351.824.11(497)
https://doi.org/10.18485/fb_nsr.2018.ch14

Branislav Todorovic
National Technical University of Athens (NTUA), Greece

"The One Belt, One Road" Initiative Related Critical Infrastructure Protection at a Crossroads in Balkans

Abstract

The B&R initiative is expected to influence the critical infrastructure (CI) expansion and development in countries in Western Balkans, but the complexity of B&R will expose CI to a number of new vulnerabilities & risks. This paper explores the status and possibilities for improvement of critical infrastructure protection (CIP) activities in the Republic of Serbia, in relation to the current situation in Balkans and globally. It pinpoints some key issues with CIP in US, EU and China, in particular within the cyber domain, and suggests a well-agued direction for CIP strategy for Balkans, being at a crossroads – in need of deciding over the joined CIP approach.

Keywords:

Critical infrastructure protection; Cyber security; Emergency situation; Legislation; One Belt One Road – B&R initiative; Serbia; Strategy

1. INTRODUCTION

One Belt One Road (B&R) initiative, as agreed by everyone, is growing to become the biggest conglomeration of projects in this century. Its sheer size requires careful thinking and planning in all phases and tasks from conceptual to detailed design, through construction and further in the exploitation for decades to come. That is one of the reasons that the B&R

initiative requires the application of state-of-art solutions, new out-of-box way of thinking and strong cooperation between China and other involved countries, including Central and Eastern European countries (CEECs). B&R should promote synergy between China and CEECs, setting new examples for cooperation on production capacity, investment, trade & finance cooperation and expanding cultural exchange.

As the part of foreseen high-tech application and planning in B&R, the establishment of think-tanks for academic research was proposed at the Third China-CEECs Summit in Belgrade in December 2014. That step was further followed, resulting in implementation of a B&R Think-Tank Network. However, besides covering the common political, financial, techno-economic, technological and cultural issues, it is important to include in B&R advanced R&D, planning and practical application of security & protection techniques and management, in particular for critical infrastructures (CI). In the case of B&R initiative, involved infrastructure might include: roads and railways for land based and ports for maritime transportation; electric power grids and other energy supply networks; information and communication technology (ICT) systems; various supporting and related infrastructure like buildings and water utilities; etc.

2. WHAT B&R INITIATIVE MEANS FOR THE WESTERN BALKANS

The influence and importance of B&R initiative has been discussed in a number of articles and papers. With regard to B&R and Western Balkans, some key elements could be derived from the except from the report prepared by Dr Jens Bastian for EBRD [Bastian 2017]:

- With the availability of capital, technology and a master plan under the heading of the B&R, Chinese investments in EU and non-EU member states create leverage for *acquisitions and infrastructure innovation* on an unprecedented scale.
- China's ambitious B&R project can contribute to help *transforming the Western Balkans*.
- The B&R includes policy initiatives, investment priorities and business decisions by Chinese authorities and companies that can have *major impact on participating countries and their regulatory authorities and civil society organizations*.

B&R initiative influences countries in Western Balkans in a number of ways which are beyond the scope of this paper. In relation to critical infrastruc-

tures we can expect that the B&R initiative would bring expansion, both in constructing new infrastructures and in upgrading and refurbishing existing ones, involving the application of new technological solutions. Unfortunately the expansion of infrastructure is followed with the growth of risks of all types, as witnessed globally in the recent years. Therefore it is essential that the expansion process is followed by the corresponding security and protection measures.

3. CRITICAL INFRASTRUCTURE RISKS & PROTECTION – CONCEPT OVERVIEW

Risks are associated with the construction, use and operation of components and systems of infrastructures. The construction and planned operation are based on engineers design, so engineers must consider the relevant risks and plan how to reduce them. After commissioning, infrastructure use, operation and other activities might produce additional risks, therefore those who plan and manage the activities must be continuously engaged to reduce those risks and minimize negative effects (Figure 1).

Figure 1. *Risk management as the integral component of infrastructure protection*

Consequently, infrastructure planning and design within B&R should include strong risk management component, as the integral part of the engineering decision making. " Risk management occurs during the system designing and in ongoing operations. Risk management leads to making decisions about whether to do something (or which action to take) to reduce risk. If one considers risk as a probability distribution over the possible

outcomes, then risk management can be seen as the selection of an action to modify that probability distribution" [Herrmann 2015]. Furthermore, taking into consideration the complexity of systems foreseen for B&R initiative, it is important to involve multi-disciplinary teams of experts in the designing process in order to provide a good coordination of activities in different fields, meticulous operational planning and best possible preparedness for various vulnerabilities and risks.

At the organizational level, business continuity and disaster recovery planning are an important risk management components. Risks range from equipment failures and natural disasters, through human errors to malicious and terrorist attacks. Risks can cover health and safety, financial, privacy and other hazards. Therefore risk management is the constant process throughout the lifetime of the infrastructure, going in circles with main components being e.g. assess, prepare, respond and recover (exact definitions may vary from author to author). It can be agreed that critical infrastructure risk & protection management targets emergency preparedness in order to ensure the business continuity (Figure 2).

Figure 2. *Risk & protection management components and segments*

The two components of critical infrastructure (physical, including human factor, and cyber) are the core of the risk management and should be integrated in the risk management process (US Department of Homeland Security – DHS, 2013). In developed countries, the operation and functioning of critical national infrastructure depends on computers and ICT technologies and may therefore be an easy target. If we take into account that the national infrastructure includes a number of systems relying on high-tech technology and support, inter alia: energy systems, nuclear power plants, public health, emergency services, government, dams, electricity and water

supplies, transport traffic, telecommunications networks, it can be clearly concluded that potential attack on these systems could have enormous consequences to the country and mostly to the civilians [Ophandt 2010].

4. CIP PROBLEMS AND TENDENCIES IN SERBIA

Republic of Serbia is well organized to respond to natural disasters, as verified in several cases over the previous decades, despite the obvious increase in the number of natural disasters worldwide, as well as in their destructiveness. Natural disasters often result in a higher loss of life, in addition to both material and non-material damage. Furthermore, the disruption of work of CI prevents or limits the vital state operation (governance, health, energy, economic, social, education and general security functions), which is further reflected in the citizens' safety. Despite the global technological development, remains the fact that the disasters and their impact on people and CI cannot be prevented, but mechanisms for the prediction and early warning of disasters can be improved. This means that the resilience and capacity for faster and more efficient recovery of CI operation and functioning of the society can be increased. Aside from the degree of destruction, the response time and strategy in an emergency situation shows the level of preparedness and in Serbia it receives the highest mark for natural disasters.

In the same time, a certain confusion and chaotic situation can be noted within the Republic of Serbia in relation to critical infrastructure security, protection and resilience topics. It continues to exist even after the proclamations of the *Law on Emergency Situations*, published in the Government Gazette of the Republic of Serbia No. 111/2009 (Zakon o vanrednim situacijama; Službeni glasnik Republike Srbije, broj 111/2009) and the *National Strategy for Protection and Rescue in Emergency Situations*, published in the Government Gazette of the Republic of Serbia No. 86/2011 (Nacionalna strategija zaštite i spasavanja u vanrednim sitaucijama; Službeni glasnik Republike Srbije, broj 86/2011). It is debatable whether there is a notion in Serbia about CI protection, since legislators haven't clearly defined that area, i.e. terms, scope and targets of CI protection and resilience. Within the described conditions and in order to cover the legislative gaps, the Government of the Republic of Serbia has defined a *Rulebook on Content and Methodology of Plans Developing for Protection and Rescue in Emergency Situations*, based on article 45, paragraph 4 of the Law on Emergency Situa-

tions. This Rulebook officially introduces the term, 'critical infrastructure' in Serbia for the first time. However, it remains unclear which infrastructure the term applies to [Todorovic et al. 2016].

Countries in transition, including Serbia and neighboring Western Balkans, are subject to a specific situation, facing severe transformation phases in all spheres (democratization of the society, overcoming authoritarian legacy, transformation of social property, deteriorating infrastructure, outdated technologies etc.). They fall significantly behind developed countries which have more organized and effective systems of CIP. They also face other problems that make establishing the appropriate protection system difficult (insufficiently developed democratic institutions, the absence of appropriate economic policies, the lack of clearly identified sources and forms of endangering critical infrastructures, the inexistence of clear classification of critical sectors and a coherent legal framework which regulates this area). While identifying such problems, which are faced by the majority of countries in transition, it is important to bear in mind that each of these countries has certain specific characteristics which make it difficult to give universal conclusions and recommendations [Kešetović et al. 2013]. Perhaps the B&R initiative might become the focal point for integrated approach to CIP in western Balkans. Starting with CIP examples and paradigms from developed and technologically advanced countries, the comparative method should be used in order to try to identify critical sectors, adopting and applying elements and methodologies which can contribute to the improvement of CI protection in Serbia, in close collaboration with countries from the region.

Another factor to be considered is the role of private security in Serbia, which is continuing to expand. There are three main reasons for this. After 18 years, private security in Serbia has finally become legalized; a special law on private security is in the process of being adopted. Also, the Serbian Association of Private Security Companies and the Association for Private Security at the Serbian Chamber of Commerce are raising awareness of private security, and the need for professionalization and standardization. Finally, CoESS (Confederation of European Security Services) is providing important assistance in the processes of preparing Serbian private security to enter a European model. Private security in CIP has clearly not yet reached its full potential in Serbia. Best practices discussed in the CoESS white paper, including the guidelines for public private partnership (PPP) with application in UK, Germany and other countries, could be very useful examples of practicing PPP in security sector not just for Serbia, but for the other countries in the region as well [Davidović et al. 2012]. As the conclusion, CIP strategy given in the ECI Directive in coordination with private

security in EU done by the CoESS, including the guidelines for enforcing PPP, could also provide basis for common CIP system in Western Balkans. Besides the private security services industry, this process should include responsible decision makers (governments, politicians), owners and operators of CI and other stakeholders.

Globalization and rapid technological development have resulted in higher ICT risks and increased number of cyber attacks, which could potentially destroy or cause difficulties in operations of the critical infrastructure in a country. Due to the involvement of ICT in virtually all aspects of everyday life and work, a large number of countries have already established the operational mechanisms that enable them to react to cyber incidents. These mechanisms include cooperation between representatives of the state authorities on one side with private sector, academia and the civil society. Like many other countries in the Balkans, Serbia is lagging behind in these fields. Operators of electronic communications networks have an obligation to protect their ICT resources, but these measures certainly are not sufficient to ensure complete safety of a country's critical infrastructure from cyber attacks. On the other hand, given that a good part of the critical infrastructure is in the hands of the private (corporate) ownership and management, and the state alone cannot provide enough safety, it is necessary to establish a special form of cooperation between the state and the private sector. On the more global level, the EU announced a revision of the regulatory framework for electronic communications and services aimed at strengthening the security and integrity of communications networks. At this point in Serbia it is difficult to recognize similar institutionalized activity [Todorovic et al. 2016].

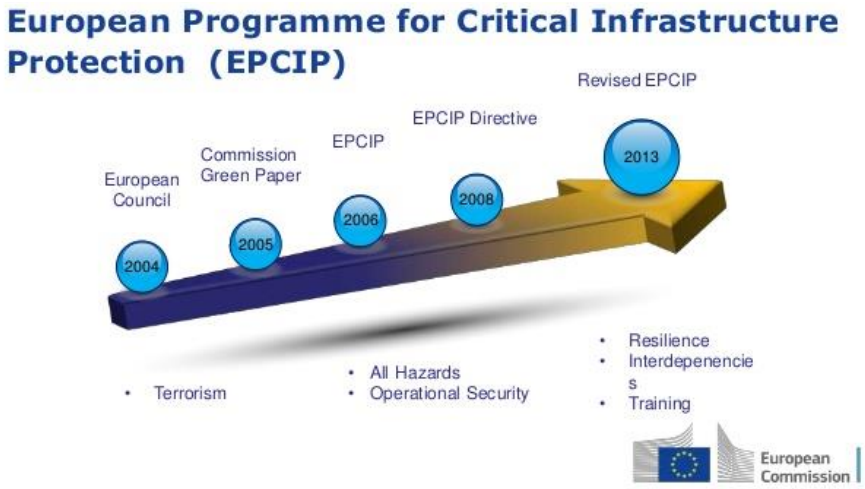
5. INTERNATIONALIZATION OF INFRASTRUCTURE PROTECTION IN PHYSICAL AND CYBER DOMAIN

CIP efforts in Balkans should certainly be linked with corresponding activities in EU, but experiences and know-how from other areas have to be taken into account as well. In this case, at least it would be the US, as traditional global leader in many areas, and China, as the new power in expansion. It is particularly important, since the rapid pace of technological innovation and adoption forces digital transformation in CI systems and in parallel increases cyber threats.

Beginning with US, the *American Presidential directive* PDD-63 of May 1998 [Web link 1] set up a national program of "Critical Infrastructure Protection". It was updated on December 17, 2003, by President Bush through Homeland Security Presidential Directive HSPD-7 for *Critical Infrastructure Identification, Prioritization, and Protection* [Web link 2]. Key elements from US paradigm [Web link 3] are: (i) National Infrastructure Assurance Plan / National Infrastructure Protection Plan (coordinating efforts of federal government and private sector) and (ii) Department of Defense (DoD) CI sectors, with focus on Public Works. Within the latest developments, in 2013 the *Presidential Executive Order 13636* ("Improving Critical Infrastructure Cybersecurity") tasked the U.S. National Institute of Standards and Technology (NIST) to lead the development of a framework to minimize cyber security risks to critical infrastructure, seeking feedback from public and private sector stakeholders and incorporating industry best practices to the fullest extent possible [Web link 4]. In 2014, NIST published the Cybersecurity Framework for Protecting Critical Infrastructure (NIST Framework), describing it as a "risk-based set of industry standards and best practices to help organizations manage cyber security risks." [Web link 5] Work on improvement and update of the Framework continues.

In Europe the equivalent "*European Programme for Critical Infrastructure Protection*" (EPCIP) [Web link 6] refers to the doctrine or specific programs created as a result of the European Commission's directive EU COM(2006) 786 which designates European critical infrastructure that, in case of fault, incident, or attack, could impact both the country where it is hosted and at least one other European Member State. Member states are obliged to adopt the 2006 directive into their national statutes. A key pillar of this programme is the 2008 Directive on European Critical Infrastructures (Figure 3). It establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for protection. The Directive has a sectoral scope, applying only to the energy and transport sectors. Methodologies used at European level do not match the maturity, in term of effectiveness and completeness, of their counterparts in US. Future projects should close that gap through close collaboration with EPCIP or ENISA, as well as with European expert groups such as the JRC.

Figure 3. *CIP in EU*



Perhaps the most advanced segment of protection in EU is in cyber domain. The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on July 6, 2016 and entered into force in August 2016. The NIS Directive provides legal measures to boost the overall level of cyber-security. However, taking into consideration the constant evolvement of cyber systems and corresponding threats, it is necessary to swiftly implement the Directive. In view of the impending deadlines for its transposition into national legislation (by May 9, 2018), and for the identification of operators of essential services (by November 9, 2018), the Commission adopted on September 2017 a Communication that aims at supporting Member States in their efforts to implement the Directive swiftly and coherently across the EU [Web link 7]. In that sense, it also envisions the "NIS toolkit" which provides practical information to Member States, e.g. by presenting best practices from the Member States and by providing explanation and interpretation of specific provisions of the Directive to explain how it should work in practice. NIS toolkit should have the following capabilities, among other: to be a pragmatic reference guide for global application, including new strategies under development; give links to existing models, evaluation tools and other references; provide accompanying evaluation tool to easily identify key areas for improvement and how they can be addressed; define best practice indicators to assess improvements over time; etc. [Web link 8]

To address the cyber domain issues, EU is also coordinating practical activities. One good example is the Cyber Europe 2016, the fourth pan-European cyber crisis exercise organised by the European Union Agency for Network and Information Security (ENISA). The exercise simulated a realistic crisis build-up over an actual period of 6 months, culminating in a 48 hour event on October 13 and 14, 2016. Targets of the exercise were to strengthen prevention, response and mitigation of larger-scale crisis, with the emphasize on cooperation at national and international levels and sound cyber security capabilities of participating public and private organisations from all 28 Member States of the EU (mostly from ICT sector). Additionally, many lessons were learned from the use of the prototype platforms developed by ENISA to support cooperation at EU level; they will reflect positively on the development of the EU-level crisis cooperation infrastructure financed by the Connecting Europe Facility (CEF) [ENISA, June 2017].

Another useful example from EU is related to the rapidly growing cyber insurance market. It is expected to further expand by the adoption of the GDPR and the NIS Directive which will incentivise organisations falling under their provisions to seek ways of residual risk transfer. However, the industry perceives the lack of commonality in risk assessment language. While some initiatives have started to take form, the industry has yet to make significant steps towards harmonisation for a variety of reasons. Following the needs, ENISA published the report that proposes two sets of recommendations, one towards the industry itself and one towards policy makers in order to support this evolution towards language harmonisation without stifling innovation. Specifically, the industry is encouraged to standardise policy language and underwriting questionnaires, promote data sharing between the stakeholders, develop industry standards, build in-house expertise in cyber security, contribute to the collection of data on aggregated loss scenarios, build offerings around information security and privacy regulations, adopt a sectorial approach in harmonising language, address the needs of the SME market and improve overall data quality by integrating various heterogeneous sources. EU and Member States Policy Makers are encouraged to create minimum coverage requirements, leverage the upcoming mandatory incident reporting schemes via the NIS Directive and the GDPR to produce meaningful data, create a central EU repository of incident data, raise awareness to increase demand and buyer maturity and develop guidelines for cyber insurance [ENISA, November 2017].

In China, a five-year plan on its national informatization (2016-2020) was issued by the State Council on December 27, 2016. According to the

plan, China will put more resources into the development of cutting-edge information technology, including 5G wireless systems, IPv6, smart manufacturing, cloud computing and internet of things. The plan also focused on cyber security, promoting legislation of relative laws and regulations, setting up risk alerts and an emergency mechanism [Web link 9]. As a part of the implementation of the China Cybersecurity Law, which took effect on June 1, 2017, the Cyberspace Administration of China (CAC) released a draft CIIP Regulation for public comment on July 11, 2017. It consists of eight chapters and 55 articles written, according to the regulation, "with a view to assuring the security of critical information infrastructure and in accordance with the Cybersecurity Law of China".

Figure 4. *Internationalization of CIP [Web link 10]*

	U.S.	E.U.	China
Primary CIP Policy Drivers	Executive Order and NIST Cybersecurity Framework	NIS Directive (Law)	China Cybersecurity Law, Draft CIIP Regulation, Cross Border Data Transfer Regulation, Cybersecurity Review Regulation, MLPS
Private Sector Participation During Legislation	Yes	Yes	No
Primary Legislation Feedback Channel(s)	Workshops and Request for Information (RFI)	Public Consultations; Surveys	30-Day Public Comment Period
Risk-Based Definition of Critical Infrastructure	Yes	Yes	Yes
Data and Operation Residency Requirements	No	No	Yes
Endorsement of Global Standards	Yes	Yes	No[19]

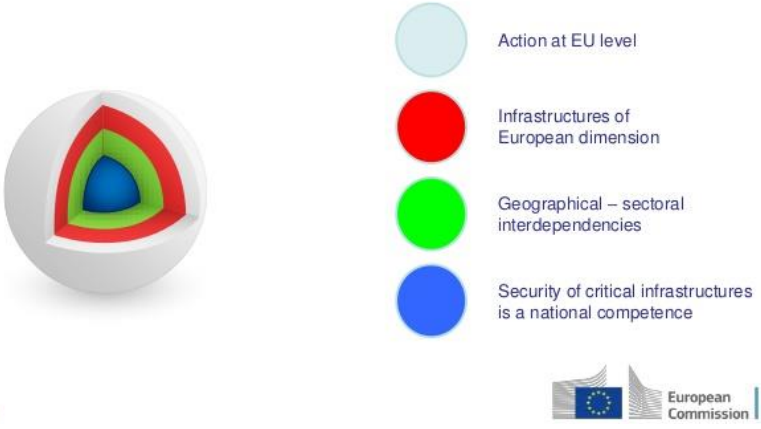
As it can be seen, the US, EU and China each remain in the formative stages of developing their approaches to CIP. Besides other differences in the approach, it is worth mentioning the ones in terms of the role of private sector. The traditional CI operators are privately-owned in the large extent in the US and some countries within EU, whereas most operators in similar CIP sectors in China are state-owned, apart from the Internet web service sector. US and EU promote the idea of private sector's participation during the legislative process, and in response, the private sector regards the sup-

port as an obligation to provide input and expectations about the CIP policy and compliance. The Chinese government also views the increased transparency as of importance. Regardless of the composition and geographic locations of the critical infrastructure operators and the technology providers, it is very important that government CIP policies maintain the characteristics of "flexible, scalable, industry agnostic, and technology neutral" [Web link 10]. Figure 4 presents a summary view of critical infrastructure protection approaches used by the governments of the US, EU and China.

6. CIP AT A CROSSROADS IN BALKANS

Once in operation, various segments of B&R initiative projects will be interdependent directly or indirectly. Following the occurrence of serious problems in one vital CI segment, such dependencies could cause serial interruptions in linked B&R structures within Balkans and further within Europe. B&R concept covers a vast area and a number of countries, with different morphology & climate, level of development, legislations, habits, and other influential parameters. As mentioned previously on examples from EU and other parts from the world, a complex system like B&R, in combination with existing infrastructures, is open to a number of vulnerabilities & risks that would require a meticulous operational planning and good coordination of activities. EU is trying to handle and balance the integral approach to CIP process with respect to individual characteristics and competences of its Member States (Figure 5).

Figure 5. *CIP approach in EU*



Taking into consideration the differences between countries in Balkans, related to their different historical, political and technological development, it is crucial to agree upon and establish the common approach to CIP in the region. Common approach should cover all levels from policies to application, with special attention on jurisdiction and finances (e.g. in presented case of cyber insurance it would be difficult, but crucial, to define for each CI roles of stakeholders and interests and responsibilities of CI owners and personnel, in order to estimate liabilities and advise on corporate risk management). However, before starting such an ambitious, huge and long-term task as common CIP strategy, countries participating in B&R initiative should define and agree, together with China, on the common platform for handling CIP.

Another aspect to be taken into consideration is the fact that CIP is not a simple task to be initiated, performed and concluded, but rather a continuous process. By focusing on CIP as a continuum, stakeholders can better plan for and manage the ongoing lifecycle of CIP, and ensure that stakeholders are sharing learned lessons among key communities in policy-making, operations and investments. It is also important to note that there is no specific area called protection. Rather, protection is the aggregate of these capabilities and functions that, taken as a whole, help reduce risk, increase resiliency, and safeguard the delivery of essential systems, services, and functions [Microsoft 2014]. The sooner the countries in Balkans agree on the way how to proceed together with CIP, the better.

7. CONCLUSIONS AND NEXT STEPS

Though as the most obvious solution for Serbia and Balkans might appear the adoption of the CIP system already in effect within EU, it is not so straightforward. As presented in previous chapters, EU still has issues of its own in handling CIP, mainly due to differences between EU member countries. B&R adds a new dimension to competences, interdependencies and legislative issues of related CIP. Therefore, once the B&R initiative and China are also included in the equation, the selection of most appropriate CIP common platform becomes even more complex and delicate. One might argue that the Republic of Serbia, due to its geopolitical position in the region, specific historical background and current international political relations, might be the ideal candidate to lead the CIP common platform development for Balkans. That would coincide with the pending task to upgrade and complete the CIP plans and legislations within Serbia.

Moreover, adversaries continue to develop innovative ways to attack, breach and disrupt operation of critical infrastructures despite various new protection measures that are constantly developed and implemented. Risk assessment has advanced significantly over years, but risk-based solutions tend to focus on assessing and strengthening components of complex systems under specific threat scenarios. Realization of the inability either completely to predict threats, or to cover extents and magnitude of incidents, including natural causes and failures, resulted in significant interest in resilience based management of CI [Todorovic and Bletas 2016]. Perhaps in parallel with CIP improvement activities in the Republic of Serbia it would be advisable to work on CI resilience, as the current most advanced concept to ensure the business continuity of CI and protect the society and people that depend on their operation.

REFERENCES

1. Bastian, J., (2017) The potential for growth through Chinese infrastructure investments in Central and South-Eastern Europe along the "Balkan Silk Road", Report prepared for the European Bank for Reconstruction and Development – EBRD (with funding from the Central European Initiative), Athens / London, July 2017.
2. Davidović, D., Kešetović, Ž., Pavicevic, O., (2012) National Critical Infrastructure Protection in Serbia: The Role of Private Security, Journal of Physical Security 6(1), pp. 59-72.
3. ENISA, (June 2017) Cyber Europe 2016: After Action Report, Findings from a cyber crisis exercise in Europe, European Union Agency for Network and Information Security (ENISA), ISBN: 978-92-9204-224-0, Heraklion, Greece.
4. ENISA, (November 2017) Commonality of risk assessment language in cyber insurance – Recommendations on Cyber Insurance, European Union Agency for Network and Information Security (ENISA), ISBN: 978-92-9204-228-8, Heraklion, Greece.
5. Herrmann, J. W., (2015) Engineering Decision Making and Risk Management, John Wiley & Sons, Inc., Hoboken, New Jersey, US, ISBN 978-1-118-91933-0
6. Kešetović Ž., Putnik N., Rakić M., National Critical Infrastructure Protection – Regional Perspective, University of Belgrade – Faculty of Security Studies, ISBN 978-86-84069-82-7, Belgrade, Serbia.
7. Microsoft, (2014) Critical Infrastructure Protection: Concepts and Continuum, White Paper, Microsoft Corporation.

8. Ophandt J. A. (2010) Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield. Duke Law Technol Rev, Page 7

9. Todorovic B., Bletas A., (2016) Resilience planning for critical infrastructure linked to "One Belt One Road"initiative in Balkans and Greece, The Belt and Road: The Balkans Perspective – Political and Security Aspects, University of Belgrade – Faculty of Security Studies, ISBN 978-86-80144-11-5, Belgrade, Serbia.

10. Todorovic B., Trifunovic D., Jonev K., Filipovic M., (2016) Chapter 22 – Contribution to Enhancement of Critical Infrastructure Resilience in Serbia, Resilience and Risk – Methods and Application in Environment, Cyber and Social Domains, Proceedings of the NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructure Safeguarding, ISBN 978-94-024-1122-5 (HB), Azores, Portugal, 26–29 June 2016

11. Web link 1: https://en.wikipedia.org/wiki/Presidential_directive

12. Web link 2: https://en.wikipedia.org/wiki/Critical_infrastructure_protection#cite_note-HSPD7bush-2

13. Web link 3: https://www.dhs.gov/water-and-wastewater-systems-sector

14. Web link 4: https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

15. Web link 5: https://www.nist.gov/cyberframework

16. Web link 6: https://en.wikipedia.org/wiki/European_Programme_for_Critical_Infrastructure_Protection

17. Web link 7: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

18. Web link 8: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf

19. Web link 9: http://english.gov.cn/policies/latest_releases/2016/12/27/content_281475526646686.htm

20. Web link 10: https://www.scribd.com/document/364544590/A-Comparative-Study-The-Approach-to-Critical-Infrastructure-Protection-in-the-U-S-E-U-and-China#from_embed