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