# Proposal for possible approach for Critical Information Infrastructure protection in Serbia

Goran Murić[1], Nataša Gospić[1], Dragan Bogojević[2]
[1] University of Belgrade, Faculty of Traffic and Transport Engineering, Belgrade, Serbia
[2] PE EPS, Belgrade

**Abstract** – *The issues of protecting critical infrastructure, especially telecommunication and information critical infrastructure are in the focus of many governments, regulatory agencies and standardization bodies worldwide. Standardization bodies are trying to establish general model and standard for the protection of critical information infrastructure, but conditions differ from country to country and each one of them must provide its unique model based on general recommendations. In this paper, the possible approach for critical information infrastructure protection in Serbia is presented regarding EU and Serbian standards and regulations. The key stakeholders are identified, and their roles in this process are discussed.*

## I. CRITICAL INFRASTRUCTURE

There are many definitions of the Critical Infrastructure - CI, but all of them in principle refer to assets which are essential to the economy and society. The CI is a subject within EU regulation too. In the EU Council directive 2008/114/EC following terminology is used [1]:

(a)"Critical infrastructure means an asset, system or part thereof located in the 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 significant impact in a Member State as a result of the failure to maintain those functions".

(b) 'European critical infrastructure' or 'ECI' means critical infrastructure located in the Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure. [1]; List of European CI is given in Annex I of [1].

The critical infrastructures within the county are a complex "system of systems." Interdependencies are generally not well understood and disruptions in one infrastructure can propagate into other infrastructures. Between those CIs interdependencies is very strong. Critical infrastructures interact at different levels, and failure in one infrastructure may impact the functionality of other infrastructures. [2]

There is a great deal of interdependency between the Telecommunication Sector and a number of the functionaries within the utility community. Almost all of the utilities have critical requirements for communications of any form. [3]. Alternatively, the communications community has a number of instances where they are dependent on the utilities, what leads to the conclusion that communications is a key infrastructure, central to all others, so that understanding and modeling the risk due to communications disruptions is a high priority in order to enhance public safety and infrastructure resiliency [2].

In general, cascading across infrastructures can occur in almost any order, but telecommunications always is a central component surrounding the disruption and is especially important in mitigating the disruptive effects [4].

## II. SITUATION IN SERBIA

Many countries worldwide have identified their Critical Telecommunications Infrastructure - CTI and related bodies responsible for CTI (USA, Canada, Germany, Sweden, Norway, The Netherlands, Switzerland…). Several countries have started projects on CTI (Brazil). Considering the situation in our region, we can say that CTI issues are not very often discussed [5].

In Serbia, National Strategy for an Information Society in Serbia 2020, deals with the protection of critical infrastructure in chapter 6.2 in relation to information security, attacks using ICT and ways of protection [6]. In this document the need for defining criteria for identification of critical infrastructure is required. National strategy for protection and rescue in emergency situations and Law on Emergency Situations [7] has not referred to CTI. Within the Project" Managing critical infrastructure for sustainable development in the postal, railway and communications sector in the Republic of Serbia" (Project No. 036 022) CI for three mentioned sectors is discussed. The main Project's objective is to identify critical infrastructure systems, whose efficiency and effectiveness is essential for the smooth growth and development of economy and society. The part of the Project is dealing with CTI and is carried out by the project team from Transport and Traffic Engineering Faculty team and Telecom Serbia. Having in mind all factors that can attack telecom infrastructure (natural disasters, targeted attacks, some unintentional disturbance) and different ownership on telecom infrastructures (public and private), the issues about CTI become regulatory issues. The National backbone network is under discussion and CTI, its regulation and operator's obligations should not be neglected in those discussions.

## III. KEY STAKEHOLDERS AND THEIR ROLES IN CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

In order to be sure that ICT infrastructures will be used at their maximum extent, a number of stakeholders should be actively involved in the process of defining critical information infrastructure protection. First of all, stakeholders must have a high level of confidence and trust in ICT infrastructure. Furthermore, it has to be emphasized that this is a shared responsibility and no single stakeholder has the means to ensure the security and resilience of all ICT infrastructures and to carry all the related responsibilities.

Therefore, in order to strengthen critical infrastructure protection, the requirement is for intensive cooperation, coordination and information between and among the relevant partners and players. The main stakeholders in the Republic of Serbia could be identified as:

- Republic Agency for Electronic Communications – RATEL
- Ministry of Foreign and Internal Trade and Telecommunications
- Ministry of Interior of Republic of Serbia (Department for Emergency Situations)
- Telecommunication operators
- Companies with large and developed communication networks
- Government
- The science and research community.

The National Strategy for Critical Infrastructure Protection (CIP), and related policies are the starting point for development of Critical Information Infrastructure Protection – CIIP.

## IV. AN APPROACH TO ESTABLISH INFRASTRUCTURE FOR NATIONAL STRATEGY DEVELOPMENT

The process of developing a National Strategy for CIIP has to be conducted by several bodies composed of representatives of all stakeholders.. These bodies are responsible for the Critical Infrastructure Protection process:

- **Government** - the government's role is in the adoption of the policies at the national level for the protection of all the critical infrastructures
- **CI sector bodies** – the specific body for the each individual sector is responsible for adoption and implementation of sectoral critical infrastructure protection plan
- **Common body** – as the result of significant level of interdependencies among different infrastructures, critical infrastructures interact at different levels, and failure in one infrastructure may impact the functionality of other infrastructures [8]. In order to comprehend and measure interdependencies, a common body, consisted of the representatives of the each CI sector is necessary.

In the Fig. 1, the process of the CIP and the roles of the bodies are illustrated. Only three CI sectors are presented just for the sake of simplicity.

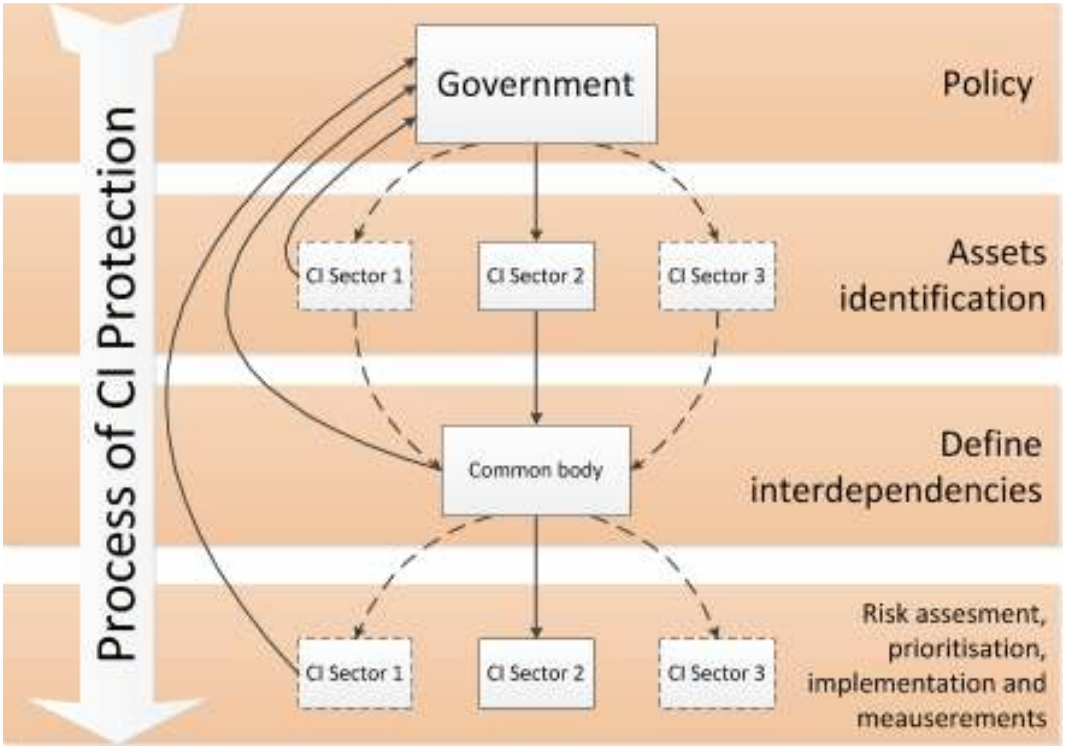


Fig. 1, Illustration of the process of the CIP and the roles of the bodies

There are some guiding principles that should be considered in the process of CIP. For example, in Germany, critical infrastructure protection is a task to be performed jointly by government, companies and/or operators and also by civil society [9]. The guiding principles regarding critical infrastructure protection are, in particular:

- Trusting co-operation between the state and business and industry at all levels; and
- The requirement for, and suitability and proportionality of, the measures taken and the use of resources made for increasing the level of protection.

As the part of a larger scope of National Critical Infrastructure, the Critical Information Infrastructure protection plan has to be developed accordingly to the national frameworks for CIP.

## V. SAME EXAMPLES ON NATIONAL STRATEGY DEVELOPMENT

Regarding USA best practice USA Communications Sector-Specific, Plan an Annex to the National Infrastructure Protection Plan issued by the Department of Homeland Security [13] is suitable guideline tool.

The process of CIIP of European Member State or Candidate can be described in several complex steps and should consider following documents: European Action Plan on Critical Information Infrastructure Protection (COM(2009) 149) [10], National Cyber Security Strategies, Practical Guide on Development and Execution by ENISA [11], European Union Council Directive 2008/114/EC [1], ISO Risk Management Framework 31000 [12]. In the paper main EU documents on CIIP are described.

### *European Action Plan on Critical Information Infrastructure Protection*

The EU initiative on CIIP aims to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures by stimulating and supporting the development of a high level of preparedness, security and resilience capabilities both at national and European level. [12]

The European CIIP action plan is built on five pillars [14]:

1. **Preparedness and prevention** – based on two major frameworks: European Forum for Member States (EFMS) and the European Public-Private Partnership for Resilience (EP3R)

2. **Detection and response** – European Network and Information Security Agency (ENISA) devised a high-level roadmap for the development of a European Information Sharing and Alert System (EISAS)by 2013

3. **Mitigation and recovery** – development of national contingency plans of the Member States and the organization of regular exercises for security incident response and disaster recovery. ENISA has developed a Good Practice Guide on National Exercises [9] to assist authorities in Member States to better understand the complexities of exercises and help them prepare local and national ones.

4. **International cooperation** - includes European principles and guidelines for the resilience and stability of the Internet [15]

5. **Criteria for European Critical Infrastructures in the ICT sector** - including the development of ICT sector specific criteria to identify European critical infrastructures in the ICT sector.

### *National CIIP action plan within EU*

A national CIIP action plan within EU is a plan of actions designed to improve the security and resilience of national information infrastructures and services. It is a high-level top-down approach to information and cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe.

The cross-border nature of threats makes it essential to focus on strong international cooperation. Cooperation at pan European level is necessary to effectively prepare, but also respond to cyber-attacks. Comprehensive national cyber security strategies are the first step in this direction.

The National CIIP strategy for EU Members can rely on a relatively recent document developed by the ENISA in the December 17th, 2012 - National Cyber Security Strategies, Practical Guide on Development and Execution [11]. The author's premise is that this document should be taken in consideration for EU Candidate Countries such as Serbia. In the next few paragraphs, the overview of the aforementioned document is presented.

ENISA has developed this document with the purpose to identify the most common and recurrent elements and practices of national cyber security strategies (NCSSs), in the EU and non-EU countries. ENISA has studied existing NCSS, in order to determine the relevance of the proposed measures for improving security and resilience [11].

Within this context, ENISA has identified a set of concrete actions, which if implemented will lead to a coherent and holistic national cyber-security strategy.

*The proposed process of development and execution of the national cyber security strategy*

ENISA adopted lifecycle approach in governing a strategy since it best fits the needs and nature of the requirements of a national cyber-security strategy. In this approach twenty actions are listed. The list of main specific objectives that should be considered is:

1. Setting the vision, scope, objectives and priorities - Setting objectives and priorities is very important to successfully reach the aim of increasing the resilience and security level of national ICT assets.

2. Following a national risk assessment approach - One of the key elements of a cyber-security strategy is the national risk assessment, with a specific focus on critical information infrastructures.

3. Identifying and engaging stakeholders – Critical step in developing successful cyber security strategy is a definition, identification and engagement of all relevant stakeholders both private and public.

4. Establishing trusted information-sharing mechanisms – The information sharing among private and public stakeholders is essential. Owners of critical infrastructure could share with authorities some information on new risks and the ways of their mitigation. On the other hand, public stakeholders can share some information on aspects related to the national security.

5. Organizing cyber-security exercises – Exercises are important for authorities to test existing emergency plans, target specific weaknesses, increase cooperation between different sectors and identify interdependencies. ENISA prepared a good practice guide to assist authorities in Member States to better understand the complexities of exercises and help them prepare local and national ones [16]

6. Establishing incident-reporting mechanisms – Incident-reporting mechanisms are important for any organization that collect and analyze data related to threats and risk management. The more a person knows about major incidents the better they can understand the threat.

7. Fostering R&D – The research and development cycle is of great importance for any process where quality matters, especially at processes regarding privacy and security

8. Establishing a public–private partnership - cooperation in the form of Public Private Partnerships (PPPs) has evolved in many Member States and word wide. It is one of the main concepts that protection of critical infrastructure is based on. ENISA developed Good Practice Guide (GPG) on Cooperative Models for Effective Public Private Partnerships [17]

9. Evaluating – evaluation is a required process of assessing whether the objectives and planned results have been effectively reached.

## IV. PROPOSED ROLES OF KEY STAKEHOLDERS IN CIIP PROCESS – "DISTRIBUTION OF RESPONSIBILITIES"

As stated above, there are several stakeholders and bodies interested in CIIP process. The list of nine most important steps is extracted from more detailed list of 20 steps


Fig. 3 – "Distribution of Responsibilities" among key stakeholders in CIIP process

initially proposed by ENISA in [11].

Each body or interested party in CIIP should have its own role and place in this complex process. The authors proposed a possible solution for roles distribution among stakeholders regarding most important nine objectives in CIIP process as it is presented in Fig. 3.

Although, all of the listed bodies have its place, the main share in distribution of responsibilities falls to government bodies (Ministry of Foreign and Internal Trade and Telecommunications and RATEL) and the science and research community. The roles of the Ministry of Interior and Telecom operators are also very important.

## VI. CONCLUSION

The process of protecting critical infrastructure is one of the emerging subjects in recent years. It turns out that this process is very complex and requires the inclusion of broad set of stakeholders. Considering Serbia's geographical and political proximity to the European Union, the EU regulation is something that should be implemented in the process of CIIP. We should implement measures considering EU standards in order to fit into European CIIP framework. The national infrastructure protection program in Serbia is still in its initial phase, and in this paper authors proposed the general framework for the CIIP within the national critical infrastructure protection plan.

The government should take a lead, but both public and private stakeholders should invest its time and resources to successfully deploy CIIP plan and protect its assets.

## ACKNOWLEDGMENT

This research activity is a part of the Project "Management of Critical Infrastructure for Sustainable Development in the Postal, Communications and Railway sectors of the Republic of Serbia" supported by Ministry of Education and Science within the framework of scientific research projects 2011-2014 and by Telekom Srbija, Pošta Srbije and Železnica Srbije.

## V. REFERENCES

[1] European Commission, "*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*," Official Journal of the European Union L, pp. 345-375, 23.12.2008..

[2] Rajmohan C., Subramanya G., Sharma N., *Telecommunication Networks: Security Management*, Tata Consultancy Services Limited, 2012.

[3] Gospić N., Bogojević D., Murić G., "*Managing critical infrastructure for sustainable development in the telecommunications sector in the Republic of Serbia,"* Zrenjanin, 2012.

[4] Conrad S. H., LeClaire R. J., O'Reilly G. P., Uzunalioglu H., *Critical National Infrastructure Reliability Modeling and Analysis*, Lucent Technologies Inc, 2006.

[5] Kljaić Z, Mandžuka S., Škorput P., "*Primjena ICT-a u upravljanju kriticnom infrastrukturom u tranzicijskim zemljama*," in TELFOR, Beograd, 2010.

[6] Vlada Republike Srbije, "*Strategija razvoja informacionog društva u Republici Srbiji do 2020*," 2010.

[7] Vlada Republike Srbije, "*Zakon o vanrednim situacijama*," Republički glasnik, vol. 111, 2011.

[8] Utne I., Hokstad P., Vatn J., "*A method for risk modeling of interdependencies in critical infrastructures,"* Reliability Engineering and System Safety, vol. 96, p. 1, 2010.

[9] Federal Republic of Germany, Federal Ministry of the Interior, "*National Strategy for Critical Infrastructure Protection (CIP Strategy)*," 2009.

[10] European Commission, "*Protecting Europe from large scale cyber-attacks and disruptions: enhancing,*" Brussels, 2009.

[11] European Network and Information Security Agency "*National Cyber Security Strategies, Practical Guide on Development and Execution,*" 2012.

[12] International Organization for Standardization, "*Risk management - Principles and guidelines*," International Organization for Standardization, 2009.

[13] Schaffer G., Keil T. M. Mayer R, "*Communications Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*," Homeland Security, 2010.

[14] European Commission, "*Achievements and next steps: towards global cyber-security*," Brussels, 2011.

[15] European Commission, "*European principles and guidelines for the resilience and stability of the Internet*," 2011.

[16] European Network and Information Security Agency, "*Good Practice Guide on National Exercises*," 2009.

[17] European Network and Information Security Agency, "*Good Practice Guide (GPG) on Cooperative Models for Effective Public Private Partnerships*," 2011.