-private partnership model and organisational structure of the information system for the management of critical infrastructure in the Republic of Croatia, we can roughly estimate that the financial resources for the direct practical implementation of the measures foreseen are relatively high. Certainly the greatest extent of the derogations in the necessary financing for the realisation of the proposed models can be assessed during the selection of the offered variants 1 or 3 in establishing NCCI. We will give a detailed analysis in the following chapters related to the assessment of the financial resources.

In the context of the cost-benefit analysis of the socio-economic factors, it is necessary to directly point out that the continuity of critical infrastructure is indispensable to the smooth development of the society. It is impossible to practically identify all the harmful consequences that may occur with the loss of the key components of this infrastructure. If taking this into account we deal with the interdependence of the functioning of critical infrastructure and society at large, we can very quickly find out that some sectors of critical infrastructure are especially exposed. In this context, it is necessary to highlight the production sector and the provision of electricity, transport and information and communication technologies, of course. The domino effect of the failure of the mentioned subsectors of critical infrastructure has, in addition to the social, also exposed the economic negative impacts for the functioning of society and the economy in this context. Of course, it is necessary to add to the complexity the fact that an important part of critical infrastructure

passes over to the environment of private owners. In this context, the proposed public-private partnership model is extremely important. The cost-benefit analysis in a company with private ownership gets this new moment, which is not necessarily in tune with the public interest. There a country must with all its levers ensure that both partners find appropriate approaches that meet their basic expectations and objectives set. At least in the field of raising awareness and perceptions of seriousness that is required by the orderliness of this area, this process will be of important help in that the key institutions and the strategic management of the Republic of Croatia will rank the area of critical infrastructure protection in the list of national priorities more importantly. In the area of raising awareness of strategic management in enterprises it is necessary to form the information on the importance of uninterrupted operation of critical infrastructure into the business framework of competitive advantages and business success of the sound operation of the infrastructure. The financial aspect for continuous operation of critical infrastructure will be the message factor that will lead strategic business organisations to better understand and thus successfully position critical infrastructure protection as one of the major priorities for the performance of their companies. Financial investments in critical infrastructure protection should become investments in continuity and efficiency of their organisations and not mere costs. This finding, however, is also on the national level when it comes to inputs of the state in providing the continuity of critical infrastructure.

2 ANALYSIS OF SOLUTION/MODELS FOR THE REPUBLIC OF CROATIA

Below, we will look in detail at the analysis of the models in all three discussed areas of development of NCCI, the system of key data exchange and the system of public-private partnership. All three areas will be analysed through the feasibility analysis by the identified positive and negative indicators, which will have an impact on the direct implementation of the foreseen solutions. Each process will be analysed through a SWOT analysis, which will give providers additional information and an analysis of the factors which could directly affect the practical implementation.

2.1 Proposal of NCCI model

Model makers have foreseen four variants for the establishment of NCCI:

1. NCCI as the organisational part of NPRD;
2. NCCI as an integral part of another state authority;

3. NCCI organised within the offices and Government services of the Republic of Croatia;
4. NCCI as an independent body of the state administration.

For a more concrete analysis, two models were identified as topical by those preparing the study, both of which are intended for a more in depth implementation of further analysis. In this context we are talking about model No. 1 and model No. 3. Hereinafter, both models will also have a more detailed analysis. Before that, we will make an analysis of the basic structure of NCCI itself and its essential tasks that are foreseen in the basic framework regardless of which model will be selected.

The tasks scheduled for NCCI by those preparing the studies are appropriate and absolutely comparable with the international practice of the countries which have established the mentioned center. In this context of the envisaged tasks, NCCI is put as a focal point and a direct promoter of the systems of public-private partnership and the model for the transfer of key information in the field of critical infrastructure protection. The Republic of Croatia gets through the foreseen tasks the central coordinative authority to manage the operational, educational, monitoring and development measures in establishing an effective system of managing critical infrastructure. A special mention in the context of the tasks goes to the supervision and guidance of identifying and making sectoral analyses of risks for the operation of critical infrastructure. This is a crucial step for an effective systemic approach and continued realisation of the currently accepted legal obligations. An inadequate and non-systemic approach to establishing the criteria for determining critical infrastructure results in a disorderly situation and in particular irrational use of resources for its protection. In small countries, which include the Republic of Croatia, such a non-systemic approach can be fatal for the operation of critical infrastructure and the significant effects that the nonsystematic use of funds have. The next step or task needs to be mentioned in this context, which through the supervision and guidance of making threat assessments and security plans provide a uniform approach and standardised measures. In this part, the system unifies with the central supervision and guidelines and directs the implementation of counselling in all sub-sectors of critical infrastructure, as well as on the other hand, prevents non-systemic approaches in risk assessment, introduction of non-systemic steps in the area of outsourcing engagement and standardisation of measures which in general reduce the amount of resources which must be invested in building security systems for critical infrastructure protection. It is important to highlight the importance of the task, which defines a focal contact point for European critical infrastructure protection. Particularly worth noting are the very demanding tasks that the Act

on Critical Infrastructure gives to other state bodies[1] in the area of the development of the system for critical infrastructure management of the Republic of Croatia.

The identification of critical infrastructure, an analysis of the risks to critical infrastructure from its sphere of tasks, the definition of the sectoral criteria, the proposal of the European critical infrastructure and the nomination of the security coordinator and his deputy are here especially highlighted. Most of these tasks are for individual ministries extremely demanding. The biggest challenge is the systemic approach in all areas which will ultimately deliver a mutually comparable and a comprehensive, well-functioning system of critical infrastructure protection. In this section, the NCCI will play the key coordinating and supporting role, which will significantly contribute to the effective functioning of this system.

In the proposed tasks of the National Council for Critical Infrastructure (NVCI), which is organisationally based on both models, organised in many forms, there are some very important open dilemmas related to its task. A very important issue in this context is the structure of the mentioned Board. In the currently proposed form of tasks it can be estimated that it is not just an advisory body which passes specific suggestions and findings in the field of critical infrastructure system to the Government of the Republic of Croatia. As its main task, the drafters of the model foresaw the primary task of monitoring and coordination of all activities related to the development of the system of critical infrastructure protection. In the detailed definition of the tasks below which have been identified as (a) proposal of measures for the development of critical infrastructure protection; (b) making recommendations, opinions and guidance on the development of the system; (c) analysis of the key issues in the field of protection and management of critical infrastructure; (d) evaluation of the reports on the state of the system that would periodically be transmitted to it by NPRD and other organs. In this detailed review of the tasks we see that it is a classical advisory body, which could serve the Government of the Republic of Croatia to facilitate the assessment of the state of CI. In this context, it is necessary to pay attention to two essential things, namely streamlining in the organisational sense. Too many consultative and coordinating bodies make the national security system and the overall management of the country extremely untransparent and hard to handle. The narrow viewing of the problems of the commited area brings in charge duplication or other arguments at national level. The Government can not escape from their essential responsibilities and tasks in the field of CI protection through the establishment of such a body. Maybe it would be reasonable to think that the mentioned consultative body

[1] -Act on State Administration System, Ofiicial Gazette no. 150/11 and 12/13.

would be set up under the National Security Council, or at least as an integral part of it. This would eliminate the fear of non-systemacy of the approach and above all, a more effective coordination at the national level. Another important thing that needs to be highlighted in this context is the division of responsibilities in the area of coordination of systemic measures to develop the system of CI protection between the NCCI and the mentioned National Council for CI. The processes where duplication or ambiguity could come up will be also clearly pointed out through an analysis of each process.

Evaluation of compliance of tasks of NVCI: The tasks of the Council must be further refined and organisationally installed according to the admission of one of the proposed models. This will require a clear decision whether it is an advisory or a co-ordinating body with clearly defined authorities. In any case, it is necessary to look for its place in the existing frameworks of the National Security Council and thus reduce the chances for non-systemic approaches and excessive proliferation of consultative organisational structures, which are not the most optimal solution for the functioning of the system. On this basis, the proposal calls for a more clear definition of its structure to be able to perform the designated tasks.

Evaluation of compliance of tasks of NCCI: The tasks are entirely appropriately designed and are fully comparable with international practice. In the subsequent assessment of the two proposed models it will be seen that these tasks are more suitable for NCCI, which is under NPRD. This estimate is based on the fact that the majority of processes in NPRD are already in place.

With reference to the above-defined tasks of NCCI also the basic processes are divided into four key areas that are adequately defined. The business processes in the field of (a) the system of critical infrastructure management; (b) critical infrastructure protection; (c) public-private partnership and (d) development and transfer of knowledge, the NCCI encompasses all the main segments where the Republic of Croatia needs a central coordinating body to manage the whole system of critical infrastructure.

Analysis of the organisational placement of NCCI:

Model No. 1.

The proposed model No. 1 provides the organisational establishment of NCCI in the form of internal organisational units within NPRD.

Not feasible	Partially feasible	Entirely feasible
		X

Positive indicators:

- NPRD already performs an essential part of the tasks in the area of coordination and system development in the Republic of Croatia;
- Knowledge and experience acquired by the employees of NPRD in the field of the establishment and operation of the system, which will be the key generator of the necessary skills for the future establishment and operation of NCCI;
- NPRD with its basic mission of the implementation of protection and rescue in addition to the police and the army constitutes the only institution which is with its mechanisms of coordination, the implementation of the activities, organisation and resources present in all parts of the Republic of Croatia. This means that, in the establishment of NCCI, this fact will through the streamlining of the resources result in the utmost importance for the future performance of the NCCI. Having developed the mechanisms it is necessary to strive to their upgrade and not to embark on an entirely new organisational and coordinative mechanisms;
- According to the analysis of threats to CI and examination of risks, which critical infrastructure has been exposed to in the international environment, it can with a lot of certainty be estimated that natural disasters and the associated risks are most exposed for the protection of critical infrastructure. Given the fact that the prevention and control of the risks of natural disasters, and the subsequent elimination of the aftermath of natural disasters are one of the essential tasks of the system of NPRD, you can very quickly find out that the organisational placement of NCCI is very suitable. From this point of view the measures brought about by the establishment of NCCI under NPRD as a result of experience, the already established mechanisms and human resources, which have among their tasks already dealt with individual parts of the protection of CI, will be much more effective;
- The Republic of Croatia ranks among the small countries, so the rational use of resources is a very important factor in the adoption of such important decisions such as the setting-up and placement of NCCI.

Negative indicators:

- In the case of legal incompleteness of authorities and duties difficulties may arise in the coordination of other ministries in the areas of their duties, as they are now allowed by the

Act of Critical Infrastructure. For this reason National Security Council should take role in the strategic coordination processes;

- There is missing important process related with intelligence and security information which would be necessary for evaluation of national and specific threats to critical infrastructure. National Security Council could be adequate body for esurience of this process;
- A change or supplement of the existing, above mentioned law is needed. In the procedure of the change partial interests of individual ministries may be encountered, which would want to take on a more important role in the field of coordination of CI protection. These interests need to be understood through the provision of a larger share of the national budget devoted to this area;
- For the effective functioning of the NCCI additional human, material and financial resources will be required. At the moment when the countries face the rationalisation of expenditure for its operation, it will be very difficult to convince the ruling policy that the mentioned area should receive additional funds. The risk that NPRD is assigned to establish and ensure the functioning of the NCCI only with the administrative act, and to ensure that funds are provided from the scope of the current resources for the operation of the NPRD. Without additional resources of NCCI, despite the establishment, it would not be able to carry out all the tasks foreseen;
- A great dependence for the establishment and realisation of the proposed model on the awareness of the importance of the regulation of this area of CI protection.

Indicators for assessing progress:

- Understanding of the ruling policy and validation of model No. 1;
- Amendments to the existing legislation;
- Definition of additional financial resources of NPRD for the establishment of NCCI;
- Providing additional human resources for the operation of the NCCI;
- Number of participating organisations and representatives;
- Percentage of carried out set tasks;
- Number of events organised by NCCI.

Figure 1: SWOT analysis of enforcing model No. 1

Strengths	**Opportunities**
Continuation of the current processes in the NPRD as the centre line of the organisation for the coordination of the establishment of CI system; Established inner circle of experts in the field of CI protection; In the national system and with the operators, NPRD is already identified as central authority of coordination up to this point; Strengthening the national network of experts; Given the current organisation the best and most rational approach to achieve the objective; Lesser corrections of existing legislation required to establish an appropriate situation;	Raising awareness of the importance of CI protection; Better coordination; Cost reduction of the establishment of the system of CI protection; Designation of state institution, which will in the future bear the weight of the coordination and development of the CI system; Central body for exchanging experience and good practices; Strengthening the public-private cooperation; Appropriate arrangement of systemic cooperation with the EU and other international partners in the field;
Weaknesses	**Threats**
Harder reaching consensus due to the level of the placement of NCCI; Regulation of the relationships of authorities and responsibilities; More difficult to reach the target group during the economic work of the CI management; No clear process for ensure adequate intelligence and security information flow.	Narrow departmental interests which might harm the national interest; Failure to provide additional resources for the establishment and realisation of the foreseen NCCI model No. 1

Model No. 3.

Proposal for model No. 3 provides for the organisational establishment of NCCI within the departments and offices of the Government of the Republic of Croatia.

Not feasible	Partially feasible	Entirely feasible
	X	

Positive indicators:

- The mentioned organisational structure is closer to the strategic decision making level and from this point of view in a particular case an easier process of persuasion for the adoption of the necessary decisions;
- In the case of the proposal NCCI would be organised within the NPRD, which would mean a certain amount of rationality and ease of organisation[2];
- Because of its strategic level it would make it easier to cooperate with industry and provide more serious approaches on the part of the strategic management of companies that manage CI;
- Easier cooperation on the international scene, in particular as a result of strategic organisational level;

Negative indicators:

- To establish this model of NCCI a fairly major change to legal regulations in the field of critical infrastructure protection, as well as the organisation of public administration would be required;
- The mentioned solution would demand considerably more financial resources for the establishment of all the necessary resources;
- The problem of lack of experts would in this case get a more explicit influence. In case of all the experts leaving the framework of the NPRD it would become personnel- and professional-wise strongly impoverished;
- All current Government departments and offices have in their function a completely different character of their mission, which in addition to editing the strategic issues is not so much aimed at direct coordinative and guidance activities. From this point of view, through the establishment of NCCI, directly under the Government certain significant logistical, communication and organisational problems would incurr, which would in the initial stage greatly reduce the already achieved level of coordination in the field of the system CI regulation;

[2] But in a previous analysis of tasks and organisation of NCCI, this solution is estimated as inadequately completed as it leaves too many open dilemmas which should be additionally defined.

- Due to the independent operation this logistical support would need additional human resources potential, which in an era of rationalisation and limited resources, mainly in smaller countries, needs to be highlighted;
- Problems would also arise in the immediate operational communication between all segments of the system, which would also in the financial and organisational sense mean a big mouthful for the size of the country, such as the Republic of Croatia;
- At the entry into force of this model it would be very difficult to exploit those levers of coordination and the transfer of sensitive information, which are already in place in NPRD;
- In a short time without major organisational and financial inputs, this model is not even possible to be established. As a result, its operational activity referred can be looked at over a long period of time in spite of the decision taken.

Indicators for assessing progress:

- Understanding of the ruling policy and validation of model No. 3;
- Amendments to the existing legislation;
- Definition of additional financial resources in the state budget for the establishment of NCCI;
- Providing additional human resources (professional and supporting) for the operation of the NCCI;
- Number of participating organisations and representatives;
- Percentage of carried out set tasks;
- Number of events organised by NCCI.

Figure 2: SWOT analysis of enforcing model No. 3

Strengths Greater impact on the strategic level of decision making; Unity of jurisdiction of NCCI and NVCI because of the strategic role; Greater impact on the processes of public-private partnership; Easier cooperation with comparable centers in an international environment;	**Opportunities** Raising awareness of the importance of CI protection in strategic management (Government of Croatia); Better coordination; The central body for exchanging experience and good practices; Strengthening the public-private cooperation; Appropriate arrangement of the systemic cooperation with the EU and other international partners in the field;
Weaknesses Harder achievement of interoperability of its operation;	**Threats** Narrow departmental interests which might harm the national interest;

Great need for a new human resources potential; Great financial difficulty for the implementation of this model; Current organisation of state administration in the field of Government offices and services is not ready for the placement of such complex and challenging organisational forms; Despite the adoption of the decision a longer period should be provided for the operational functioning of NCCI;	Non-acceptance of the decision for the establishment of NCCI; Failure to provide additional resources for the establishment and realisation of the intended NCCI model No. 3; Establishment of a new administrative organisation without the necessary operational and coordination capacity;

The findings of the analysis of the organisational placement of NCCI:

After a detailed analysis of all factors of impact on the implementation of the proposed solutions of model No. 1 and model No. 3, we find that the current level of the structure of the system of CI protection and acknowledgement for the individual system measures model No. 1 is more plausible and rational. The finding can be substantiated above all with the facts that model No. 1 would mean a continuation of the current systemic measures for the final regulation of the situation in the field of CI protection. The fact that the rational deployment of the solution at this point is a very important factor helped a lot in supporting the decision, especially due to the fact that the Republic of Croatia is just about to undergo important structural reforms, which will require a large amount of resources. In addition to operativeness, the suitability of coordination and other professional references, rationality of investment for building this system will have a major influence on the choice of suitability. Through cost-benefit analyses, it is necessary to accept the fact that input in this solution is a lot lower, the results, however, as expected much higher due to the continuation of the current processes. The next important fact, which turns the decision in the favour of model No. 1, is definitely the analysis of processes, which shows that the system of CI protection is very much associated with the system of providing protection and rescue and handling the aftermath of natural and other disasters. In this context, the operation of NCCI can lean very closely on those processes that are already running and are effectively tested. This segment provides more effective and certainly more high-quality operation of the new organisational structure, which would be a logical continuation of already up to now set bases. Of course, it is necessary to be aware of the importance of the impact on the strategic decision-making level, which is definitely formed by the Government of the Republic of Croatia. In this model,

additional efforts need to be devoted to this factor as model No. 3 would be, due to its placement, by all means more effective.

3 ANALYSIS OF THE BASIC BUSINESS PROCESSES IN THE NCCI

A. THE SYSTEM OF CRITICAL INFRASTRUCTURE MANAGEMENT

I. Development and upgrade of the normative framework of management

Within the framework of this task all the necessary processes are provided for the proper completion and adoption of a normative basis, which will allow the final regulation of a comprehensive system of critical infrastructure protection. Processes are properly planned through the entire task and have, in addition to clearly defined operators, defined mechanisms to achieve the target state. Of utmost importance is the awareness that it is possible to effectively implement the legislation changes only with preliminary detailed analysis and taking into account the full set of factors that influence or are responsible for the development of CI field.

In the case of individual processes we would propose the following amendments:

Figur 3: Step A.I. Development and update of the normative framework of management

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
A.I-1	Adapting the changes and amendments of the Law on Critical Infrastructure	It is essential to include public-private partnership in the mechanisms; It is essential to include also the direct managers of CI among participants;
A.I-2	Proposing the changes and amendments to defining CI sectors	It is essential to include public-private partnership in the mechanisms; It is essential to include also the direct managers of CI among participants. Without them an appropriate analysis which would imply the reality of legal provisions and

		their potential for practical implementations can not be carried out;
A.I-3	Proposing the changes and amendments to defining CI priorities list	To take account of public-private partnership in the mechanisms. When integrating operators of CI, we have to be cautious about that the priority will not be affected by the narrow interests of individual operators of CI.
A.I-4	Making changes and amendments of the "Ordinance on methodology for critical infrastructure operation risk analysis"	It is essential to include business entities in the role of CI operators; To associate the mentioned process very closely with the process of the D.I-1, which should serve as a basis for future changes.
A.I-5	Drafting and review of cross-sectoral and specific sectoral criteria	It is essential to install an analysis of the current situation among the mechanisms, which should be a primary basis for the continuation of the other comparative analyses. To install an analysis of the financial impact, in the above analysis, which is highly correlated with the change in the criteria; To install all sectoral coordinators among the participants.

Figure 4: SWOT analysis of enforcing step A.I.

Strengths The current legislation is adecvate base for development additional legal amendments, especially if the chosen model for the organisation of NCCI is model No.1; All major normative documents are adopted and need to be adapted to current changes and the changes in the security environment;	**Opportunities** To achieve raising of awareness of the importance of the protection of CI in strategic management through the proposals based on the quality analysis (Government of RC); To improve the speed of implementation of the necessary solutions and operation of CI with the appropriate changes; This process can be used to strengthen public-private cooperation by taking into account all partners; Appropriate regulation of the legal field at the national level is an adequate basis for achieving the EU requirements; Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses Inadequate awareness in individual sectors of CI and directly with CI operators can highly	**Threats** Narrow departmental interests which might harm the national interest;

limit and worsen the process of the analysis of necessary changes;	Non-acceptance of the decision for legislative changes; Declarative adoption of legislative changes without subsequent implementation in practice.

II. Coordination of work and activities of the stakeholders of the CI management system

Within the framework of this task all the necessary processes are provided for the appropriate coordination of the work of stakeholders of the CI management system. It is particulary necessary to point out that effective coordination needs to be taken into account, in addition to the sectoral co-ordinators, as one of the key segments for the effective transfer of information, also the operators of CI themselves. Public-private partnership has an extremely important role in this context.

Figure 5: Step A.II. Coordination of work and activities of the stakeholders of the CI management system

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
A.II-1	Coordination of work of the security co-ordinators at NPRD	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.
A.II-2	Coordination of the activities of the owners/operators of critical infrastructure in the process of protecting it	It is essential to include security co-ordinators for each sector among the participants; This is one of the key processes of strengthening public-private partnership.
A.II-3	Coordination of activities with other EU Member States	No comments and additional proposals.
A.II-4	Coordinating of activities with EU bodies	No comments and additional proposals.

Figure 6: SWOT analysis of enforcing step A.II.

Strengths Current bases of the so far carried out activities to establish a system of coordination in the field of CI protection provide a good basis for a substantive and quality progress; Security coordinators are already determined by sectors of CI; It is necessary to start from the frameworks of good practice, which is already present in specific sectors and transfer it to other sectors;	**Opportunities** To achieve raising of awareness of the importance of CI protection in strategic management through the proposals based on the quality analysis (Government of RC); To improve the speed of implementation of the necessary solutions and operation of CI with the appropriate changes; This process can be used to strengthen public-private cooperation by taking into account all partners; Increasing the efficiency of coordination in the national and international environment; Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses Inappropriate awareness of the importance of security coordinators can strongly paralyse this process; Staffing in jobs of security co-ordinators must be extremely careful; Misunderstanding of the importance of public-private partnership can deter the private sector from effective collaboration.	**Threats** Narrow departmental interests which might harm the national interest; Failure of coordination or neglect of its priority role may be reflected negatively on the the entire system of CI functioning.

III. Collection, analysis and information exchange

Within the framework of this task all the necessary processes are provided for the appropriate collection, analysis and exchange of information. It is particularly necessary to point out when we assessed the processes of setting up an appropriate system of key information exchange that it is necessary to invite the representatives of institutions among the participants which are in the Republic of Croatia responsible for the protection of classified information and cyber security. The establishment of appropriate information systems to share key information

constitutes a major cost that can deter the strategic management from the intention to support the fulfillment of this task with the relevant resources.

Figure 7: Step A.III. Collection, analysis and information exchange

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
A.III-1	Management of databases on national and European CI	It will be necessary to include also security co-ordinators in the process of cooperation, who will confirm the relevance of the information from 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.
A.III-2	The development and upgrading of standard operating protocols for the exchange of key data	The operating level of this process may remain in this part. The development section would be worth transfering in the context of step D. Definitely add security sectoral co-ordinators, managers and international partners among the participants.
A.III-3	Management of the system for the key data exchange	Definitely add representatives of the relevant state institutions among the participants, such as the Office for national security and other authorities responsible for the area of data protection and cyber security. Add among the mechanisms: - Identification of problem - Comparative analysis - Technical discussion
A.III-4	Management of information security for the key data exchange	Definitely add representatives of the relevant state institutions among the participants, such as the Office for national security and other authorities responsible for the area of data protection and cyber security. Add among the mechanisms: - Identification of problem - Comparative analysis - Technical discussion

Figure 8: SWOT analysis of enforcing step A.III.

Strengths	**Opportunities**
With the final establishment of the system of transmission of key data it is necessary to stem from the so far existing schemes of national security; When transferring key information it is necessary to take into consideration the good practices on the area of networking form previous projects in Republic of Croatia.	To achieve raising of awareness of the importance of CI protection for security coordinators in the various sectors of CI and CI managers; To improve the speed of coordination of the necessary solutions and operation of CI system which will be based on an appropriate system of exchange of key data; This process can be used to strengthen public-private cooperation by taking into account all partners; Increasing the efficiency of coordination in the national and international environment; Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses	**Threats**
Inappropriate awareness of the importance of security coordinators can strongly paralyse this process; The cost of introducing these systems can force certain administrators to the acceptance of non-systemic and seemingly cheaper measures; Misunderstanding of the importance of public-private partnership can deter the private sector from effective collaboration.	Narrow departmental interests which might harm the national interest; Unawareness of the need for the secure exchange of key information would place this task in a very low place on a scale of priorities by decision makers due to the scale of the costs.

B. CRITICAL INFRASTRUCTURE PROTECTION

I. Identification of critical infrastructure

In the context of this task all the necessary processes for the proper identification of critical infrastructure will be provide when the sectorial and intersectors criterias will be in place. Given the fact that this process in the Republic of Croatia is not yet fully implemented, it will represent one of the critical processes for the effectiveness of the establishment of a

comprehensive system of CI. This process has a special place mainly due to the fact that every decision has important financial implications. This step is also important from the standpoint that the proper definition of the criteria and the setting of national and European CI, the cooperation of all parties concerned is needed. Therefore the effective importance of coordination, cooperation and harmonization are given a particularly exposed position. In this regard, it is necessary to re-emphasise public-private partnership that is through these processes adequately strengthened.

Figure 9: Step B.I. Identification of critical infrastructure

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
B.I-1	Validation of the designed cross cutting criteria in the process of identifying national CI	It is essential to include public-private partnership into mechanisms; It is essential to include direct managers of CI;
B.I-2	Proposing European CI in the Republic of Croatia	It is essential to include public-private partnership into mechanisms; It is essential to include the direct managers of CI and international partners in the CI management of neighbouring countries among the participants.
B.I-3	Control over the introduction of interdepartmental criteria with all stakeholders of CI protection	To include methods of control (regular, irregular), counselling and evaluation and demonstrations of good practices among the mechanisms. It is essential to include the direct managers of CI among the participants;

Figure 10: SWOT analysis of enforcing step B.I.

Strengths	**Opportunities**
Implementation of the RECIPE project can serve as a good basis for the acquisition of experience in the preparation of the criteria for determining critical infrastructure installations; Appropriate coordination can further enhance the quality of the implemented system through NCCI;	To achieve a definition of national through the proposals based on quality analysis; To reduce the amount of financial resources required for the establishment of CI protection with the rational introduction of criteria; This process can be used to strengthen public-private cooperation by taking into account all partners; Appropriate definition of that CI which has international character and will be defined as ECI; Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses	**Threats**
Inadequate definition of the criteria could mean non-systemic approach and a significant increase in requests for financial and other resources for the protection of CI; Inadequate implementation of control can mean the inconsistent enforcement of norms in practice, resulting in a non-systemic determination of the scope of CI.	Narrow departmental interests which might harm the national interest; Failure to adopt realistic standards for determining CI; Declarative acceptance of norms without implementation in practice.

II. Assessment of risks

In the context of this task, two processes are anticipated to adequately assess the risks for the continuous operation of CI. This process is of utmost importance for the real execution and solid foundations of any system. The risk assessment for continuous operation of CI is the basis from which all the necessary systemic measures for the proper management of these risks subsequently derive. Two basic processes that are geared towards sectoral coordinators and direct managers of CI are planned for that. Because of that the systemacy of control, which must also be directed at advisory measures and assistance in the preparation of relevant

risk assessments, will have to be specifically highlighted. It should be understood that the two processes are very closely related, and it is impossible to run them separately.

Figure 11: Step B.II. Assessment of risks

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
B.II-1	Control and guidance of making sector risk assessments in NPRD	It is essential to include the transmission of guidelines and standards and good practices in the mechanisms; Consultancy and evaluation; Participation of representatives of relevant institutions and other experts.
B.II-2	Control and guidance of making security plans of owners / operators of CI in coooperation with competent government authorities and NPRD	It is essential to include public-private partnership in the mechanisms; Transmission of guidelines and standards and good practices; Consultancy and evaluation;

Figure 12: SWOT analysis of enforcing step B.II.

Strengths The transfer of experience from other parts of the national security system in the field of risk assessment; Continued building of the system on the bases which have already been placed under NPRD.	**Opportunities** Through quality products of risk assessments we get a good basis for the continuation of the process of CI protection; To reduce the amount of financial resources needed to establish the protection of CI by rational implementation of risk assessments; NCCI representatives can ensure their visibility by their professional work; Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses Inadequate definition of criteria can greatly complicate the implementation of control and risk analysis; Inadequate implementation of control may later mean inconsistent implementation of risk management measures in practice, resulting in security gaps and inconsistencies.	**Threats** Narrow departmental interests which might harm the national interest; Failure to adopt real threat assessments results in inadequate implementation of measures for CI protection; Declarative preparation of threat assessments without any real basis.

III. Monitoring and evaluation

In the context of this task all necessary processes for appropriate monitoring and evaluation of the implemented security plans of CI protection are provided for. The reality of programming represents also an appropriate response to the risks CI is exposed to. In the context of this task, four processes, which in individual work permit monitoring and evaluation of the adequacy of the measures implemented in the sectors and directly with the managers / owners of CI, are clearly defined. In a rough estimate, we could say that the process No. 1 and the process No. 4 may be combined in one process and thus make the matter even more transparent. However, the demarcation of these two processes does not significantly affect the possibility of the plan implementation.

Figure 13: Step B.III. Monitoring and evaluation

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
B.III-1	Control and guidance of making sector risk assessments in NPRD	It is essential to include the transmission of guidelines and standards and good practices in the mechanisms; Consultancy and evaluation; Participation of representatives of relevant institutions and other experts.
B.III-2	Control over the implementation of the annual audit of security plans in collaboration with departmental ministries	It is essential to include public-private partnership in the mechanisms; Transmission of guidelines and standards and good practices; Consultancy and evaluation; Participation of representatives of relevant institutions and other experts.
B.III-3	Control and guidance of implementation of sectoral plans to protect critical infrastructure	It is essential to include public-private partnership in the mechanisms; Transmission of guidelines and standards and good practices; Consultancy and evaluation;
B.III-4	Control and guidance of making security plans of owners / operators of	It is essential to include public-private partnership in the mechanisms;

	CI in collaboration with competent government authorities	Transmission of guidelines and standards and good practices; Consultancy and evaluation; Participation of representatives of relevant institutions and other experts.

Figure 14: SWOT analysis of enforcing step B.III.

Strengths Current bases of the so far carried out activities to establish a system of coordination in the field of CI protection provide a solid basis for a substantive and quality progress; Security coordinators are already determined by sectors CI; It is necessary to start from the frameworks of good practice, which is already present in specific sectors and transfer it to other sectors; Appropriate coordination through NCCI can further strengthen the quality of control over the adequacy of security plans;	**Opportunities** To achieve a definition of national and European CI through the proposals based on quality analysis; To achieve a higher quality of measures implemented to protect CI with the rational implementation of planning; This process can be used to strengthen public-private cooperation by taking into account all partners; Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses Inadequate planning of security can mean a non-systemic approach and an inadequate response in the necessary measures to respond to prevent threats; Inadequate implementation of control may mean inconsistent enforcement of risks for the continuous operation of CI.	**Threats** Narrow departmental interests which might harm the national interest; Making unrealistic plans of CI protection; Declarative preparation of plans without implementation in practice.

IV. Monitoring and verification

In the context of this task all the necessary processes for the proper monitoring and checking the condition of the field of CI protection are provided for. Annual reporting and analyses on the state of the national and European CI are essential indicators for the upgrading of the integrity of the system and monitoring the situation. The legislative and executive branches of authority provides relevant data to enable control of the efficiency and functioning of the comprehensive system of CI protection.

Figure 15: Step B.IV. Monitoring and verification

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
B.IV-1	Making an annual report on the number, criticality and carried out dimensions of CI protection	No additional suggestions or comments.
B.IV-2	Making an annual report on the number of ECI by sectors and the number of interested countries that are dependent on certain CI	No additional suggestions or comments.

Figure 16: SWOT analysis of enforcing step B.IV.

Strengths - It is necessary to stem from the frameworks of good practice, which is already present in individual sectors and transfer it to other sectors; - Appropriate coordination can, through NCCI, further enhance the quality of reports for the legislative and executive branches of power;	**Opportunities** - Highly qualified staff constitutes an appropriate basis for better quality reports; - With an adequate system of reporting and monitoring in the central point, represented by the NCCI, we can achieve substantively more qualitative reporting; - Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses - Inadequate implementation of control and reporting reduces the reality of the data necessary for reporting and monitoring in the field of CI protection; - Inadequately trained personnel are a negative factor impacting the quality of reports;	**Threats** - Narrow departmental interests which might harm the national interest; - Making reports that do not reflect the real situation in the field of CI protection; - Deliberate adjustment of the data to achieve higher inputs of financial resources in the field of CI protection.

C. PUBLIC-PRIVATE PARTNERSHIP

I. Projects of public-private partnership

In the context of this task all the necessary processes for the proper monitoring and analysis of processes of public-private partnership are provided for. 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 in the later period the functioning of critical infrastructure protection. In making a strategic and legislative frameworks in the Republic of Croatia, 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 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 the Republic of Croatia. In any case, it is necessary also in the case of voluntariness to clearly impose certain limits and arrangements of functioning of the national forum for critical infrastructure protection. The cultural dimension of the agreement on the important information exchange, which will not be aimed at the general public, will also have a 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. The fact is that we, in this work, have at least two key categories of information, namely the information that is essentially important for ensuring national security and on the other hand, the information, which in the business environment represents important business data, which may reduce the competitive advantage of the company which manages critical infrastructure. In particular it will come to the fore in the cases when ownership passes into private hands and several companies will appear in a certain area that will be in competition in the logic of the market economy. At this time, in the Republic of Croatia this should not pose a major problem as most of the major infrastructure companies are currently in state ownership and in most cases monopolists. Exempt is only the area of banking, where competition is very fierce. In this part, the Central Bank of Croatia will also need to play its role besides the state.

Figure 17: Step C.I. Projects of public-private partnership

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
C.I-1	Preparation and audit of the model of public-private partnership	It is essential to include public-private partnership in the mechanisms; It is essential to include sectoral security coordinators among the participants;
C.I-2	Initiating projects of public-private partnership	It is essential to include public-private partnership in the mechanisms; It is essential to include sectoral security coordinators and academic and research community among the participants;
C.I-3	Monitoring and supervision of the project of public-private partnership in CI protection	It is essential to include sectoral security coordinators and academic and research community among the participants;

Figure 18: SWOT analysis of enforcing step C.I.

Strengths - NCCI could become a focal point for the strengthening of public-private partnership in the field of CI protection; - The bulk of CI in the Republic of Croatia is still in public ownership, which could in the initial phase of public-private operation somewhat facilitate cooperation;	**Opportunities** - To strengthen cooperation in all sectors of CI through the examples of good practice; - Regulation of models of public-private partnership can facilitate the transition of CI in the management of private owners; - Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses - Failure to comply with the specificity of the private sector can have negative consequences on the quality of strengthening public-private partnership; - Inadequate security awareness on the importance of CI protection by private organisations can significantly inhibit the	**Threats** - Narrow departmental or management interests which might harm the national interest; - Inadequate legislation on the management of CI may enable the avoidance of taking the necessary measures of CI protection;

preparedness for effective participation;	- Declarative adoption of models of public-private partnership without implementation in practice.

II. Invitation to participate in the program of public-private partnership

In the context of this task all the necessary processes for an adequate increase of participation in the program of public-private partnership are provided for. Public-private partnership can be effective only if it includes all the stakeholders, and if everyone achieves at least a partial realisation of their goals and expectations through compromise solutions. It is necessary to add security coordinators across sectors and managers / owners of CI among the participants of both processes.

Figure 19: Step C.II. Invitation to participate in the program of public-private partnership

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
C.II-1	Preparation and audit of the model of incentives for owners / managers of CI who participate in the public-private partnership	It is essential to include public-private partnership in the mechanisms; It is essential to include sectoral security coordinators and managers / owners of CI;
C.II-2	Making certificates for owners / managers who participated through a program of public-private partnership	It is essential to include managers / owners of CI;

Figure 20: SWOT analysis of enforcing step C.II.

Strengths	**Opportunities**
- NCCI could become a focal point for the strengthening of public-private partnership in the field of CI protection;	- To strengthen cooperation in all sectors of CI through the examples of good practice; - Regulation of models of public-private partnership can facilitate the transition of CI in the management of private owners; - Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses	**Threats**
- Failure to comply with the specifics of the private sector can have negative consequences on the quality of strengthening public-private partnership; - Inadequate security awareness on the importance of CI protection by private organisations can significantly inhibit the preparedness for effective participation;	- Narrow departmental or management interests which might harm the national interest; - Inadequate legislation on the management of CI may enable the avoidance of taking the necessary measures of CI protection; - Declarative adoption of models of public-private partnership without implementation in practice.

D. DEVELOPMENT AND TRANSFER OF KNOWLEDGE

I. Development and improvement of methodology

In the context of this task all the necessary processes for the proper development and improvement of methodology are provided for. The development of new approaches and introducing them in 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 CI. Four key processes that touch the methodogy to identify CI, cross-sectoral and specific sectoral criteria, methodologies for risk assessment and methodology for risk management are defined in the foreseen task. The real and effective methodology can significantly contribute to the reality of planning and determining the measures required to determine those minimum standards and the CI scope and the measures

necessary for the implementation of CI protection. All this is very much linked to the planning and use of resources that need to be given to the operationalisation of plans and results.

Figure 21: Step D.I. Development and improvement of methodology for identification of CI

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
D.I-1	Development and improvement of methodology for identification of CI	It is essential to include sectoral security coordinators and individual managers / owners of CI;
D.I-2	Development and improvement of methodology for making cross-sectoral and specific sectoral criteria	It is essential to include sectoral security coordinators and individual managers / owners of CI;
D.I-3	Development and improvement of methodology for risk assessment	It is essential to include sectoral security coordinators and individual managers / owners of CI;
D.I-4	Development and improvement of methodology for risk management	It is essential to include sectoral security coordinators and individual managers / owners of CI;

Figure 22: SWOT analysis of enforcing step D.I.

Strengths - Experience of NPRD representatives must be considered in making supplements of methodology in the field of CI protection; - To take into account experience of sectoral coordinators in the development of methodologies; - To take into account comparable solutions in the development of methodologies in the international environment.	**Opportunities** - To strengthen cooperation in all sectors of CI through the examples of good practice; - To include scientific-research institutions in the creation and development of methodologies; - To strengthen public-private partnership through updating of methodologies; - Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses - Failure to follow the opinions of the direct	**Threats** - Narrow departmental or management

managers may have a negative impact on the quality of the methodological solutions; - Inadequate methodology results in flat-rate estimates which require an excess of resources which are non-systemically consumed;	interests which might harm the national interest; - Inadequate legislation prevents a quality preparation of efficient methodology; - Declarative and non-systemic upgrading of methodologies in practice causes serious problems.

II. Training

In the context of this task all the necessary processes for the appropriate training system are provided for. Training is one of the key segments of each system. Staff potential is very important for the success of the implementation of processes. Hence there is an urgent need to implement training for all levels and groups of staff potential, which is involved in CI protection. For that it is necessary to integrate the various forms of training and use a variety of methods including e-learning. The changes in the dynamic security environment force us to constantly update the training content.

Figure 22: Step D.II. Training

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
D.II-1	Training of security coordinators and managers in sectors/competent government authorities	It is essential to include educational institutions among participants;
D.II-2	Training of managers / owners of CI	It is essential to include educational and scientific institutions among participants;

Figure 23: SWOT analysis of enforcing step D.II.

Strengths	Opportunities
- Experience of NPRD representatives must be considered in making supplements of methodology in the field of CI; - To take into account experience of sectoral coordinators in the development of programs; - To take into account comparable solutions	- To strengthen the training in all sectors through the examples of good practice; - To include scientific-research institutions in the training; - To strengthen public-private partnership through updating of programs; - Croatia can become a mentor to other

in the development of programs in the international environment.	Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses - Low level of awareness among competent government authorities may limit the effects of training; - Lack of knowledge of providers of training; - Failure to follow the novelties in the preparation and implementation of training programs.	**Threats** - Narrow departmental or management interests which might harm the national interest; - Non-systemic implementation of training in practice causes serious problems and reduces the level of CI protection.

III. Counselling

In the context of this task all the necessary processes for an adequate system of counselling are provided for. The process of counselling is an added value, which is introduced into the system of CI protection. It is used for certain specific processes, where special knowledge is needed which can be applied in a particular environment. Advice is also provided to assist the security coordinators in the sectors as well as the management structure.

Figure 24: Step D.III. Counselling

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
D.III-1	Counselling of security coordinators in sectors	It is essential to include external experts among participants;
D.III-2	Couselling of managers / owners of CI	It is essential to include external experts among participants;

Figure 25: SWOT analysis of enforcing step D.III.

Strengths - Experience of NPRD representatives must be considered in the implementation of counselling; - To take into account experience of sectoral coordinators in the implementation of counselling; - To take into account comparable solutions	**Opportunities** - To strengthen the counselling in all sectors through the examples of good practice; - To include external experts in the counselling; - To strengthen public-private partnership through counselling activities; - Croatia can become a mentor to other

in the planning of counselling in the international environment.	Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses - Low level of awareness may limit the effects of counselling; - Lack of knowledge of providers of counselling; - Failure to follow the novelties in the preparation and implementation of training programs. - Failure to comply with the specifics of each organisation in the implementation of counselling.	**Threats** - Narrow departmental or management interests which might harm the national interest; - Non-systemic implementation of counselling in practice causes serious problems and reduces the level of CI protection.

IV. Exercises

In the context of this task all the necessary processes for the implementation of an appropriate system of exercises are provided for. The process of exercising is the added value that is introduced into the system of CI protection. It is used for training where there is a need of special knowledge which can be applied in a particular environment. Through exercises the readiness and capacity of the various structures in the systems of CI protection is checked. Exercises induce a direct practical training of theoretical procedures and foreseen plans. The more the exercises get closer to real situations the more effective their results.

Figure 26: Step D.IV. Exercises

Not feasible	Partially feasible	Entirely feasible
		X

Step and task	Process	Proposals of updates
D.IV-1	Implementation of exercises for security coordinators in sectors	It is essential to include external experts, scientific research institutions, other stakeholders in the management system for CI protection among participants;
D.IV-2	Implementation of exercises for managers / owners of CI	It is essential to include external experts, scientific research institutions, other stakeholders in the management system for CI protection among participants on different scale of excersises (full-scale excersise);

Figure 27: SWOT analysis of enforcing step D.IV.

Strengths	**Opportunities**
- Experience of NPRD representatives must be considered in the planning and implementation of exercises; - To take into account experience of sectoral coordinators in the implementation of exercises; - To take into account comparable solutions in the planning of exercises in the international environment. - The use of simulation models for the playing of individual situations.	- To strengthen the exercises in all sectors of CI through the examples of good practice; - To include external experts in the exercises; - To strengthen public-private partnership through exercises; - Croatia can become a mentor to other Member States in the region, which are at the stage of approaching the full membership in the EU.
Weaknesses	**Threats**
- Low level of awareness of strategic management may limit the effects of exercises; - Lack of knowledge of providers of exercises; - Failure to comply with the specifics of each organisation in the implementation of exercises; - Lack of financial and other resources.	- Narrow departmental or management interests which might harm the national interest; - Non-systemic implementation of exercises in practice causes serious problems and reduces the level of CI protection.

4 ESTABLISHING A SYSTEM OF SENSITIVE DATA EXCHANGE IN CRITICAL INFRASTRUCTURE

The makers of the model of managing CI protection in the Republic of Croatia note that the functioning system of information exchange is one of the key preconditions for the smooth functioning of the system for CI protection. The protection of information has, in the information age, an extremely important role in the systemic approach of risk management for the operation of CI. The foreseen holistic approach in the field of information security linked to CI includes the necessary steps to ensure the establishment and functioning of an information system for the protection of critical/sensitive data.

The proposed model of information security is based on the strategic and normative documents, which were adopted in the Republic of Croatia. In the review of existing

legislation it can be seen that it contains all the necessary foundations which enable the practical establishment of the information system of transmission of key data in CI.

The organisational structure of the information system for management of CIprotection is pyramid structured regarding the foreseen model, which was discussed in the initial analysis of the feasibility study. Given the necessary resources and the possibility of establishing NCCI the only realistic model is model No.1. Setting up the system and all the necessary resources for the functioning of NCCI would in model No. 3 wherein the NCCI is foreseen as an independent organisational unit within the offices of the Government of the Republic of Croatia, exceed the manageability and the rationality of the needs of invested resources. As a result of the foregoing, it is necessary to take into account in the analysis of the factors for the establishment of an information system the only real proposal for the establishment of the NCCI, to be organised as an internal organisational unit of NPRD. This will ensure the continuation of the already implemented measures for the establishment of an information system for the key data exchange and partly the use of already existing resources in the field of key data protection.

The proposed organisational structure that is organised from the highest point is appropriate and expected. The highest strategic place is organisationally represented by the Government of the Republic of Croatia, hereinafter managing the system through the National Council and NCCI, all the way to the CI managers as the lowest point of the system. With that related requirements for the establishment of an information system are common, but include the necessary basis, which would allow for the beginning of the establishment of the proposed information system. To the extent these initial requirements just one essential information is missing, namely on which basis the ensurance of financial resources for the establishment of this system will be carried out. It is not clear from the proposal whether the financial foundation of the construction of the system will be provided directly in the context of the Government of the Republic of Croatia, or the system will be planned and financed from the resources of NPRD as an additional range of resources in its budget. The obligation of direct managers is also not clear in relation to the establishment of this system or provision of software and hardware prerequisites for that part of the system which will need to be established for the transfer of key information between operators of CI and NCCI or sector security coordinators (departmental ministries).

There is a dilemma whether the use of the BYOND devices in the system of CI data exchange is authorised or appropriate. In any event, it is positive that these frameworks foresee that

already in the proposal of the model because thus this problem will be given enough attention for the systemic installation of the use of these devices.

The proposed technical solutions of establishing a two-way independent parallel communication system are 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 pull behind the choice of the technological solution, which among other things will have to be compatible with the current system, which is in use in the State Administration.

Among these requirements, it is particularly necessary to highlight the competence of the personnel that will be needed for the establishment of this system. Below, the layout of the training system of all employees in the system of CI protection is missing. In part, this is defined below under the tasks of the NCCI.

In the context of the proposed tasks of the NCCI in the sensitive data exchange the things are foreseen in the appropriate format. In the analysis, we estimate that most problems, in addition to adequate financial resources, will be raised in the substantive defining the information which will be eligible for the transmission through this information system. We definitely suggest trying to be based on 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 the strategic management will define as a business secret in the companies (operators). This part can also due to a competitive relationship, where there will be more operators on the market, which deal with the same or similar content, bring some problems. These problems are going to result in deterioration of an appropriate public-private partnership and to reflect on the quality of cooperation. Although the Republic of Croatia introduced a "top-down" approach of introducing a system of CI protection, 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 sensitive data. For this reason, it is necessary to pay particular attention to these elements.

From the proposed model it is not clear on which part of the information communication means, which are already in use, the proposed model for the transmission of thesensitive data of the protection system will be upgraded to. In the continuation of the making of the model proposal it would be necessary to assess what resources already exist and to suggest the upgrade of that part of the information system necessary for the establishment of the target

state. In this context, it will be easier to realistically assess the financial aspect of the necessary funds for the necessary upgrading of the system.

Not feasible	Partially feasible	Entirely feasible
	X	

Positive indicators:

- NPRD already carries out a key part of tasks in the field of coordination and development of the CI system in the Republic of Croatia;
- The knowledge and experience acquired by the employees of NPRD in the field of the establishment and functioning of the system of CI will be the key generator of the skills necessary also for the future establishment and functioning of the NCCI and the related tasks in the field of the sensitive data exchange;
- NPRD has developed certain segments of the information system, which will be in this case possible to upgrade to the corresponding whole;
- The legal basis in the field of the classified information protection and management of cyber threats is in RC quite properly set. Because of that, we estimate a small supplement in the field of systemic Act 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 of CI protection;
- The applicable information security standards can be an important help to the system measures of the introduction of the system and the provision of minimum conditions for its safe and continuous operation;
- The proposed solution, where the NCCI represents a central co-ordination body, is also good in the light of the establishment of a secure information-communication system;
- The Republic of Croatia ranks among the small countries, so the rational use of resources is a very important factor in the adoption of such important decisions such as the setting-up and placement of the NCCI.

Negative indicators:

- In the case of a legal incompleteness of the authorities and duties, difficulties in the coordination of other ministries may arise in the field of their tasks related to the establishment of a comprehensive information system, as the proposed model now provides for;
- The responsibility to provide financial resources for the financing of the establishment of the proposed information system is not evident from the proposed model;
- Hereinafter this problem also appears in a rough estimate of the necessary financial resources that will be necessary to establish a functioning system;
- It will be necessary to foresee in more detail the relationships in the context of public-private partnership and in particular in the extent of resources that each side will have to invest in the construction of such a system;
- For the effective functioning of the safe information system it will be necessary to provide additional human, material and financial resources in the NCCI. At the moment, when the countries face with the rationalisation of expenditure for their operation it will be very difficult to convince the ruling policy to give additional funds to the menitoned field. The risk of imposing the stablishment and the provision of the functioning of the NCCI only by an administrative act to NPRD, and ensuring the funds from the scope of the current resources for the operation of NPRD. Without additional resources, the NCCI, despite the establishment, would not be able to carry out all the tasks foreseen in the field of ensuring the operation of the security system by the transfer of key data;
- A great dependence for the establishment and realisation of the proposed model on the awareness of policy regimes on the importance of the regulation of this field of CI protection.

Indicators for assessing progress:

- Understanding of the ruling policy and the validation of model No. 1 and consequently the establishment of a secure information-communication system;
- Amendments to the existing legislation;
- Allocation of additional financial resources for NPRD and other national institutions;
- Providing additional human resources for the operation of the NCCI and secure information and communication system;
- Number of participating organisations and representatives;
- Percentage of carried out set tasks;
- Number of events organised by NCCI (training, checking links, audits, counselling).

Figure 28: SWOT analysis of establishing a system of data exchange in critical infrastructure

Strengths	**Opportunities**
- Continuation of the current processes in the NPRD as the central organisation for the coordination of the establishment of CI system; - Established inner circle of experts in the field of CI protection; - In the national system and with operators NPRD is already recognised as the central body of the previous coordination; - The strengthening of the national network of experts; - Given the current organisation, the best and the most rational approach to achieve the objective; - To establish an appropriate situation lesser corrections of existing legislation are required;	- Raising awareness of the importance of CI protection; - Better possibility of coordination and the safe exchange of sensitive data; - The cutback of cost of establishing a system for the safe transfer of data; - The designation of the state institution which will in the future carry the weight of the co-ordination and development of information system of CI; - The central body for exchanging experience and good practice; - Strengthening the public-private cooperation; - Appropriate arrangement of the systemic exchange of information with the EU and other international partners in the field;
Weaknesses	**Threats**
- Harder achievement of consensus due to the incompleteness of competence and the necessary financial resources; - Regulation of the relationships of the authorities and responsibilities; - Harder achievement of the objective group among the economic part of CI operators.	- Narrow departmental interests which might harm the national interest; - Failure to provide additional resources for the establishment of an information and communication system in NCCI and the realisation of the intended model No. 1; - Low awareness of the ruling policy about the need for the implementation of the proposed model of setting up a secure information-communication system.

5 A MODEL OF PUBLIC-PRIVATE PARTNERSHIP IN CRITICAL INFRASTRUCTURE PROTECTION

It should be remembered that an effective model of public-private partnership is a key factor that will considerably improve the quality and speed of building an effective system of critical infrastructure protection in the Republic of Croatia. The drafters are well aware of this fact,

and they in particular highlight that fact in their proposal. Unfortunately, the situation in transition countries, including the Republic of Croatia, especially when it comes to companies that are in majority owned by the state, is primarily focused on satisfying narrow political and economic goals, which are often not based on good governance and care for continuous operation of critical infrastructure. Most often we conclude that the country with its governance structures is a bad master. Unfortunately, the transition of these companies into the hands of private owners in the field of the management of critical infrastructure is not significantly improved. Private owners in transition countries follow the main objective, which is reflected in the profit and investment in the maintenance and safe operation of critical infrastructure is not one of their important strategic objectives. In particular, in the case of certain multinational companies, whose financial and other power pressure on the governments of the countries in transition, thereby achieve adoption of a milder and more lax legislation, which they later can avoid. Unfortunately, the Republic of Croatia is no exception in this process, which has very negative effects on the state of critical infrastructure protection in the country. Therefore, the key factor for ensuring an adequate protection of critical infrastructure is the country with its strategic management itself. It is necessary to emphasise that the Republic of Croatia, unlike other transition countries in the region, has quite a well defined legislation on public-private partnership. This model is identified as a key also in the strategic documents in the field of ensuring national security, critical infrastructure protection and measures to prevent terrorist threats. The newly emerging National Security Strategy should in the first draft also contain a part connected with critical infrastructure protection and the importance of public-private partnership. This is definitely one of the key mechanisms for a more effective implementation of the system, given the limited resources that are available in both the public as well as in the private sphere. The practice is unfortunately different, so in a real environment, this model of partnership is not yet fully operational.

In the area of raising awareness of strategic management in enterprises it is necessary to form the information on the importance of continuous operation of critical infrastructure into the business framework of competitive advantages and business success of the sound operation of infrastructure. The financial aspect for continuous operation of critical infrastructure should be the message factor that will be better understood by the strategic management of business organisations, which will thus position critical infrastructure protection as one of the major priorities for the successful performance of their companies. Financial investments in critical infrastructure protection should become investments in continuity and efficiency of their organisations and not mere costs.

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 in the later period the functioning of critical infrastructure protection. In making strategic documents and amendments of legislative frameworks in the field of public-private partnership in the Republic of Croatia, 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 authorities and responsibilities also at the level of critical infrastructure operators themselves. This is an important basis for the establishment of long-term trust among all partners in the process of critical infrastructure protection in the Republic of Croatia. Each participating entity needs to meet the agreed things that will be adopted in the forum. The cultural dimension of the agreement on the exchange of important information will also have a major importance, which will not be aimed at the general public.

Through a concrete analysis of the proposed model it can be stated that the legal basis needs minor adjustments, which will further define the basis for a public-private partnership in CI protection. We are pleased by the fact that it was the desire of preparers to derive from examples of good practice offered by the example of Great Britain and Australia. Although these are two countries with vastly greater volumes of resources, the primary solution is the NCCI, which is as a central institution, among other things, responsible for the appropriate platform in which a public-private partnership is developed, adequately designed.

The model of public-private partnership in the Republic of Croatia foresees in the direction of a joint long-term relationship, where public and private environments recognise their advantages and benefits. Of course, thus it is on the other hand willing to accept the responsibilities arising from this relationship and agreement. Given the scarcity of resources on both sides, this lever is the only appropriate one if we want to talk about a comprehensive approach to risk management for the smooth functioning of CI. Although the drafters for the most part assume that the public sector is the one that will transmit knowledge to the private sector, we believe that there should be a two-way process. The public sector has problems understanding the dynamics and needs of a complex business environment, therefore, it sometimes by their own actions and the preparation of legal solutions, without the presence of the private sector, carries them out unsystematically and in particular anachronistically. However, it is necessary to look at knowledge transfer in both directions, mainly with the aim of reducing costs and increasing efficiency. As well as in the national interest, it must also be

in the interest of private operators of CI to run continuously, thereby not only ensuring the smooth functioning of the community, but also generating profits from business operations.

The levers of public-private partnership in the area of CI protection, which the model envisaged, are wide enough to provide the necessary basis for the concretisation of activities in this area. It is important to highlight the implementation of joint projects, which reinforce the trust and mutual cooperation.

Good practices already exist in the Republic of Croatia, which have their basis also in the strategic documents, namely the National strategy for cybersecurity and the National strategy for the prevention of terrorism. In both public-private partnership is highlighted as one of the remarkably important models for achieving strategic goals. An important finding binds on the fact that the drafters correctly understood the width of the importance of public-private partnership and they included a very wide range of subjects in it that may via their operation add an added quality in the field of public-private partnerships and in the entire field of critical infrastructure protection. Here they are not confined to the institutions of national security, but entities of private security, interest links from the area of corporate and private security at the national as well as international arena are also correctly included.

In the concrete proposal of the conditions for the realisation of those requirements to establish an effective system of public-private partnership, the drafters suggested 6 basic processes. All proposed processed No. 2-6 are appropriate and consistent with realistic expectations that their realisation is necessary to increase the efficiency of work in this area. In this context, the importance of education module needs to be especially highlighted, which will in long term allow for sufficient experts. The current dynamics of development and the environment urgently need them to properly undersand and improve the state of the public-private partnership with their new knowledge and quality. It is important to also focus on project fundraising through various tenders within the EU and beyond. Total integration and preparation of project activities will be an excellent opportunity for even closer cooperation between the public and private sectors.

Regarding the proposal for the establishment of a permanent national body which would, according to the proposal, be named the NVCI caution would be advised. The risk of duplication and an excessive number of bodies in the field of critical infrastructure can become counterproductive. In this context, we would propose a consideration whether the mechanisms that are already in place can serve as the exchange of key interests in the field of critical infrastructure protection. NCCI should definitely become the central body, which will have the task of supporting only these forums, whose task will not only be to support the

mentioned forums, but will in a certain stage of development take more concrete tasks to define and coordinate the common interests of all stakeholders of public-private environment. The currently foreseen tasks of the Forum on critical infrastructure (NVCI) are rather widely defined. The question is if the Republic of Croatia can, due to the scarcity of their resources, afford the creation of a further body, which would in this complex structure work in this specific area.

In any event, the proposed model of establishing public-private partnership can be assessed as correct and feasible. Some additional analyses and elaborateness of specific solutions that will ultimately ensure an effectively functioning system of public-private partnership will be submitted in its direct execution.

Not feasible	Partially feasible	Entirely feasible
		X

Positive indicators:

- NPRD now performs an essential part of the tasks in the field of coordination and development of the system of CI in the Republic of Croatia. In this context the activities of communication and coordination are already under way in order to integrate the private environment in the processes of CI protection. This can serve as a basis for the continuation of processes;
- Knowledge and experience acquired by the employees in the NPRD in the field of establishment and functioning of the CI system will be a key generator of the necessary skills for the future establishment and functioning of the NCCI and thus also the work int he field of strengthening the levers of public-private partnership;
- NPRD has already developed certain segments of public-private partnership in the areas associated with the system of protection and rescue and civil protection, which in this case will be upgraded to the appropriate whole;
- The legal basis for public-private partnership represents a solid foundation for the integration of the protection of CI. Because of that, we estimate the need for amendments in the field of strategic and legal documents (Act of Critiacl Infrastructure and Act of Public-private partnership) in which the leverage of public-private partnership will be further embedded;

- Certain educational institutions, among which we highlight the University of Applied Sciences Velika Gorica, introduce into their curricula the contents related to critical infrastructure and the importance of public-private partnership in this area;
- The Republic of Croatia is one of the smaller countries, therefore, the rational use of resources is an important factor in taking such important decisions related to the protection of CI. From this perspective, the quality of the system of public-private partnership is even more important and vulnerable;
- Given the fact that the processes of privatisation are still very active in the Republic of Croatia, this is also an opportunity to start setting at this stage relevant foundations of subsequent effective public-private partnership in CI protection.

Negative indicators:

- Failure to understand the importance of the integration of the private environment in certain processes of harmonisation of interests in the field of CI may result in lower response of CI managers coming from the private environment;
- According to the proposed model it is not possible to figure out the financial implications so it is impossible at this stage to analyse and assess them;
- The proposed new mechanisms for coordination and harmonisation such as the Forum on critical infrastructure should be very sensitively accomplished. It is necessary to consider the current relationships and competences of the already established mechanisms or forums and to avoid duplication or the excessiveness of the bodies in the field of management. Any incomplete solution can have a very large impact on the entire system. In particular, it is necessary to avoid an excessive number of authorities or bodies. For this reason we suggest the incorporate tasks of strategic coordination in to National security Council;
- It will be necessary to foresee more in detail the relationships in the context of public-private partnership and in particular in the extent of the resources each of the parties will need to invest in the construction of such a system;
- The risk that NPRD or NCCI will not become the central point of support on which the system of public-private partnership in the field of CI protection will be based;
- Great dependence for the establishment and implementation of the proposed model on awareness of the policy and company management about the importance of organisation in the field of CI protection.

Indicators for assessing progress:

- Understanding of the ruling policy and confirmation of model No. 1 and thus the establishment of effective bases for the development of public-private partnership;
- Amendments to the existing legislation;
- Identification of additional financial resources for NPRD (NCCI) and other state institutions on projects in the field of public-private partnership;
- Providing additional human resources for the operation of NCCI and projects of public-private partnership;
- Number of participating organisations and representatives;
- Number of registered projects under the acquisition of financial assets;
- Number of approved projects;
- Percentage of carried out set tasks;
- Number of events organised by NCCI.

Figure 29: SWOT analysis of establishing a system of public-private partnership

Strengths	**Opportunities**
- Continuation of the current processes in the NPRD as the central organisation for the coordination of the establishment of CI system; - Established inner circle of experts in the field of CI protection; - In the national system and with operators NPRD is already recognised as the central body of the previous coordination; - Strengthening the national network of experts; - Good practices from some other areas that are indirectly related to CI protection; - To establish an appropriate situation lesser corrections of existing legislation are required;	- Raising awareness of the importance of CI protection; - The cutback of cost of establishing a system of public-private partnership; - The designation of the state institution, which will in the future carry the weight of the co-ordination and development of public-private partnership; - NCCI as the central body for exchanging experience and good practice; - Strengthening the public-private cooperation in the field of international projects; - Appropriate arrangement of the system of public-private partnership in the international arena;
Weaknesses	**Threats**
- Harder achievement of consensus due to the incompleteness of competence and the necessary financial resources; - Regulation of the relationships of the authorities and responsibilities; - Harder achievement of the objective group among the economic part of CI operators.	- Narrow departmental interests which might harm the national interest; - Lack of interest of the private sector to participate; - Low awareness of the ruling policy about the need for the implementation of the proposed model of setting up an effective partnership in the filed of public-private partnership; - Low level of knowledge of human

	resources potential, which will be determined for the development of this mechanism.

6 ANALYSIS OF PROPOSED RESOURCES NECESSARY FOR IMPLEMENTING PROPOSED SOLUTIONS IN THE PROJECT AND FINANCIAL ANALYSIS

Through the feasibility analysis of the proposed model to establish a system of CI protection in the Republic of Croatia, we included among factors a concrete analysis of the resources needed to carry out each of the main goals set by the RECIPE project through the establishment of NCCI, the establishment of an effective system for the key information exchange, and the system of public private partnership in the field of CI protection. In the strategic assessment of the necessary financial resources mainly the first two are very dependent on the provision of sufficient financial, human and other resources for their final implementation. Of course, in the context of the entry into force of the first objective, the decision of the Government of the Republic of Croatia on one of the four proposed models of the establishment of NCCI will play a key role. In the analysis and evaluation, we anticipated that model No. 1, which foresees the establishment of NCCI within NPRD, will deliver the most optimal effects and will represent a significant streamlining of the necessary funds. Here we emphasise the complexity of the second set goal. The establishment of a system for the exchange of key information will represent primarily from the financial, but partly also from the technological and human resources point of view, a major challenge. Its rationality and feasibility will strongly depend on the chosen technological solutions and understanding of all concerned stakeholders about the need for this project. This model will be the first serious test and answer to the question whether the bases for the operation of public-private partnership are appropriate. Namely in the realisation of the objective of establishing an effective system of secure communication all partners of public and private environment of CI management will have a very important role. The Republic of Croatia will have the largest part of setting up the first two goals through budgetary resources, which are in the current situation very limited. For this reason it will be necessary to resort to those solutions that will be at any given time the most optimal depending on the funds invested and the results obtained. Another important factor will be represented by the CI managers themselves, who will, with their financial and other participation, need to ensure the continuity of functioning of CI which they manage. An important source of funds must be presented by the European projects

in the field of CI protection. There, all parts of the system will be given once again a very important role. The RECIPE project represents an excellent display of this, as an example of good practice in the area of obtaining funds from international mechanisms to resolve certain objectives in the area of building an effective system of CI protection.

In conclusion, the need and the importance of adequate human resources should be mentioned. It can be confidently concluded that through the educational structure of the state administration of the Republic of Croatia the whole system hasn't a sufficient number of highly qualified experts in the fields covered by the model of CI protection. Especially if we take in consideration proposed model of development CI protection. We hope that the prioritisation of key processes in the country will place CI and its system of protection on a high position. In this case, when making the necessary decisions it will possible to redistribute that part of the experts in the NCCI that will be essential to raise the volume and quality of previous processes in the field of the CI protection system. An important part of ensuring key personnel must be taken by the educational system, which will through its programs give relevant and applicable knowledge for future experts in the field of CI protection. Finally, in the private sector in terms of better material and financial conditions, especially in organisations that manage CI, we can talk about very high-quality personnel, which came from the field of public administration in search of better financial conditions some time ago. The advantage of these experts is to know the functioning of the two areas, which is crucial for effective work with the system of CI protection.

Below, let's take a look at some factors in the area of the necessary resources that will have an impact on the realisation of the proposed model:

- The decision on the amount of budgetary funds for the realisation of the model;
- The share of invested funds of CI managers;
- The percentage of the gained projects and the amount of the related assets;
- The amount of private resources provided through the public-private partnership;
- The appropriate scope of human resources;
- Proper training of human resources.

Figure 30: SWOT analysis of the resources required for establishing a model of systemic CI protection

Strengths	**Opportunities**
- NPRD as the national coordinator for CI actively introduce systemic solutions in the field of CI protection; - Some examples of good practice of public-private cooperation in the field of financing joint projects; - Specific experience in acquiring European and other assets; - Partly set up curricula in the field of CI protection; - Specific scope of experts in the field of CI protection in public and private organisations; - Examples of good practices in integrating the profession into interest groups.	- Raising awareness of the importance of CI protection; - Reducing the burden on the public budget with a good public-private partnership; - NCCI as the central body for exchanging experience and good practice; - Strengthening the public-private cooperation in the field of international projects;
Weaknesses	**Threats**
- Harder achievement of consensus due to the incompleteness of competence and the necessary financial resources; - Regulation of the relationships of the authorities and responsibilities; - Harder achievement of the objective group among the economic part of CI operators. - Necessary amendments to existing legislation.	- Narrow departmental interests which might harm the national interest; - Lack of interest of the private sector to participate in financing; - Low awareness of the ruling policy about the need for the implementation of the proposed model of setting up an effective partnership in the field of public-private partnership; - Failure to provide the necessary budgetary resources.

7 RESULTS AND CONCLUSION

The feasibility study of the foreseen model of critical infrastructure protection in the Republic of Croatia points to the fact that it can be implemented in all steps. Structurally, the study needs to be in some parts concretised in more detail. This will of course be affected by the

decision of the competent decision-makers for which of the suggested solutions they will decide. Below, the mentioned solutions will be concretised and further analysed in detail from all angles. The biggest shortcoming of the proposed model is represented by the estimate of the needed financial resources that will be necessary to provide for the realisation of the proposed. This is partly understandable because at this stage the model identifies a variety of solutions that will be with the appropriate choice of one of the proposed options later concretised, including the foreseen resources.

NCCI will in any case constitute a turning point, which will by taking the correct decisions and measures represent an important step forward to the appropriate systemic regulation of the CI protection field. Proper operation of the NCCI will provide an adequate platform for guidance, help, exchange of good practice, advice and ultimately control over the measures taken at different levels of functioning of the CI protection system. This support, which will be given on the one hand by the NCCI to the strategic management (the Government of the Republic of Croatia and Sabor/Parliament with its commissions) in the public sector, as well as to the operators of CI in the private sector, will represent an added value, which will be reflected in the quality of decisions, better understanding of the situation and the problems, a higher level of awareness and ultimately higher financial resources to ensure the effective functioning of the CI protection system.

In the information age, with the need of rapid and secure transfer of data, the awareness of the strategic structures in the public and private environment will play an important role in establishing a system of k sensitive information exchange in the field of CI. All three main objectives which have been placed in the RECIPE project, are closely intertwined and are in their implementation in a strong relationship of interdependence. This means that the system of key information transfer will be successfully implemented only in case of effective realisation of the model, which will be chosen by the Republic of Croatia for the establishment of NCCI. Given the fact that the ownership of CI is in public and private property, however, it is impossible to expect the implementation of any project in this area without a solid and effective public-private cooperation. Especially not in the direction that could be evaluated as a systemic approach that represents optimal solutions according to the height of the financial inputs and the results obtained. In smaller countries, including the Republic of Croatia, this is crucial. Solutions that are essentially offered by the drafters of the model are in the field of the safe transfer of key data in the field of CI protection, appropriate and comparable in all standard lines of international practice. The volume, efficiency and the amount of resources will be strongly influenced by the selected model of the establishment of

NCCI. It is necessary to strive to the greatest use of existing information facilities available to the state administration in the field of classified information protection, and to systemic upgrading of a specific part of the software and hardware to the existing IT backbone. In any case, relevant foundations have already been conducted in the Republic of Croatia, which are clearly outlined through a normative legal aspect in the field of the protection of classified information, coping with cyber threats and ultimately the protection of business secrets, when talking about the private sector.

It is difficult to assess whether a well-functioning model of public-private partnership is the need or the result of a properly functioning system of CI protection. Recognising that an increasing proportion of CI passes into private ownership, the good cooperation between the public and private environment will in the future have an even more important role. Appropriate awareness of strategic leadership in both systems must result in the pursuit of common goals in the direction of positive factors which are brought about by such cooperation. The public sector with the State at the forefront must clearly support this cooperation due to the dependance of the society on the continuous operation of CI, on the other hand, the continuity of the functioning of the private sector, which is, in certain cases, the operator of CI, brings better business and an adequate income. In an era of limited resources, however, cooperation on major projects is the only possible one. Participation in joint projects, including in the framework of the EU, will further strengthen the cooperation and put it on stronger foundations of good practices and experiences gained in the process.

The main factor certainly remains the political will and determination to establish and systemically regulate this important area of critical infrastructure in the Republic of Croatia. Although it is necessary to define clearly at the end that the Republic of Croatia has set up a solid foundation of the system of CI protection. The legal framework and the role that in this context was brought about by NPRD with the national coordinator for CI, deliver positive results. The RECIPE project is a good opportunity and gives the right bases to upgrade the system for CI protection. Thus the Republic of Croatia will become an example of good practice, which will be applied to other countries in the region, especially candidates for accession to the EU.

At the strategic level, however, it will be necessary to touch a few open issues that will, as a logical consequence of the implementation of the conclusions of the RECIPE project, have to follow in practice. Clearly it will be necessary to define the relationship and responsibilities between national, regional and local responsibility in the management of CI. It is true that the Republic of Croatia is a small country and these ratios do not play such a critical role,

however, they will need a proper attention. And for the end, it is necessary to stress the crucial moment, namely the appropriate criteria for defining CI in each sector and thus later also a realistic and rational definition of national and European CI. In this section we estimate the key role which the NCCI will bring.

REFERENCES

- Act on State Administration System, Oficial Gazette no. 150/11 and 12/13.
- 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).
- COM (2010) 673 final. The EU Internal Security Strategy in Action: Five steps toward a more secure Europe. Objective 2: Prevent terrorism and address radicalization and recruitment. Objective 5: Increase Europe's resilience to crisis and disasters.
- COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, Brussels, 28.8.2013 SWD (2013) 318 final. p. 2-11.
- Communication from the Commission, n. COM (2006) 786 final, Brussels 12.12.2006., p. 3.
- Conclusions of the European Council of 10/11 December 2009 on 'The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010-2014)'; 17024/09. (accessed, 07. jan. 2016)
- Council Directive 2008/114/EC of December 8.2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (SL L 345/75, 23.12.2008.).
- Croatia Workshop Evaluation Report, 2015.
- 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 December 2015).
- Croatian Parliament (2007) *Data Confidentiality Act*, available at: http://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka, (accessed on 20 December 2015).

- Croatian Parliament (2007) *Information Security Act*, available at: http://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti, (accessed on 20 December 2015).
- Croatian Parliament (2013) *Critical Infrastructures Act*, available at: http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, (accessed on 20 December 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).
- 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)*
- Croatian Standards Institute (2014) *HRN ISO/IEC 27001:2014 standard (information security)*
- 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 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 15 December 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 December 2015).
- Feasibility Study, Comparative Overview and Analysis, Part 1, October, 2015.

- Good practices manual for CIP policies, For policy makers in Europe, RECIPE project manual.
- 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 December 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).
- 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 January 2016).
- Keković, Z., Savić, S., Komazec, N., Milošević, M., Jovanović, D. (2010) *Procena rizika u zaštiti lica, imovine i poslovanja,* Centar za analizu rizika i upravljanje krizama, Beograd.
- Klaver, M. on behalf all RECIPE team (2011). Good practices manual for CIP policies, p.40-43.
- 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 December 2015).
- National standpoints, August, 2015.
- National Strategy of Cyber Security and Action Plan for Development National Strategy of Cyber Security, Official Gazette No. 108/2015.
- 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 15 December 2015).
- Decision on the determination of sectors from which the central government bodies identify national critical infrastructure and lists the order of the critical infrastructure sectors, Official Gazette No. 108/2013.
- Regulations of methodology for development of risk analysis of operations critical infrastructure, Official Gazette No. 128/2013.

- 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.
- Serbia Workshop Evaluation Report, 2015.

CONTENTS OF FIGURE

Figure 1: SWOT analysis of enforcing model No. 1…..... 22

Figure 2: SWOT analysis of enforcing model No. 3……... 24

Figure 3: Step A.I. Development and update of the normative framework of management …… 26

Figure 4: SWOT analysis of enforcing step A.I. …… 27

Figure 5: Step A.II. Coordination of work and activities of the stakeholders of the CI management system ……. 28

Figure 6: SWOT analysis of enforcing step A.II …… 29

Figure 7: Step A.III. Collection, analysis and information exchange ……. 30

Figure 8: SWOT analysis of enforcing step A.III. ……. 31

Figure 9: Step B.I. Identification of critical infrastructure …….…… 32

Figure 10: SWOT analysis of enforcing step B.I. …….. 33

Figure 11: Step B.II. Assessment of risks ……... 34

Figure 12: SWOT analysis of enforcing step B.II. ……. 34

Figure 13: Step B.III. Monitoring and evaluation …….. 35

Figure 14: SWOT analysis of enforcing step B.III. …… 36

Figure 15: Step B.IV. Monitoring and verification ……. 37

Figure 16: SWOT analysis of enforcing step B.IV. …… 37

Figure 17: Step C.I. Projects of public-private partnership …… 39

Figure 18: SWOT analysis of enforcing step C.I. ……... 39

Figure 19: Step C.II. Invitation to participate in the program of public-private partnership ……... 40

Figure 20: SWOT analysis of enforcing step C.II. ……. 41

Figure 21: Step D.I. Development and improvement of methodology for identification of CI …….. 42

Figure 22: SWOT analysis of enforcing step D.I. …….. 42

Figure 22: Step D.II. Training ……. 43

Figure 23: SWOT analysis of enforcing step D.II. …… 43

Figure 24: Step D.III. Counselling ……. 44

Figure 25: SWOT analysis of enforcing step D.III. …….. 44

Figure 26: Step D.IV. Exercises ……. 45

Figure 27: SWOT analysis of enforcing step D.IV. …… 46

Figure 28: SWOT analysis of establishing a system of key data exchange in critical infrastructure ……... 51

Figure 29: SWOT analysis of establishing a system of public-private partnership ……... 57

Figure 30: SWOT analysis of the resources required for establishing a model of systemic CI protection ……. 60

ABBREVIATIONS / ACRONYMS

CI	Critical infrastructure
EU	European Union
EC	European Commission
NCCI	National Centre for Critical Infrastructure
NVCI	National Council for Critical Infrastructure
RECIPE	Resilience of Critical Infrastructure Protection in Europe
NPRD	National Protection and Rescue Directorate

Feasibility Study of Serbian Model for Establishment of Critical Infrastructure Protection System

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

Date: 15. JANUARY 2016

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

CONTENTS

1 FEASIBILITY STUDY OF ESTABLISHING A SYSTEM OF CRITICAL INFRASTRUCTURE PROTECTION IN THE REPUBLIC OF SERBIA …….. 3

2 METHODOLOGY ……..... 5

3 THE MODEL OF PUBLIC-PRIVATE PARTNERSHIP TO ESTABLISH A SYSTEM OF CRITICAL INFRASTRUCTURE PROTECTION IN THE REPUBLIC OF SERBIA……..... 5

3.1 Human resources and the system of education of future experts in the field of critical infrastructure protection…… 7

3.2 The establishment of an appropriate legal framework for the operation of critical infrastructure ……... 9

3.3 The establishment of an adequate system of public-private partnership and trust among all stakeholders in the field of critical infrastructure protection ……. 10

3.4 Establishment of the relevant criteria for determining critical infrastructure in the Republic of Serbia……... 11

3.5 The establishment of an appropriate system of a clear definition of authorities and responsibilities in the field of critical infrastructure protection ……. 12

3.6 Implementation of the relevant European normative in the process of approaching of the Republic of Serbia to the EU ……... 13

3.7 Financial resources ……..... 14

3.8 Human resources and the system of education of future experts in the field of critical infrastructure protection ……. 14

4 ANALYSIS AND CONCRETE EVALUATION OF THE FEASIBILITY OF THE PROPOSED STEPS TO GIVE EFFECT TO THE SERBIAN MODEL FOR THE ESTABLISHMENT OF CRITICAL INFRASTRUCTURE PROTECTION ……. 15

5 CONCLUSIONS ……. 34

1 FEASIBILITY STUDY OF ESTABLISHING A SYSTEM OF CRITICAL INFRASTRUCTURE PROTECTION IN THE REPUBLIC OF SERBIA

The creation of an appropriate system of critical infrastructure protection constitutes an extremely demanding task for any country. Critical infrastructure 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. The complexity of the security environment and threats that arise for the functioning of this infrastructure put the state, its bodies and operators themselves in front of an extremely challenging task. 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 has occured in the EU as a term in the last twenty years. Terrorist threats, cyber-risk and natural disasters have set the need for continuity of critical infrastructure in the high priorities of the state regulation. Of course, it is necessary to realise that the system approaches of regulating that area are different from country to country. This diversity of 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 belongs to the group of countries where the organisation of the state and legal order stems from the European continental tradition. In this context, the state represents a very important and central place for the regulation of relationships in terms of the authorities and responsibilities of the institutions for regulating individual social processes. Managing and ensuring the continuity of critical infrastructure certainly belongs among them. Certainly it cannot be said that the Republic of Serbia has no 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 a 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 the Republic of Serbia has no experience in the field of the protection of key facilities, institutions and processes that are today terminologically defined as critical infrastructure. In this work not only in the Republic of Serbia, but in the majority of transition countries it has always come mainly to inadequate understanding of the term critical infrastructure and the process itself, which it brings together in its 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 in the direction of a market economy, in the extent of stakeholders that are important for the effective operation of the system of critical infrastructure, private capital appeared, which through the ownership in companies which manage critical infrastructure is becoming one of the key factors. This represents that one additional moment, which is crucial for the perception of changes in the situation from the system which operated 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 stakeholders understand the positive aspects of the regulation of the system of critical infrastructure protection, and are from this point ready to invest the necessary efforts and other resources in building this system. In this stage of development in the Republic of Serbia, the level of awareness and understanding of the importance of uninterrupted operation of critical infrastructure and of the process itself covered by critical infrastructure is a necessary factor as a relatively new concept in social relations. From this perspective, it is necessary to congratulate the research team at the Faculty of Security, which also through the RECIPE project guarantees exactly that basis which is essential for faster and more effective steps in establishing a system of critical infrastructure protection. This is definitely a proper understanding of the importance of critical infrastructure and familiarisation with the possible steps that are the result of the comparative study and good practices, which are included in the proposal for the establishment of the Serbian model of building a system of critical infrastructure protection.

2 METHODOLOGY

The methodological framework of the feasibility study of the proposed model to establish a system of critical infrastructure protection of the Republic of Serbia is based on an interdisciplinary approach of assessment of the proposed model. Through the method of deduction, we checked the proposed solutions according to the wider social processes. In the following part the method of induction was used, in which a concrete solution was analysed in the direction of placing conclusions and their impact for a further understanding and the response of the wider social environment, especially the institutions of the state and operators of critical infrastructure, to the proposed concrete solutions.

By the method of analysis, we dissected the individual components of the proposed model and analysed the individual processes and factors. The analysis of the individual components of the key processes in the field of critical infrastructure has also allowed to set certain indicators that can, in practice, later serve the operators as a proper basis and help in the evaluation of the implementation of the proposed model into the direct practical social environment. By the method of synthesis we then ensured that all the essential findings of the individual parts of the process were combined into a whole and evaluated from the perspective of the feasibility and effectiveness of the overall operation of the proposed model. Of course, in the feasibility study, we could not avoid the comparative historical method, since the historical dimension of the development of each company is one of the key determinants to understand the situation and the consequences of the company's development in the Republic of Serbia and of course the current regulation of relations in the field of critical infrastructure protection.

Through the method of expertise we have, with the involvement of all of the above methods, also considered the direct good practices and our own years of experience in setting up systems of critical infrastructure protection in the various projects within individual countries in transition in the region.

3 THE MODEL OF PUBLIC-PRIVATE PARTNERSHIP TO ESTABLISH A SYSTEM OF CRITICAL INFRASTRUCTURE PROTECTION IN THE REPUBLIC OF SERBIA

In the introduction, it should be noted that the establishment of this model is a key dimension for the success of later establishing a comprehensive and effective system of critical infrastructure protection in each country but also in the Republic of Serbia. Without

establishing this cooperation all attempts are doomed to low-level performance, and often non-systemic measures which bring their increase of the need to the resources invested. The result of such an approach through clearly established experiences in several cases is lower than expected.

The next fact, which is very important in the introduction of the analysis of this part of the model, is the role of the state. The state represents the central point in any system and the motor in ensuring an effective system of critical infrastructure protection. The state's biggest interest is, in fact, that critical infrastructure, irrespective of which ownership structure the organisation that manages critical infrastructure is currently in, operates continuously, thus ensuring the smooth functioning of the community. From this perspective, it is necessary to put the understanding of the situation and the measures into raising of awareness and proper understanding of the importance of critical infrastructure in the strategic management of the state and its institutions. The proposed model of the combined "bottom-up" approach is optimal at this moment of the development, mainly because of the mentioned ensurance of proper understanding of the importance of uninterrupted operation of critical infrastructure in the strategic management of the Republic of Serbia on the one hand and on the other hand the strategic management of the companies that manage critical infrastructure. It is a fact that at this moment the academic and professional environment is at the highest level of awareness of the importance of this process for the community and according to the amount of knowledge and experience that has been gained through a variety of research projects, analysis, cooperation with other partner institutions of the international environment. This means that the success of this model is very heavily dependent on the readiness, pervasiveness and the energy of the academic community which has to take the leading role in this part of the realisation of the proposed model with the support of various expert associations. In any case, it is necessary to realise that at the time when the "bottom-up" model reaches a critical component, which will be reflected in an appropriate level of awareness of key state structures in the Republic of Serbia, the model will be required to be replaced with the "top -bottom" approach where the state will with its own organisational levers take over the essential legal and substantive steps for the final establishment of an effective model of critical infrastructure protection. This 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 determining the criteria for determining critical infrastructure in specific sectors. In the comparative practice, because of the different views, understanding of the importance of critical infrastructure, and not least because of partial interests of individual

organisations and also state institutions (ministries), here came the biggest tensions that accompanied by inadequate management of this process endangered the functioning of the entire system of critical infrastructure protection in the country. This position could bring about significant delays in the development of a system of critical infrastructure protection, which had the effect of undermining the normal functioning of the wider community, which was in the situations of the need of continuous operation of critical infrastructure directly affected.

Below we present the key factors that will influence the pace of implementation of the proposed solutions and the establishment of an effective and internationally comparable system of critical infrastructure protection in the Republic of Serbia.

- Raising awareness of the importance of critical infrastructure in key groups forming public-private partnership;
- Establishing an adequate legal framework for the operation of critical infrastructure;
- Establishing an adequate system of public-private partnership and trust among all stakeholders in the field of critical infrastructure protection;
- Building appropriate criteria for determining critical infrastructure in the Republic of Serbia;
- Establishing an appropriate system of a clear definition of the authorities and responsibilities in the field of critical infrastructure protection;
- Implementing the relevant European norms in the process of the Republic of Serbia in the EU;
- Financial resources;
- Human resources and a system of education of future experts in the field of critical infrastructure protection.

3.1 Human resources and the system of education of future experts in the field of critical infrastructure protection.

As was already indicated above, this work is about the key factor that will considerably improve the quality and speed of building an effective system of critical infrastructure protection in the Republic of Serbia. It was found that within the academic community, there is currently the highest level of awareness and knowledge of the field in question. This means that this segment will be the key in the measures of raising awareness and knowledge of two key groups that are formed by the strategic management in public administration and the

strategic management in business organisations that manage critical infrastructure. The model, in step 2, "Initial assessment", places too high expectations on strategic management in enterprises, so that it can with its links to key state institutions form a suitable initial factor that will significantly stimulate the exchange of information and in particular the need for proper protection of critical infrastructure. Unfortunately, the situation in transition countries, including the Republic of Serbia, especially when it comes to companies that are in majority owned by the state, primarily focuses on satisfying narrow political and economic goals, which often are not based on good governance and concern for the continuous operation of critical infrastructure. Most often it is concluded that the state with its own management structures, is a bad master. Unfortunately, also in the transition of these companies into the hands of private owners the state of management of critical infrastructure is not significantly improved. Private owners in transition countries follow the main objective which is reflected in the profit and the investment in the maintenance and safe operation of critical infrastructure is not one of the important strategic objectives. In particular, in the case of certain multinational companies, which with their financial and other power press on the governments of the countries in transition, thereby achieving adoption of a milder and more lax legislation, which they later can avoid. Unfortunately, the Republic of Serbia is not an exception in this process, which has very negative effects on the state of protection of critical infrastructure in the country. Therefore, the key factor for ensuring an adequate protection of critical infrastructure is the state itself with its strategic management. As a result, the academic environment has in the initial step that essential task to raise awareness for the representatives of the ruling policy and strategic structures of the state administration, which in a later stage will be able to start to set up and coordinate the building of an effective system of critical infrastructure. The European path of Serbia will also take an important part in raising awareness, where through the processes of negotiating positions for the implementation of EU legislation, this part of the critical infrastructure will be significantly present. At least in the area of raising awareness and perception of the seriousness that is required by the regulation of this field, this process will help significantly in that key institutions and strategic management of the Republic of Serbia will position more importantly the area of critical infrastructure protection in the list of national priorities. In the area of raising awareness of strategic management in enterprises it is indispensable to form the information on the importance of uninterrupted operation of critical infrastructure into the business framework of competitive advantages and business success of the sound operation of the infrastructure. The financial aspect for continuous operation of critical infrastructure

should be the message factor that the strategic management of business organisations will better understand and thus position the critical infrastructure protection as one of the major priorities for the successful performance of their companies. Financial investments in critical infrastructure protection should become investments in continuity and efficiency of the performance of their organisations and not mere costs.

3.2 The establishment of an appropriate legal framework for the operation of critical infrastructure

The establishment of an appropriate legal framework is another very important factor, to which also the builders of the Serbian model of critical infrastructure protection draw attention very strongly. Political culture reflects the fact that the legislation in itself is not a guarantor for its effective implementation in a real environment. Preparation and adoption of appropriate legislation represents only the first step of the several necessary to ensure an effective and high-quality system of critical infrastructure protection. The finding that the Republic of Serbia needs an appropriate strategic plan which will ensure in the form of a Strategy for critical infrastructure protection the key basis and the vision of regulating the field of critical infrastructure in the Republic of Serbia. In this section the so called National Forum for Critical Infrastructure in the formation will take on an extremely important role in the formation of the draft text, which will be duly discussed in public and in-house professional discussion, and thus a certain consensus will be reached. The perception of the need to draw up a new law concerning the protection of critical infrastructure is in place. In this part, the national institution (in the proposed model Directorate for Risk and Emergency Management), will again play an important role, which will be centrally responsible for the preparation and coordination of the aforementioned legislative proposal for critical infrastructure protection. In any case, the most difficult task will be related to the harmonization of all other national strategic documents and their amendments to the relevant basis for the implementation of the area of critical infrastructure protection. Critical infrastructure is, by its nature and content, extremely complex and from this perspective requires an interdisciplinary approach that is also reflected in the preparation of a strategic and legislative framework. Another very important factor is in the legislative field also the transfer of foreign legal solutions and practices into the legal system of the Republic of Serbia. All countries in transition have been exposed to this, especially those which have joined or are in the phase of integration into the EU. Due to the huge amount of legal

regulations, which must be reconciled through negotiation areas, adapted or newly adopted, it is often reached for the shortest route, namely the direct attribution of the solutions to the national legal framework. This path is without taking into account national specifics and good practices extremely harmful and the most frequently enacted situation in reality deviates significantly from the immediate needs of a dynamic environment. The model builders are very well aware of this and have paid special attention and warning to this problem. However, the international dimension and the need for harmonization of legal regulations also have positive implications, especially in the perception of the importance of the mentioned field of critical infrastructure protection in the ruling political structures in the Republic of Serbia, which are currently responsible for the political and the resulting administrative support to this nationally important project.

There is a fear that was considered in the preparation of the Serbian model, in order to transfer the legal over-regulation that is present in other areas also to the field of critical infrastructure protection. In any event, a very meaningful approach should be taken to the preparation of legal and regulatory provisions and in particular the relationships should be harmonized with all the other strategic, normative and other requirements.

3.3 The establishment of an adequate system of public-private partnership and trust among all stakeholders in the field of critical infrastructure protection

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 in the later period the functioning of critical infrastructure protection. In making a strategic and legislative frameworks in the Republic of Serbia, it is necessary to ensure the widest possible participation of proposals. This is an important basis for the establishment of long-term trust among all partners in the process of critical infrastructure protection in the Republic of Serbia. The proposed model respectively the "bottom-up" approach will in some forums that will be set up by the Republic of Serbia to exchange views and participation in the development of the system of critical infrastructure protection, have to be very cleary defined whether it is a voluntary association, or the matter will at a particular point[1] become a compulsory form of association. In any case, it is also necessary in the case of voluntariness to clearly impose certain limits and arrangements of functioning of the national forum for critical infrastructure

[1] See comment on page 3, where it will be necessary to change the approach at some stage.

protection. Each participating entity needs to meet the agreed things that will be adopted in the forum. Also the cultural dimension of the agreement on the sharing of important information, which will be aimed at the general public, will have a major importance. This factor is of great importance and it is impossible to regulate 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. The fact is that we have in this part at least two key categories of information, ie. 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 a company which manages critical infrastructure. In particular, it will come to the fore in cases when ownership passes into private hands and several companies that will be in the logic of market economy between them in competition will appear in a certain area. At this time, in the Republic of Serbia this should not pose a major problem as most of the major infrastructure companies are currently in state ownership and in most cases monopolists. Exempt is only the area of banking, where competition is very fierce. In this part, the Central Bank of Serbia will also need to play its role besides the state. This fact can be at the stage of drafting legislative framework and its establishment even a positive aspect, which with good ties between the ruling policy and strategic management in these companies can quickly deliver relevant results. Of course, it must be considered that the level of awareness in the two structures will be at an appropriately high level. In any case, the academic environment can play an important role in building this trust, offering a suitable platform for the initiative meetings, which will constitute an informal beginning of an important process.

3.4 Establishment of the relevant criteria for determining critical infrastructure in the Republic of Serbia

The definition of the criteria for determining critical infrastructure is a key issue of any building of this system. The Republic of Serbia in this context is no exception. This fact and the conclusion is defined in the proposed model for the establishment of the system of critical infrastructure protection in the Republic of Serbia. Rightly we may ask ourselves the question whether the proposed national forum for CI is that body which will produce the final starting points for the adoption of criteria for determining critical infrastructure. In any event, it is and it should be an important stakeholder in the management of professional discussion and formulation of key proposals. An essential component that must be clear in the awareness of

how important it is to determine the criteria for the preparation and adoption of appropriate criteria for determining what in the Republic of Serbia is actually critical infrastructure. The definition of the criteria is directly related to the extent of which systems, processes and activities will become critical infrastructure. This directly pulls behind the provision of adequate resources which will have to be provided by all stakeholders in the system of the protection of this infrastructure. In any case, the admission of the criteria for the determination of the critical infrastructure will be a political act since the professionally prepared proposal will be adopted by the Government of the Republic of Serbia, where certain political interests will be established. The Republic of Serbia will have to, in this process of public-private partnership, clearly realise that the total cost and providing resources will not be able to fully pass on the shoulders of businesses or organisations that manage critical infrastructure. This participation of providing resources should be adequately defined and guaranteed by both sides. Of course, the danger of promoting the interests of individual groups can occur during the phase of the preparation of the criteria, where with the expansion of the definition of critical infrastructure in specific sub-sectors, these stakeholders of the state administration or the economy in the continuation would expect a larger share of the budget or other financial sources. An excessive and unrealistic definition of the criteria for determining the critical infrastructure could result in the creation of a theoretically defined system which in practice cannot be established. The struggle to increase the impact among the institutions of the state administration represents a very important risk, which does not have a negative impact only in the field of the criteria but also in the field of the authority of control and subsequent management of the system of critical infrastructure, and, consequently, a higher impact and financial resources.

3.5 The establishment of an appropriate system of a clear definition of authorities and responsibilities in the field of critical infrastructure protection

As was already indicated above, the factor of clear authority and responsibilities is the next important moment that should be considered when establishing an effective system of critical infrastructure protection. In this work, not only relationships tied to participation of individual ministries or government departments are problematic, but it is also necessary to take into account the relationships among businesses, especially those which are in competition on the same sub-sector of critical infrastructure management. The next moment, which is forgotten in certain analyses, is the relationship between the state and local level of governance. In this

relationship it may come due to the unsettled relations of jurisdiction and control to certain disagreements, which can result in a worse functioning of critical infrastructure protection. In the Republic of Serbia, this problem should not be so acute as it is on a worldwide scale a smaller country. Critical infrastructure should be because of its importance in a systemic approach centrally managed. Of course, it is necessary through various forms of cooperation to ensure that in developing a system of critical infrastructure protection local interests and needs will also be taken into account in the Republic of Serbia. In any event, the measures taken by the Republic of Serbia in the field of security and elimination of consequences of natural disasters have a special role in this relationship. Here, in the systemic view of the response, the local community has a very important role. From this point of view, this coordination and a clear division of authorities and responsibilities is extremely important also in the field of critical infrastructure protection. In this regard, a cross-sectoral coordination group established under the logistic support of the Sector for Emergency Management of the Ministry of Interior will have a very important role.

In this context, the functioning of the National Security Council should be mentioned, which requires to be appropriately installed in the system of authority and responsibilities and anticipates for a certain part of authority, and thus avoid some duplication or confusion in the area of competence among it, the national forum for critical infrastructure and other planned levels or decision-making bodies.

Among the state institutions and companies which manage critical infrastructure for direct and clear relationships, in addition to the normative basis we suggest the signing of contracts, which for each partner clearly define the authority and responsibilities.

3.6 Implementation of the relevant European normatives in the process of approaching of the Republic of Serbia to the EU

The importance of the adoption of the relevant European normatives has already been partially touched upon in the chapter of legal aspects. It is important to establish the awareness that today's security environment has become very dynamic and it is impossible to manage only at the national level. After the review and establishing the national critical infrastructure, in cooperation with neighbouring countries and in continuation also with the EU, the Republic of Serbia will have to define which part of this infrastructure has cross-border effects. Identifying the part of the so called European critical infrastructure will have to be coordinated at the international level both at the bilateral as well as the European level. The

determination of an appropriate contact point and, of course, of the national body will be needed, which will be responsible for coordinating the preparations for the protection of critical infrastructure at cross-border level. The European orientation of the Republic of Serbia and the need for planning these factors were taken into account in the preparation of the proposal of the model. This is a good signal, but needs more decisive steps in the organisation of first the national field and immediately afterwards also the international field. The academic environment with the leading scientific-research organisations is fully integrated into the international system of research and the exchange of the latest findings in this area. Proof of this is also the RECIPE project. Now a more active involvement in national, governmental and expert level will be needed.

3.7 Financial resources

The limited financial resources can certainly be a significant risk factor or a restriction for the normal development of the system of critical infrastructure protection. More importantly, the financial resources can have influence at a time when the economic crisis is still fairly expressed. The Republic of Serbia is a country in transition which also carries out a process of privatisation of certain companies that are currently state-owned, but are significant operators of critical infrastructure. In this context, a realistic and effective system of protection will be even more important as the funding of this project will in any event take place on the basis of legal provisions and negotiations between the parties, where the state and a private company face each other, which mainly targets particularly good performance and maximum profit. Because of this complex process it will be even more important to preliminary create an adequate understanding of the importance of critical infrastructure protection and on the other hand a high level of trust between the partners in this process. The Republic of Serbia will in the stage of integration into the EU have to step up activities related to projects of drawing on pre-accession funds, which may be allocated to financing certain infrastructure measures and improvements in the field of protection of critical infrastructure.

3.8 Human resources and the system of education of future experts in the field of critical infrastructure protection

Human resources in each system represent one of the most important components of successful operation. In the case of the needs of personnel which will be able to successfully

operate in the field of critical infrastructure protection, we speak about a fairly complex story, which should be considered when planning the development of the system. It is impossible to provide the personnel with the necessary multi-disciplinary knowledge in a very short period of time. It is about the necessary knowledge and especially experience that the experts in the field need to gain in a variety of formal and informal forms of education and training. In this context, it is necessary already in the initial phase of setting up a system of critical infrastructure protection, depending on the needs of the real environment to very quickly develop also the appropriate training programs. Here the academic environment has a very important role and also the responsibility that the program and subject content will be prepared and carried out primarily with quality. In the preparation and execution of training it is necessary to monitor the needs of target groups which are in a certain part different because we talk on the one hand about the national-security environment, and on the other hand, the business environment, where the skills and experience necessary are different to a certain extent. The changes in the dynamic security environment anyway force us into permanent change and upgrading of the existing contents, taking into account lessons learned, good practices and certain experience gained in the national and international professional environment.

4 ANALYSIS AND CONCRETE EVALUATION OF THE FEASIBILITY OF THE PROPOSED STEPS TO GIVE EFFECT TO THE SERBIAN MODEL FOR THE ESTABLISHMENT OF CRITICAL INFRASTRUCTURE PROTECTION

Step 1: Assign responsibility

The foreseen step is entirely feasible.

Not feasible	Partially feasible	Entirely feasible
		X

Indicators

Positive:

- The state of threat calls for urgent measures to establish a system the Basis for raising awareness about the importance of adequate CI protection;

- Identification and assignment of relevant persons among experts dealing in different fields with security processes that can be linked to the system of CI protection;
- Establishment of a national forum of experts is an administrative task;
- The decision of the Government of the Republic of Serbia to set Direction for Risk and Emergency Management for co-ordinating body that will provide logistical and administrative support to the functioning of the national forum;
- The basis for the strengthening of public-private partnership;

Negative:

- The level of knowledge and experience of the proposed personnel;
- Difficult to achieve the consensus on important decisions in relation to the diversity of the composition of the mentioned forum;
- Attempt of enforcing the narrow interests contrary to national interests;
- Opposition to the Ministry of Defence or Ministry of Interior for the appointment of the Directorate for the co-ordinating body of support to the national forum;

Indicators for assessing progress:

- Implementation of the agreed deadlines;
- Number of participating organisations and representatives;
- Percentage of carried out set tasks;
- Quality of support of the ruling policy and strategic leadership in companies;
- Number of events organised by the national forum for CI.

Figure 1: SWOT analysis of step 1

Strengths - Identification of experts from various fields; - Establishing a national forum for CI; - Strengthening the national network of experts;	**Opportunities** - Raising awareness of the importance of the CI protection; - Arrangement of the important area represented by CI; - Appointment of state institution, which will in future bear the weight of coordination and CI system development; - Sharing experiences and good practices; - Strengthening of public-private cooperation;
Weaknesses - Different level of knowledge of experts of forum for CI; - Setting the task of CI protection in companies, as an additional task for the foreseen parties; - Difficult to reach a consensus due to the heterogeneity of the working group;	**Threats** - Narrow departmental interests which might harm the national interest;

Step 2: Initial assessment

The foreseen step is entirely feasible. But it is necessary to be aware that in this step it is necessary to put more effort for the establishment of appropriate working groups and forms of cooperation. Based on an assessment this represents a key step in the overall-defined process. A successful progress in other planned steps will also depend on it.

Not feasible	Partially feasible	Entirely feasible
		X

Indicators

Positive:

- Creating a comprehensive analysis, where various stakeholders will participate and serve as a good basis for the further implementation of measures;
- Through the process of making it will also be found which experts, enterprises and organisations may due to the level of knowledge and experience assume a more important role in the formation of the system of CI protection;

- Raising awareness of the importance of CI protection in all segments of society (government, business academic and other environments);
- Increasing importance of Direction for Risk and Emergency Management, as a coordinating body that will in the next steps play an important role for the successful construction of the system of CI protection;
- The analysis will be a good basis for the international cooperation in the field of CI protection;

Negative:

- It will be very difficult to attract the participation of relevant personnel, in particular the strategic management of companies that do not put this problem in an important position of priorities;
- The level of knowledge and experience of the proposed personnel;
- Difficult achievement of consensus on important decisions in relation to the diversity of the composition of the mentioned forum;
- Attempts of implementing the narrow interests contrary to national interests;
- A very large group of participants which will be very difficult to coordinate;
- The factor of how the Direction for Risk and Emergency Management will accept the role of the academic community, particularly the makers of this RECIPE project, which are the key to a successful analysis in accordance with the agreed;

Indicators for assessing progress:

- Creating a comprehensive analysis;
- Implementation of the agreed deadlines;
- Number of participating organisations and representatives;
- Percentage of carried out set tasks;
- Quality of support of the ruling policy and strategic leadership in companies;
- Number of events organised by the national forum for CI.

Figure 2: SWOT analysis of step 2

Strengths - Identification of experts and organisations, which will have a leading role in the process of formation of the CI system; - Strengthening the role of the Directorate; - Strengthening the role of a national forum for CI; - Strengthening the national network of experts;	**Opportunities** - Obtaining high-quality analyses that will serve as the basis for the continuation of set steps; - Raising awareness of the importance of the CI protection; - Arrangement of the important area represented by the CI; - Sharing experiences and good practices; - Beginning the formulating of basic sectors of CI through the analysis;
Weaknesses - The various level of knowledge of experts of forum for CI; - Setting the task of cooperation in the analysis in companies as an additional task of the foreseen parties; - Difficult to reach a consensus due to the heterogeneity of the working group; - Demanding coordination of such a heterogeneous and large group; - Demanding coordination between the Directorate and the academic community (RECIPE)	**Threats** - Narrow departmental interests which might harm the national interest; - Unsuitably based methodology that will bring a broken image in certain segments; - The strategic management will not respond in companies and contribute a significant part in the project;

Step 3: Initial leverage of existing relations

The foreseen step is according to assessment partially feasible only in this step. At this level of cooperation it is difficult to predict that a framework or the basis for the effective functioning of the public-private partnership will be at the appropriate level, which will enable more efficient cooperation. This is a continuous process, the end-state of which may be difficult to define. A significant attention will need to be devoted to the process of exchange of information and good practices and the establishment of appropriate channels of communications. Only the legislation for the transfer of key information is not a sufficient guarantor for effective process. Confidence building is essential.

Not feasible	Partially feasible	Entirely feasible
	X	

Indicators

Positive:

- Identification of all possible bases and established relationships that will bring an upgrade in the field of trust and thus exchange of relevant information;
- To build cooperation on examples of good practices and contacts between the operators of national-security and business environment;
- Raising awareness of the importance of CI protection in all segments of society (government, business academic and other environments);
- Increasing importance of Direction for Risk and Emergency Management as a coordinating body that will play in the next steps an important role for the successful construction of the system of CI protection;
- Fruitful cooperation in the national forum for CI which will serve to strengthen cooperation between the whole set of participants;

Negative:

- It will be very difficult to attract the participation of relevant personnel, in particular the strategic management of companies that do not put this problem to an important place of priorities;
- It will take a lot of energy and understanding for the raising of trust between all parties. It is a long process which is impossible to complete in a short time;
- The level of knowledge and experience of the proposed personnel;

Indicators for assessing progress:

- Establishment and partial standardisation of the foreseen forms for the establishment of communication;
- Implementation of the agreed deadlines;
- Number of participating organisations and representatives;
- Percentage of carried out set tasks;
- Quality of support of the ruling policy and strategic leadership in companies;

Figure 3: SWOT analysis of step 3

Strengths - Identification of good practices and examples of cooperation; - Strengthening the role of the national forum for CI; - Strengthening the national network of experts;	**Opportunities** - Establishing adequate bases for the exchange of information and their standardisation; - Raising awareness of the importance of the CI protection; - Arrangement of important area represented by CI; - Sharing experiences and good practices;
Weaknesses - Different forms of communication channels based on previous established practice; - The dilemma of whether the Directorate employees have sufficient knowledge and skills to manage this process and establish a system to a common denominator and a maximised co-operation;	**Threats** - Narrow departmental interests which might harm the national interest; - The strategic management will not respond in companies and contribute a significant part in the project;

Step 4: Stakeholder engagement

The foreseen step is in this form partially feasible. The problem with this step is that it is in such a form incorrectly placed in the process. Part of this step must be carried out in steps 1-3. This is the part that relates to training to raise awareness of different target groups of CI managers. The remainder must be included in the national plan for the establishment of the system of CI protection and implemented in step 6.

Not feasible	Partially feasible	Entirely feasible
	X	

Indicators

Positive:

- Activities to engage CI managers which are very well defined and will serve as a good basis for a substantive amendment of the national plan;
- Raising awareness of the importance of CI protection in all segments of society (government, business academic and other environments);

- Increasing the importance of Direction for Risk and Emergency Management as a coordinating body that will play in the next steps an important role for the successful construction of the system of CI protection;
- Establishment of appropriate models and programs for the training of professionals in the field of CI protection;
- Strengthening the role of the academic environment and its role in the CI protection;
- Enhancing cooperation in the field of public-private partnership;
- Development of common methodology for risk assessment;

Negative:

- Incorrect positioning of the step, thereby reducing the impact of the measures envisaged;
- The level of knowledge and experience of personnel who will be involved in the activities;
- Attempts of implementing the narrow interests contrary to national interests;

Indicators for assessing progress:

- The number of prepared and adopted standards;
- Number of risk assessment;
- Implementation of the agreed deadlines;
- Number of participating organisations and representatives;
- Percentage of carried out set tasks;
- Quality of support of the ruling policy and strategic leadership in companies;
- Number of events organized by the national forum for CI and other institutions.

Figure 4: SWOT analysis of step 4

Strengths - Good base to complement the national plan; - Stregthening the role of Directorate; - Stregthening the role of the national forum for CI; - Strengthening the national network of experts; - Strengthening the public-private partnership; - Strengthening the academic environment and its role in the field of CI protection;	**Opportunities** - Raising awareness of the importance of the CI protection; - Arrangement of important area represented by CI; - Sharing experiences and good practices; - Obtaining new standards; - Creation of risk assessments as a basis for further action; - Acquisition of the bases for the upgrading of early warning systems and exchange of confidential information;
Weaknesses - Incorrect positioning of step 4; - The various level of knowledge of experts of forum for CI; - Demanding coordination of such a heterogeneous and large group; - Very extensive expertise areas of engagement of all managers; - The dilemma of whether there is sufficient expertise within the Directorate personnel to be able to cope with the support and coordination tasks.	**Threats** - Narrow departmental interests which might harm the national interest; - The strategic management will not respond in companies and contribute a significant part in the project;

Step 5: Develop a national plan

The foreseen step is entirely feasible.

Not feasible	Partially feasible	Entirely feasible
		X

Indicators

Positive:

- The topics identified by the RECIPE research team are a very good framework for the elaboration of the national plan;
- With the inclusion of the part of the content of step 4 this national plan will set the systemic measures in the field of critical infrastructure protection even more comprehensively;

- Raising awareness of the importance of protection in all segments of society (government, business academic and other environments);
- Well-conceived plan will be a solid basis for systemic implementation of measures on a whole series of areas that are required by the interdisciplinarity of the field of critical infrastructure protection;
- Preliminary analysis of the situation, which will be carried out in step 2 will be an indispensable basis for the preparation of the national plan;
- Increasing the importance of Direction for Risk and Emergency Management as a coordinating body that will play in the next steps an important role for the successful construction of the system of CI protection;
- Ensuring the strengthening of cooperation in the field of public-private partnerships with the inclusion of the business environment;
- Providing expertise bases, which will lead to the adoption of normative solutions in the field of critical infrastructure protection with the inclusion of a public-private partnership, the transmission of confidential information and in the ultimate consequence of the organisational placement of the National Centre for Critical Infrastructure;

Negative:

- Adequate awareness is needed that the national plan should be very detailed and long-term;
- The level of knowledge and experience of personnel who will prepare the national plan;
- Attempts of implementing the narrow interests contrary to national interests;
- A very difficult task of establishing the indicators that will enable the monitoring of performance in a whole series of areas;

Indicators for assessing progress:

- An established national plan;
- The number of prepared and adopted standards;
- Implementation of the agreed deadlines;
- Number of participating organisations and representatives;
- Percentage of carried out set tasks;
- Quality of support of the ruling policy and strategic leadership in companies;

- The number of consultations carried out in the organisation of the national forum for CI and other institutions that will be organized in the field of the preparation of the national plan.

Figure 5: SWOT analysis of step 5

Strengths - A good base of the RECIPE project for making the national plan; - Strenghtening the role of Directorate; - Strenghtening the role of the national forum for CI; - Strengthening the national network of experts; - Strengthening the public-private partnership; - Strengthening the academic environment and its role in the field of CI protection; - Quality analysis of step 2 a good basis for drawing up the plan;	**Opportunities** - Raising awareness of the importance of the CI protection; - Arrangement of important area represented by CI; - Sharing experiences and good practices; - Obtaining new standards; - Creation of risk assessments as a basis for further action; - Acquisition of new standards and the bases for concrete steps in the field of CI protection, in particular the establishment of public-private partnership, the exchange of confidential information and the establishment of the National Centre for Critical Infrastructure;
Weaknesses - It is necessary to recognise that the national plan should be based on the realisation of a long-term basis; - The various level of knowledge of experts of forum for CI; - Demanding coordination of such a heterogeneous and large group; - Very extensive expertise areas of engagement of all managers; - A very difficult task of establishing the indicators that will enable the monitoring of performance in a whole series of areas; - The dilemma of whether there is sufficient expertise within the Directorate personnel to be able to cope with the support and coordination tasks. - The level of knowledge of experts who will prepare the national plan.	**Threats** - Narrow departmental interests which might harm the national interest; - The strategic management will not respond in companies and contribute a significant part in the project;

Step 6: Implementation of the national plan

The foreseen step is entirely feasible.

Not feasible	Partially feasible	Entirely feasible
		X

Indicators

Positive:

- Quality construction of a national plan will be the basis for quality implementation;
- Making clear instructions to carry out individual areas will provide faster and more efficient implementation of the national plan;
- Raising awareness of the importance of protection in all segments of society (government, business academic and other environments);
- A well-conceived plan will be a solid basis for systemic implementation of measures on a whole series of areas that are required by the interdisciplinarity of the field of critical infrastructure protection;
- Clearly expressed contractual obligations will be the guarantor for the effective implementation of the obligations and will be the basis for strengthening public-private partnerships;
- Increasing the importance of Direction for Risk and Emergency Management as a coordinating body that will in this part of demonstrate its coordinative capability;
- Providing expertise bases which will lead to the adoption of normative solutions in the field of critical infrastructure protection with the inclusion of public-private partnership, the transmission of confidential information and in the ultimate consequence of the organisational placement of the National Centre for Critical Infrastructure;

Negative:

- Poor preparation of the national plan will be a problem in the implementation;
- Adequate awareness is needed that the national plan should be designed very detailed and long-term;
- The level of knowledge and experience of personnel who will prepare the national plan;

- Attempts of implementing the narrow interests contrary to national interests;
- A very difficult task of establishing the indicators that will enable the monitoring of performance in a whole series of areas;
- Limited financial resources;
- Inadequate support of the management of organisations that manage CI may limit the quality of performance.

Indicators for assessing progress:

- Implementation of the national plan;
- Implementation of the agreed deadlines;
- Number of participating organisations and representatives;
- Percentage of carried out set tasks;
- Quality of support of the ruling policy and strategic leadership in companies;
- The number of consultations carried out in the organisation of the national forum for CI and other institutions that will be organised in the field of the implementation of the national plan.

Figure 6: SWOT analysis of step 6

Strengths	**Opportunities**
- A national plan is a good basis for the realisation of the tasks; - Strengthening the role of Directorate; - Strengthening the role of the national forum for CI; - Strengthening the national network of experts; - Strengthening the public-private partnership; - Strengthening the academic environment and its role in the field of CI protection;	- Raising awareness of the importance of the CI protection; - Arrangement of important area represented by CI; - Sharing experiences and good practices; - Acquisition of new standards and the bases for concrete steps in the field of CI protection, in particular the establishment of public-private partnership, the exchange of confidential information and the establishment of the National Centre for Critical Infrastructure;
Weaknesses	**Threats**
- It is necessary to recognise that the national plan should be based on the realisation of a long-term basis; - The various level of knowledge of experts of forum for CI; - Demanding coordination of such a heterogeneous and large group; - A very difficult task of establishing the indicators that will enable the monitoring of performance in a whole series of areas; - The dilemma of whether there is sufficient expertise within the Directorate personnel to be able to cope with the support and coordination tasks; - The level of knowledge of experts who will prepare the national plan; - The level of knowledge of expert personnel who will prepare the national plan; - Limited financial resources.	- Narrow departmental interests which might harm the national interest; - The strategic management will not respond in companies and contribute a significant part in the project;

<u>Step 7: Monitor implementation and evaluate results</u>

The foreseen step is entirely feasible.

Not feasible	Partially feasible	Entirely feasible
		X

Indicators

Positive:

- High-quality control and monitoring of the implementation of the national plan will give the relevant institutions adequate information on the effectiveness of implementation and the necessary changes in specific fields;
- Making clear criteria will significantly contribute to the quality and performance of control;
- Raising awareness of the importance of protection in all segments of society (government, business academic and other environments);
- Clearly expressed contractual obligations will be the guarantor for the effective implementation of the obligations and will be the basis for strengthening public-private partnerships;
- Increasing the importance of Direction for Risk and Emergency Management as a coordinating body that will in this part of demonstrate its coordinative capability;
- Complete implementation of the national plan, which will entail systemic regulation of critical infrastructure protection in the Republic of Serbia.

Negative:

- Poor preparation of the indicators and criteria of control of the national plan will be a problem in the implementation;
- Adequate awareness is needed that the realisation of the national plan should be carried out over a longer period and the results can not be expected overnight;
- The level of knowledge and experience of personnel who will carry out the control of the implementation of the national plan;
- Attempts of implementing the narrow interests contrary to national interests;
- A very difficult task of establishing the indicators that will enable the monitoring of performance in a whole series of areas;
- Limited financial resources;
- Inadequate support of the management of organisations that manage CI may limit the quality of performance.

Indicators for assessing progress:

- The scope of the realisation of the national plan;
- The number of checks carried out;

- Implementation of the agreed deadlines;
- Number of participating organisations and representatives;
- Percentage of carried out set tasks;
- Quality of support of the ruling policy and strategic leadership in companies;.
- The number of consultations carried out in the organisation of the national forum for CI and other institutions that will be organised in the field of the implementation of the national plan.

Figure 7: SWOT analysis of step 7

Strengths - The criteria and indicators are a good basis for the realisation of the foreseen tasks; - Strengthening the role of Directorate; - Strengthening the role of the national forum for CI; - Strengthening the national network of experts; - Strengthening the public-private partnership; - Through the implementation of the control of the implementation a clear picture of the situation is created. The process of learning from experience is carried out through the analysis;	**Opportunities** - Raising awareness of the importance of the CI protection; - Arrangement of important area represented by CI; - Sharing experiences and good practices; - Acquisition of new standards and the bases for concrete steps in the field of CI protection, in particular the establishment of public-private partnership, the exchange of confidential information and the establishment of the National Centre for Critical Infrastructure;
Weaknesses - It is necessary to recognise that the national plan should be based on the realisation of a long-term basis; - The various level of knowledge of experts of forum for CI; - Difficult to coordinate the control of the implementation of such a demanding plan; - A very difficult task of establishing the indicators that will enable the monitoring of performance in a whole series of areas; - The dilemma of whether there is sufficient expertise within the Directorate personnel to be able to cope with the support and coordination tasks. - The level of knowledge of experts who will carry out the control of the implementation of the national plan. - Limited financial resources.	**Threats** - Narrow departmental interests which might harm the national interest; - The strategic management will not respond in companies and contribute a significant part in the project implementation and provide impartial supervision;

Analysis of placement and tasks of the National Center for Critical Infrastructure Protection

The foreseen step is entirely feasible and is entirely dependent on the political will and the decision of the Government of the Republic of Serbia. The organisational placement and extent of the tasks is analysed in further evaluation.

Not feasible	Partially feasible	Entirely feasible
		X

Indicators

Positive:

- Part of the Directorate transforms into the NCIP and thus achieves a continuity of work;
- NCIP represents the pivotal point in the Republic of Serbia, which provides coordination, the conditions for the development of the system of critical infrastructure protection and a contact point for cooperation with international partners;
- Proposed organisational placement directly under the Government of the Republic of Serbia can significantly contribute to the effectiveness of coordination and the more pronounced role of the NCIP;
- Its role becomes a key factor for the field of CI protection in all segments of society (government, business academic and other environments);
- Clearly expressed contractual obligations will be the guarantor for a stronger development and strengthening public-private partnerships;
- Concern for the long-term implementation of the national plan will be more effective at a constant concern of the competent body;
- Centralisation of experts in the field of CIP will have a more important influence on the quality of systemic development of CI;
- Centralisation of resources within the NCIP will provide a more efficient use and higher results in the field of CI protection.

Negative:

- Poor preparation of the proposal for the establishment of NCIP may deter the ruling policy from the adoption of necessary decisions for the establishment;
- Non-systemic approach which would at the founding only normatively foresee the establishment of NCIP will not provide adequate results in practice;
- Attempts of implementing the narrow interests contrary to national interests;
- Too large range of tasks according to current resources;
- Limited financial resources;
- Inadequate support of the ruling policy;
- The placement directly under the Government of the Republic of Serbia can have negative effects in terms of logistical support for the operation of the center.

Indicators for assessing success of NCIP:

- Creation of a legal basis;
- Provision of financial resources;
- Provision of human resources;
- The number of checks carried out;
- Implementation of the agreed deadlines;
- Number of training and consultations;
- Percentage of carried out set tasks;
- Quality of support of the ruling policy and strategic leadership in companies;.
- A system for the exchange of confidential information.

Figure 8: SWOT analysis of the National Center for Critical Infrastructure Protection

Strengths	**Opportunities**
- Directorate serves as the basis for the transformation of the NCIP; - Centralisation of tasks and responsibilities of the establishment of the system and its development; - The central institution for the strengthening of public-private partnership; - Increased rationalisation of the use of financial resources and better control of expenditure; - Strengthening the role of the national forum for CI; - Strengthening the national network of experts; - Strengthening the public-private partnership; - Through the implementation of the control of the implementation a clear picture of the situation is created. The process of learning from experience is carried out through the analysis;	- Raising awareness of the importance of the CI protection; - Arrangement of important area represented by CI; - A central body for sharing experiences and good practices; - Acquisition of new standards and the bases for concrete steps in the field of CI protection, in particular the establishment of public-private partnership, the exchange of confidential information;
Weaknesses	**Threats**
- Level of awareness of decision-makers at the national level; - The risk that the scope of the tasks in the initial phase exceeds the available resources; - Demanding coordination among the entire set of authorities and companies in the field of CI ; - Limited financial resources; - Poor cooperation between the Ministry of Internal Affairs and NCIP in the creation of a new body; - The level of knowledge of experts who will be employed in the NCIP; - Limited human resources.	- Narrow departmental interests which might harm the national interest; - The Government of the Republic does not recognise the need for the establishment of a central body;

5 CONCLUSIONS

The feasibility study of the foreseen model of critical infrastructure protection in the Republic of Serbia reflects the fact that it can be implemented in all the foreseen steps. Structurally the study needs to be combined in some parts and thus make the steps with measures more rational and efficient. The academic community with a part of individual experts employed in state institutions will continue to constitute the main professional capacity in the further making and preparation of the national plan of the critical infrastructure protection and in raising awareness on the importance of its protection. However, the political will and determination to establish and systemically regulate this important area of critical infrastructure in the Republic of Serbia remains the main factor.

References

- COM (2010) 673 final. The EU Internal Security Strategy in Action: Five steps toward a more secure Europe. Objective 2: Prevent terrorism and address radicalization and recruitment. Objective 5: Increase Europe's resilience to crisis and disasters.
- COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, Brussels, 28.8.2013 SWD (2013) 318 final. p. 2-11.
- Communication from the Commission, n. COM (2006) 786 final, Brussels 12.12.2006., p. 3.
- Conclusions of the European Council of 10/11 December 2009 on 'The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010-2014)'; 17024/09. (accessed, 07. jan. 2016)
- Council Directive 2008/114/EC of December 8.2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (SL L 345/75, 23.12.2008.).
- Klaver, M. on behalf all RECIPE team (2011). Good practices manual for CIP policies, p.40-43.
- Serbia Workshop Evaluation Report, 2015.
- National Standpoints Republic of Serbia, 2015.
- Feasibility Study, Comparative Overview and Analysis, Part 1, October, 2015.
- Data Secrecy Law ("Off. Gazette of RS", no. 104/2009).
- Keković, Z., Savić, S., Komazec, N., Milošević, M., Jovanović, D. (2010) *Procena rizika u zaštiti lica, imovine i poslovanja,* Centar za analizu rizika i upravljanje krizama, Beograd
- Narodna Skupština Republike Srbije (2009) *Strategija nacionalne bezbednosti Republike Srbije*, dostupno na: http://www.kombeg.org.rs/Slike/CeBezbednost/statika/Strategija%20nacionalne%20bezbednosti%20Republike%20Srbije.pdf , (accessed January 2, 2016.).
- Narodna Skupština Republike Srbije (2011) *Zakon o javno-privatnom partnerstvu i koncesijama*, dostupno na: http://www.paragraf.rs/propisi/zakon_o_javno_privatnom_partnerstvu_i_koncesijama.html , (accessed January 2, 2016.).

- Decision on Types of Investment Facilities and Spatial and Urban Plans of Importance for National Defence ("Off. Gazette FRY", no. 39/95).
- Decision on Facilities of Particular Importance for National Defence ("Off. Gazette of RS", no. 112/2008)
- Decision on Identification of Large Technical Systems Important for National Defence ("Off. Gazette of RS", No.41 / 2014 and 35/2015)
- Decision on Identification of Products and Services of Special Importance for the National Defence of the Republic of Serbia ("Off. Gazette of RS", no.58 / 2008);
- Law on Emergency Situations ('Official Gazette of RS' no.111/2009),
- National Strategy of Protection and Rescue in Emergency Situations ('Official Gazette of RS', no. 86/2011),
- Law on Private Security ('Official Gazette of RS', no. 104/2013),
- Law on Environmental Protection ('Off. Gazette of RS', no. 135/2004, 36/2009, 36 / 2009 – other law 72/2009 and 43/2011 - Decision),
- Data Secrecy Law ("Off. Gazette of RS", no.104/2009),
- Law on Planning and Construction ("Off. Gazette " no.72/2009),
- Law on Water (Official Gazette. Gazette no.30/10, 93/12).
- Law on Defence ("Off. Gazette of RS", no. 116/2007, 88/2009, 88/2009 - ot. Law 104/2009 - other. Law 10 / 2015)

Contents of Figure

Figure 1:
SWOT analysis of step 1 …..... 17
Figure 2:
SWOT analysis of step 2…….. 19
Figure 3:
SWOT analysis of step 3…… 21
Figure 4:
SWOT analysis of step 4……. 23
Figure 5:
SWOT analysis of step 5……. 25
Figure 6:
SWOT analysis of step 6…… 28
Figure 7:
SWOT analysis of step 7…… 30
Figure 8:
SWOT analysis of the National Center for Critical Infrastructure Protection…… 33

ANNEX VII

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 5

1. SUMMARY 7

1.1. PROJECT RECIPE DESCRIPTION 9

1.2. JOINT WORKSHOPS RESULTS 12

1.2.1. SERBIAN WORKSHOP RESULTS 13

1.2.2. CROATIAN WORKSHOP RESULTS 18

1.3. FEASIBILITY STUDIES RESULTS 22

2. RECCOMENDATIONS 27

2.1. ESTABLISHMENT OF THE PLATFORM FOR PUBLIC-PRIVATE PARTNERSHIP 29

2.1.1. RECOMMENDATIONS FOR THE REPUBLIC OF SERBIA 33

2.1.2. RECOMMENDATIONS FOR THE REPUBLIC OF CROATIA 37

2.2. ESTABLISHMENT OF MECHANISMS FOR EXCHANGE OF SENSITIVE INFORMATION/DATA AMONG PARTICIPANTS IN THE CRITICAL INFRASTRUCTURE PROTECTION SYSTEM 41

2.2.1. ESTABLISHMENT OF MECHANISMS FOR EXCHANGE OF SENSITIVE INFORMATION/DATA IN THE REPUBLIC OF SERBIA 42

2.2.2. ESTABLISHMENT OF MECHANISMS FOR EXCHANGE OF SENSITIVE INFORMATION/DATA IN THE REPUBLIC OF CROATIA 44

2.3. ESTABLISHMENT OF PRECONDITIONS FOR DEVELOPMENT OF THE NATIONAL CENTRE FOR CRITICAL INFRASTRUCTURES 48

2.3.1. RECOMMENDATIONS FOR THE REPUBLIC OF SERBIA 49

2.3.2. RECOMMENDATIONS FOR THE REPUBLIC OF CROATIA 51

2.4. CREATING NORMATIVE AND STRATEGIC FRAMEWORKS IN STRENGTHENING RESILIENCE AND PROTECTION OF CRITICAL INFRASTRUCTURES 56

2.4.1. RECOMMENDATIONS FOR THE REPUBLIC OF SERBIA 57

2.4.2. RECOMMENDATIONS FOR THE REPUBLIC OF CROATIA 59

3. CONCLUSION 65

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

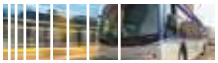
Critical infrastructure is the backbone in the development of the contemporary societies; its deficient or inadequate protection may pose a threat to the national, regional and European security, economy and stability. Notwithstanding various efforts done by the European Commission and the Member States 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.

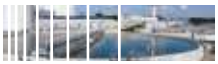
ENERGY

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

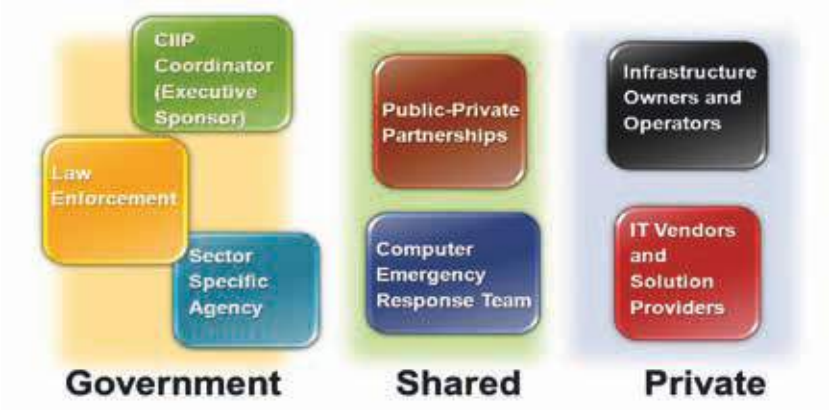
The first Joint Workshop of project partners, Serbian and international CIP experts was held on 13th of October 2015 in Belgrade, Republic of Serbia. The Second Workshop of the project partners and Croatian and foreign experts was held on 15 October 2015 in Zagreb, Republic of Croatia.

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.

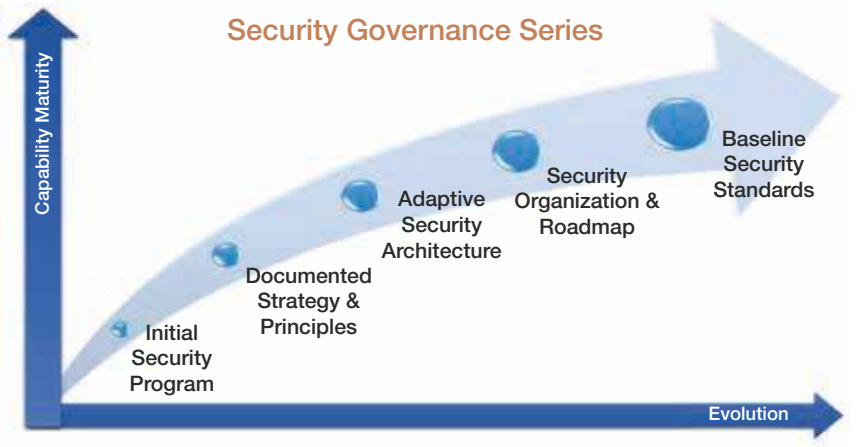
1.3. RESULTS OF THE FEASIBILITY STUDIES

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

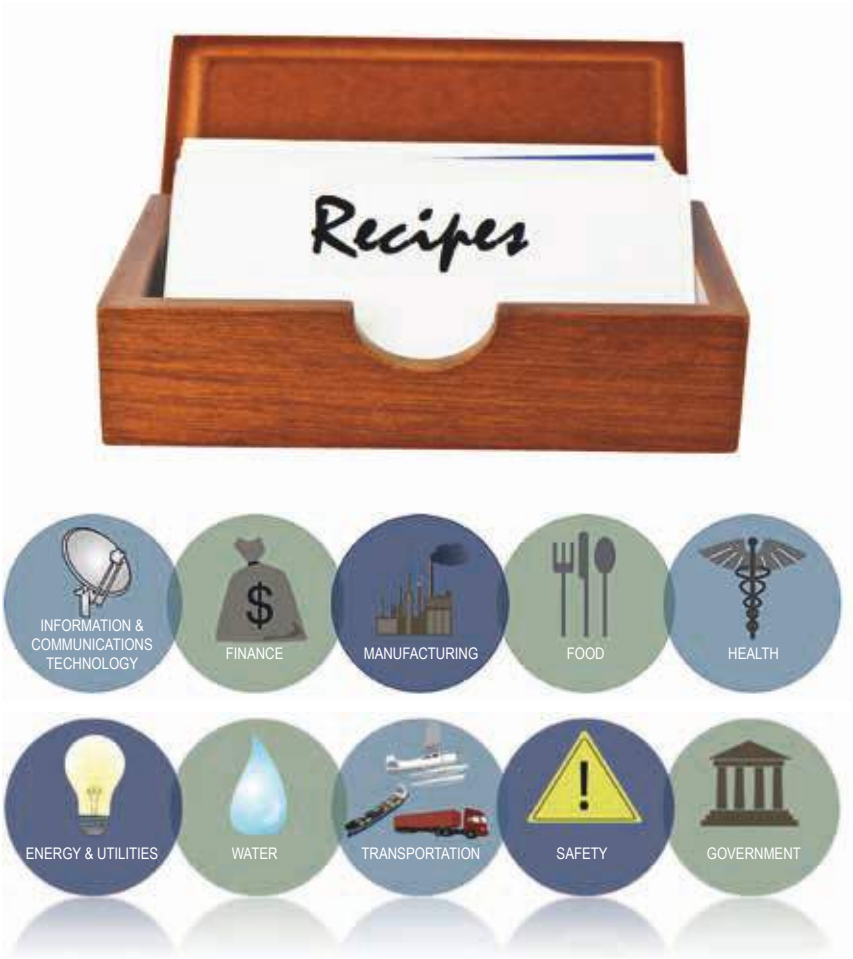
for the effective operation of the system of critical infrastructure, private capital appeared which is becoming one of the key factors in the ownership of companies which manage critical infrastructure. This represents one additional element which is crucial in the perception of changes in the system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

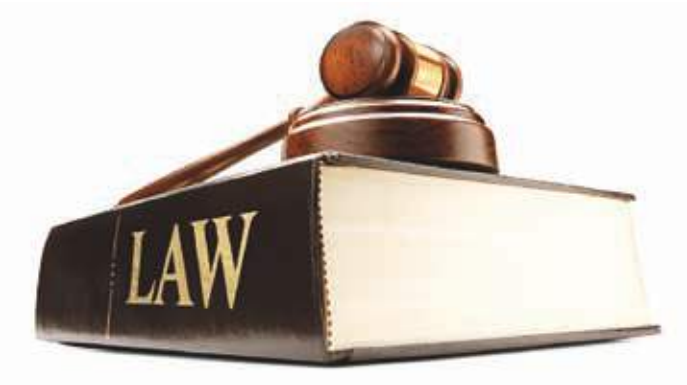
operators. The main role in the awareness raising will need to be played by the academic sector and the state institutions, which are best acquainted with "good practices". During the critical infrastructure identification and prioritization, as well as during the drafting of CIP strategy or guidelines, 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.

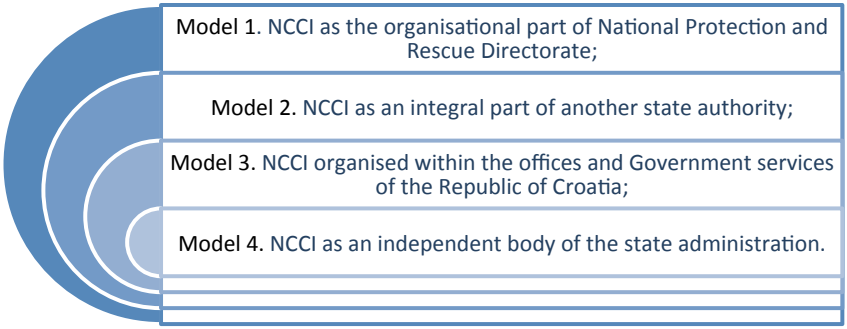
Instead of simple information collection and distribution, the Centre needs to have capacities for their analysis, as well as capacities for supervision over the implementation of the Law on Critical Infrastructure at the national level. National Centre for Critical Infrastructure should have the following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

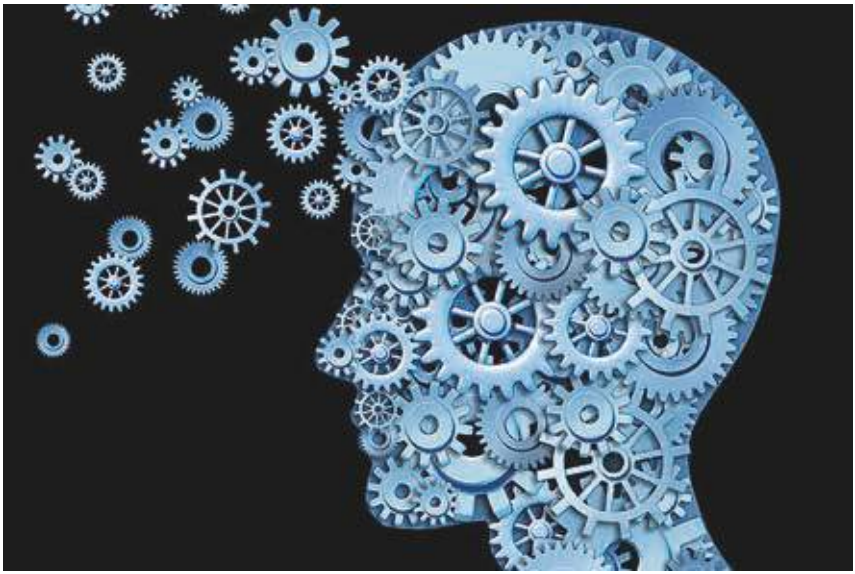
CONCLUSION

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.

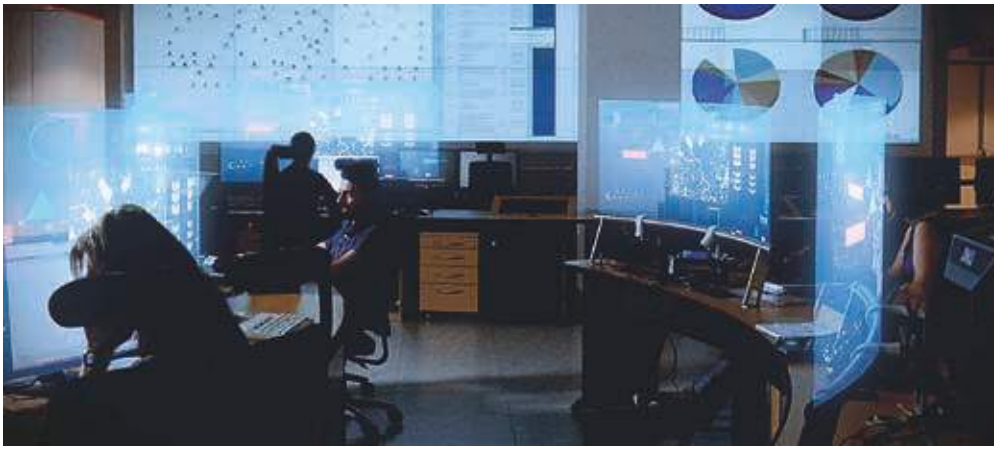
Considering the establishment of the National Centre for Critical Infrastructure, it is necessary to take into account that the exchange of sensitive information is a delicate subject not yet addressed in a satisfying and uniform manner. Information exchange among all stakeholders is extremely important 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

ANNEX VIII

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

recipe 2015

"RESILIENCE OF CRITICAL INFRASTRUCTURE PROTECTION IN EUROPE" CONFERENCE EVALUATION REPORT

International scientific conference „Resilience of Critical Infrastructure Protection in Europe", that took place in Split, Croatia, 11-12 April, is the third and most important activity within the project „RECIPE 2015" funded by the European Commission - Directorate General for Humanitarian Aid and Civil Protection of the Financial Instrument for Civil Protection.

The aim of the conference was to consolidate the results achieved at national panel discussions related to national standpoints defined at Croatian and Serbian joint workshops as well as the Feasibility Study and provide conclusions and guidelines for the Follow-up strategy for critical infrastructure protection. In this sense, the participants, who were representatives of the scientific community, private and public sectors from partner countries (Croatia, Serbia, Sweden), EU (Netherlands, Greece, France, Slovenia, Hungary, Finland) and non - EU countries (Bosnia and Herzegovina, Montenegro and Macedonia), even from USA, presented their views, experiences and conclusions regarding mentioned activities and the project objectives, thus summing up all the efforts done throughout the project.

The conference was opened on 11 April 2016. In the introductory part the conference participants were greeted by conference host Mr. Jadran Perinić, NPRD Director General and Mr. Robert Mikac, "RECIPE 2015" project manager and conference moderator.

In introductory session, guest speakers were: Mr. Alessandro Lazari, European Reference network for Critical infrastruction protection, Joint Research Centre, European Commission; Mr. Goran Kovačević, Deputy Mayor of Split; Mr. Ante Šošić, Deputy Prefect of Split - Dalmatia County and Mr. Davor Blažević, Deputy Minister of the Interior.

Also, as an introduction, Mr. Robert Mikac presented an overview of the current status of the project and representatives of the project partners (Mr. Alen Stranjik, University of Applied Science Velika Gorica, Croatia, Mr. Želimir Kešetović, University of Belgrade, Faculty of Security Studies, Serbia and Mrs. Anna Rinne, Swedish Civil Contingencies Agency) have briefly presented their roles in the project, as well as importance of the project for their countries and institutions.

All above named speakers talked about the importance of critical infrastructure for national security, general safety and well-being of the population and economy, as well as for safety at the EU level. They emphasized the need and importance of well-established risk management

systems as well as the importance of active involvement and mutual cooperation of all stakeholders in this system. They also expressed their awareness of insufficiency of the current CIP and the need for its improvement. In this sense "RECIPE 2015" project has been recognized as an instrument and a great opportunity for finding methods and modes to overcome the shortcomings through exchange of experience and good practice and the cooperation of the competent institutions at national and international level.

The conference program was split into three thematic areas/panels in line with the project objectives.

Beyond the panels, „RECIPE 2015" Feasibility Study and „RECIPE 2015" Mobile Application were presented by Mr. Denis Čaleta from „Institute for Corporative Security Studies", Ljubljana who conducted Feasibility studies and Alen Lukajić from „CROZ" company, alongside with Igor Cvitanić (National Protection and Rescue Directorate), creators of application.

In addition beyond the panels, it was presented the theme entitled „Resilience of Critical Infrastructure protection – European Union Dimension", with view on „The Dutch approach to Critical Infrastructure Protection" by Mr. Marc van der Velde, Ministry of Security and Justice, Netherlands and enclosure on „Role of the Union Civil Protection Mechanism in strengthening infrastructure resilience" by Alessandro Lazari, PhD, European Reference Network for Critical Infrastructure Protection; Joint Research Centre, European Commission.

The first panel was held on 11 April, entitled ***"*The establishment of public - private partnership in the field of CIP"** (moderator: Jan-Olof Olsson, Swedish Civil Contingencies Agency) with following sub-topics: Strategic and legislative framework of CIP; Methods of CIP systematic approach CIP Assessment Methodology; Scientific and research activities in the field of CIP risk management.

<u>Presentation topics under Panel 1:</u>

- „State and Operators Cooperation for CIP: Building Trust for Common Interests"
- „Communication and cooperation between stakeholders in critical infrastructures protection - Serbian perspective"
- „US Structure for Collaboration and Cooperation between US Government, Private and Non-Profit Sectors to secure Critical Infrastructure and Manage Risk"
- **"**Joint venture analysis of electric power plant management from the aspect of a Public-Private Partnership in the field of Critical Infrastructure"
- "E.ON; How to Become "Security Fit"

Main conclusions of first panel after presented topics:

- Interdependency of society and private actors is unquestionable;
- There are differences between different countries' history and how long they focused on CIP issues;
- Local, regional, national, EU and global aspects must be considered in risk continuity management;
- No sector can work alone without cooperation and securing their dependence. Cyber, electricity, communications and transport are sector's with high dependency;
- All hazard approach is a key to success;
- PPP often doesn't exist if it isn't somehow obligatory;
- In PPP, trust is difficult to establish and maintain;
- Security planning using common tools and common language is needed same as strengthen coop between public entities and operators;
- There is importance of ISO 31000:2009 and other standards, also exists the difference between standards used by the society and private sectors.

The second panel was entitled **„Establishment of a mechanism for the sensitive information/data exchange between participants in CIP"** (moderator: Mr. Dejan Škanata, PhD, University of Applied Sciences Velika Gorica). Sub-topics of this panel were: Mechanisms for the sensitive information/data exchange of between stakeholders in CIP; Communication and collaboration between stakeholders in CIP system-relevant partners from the public and private sectors; Establishment of an optimal system CI risk management.)

<u>Presentation topics under Panel 2:</u>

- „Public-Private Partnership: Considerations for Critical Infrastructure Security"
- „Model of Critical Infrastructure Protection in the Republic of Serbia-learning from good Practice"
- "Public-Private Partnership to Protect the Critical Infrastructure with an Emphasis on Private Protection"
- "Enhancing Resilience of Critical Infrastructure due to Threats by Extending Concepts of Regional Defence and Public–Private Cooperation"
- "An Overview of CIP activities in Greece and Future Prospects"
- "Safe Data Exchange for Critical Infrastructure System"

Conclusions of Panel 2:

- Synergy between state and private sector should be achieved
- Harmonisation of legal framework in CIP field is essential;
- International cooperation in the field of CIP, particularly in the Balkans is important, same as exchange of good practice and information by well-developed countries;
- Need of continuous education in CI topics;
- Application of ISO/IEC standards is a minimal requirement for the safe information/data exchange.

The third panel was held on 12 April, entitled **„The establishment of the preconditions for the development of the national Critical Infrastructure Centre“** (moderator: Mr. Želimir Kešetović, PhD, University of Belgrade, Faculty of Security Studies)
Sub-topics for these panel were: Education and training in a related field; CI elements and their interdependence; Measures and incentives for CIP-experience; CIP in the EU in accordance with Directive 2008/114/EC; Preliminary proposals for developing of the National CI Centre and software solutions.)

Presentation topics under Panel 3:

- “Establishment of National Centre for Critical Infrastructures – case study of Hungary”
- “The Health of Nations: Protecting National Security and Critical infrastructure against the Unknown”
- “Establishment of the National Centre for Critical Infrastructures in the Republic of Croatia”
- “Twin Cities CIKR Assessment and Protection”
- “Flood Risks and the Energy Critical Infrastructure Sector Protection Measures in the Republic of Serbia”
- “A Comparative Overview of the Critical Infrastructure Protection Systems of the Republic of Croatia and the Kingdom of Sweden: the process of determining the criteria for intersectoral measures”

After third Panel some of accentuates were:

- Support of decision makers and financial aspect are very important for establishment of well-functioning and fully operational NCCI;
- All existing best practices should be considered - such as ones on local level which can be implemented at the national level (bottom-up approach);
- “Critical of the critical”

- CI systems are supposed to be not only secure but also safe (process safety) – considering resilience concept.

In summary, "RECIPE 2015" conference highlighted importance of below listed aspects, with emphasis on the need for improvement on named subjects:

- The identification of the critical business assets and the major threats that may occur on those assets, the estimation of the probability that those threats could occur and the evaluation of their impact (consequences on organization's capability to perform business activities) are cornerstones activities to design organization's protection system. In mission critical contexts is strongly recommended to consider not only the traditional, well-known threats, but also to explore the possible events and conditions (internal and external to the organization) that may engender unexpected negative consequences never considered before on the organization. Furthermore, considerations on the emerging threats scenario and the consequent updates of threat catalogue potentially affecting the organization should always be taken into account.

- Through institutional cooperation and exchange of practice has been recognized that critical infrastructure protection in many countries is not sufficiently developed at the national level because of lack of awareness both in public and in the governing structures. In order to change this situation it is necessary to encourage and stimulate the interest of both of these factors, and to raise awareness about the importance of protecting critical infrastructure at a satisfactory level.

- In the CIP system development it is necessary to understand the crucial role of state. The state represents the central point in any system and the motor in ensuring an effective system of critical infrastructure protection. The state's biggest interest is that critical infrastructure, irrespective of which ownership structure the organization that manages critical infrastructure is currently in, operates continuously, thus ensuring the smooth functioning of the community. From this perspective, it is necessary to put the understanding of the situation and the measures into rising of awareness and proper understanding of the importance of critical infrastructure in the strategic management of the state and its institutions.

- Due to the complexity of the CIP system, there is no doubt that it would be necessary to establish a central point for coordinating activities related to CI risk management. In accordance with the proposed models and the results of feasibility studies, it is clear that such a focal point should be established within the administrative body that is responsible for civil protection in Croatia as well in Serbia. Conference participants agreed that such a model could be optimal and in other countries.

- A wider social perception is also important that the critical infrastructure protection and the insurance of its continuous operation is an important goal not only in the narrow domain of individual state agencies or operators of critical infrastructure, but it is the task of the whole spectrum of different institutions, in both public and private environments. For the

construction of such an approach there is a need to ensure a strong and functioning public-private partnership.

- It was concluded that cooperation between the public and civil sectors is necessary in order to improve the realization of investments in infrastructure projects or other types of operations which makes public-private partnerships an effective way of implementation of commitments to ensure the achievement of the objectives of public policy by linking the various forms of public and private resources.

- The public-private partnership is required to put focus on certain elements, i.e. guidelines for the success and sustainability of cooperation in order to implement the objectives of strengthening the resistance and protection of critical infrastructure, and to:

• Define the roles and responsibilities;
• The use of resources;
• Openness to capacity development and change;
• Realistic expectations.

- 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 stakeholders understand the positive aspects of the regulation of the system of critical infrastructure protection, and are from this point ready to invest the necessary efforts and other resources in building this system.

- The normative framework of the activities of public-private partnerships must be improved to strengthen the resilience and protection of critical infrastructure as to be clearer, more flexible and open to new investments and greater cooperation between the public and private sectors.

- When we talk about the handling of sensitive information on national and European critical infrastructure, we should say that it is taking place in accordance with special regulations in the field of information security and international treaties. However, in practice it is found that the existing regulations are not implemented in its entirety and therefore it is necessary to take additional actions to increase efficiency and security in the exchange of sensitive information related to critical infrastructure.

The summaries of all conference presentations have been collected and published in the Book of Proceedings.