Review paper

THE ROLE OF CORPORATE SECURITY IN THE PROTECTION OF CRITICAL INFRASTRUCTURE

Marjan Gjurovski, PhD[1]
Gjorgji Alceski, PhD[2]

Abstract: One of the main features of corporate security is the protection of the interests of the company from all types and forms of endangerment. However, many of the corporations have a part of determining the objects that are of vital interest to the state, i.e. belonging to the category of critical infrastructures. There is the need for a different approach that is shaped according to changed security conditions. The field of competencies, based on the national interest, is changing and it is different from the standard measures i.e. ways of security, this is so the measures that are already in place should be focused on both, the corporate needs and the national security system.

The constant terrorist attacks on the corporations of vital interest show that terrorism does not recognize state borders nor the political systems or areas on which it is directed to. The tragic past events directed at corporations are defined as critical infrastructures and represent a clear indicator to continuous improvement of security, extending the corporate security interest both, to the state and even to the global security interest.

The increase development of the national security through corporations with a clearly defined security policy and co-operation is grounded over subjects that have a precise task in dealing with security challenges that arise from the complex sources of endangerment, and give a new impulse to the transformation of security awareness of both, the security and the other qualified staff. For those reasons, this paper has the purpose to raise the awareness into achieve a standardized level of security in all corporations that have the status of critical infrastructures with direct cooperation and coordination between the state security sector and the private security sector, which this key factor in the overall security system.

Keywords: security corporate security, national security, critical infrastructures, coordination

[1] Faculty of Security – Skopje, University "St.Kliment Ohridski"-Bitola. E-mail: marjan.gjurovski@uklo.edu.mk

[2] Dep. Airport Manager, TAV Macedonia Airport St. Paul The Apostle Ohrid. E-mail: Gjorgi.Alceski@tav.aero

THE IMPORTANCE OF NATIONAL CRITICAL INFRASTRUCTURE AS AN ESSENTIAL STATE INTEREST

The need to keep track with contemporary security trends, especially in the segment of "critical infrastructures", or the so-called "vital facilities", "facilities of special interest to the state and security", etc., as terms used in our country, is the foundation of security in modern societies. The complexity of contemporary threats, reflected through the corporations that operate the critical infrastructures, implies that they have a direct impact on national security and the efficient functioning of the state systems.

The determination of the need for security, as an essential interest of the state, is expanded with concepts of reference facilities whose security must be guaranteed. Hence, the infrastructures that bear such importance for society, where their non-functioning or limited functioning may create serious consequences and problems, are defined as "critical infrastructures" and need to be treated both on national and international level.[3] As critical infrastructure has become an important segment of national security, critical infrastructure protection has started to develop as well and it is listed among the top priorities of every state. In the context of contemporary global security threats, critical infrastructure protection is a priority issue of the national security of every state.[4]

The complexity of the issue of critical infrastructure security is directly linked with the national security strategies of a number of states, where it acquires a broader vital dimension that includes economic, business, political and environmental issues. National security no longer refers solely to military strategies, but rather tries to eliminate non-military threats by detecting the real threats and efficiently eliminating them. It often presupposes the creation of national security strategies through the corporations that are considered critical infrastructures, as a delicate and comprehensive process which constitutes an integral part of the security concept of each state.

Generally, there are a number of definitions of critical infrastructure. The generally accepted definition of critical infrastructure across the European Union is presented in Directive 114/2008. Here, the European Commission defines critical infrastructure' as a 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

[3] http://zastita.info/hr/clanak/2013/2/denis-caleta-(ics)-slovenska-iskustva,311,10204.html,Преземено 14.03.2014

[4] О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год. Стр.84

result of the failure to maintain those functions[5]. The analysis of the term critical infrastructure perceived through the need for its adequate protection, indicates that there are minor differences in the national definitions of the states, which highlight systems, assets, properties, products, etc. as crucial for normal functioning of the state in terms of its economic, social, health and security needs. Based on the overall analyses of the notion of "critical infrastructure", viewed through the prism of security and the offered Western indicative lists of critical infrastructures, and guided by the European Union, we may formulate the following definition: *Critical infrastructures refer to facilities, assets, installations, products, services and all systems that are directly or indirectly linked with the normal functioning of the state and whose disruption would cause serious consequences to national security, economy, health, state functionality, social and other consequences*.

In that context, we would fully accept the areas identified by the European Commission, inter alia, energy, information and communications technologies, water, food, finances, public and legal protection, public administration, transport, chemical industry, research[6], with all their capacities and activities, products or services. On the other hand, viewing national security as a state of continuing accomplishments, development, welfare and optimal protection of national and state values and interests, the companies that operate critical infrastructures are assigned an exceptional place within the national security system. National security is necessary, inter alia, to accomplish, maintain and promote the security of the citizens, the national security system and the supranational security mechanism, as well as the absence (individual, group and collective) of fear of being threatened, and the collective feeling of peace, certainty and control of the development of future occurrences and events important to societal life and the state.[7]

NON-MILITARY RISKS AND THREATS TO NATIONAL SECURITY REFLECTED THROUGH THE CORPORATIONS DESIGNATED AS CRITICAL INFRASTRUCTURES

Non-military risks and threats to national security, which are ever more present in everyday life, asymmetric threats focusing on the new forms of action and the examples of the past imply that critical information

[5] EU Directive 2008/114/23.12.2008 EN Official Journal of the European Union L 345/75"

[6] Green paper on a European Programme for critical infrastructure protection Brussels, 17.11.2005 COM(2005) 576 final Annex II

[7] Саша В. Мијалковић- НАЦИОНАЛНА БЕЗБЕДНОСТ - треће, измењено и допуњено издање КРИМИНАЛИСТИЧКО-ПОЛИЦИЈСКА АКАДЕМИЈА Београд, 2015 стр.82

infrastructures, electrical energy infrastructures, oil and natural gas transportation, civilian aviation, water resources and other critical infrastructures have been the target of terrorist attacks. The attacks on critical infrastructures, regardless of whether they are triggered by political, religious, separatist or other types of organizations or they involve terrorism, industrial espionage, hacker attacks are real threats that are directly linked to national security. The omissions of the security services and the preparedness of the terrorists to manipulate, or break into the security protection systems of the corporations determined as critical infrastructures, increase the danger of future illegal acts.

It is evident that national security should be considered on three levels through several areas of human activity. The levels of consideration are individual, state (national) and international, whereas the spheres of human activity include at least the military, political, economic, social and environmental areas. State level is the most important since it determines the other two levels: in contemporary world, the standard unit of security is the sovereign territorial state. The areas important for national security are military, including the offensive and defensive capabilities of the state; economic, that is, the access to natural resources, the market and the finances that determine the acceptable level of welfare; the social, that determines the existence and evolution of traditions, culture, language, national identity and customs and environmental protection that includes the care for the biosphere on which all human activities are dependent.[8] Critical infrastructure is the backbone of every nation as it is linked with national security, economy, industry and health[9].

With respect to the threats to the critical infrastructures, they may be man-made, as a result of terrorism or other criminal activities, or natural, as a consequence of weather conditions, such as storms, volcanic eruptions, floods and other environmental disasters. Furthermore, critical infrastructures may be jeopardized by diseases or pandemics that affect large numbers of critical personnel.[10]

[8]https://kupdf.com/download/nacionalna-bezbednost-knjiga_58ac2d4b6454a70654b1e90d_pdf 96 Buzan, B.:
People, States & Fear – An Agenda for International Security Studies in the Post-Cold War Era , стр. 19–20. Саша Мијалковиќ : Национална безбедност 2017год. стр. 37
[9]http://www.dhs.gov/what-critical-infrastructure Accessed on 26.03.2015г.
[10]Critical Infrastructure Security and Protection: The Public-Private Opportunity White Paper by CoESS – Confederation of European Security Services © December 2010.

CORPORATE SECURITY AS A SECURITY FACTOR OF NATIONAL SECURITY

Considering the fact that in many Western countries the largest portion of critical infrastructures is privately owned, there is a need for active involvement of the state in this type of security. In Germany, four fifths of the critical infrastructures are in private hands. In the USA, about 85% of the critical infrastructures are privately owned, but reality shows that market powers are not sufficient by themselves to incite the required investment in protection. The complexity of this security concept arises from the need to implement a number of measures and activities that extend throughout different areas of expertise and activities, all united under national security. Critical infrastructure consisting of numerous sectors is a system of elements that are most often on the territory of one state and crucial to the maintenance of the vital functions, health, security, safety, economic and social welfare of the population and its disruption or destruction would significant consequences in a given state as a result of its inability to preserve these functions. [11]

If we draw a parallel between the basic principles of corporate security for protection of the company's interests against all types and forms of threats and making profit on the one hand, and the need for national security, in terms of critical infrastructures that permeate all pores of national security, on the other hand, it is evident that their roots are stemming from the national values and their ensuing state interests. Many scientists view National security on three levels (individual, state/national and international), including important areas of human activity, *inter alia*, the level of technical – technological development, the educational and age structure of the population, the influence of the state on the decisions made by the international organizations, the power and potential of the states, etc.[12]

All offered definitions or considerations of the term national security refer to the connection between critical infrastructures and national security. Therefore, the complexity of this security concept stems from the need for implementation of plethora of measures and activities that encompass various areas of expertise and activities, all united under the area of security.

---

[11] О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год. Стр.35

[12] More details in: Art J. Robert "The Fungibility of Force" in Art J. Robert, Waltz N. Kenneth (eds), The use of Force – Military Power and International Politics, Rowman & Littlefield Publishers Inc., Oxford 2004., pp.8-15 . – Корпорациски Безбедносен Систем О. Бакрески, Д. Триван, С. Митевски Скопје 2012

NATIONAL CONCEPTS IN FUNCTION OF THE SECURITY OF CI THROUGH THE CORPORATIONS OF VITAL INTERESTS

If we consider the need to protect critical infrastructure in the US by managing risks it is evident that it is wide-ranging, composed of partnerships among owners and operators; Federal, State, local, and territorial governments; regional entities; non-profit organizations; the academia, etc.

Managing the risks from significant threat and hazards to physical and cyber critical infrastructure requires an integrated approach to:

- Identify, deter, detect, disrupt, and prepare for threats and hazards to the Nation's critical infrastructure;
- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur[13].

The success of this integrated approach depends on the overall spectrum of capabilities, expertise and experiences in infrastructures and their concerned parties.[14]

Although the US and the EU differ in their positions on the risks and threats to general national security and the critical national goods, they recently established a common determination on two levels that define:

- The resources that constitute critical infrastructure, and
- The measures required for their protection[15].

If we make an overview of the security concepts through a legislative framework, we will see that many contemporary countries regulate this area by directives, strategies, laws, etc., in line with their national interests, designed to enhance the security and persistence of their critical infrastructures in the face of today's threats. The CIP concept, viewed through the prism of providing a framework for a consistent national approach to protection of the state, government and business, designs security concepts that will enable the corporations, that is, the owners – operators of critical infrastructures to deal with the potential risks to the infrastructure or the relevant sector.

CI protection is largely decentralized in the EU member states. In each state, a significant part of the infrastructure is in private ownership and

---

[13] NIPP 2013 Partnering for Critical Infrastructure Security and Resilience Homeland Security - USA

[14] Ibid, p. 7

[15] Zastita kriticne infrastructure i osnovni elementi uskladivanja sa direktivom saveta Evrope 2008/114/ES, Mirko Škero Bezbedno-informativna agencija Vladimir Ateljević Vlada Republike Srbije, Kancelarija za evropske integracije - Visoke studije bezbednosti i odbrane стр.197.

therefore, there must be cooperation with the state institutions. The level and degree of participation of privately-owned corporations in the protection of critical infrastructures are different. In certain countries, the representatives of the private sector are actively or systematically involved in the policy creation process, whereas in others, the private sector is involved only if necessary and mostly for the purpose of implementing the minimum protection standards set up by the state sector. There are many efforts in the EU to consider CIP for each sector separately.[16] As a result, experts describe the EU work on protecting CI as assisting the states in clearly defined sectors in conditions of relevant sectoral coordination.[17] The problem of the cooperation between the EU and member states for CIP may lie in some states' position that certain data must be kept within national frames only.[18]

In Norway, the concept of "a vulnerable society" has become a major part of both public and political debates, following a report by a government commission headed by former Prime Minister Kåre Willoch.[19] The Willoch commission listed several new challenges regarding societal vulnerability and proposed a set of measures in its Report, which constituted the foundation of Norways's White Paper. These included technological changes, increased complexity in society, increased cost- and efficiency pressure, reduced manning in public services and outsourcing of public services to commercial enterprises.[20] These challenges, together with the emergence of "new" threats like terrorism, organized crime and climatic changes, represent a fundamentally changed context for the organizations responsible for the maintenance and protection of critical infrastructures. France follows the doctrine for defense and national security and its approach focusing on "operators of vital importance" means that the inaccessibility of those operators will strongly undermine the economic or military potential and nation's security and resilience. Each operator identifies the critical components in its production system and is

[16] Eriksson, P., Barck-Holst S., Critical Infrastructure Protection policy in the EU and in Sweden –Comparative analysis, FOI, Stockholm, 2005.

[17] Larsson, R., *Tackling Dependency: The EU and its Security Challenges*, Swedish Defense Research Agency, 2007, стр. 9-24.

[18] Jarlsvik, H., Castenfors, K., *Security and Preparedness in the EU*, Stockholm, 2004, стр.64.

[19] Project description: Critical infrastructures, public sector reorganization and societal safety (CISS) https://www.sintef.no/globalassets/project/samrisk/ciss/critical-infrastructures-and-societal-safety.pdf посетена 03/12/2016.О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год.

[20] Report on Safety and Security of Society. Report no. 17 to the Storting (2001-2002). Government Norway: https://www.regjeringen.no/en/dokumenter/Statement-on-Safety-and-Security-of-Soci/id420173/посетена на 6/12/2016.О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год.

obligated to offer them as points of vital interest that require special protection.[21]

In the legal code of the Czech Republic, the CI issues ensue from the legal regulations and fall under four steps:

1. Selection of CI within individual sectors.
2. Applying the definition of critical infrastructure.
3. Applying the definition of European critical infrastructure (ECI).
4. Applying the cross-cutting criteria.[22]

With respect to the legal regulation for CI protection, the Republic of Croatia has advanced in comparison with the other states of former Yugoslavia, by regulating CI protection, or more specifically, the management and protection of CI is regulated by the Law on Critical Infrastructures, adopted in 2013,[23] which is based on EU Directive 114 of 2008. In addition to adopting this law, the Republic of Croatia has passed two additional bylaws: the Decision designating the sectors in which the central state administration bodies identify national critical infrastructures,[24] and the List determining the order of critical infrastructures sectors and the Rulebook on the risk analysis methodology in managing critical infrastructures.[25] With the Law on Critical Infrastructures, the Republic of Croatia regulates national and European critical infrastructures, the sectors of national critical infrastructures, the management of critical infrastructures, the risk analysis development, the security plan of the owners, the security coordinator of critical infrastructures, the procedures for handling sensitive and classified information and the mechanism for supervising the implementation of the law.[26]

The Federation and local governments are required jointly to enhance and implement critical infrastructure protection in their respective areas of responsibility. This purpose is served by a structured implementation. This procedure comprises the following work packages, which are implemented in parallel, and is based on the co-operative approach adopted by the Federal

[21]Secrétariat Généraldela Défenseetdela Sécurité Nationale: http://www.sgdsn.gouv.fr/site_rubrique70.html, посетена 06.12.2016.

[22] International jurnal of mathematical models and methods in applied sciences - Measures for critical infrastructure protection – Ludek Lucas, Lubos Necesal – Issue 7, Volume 5, 2011.

[23] Zakon o kritičnim infrastrukturama, (Narodne novine 56/2013).

[24] Odluku o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura, (Narodne novine 108/2013).

[25] Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura, (Narodne novine 128/2013).

[26] Закон о критичним инфраструктурама NN56 13, http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, посетена на 14/11/2016.

Administration with the involvement of the other major players, i.e. operators and the relevant associations:

1. definition of general protection targets;
2. analysis of threats, vulnerabilities, and management capabilities;
3. assessment of the threats involved;
4. specification of protection targets, taking account of existing protective measures; analysis of existing regulations and, where applicable, identification of additional measures contributing to goal attainment.

For the implementation of the protection strategy, an extensive set of instruments is available in the form of

- programmes and plans (e.g. the National Plan for information infrastructure protection and the related implementation plans as a strategic concept for IT infrastructure protection;
- specific recommendations for action (e.g. the national Baseline Protection Concept as a basic guidance to physical critical infrastructure protection; the Risk and Crisis Management Guide for Critical Infrastructure Operators, or the national special protection concepts as detailed recommendations for action for the protection of individual CI sectors;
- standards, norms and regulations (e.g. the BSI Information Security Standards as a basic recommendation for action addressed to critical infrastructure operators; or the regulations of the German Gas and Water Supply Association on risk management in the field of drinking water supply.[27]

On account of the chosen co-operative approach that must be given priority, suitably institutionalized platforms involving the state and public authorities, companies and associations are required in view of the procedural steps and instruments that serve to implement the politico-strategic framework.

These security partnership platforms may be organized as: round tables; on federal level; on federal states level; on local government level; joint round tables of the afore-stated entities[28].

CI security, viewed through the prism of national guidelines for protection of CI from terrorism, adopted by the Committee for fight against terrorism of Australia and New Zealand, provides a framework for a national, consistent approach on the protection of CI for the state, the government and the businesses. The Strategy is designed to aid the owners and operators of CI in their dicussions with their jurisdictions (including the Government) about protecting the CI from terrorism. It defines that the treatment of individual CI assets will depend on an assessment of the criticality of the asset in question,

[27] National Strategy for Critical Infrastructure Protection (CIP Strategy) Federal Republic of Germany
Federal Ministry of the Interior Berlin, 17th June 2009
[28] Ibid.

the nature of the security environment and the risk profles for that asset or relevant sector[29].

The term critical infrastructure has not yet been adopted in the framework of the National legislation of the Republic of Macedonia, however, it does not mean that the objects of special significance or the vital facilities in the Republic of Macedonia have not been determined or defined. The Republic of Macedonia has continuity in defining these facilities, in terms of foreseen security measures and delegated duties and responsibilities, however, they are not harmonized in accordance with the guidelines of the European Union. In this regard, the terms are not clearly specified, that is, critical infrastructures are not covered in accordance with the recommendations of the Union. One of the more important steps in this direction was made with the adoption of the Decision on determining the legal entities that are obligated to have private security. This Decision was adopted by the Government of the Republic of Macedonia in 2013, and pursuant to Article 44 of the Law on Private Security ("Official Gazette of the Republic of Macedonia" No. 166/12) and the Law on Amending the Law on Private Security ("Official Gazette of the Republic of Macedonia" No. 164/13), which stipulates the time of their entry into force. According to Article 44 of this Law, the Government of the Republic of Macedonia determines which legal entities are obligated to have private security, if the performance of their activity is related to handling radioactive substances or other hazardous substances for people and the environment, objects of particular cultural and historical significance, as well as in other cases when it is in the interest of security, that is, defense of the Republic of Macedonia.

It must be noted that the regulations treating critical infrastructures include the legal regulations on protection and rescue, as well as crisis management.

CONCLUSION

Corporate security may be defined as one of the most important processes in the organizations as it has a significant role in the functioning of the systems. The strategic planning and operational measures stemming from corporate security must provide answers to the numerous threats and risks the companies face, especially in the segment of critical infrastructure. This process

[29]https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf Превземено 11.11.2015година

requires much more attention and awareness at the highest level of company management[30].

The key personnel in corporate security must take dominant positions, primarily due to the dependence of the state on these companies determined as critical infrastructures. It is the the responsibility of the state to protect the public and ensure a certain level of social functionality and secutity. However, the fact that part of CI is state-owned, whereas part is in orivate ownership (domestic or foreign companies) and that some owners do not share the same values and positions with respect to the protection of the CI system calls for a multifaceted approach of the state and the operators.

Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that have institutional knowledge and specialized expertise about the sector.[31] Therefore, security policy, which is a complex and interdependent set of measures, plans, activities and programs, should be directed towards upgrading the existing regulations and practices in view of seeking and defining the possibilities and conditions for applying advanced practices, procedures and systems and implementing them in the development of security. The practical application of certain standards and procedures that ensue from the final operationalization of the offered solutions should be the priority of each state, which requires a new approach to security by activating advanced security systems that follow the technological achievements non-stop, 24 hours a day. There is no dilemma that equipping the security services in accordance with the latest sophisticated achievements in this area will ensure unobstructed execution of the assigned tasks, adequate to contemporary risks and threats.

Corporations, defined as CI, should develop legislation-based security programs or plans that will be approved, accepted and coordinated with all national security stakeholders, especially with the Ministry of Interior and the Ministry of Defense and other relevant members of the national security system. On the other hand, the national security bodies should develop guidelines for the critical infrastructures to adapt their security systems in terms of personnel and technical equipment, so as to guarantee the implementation of standard measures and activities within their scope of work.

---

30 http://www.asadria.com/index.php/teme/kolumne/276-kriticna-infrastruktura-i-znacaj-osiguravanja-njenog-neprekidnog-djelovanja - Denis Caleta - Kritična infrastruktura i značaj osiguravanja njenog neprekidnog djelovanja, Превземено на 17.09.2015г.

31 Presidential Policy Directive -- Critical Infrastructure Security and Resilience The White House Office of the Press Secretary February 12, 2013

BIBLIOGRAPHY

1. О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год.
2. Саша В. Мијалковић- Национална безбедност - треће, измењено и допуњено издање Криминалистичко-полицијска академија Београд.
3. О. Бакрески, Д. Триван, С. Митевски Скопје 2012 Корпорациски Безбедносен Систем.
4. http://zastita.info/hr/clanak/2013/2/denis-caleta-(ics)-slovenska-iskustva,311,10204.html
5. Директива на ЕУ2008/114/23.12.2008 EN Official Journal of the European Union L 345/75”
6. Green paper on a European Programme for critical infrastructure protection Brussels, 17.11.2005 COM(2005) 576 final Annex II
7. Critical Infrastructure Security and Protection: The Public-Private Opportunity White Paper by CoESS – Confederation of European Security Services © December 2010.
8. NIPP 2013 Partnering for Critical Infrastructure Security and Resiliencehomeland security - USA
9. Zastita kriticne infrastructure I osnovni elementi uskladivanja sa direktivom saveta Evrope 2008/114/ES Mirko Škero Bezbedno-informativna agencija Vladimir Ateljević Vlada Republike Srbije, Kancelarija za evropske integracije - Visoke studije bezbednosti i odbrane Eriksson, P., Barck-Holst S., Critical Infrastructure Protection policy in the EU and in Sweden –Comparative analysis, FOI, Stockholm, 2005.
10. Larsson, R., Tackling Dependency: The EU and its Security Chalenges, Swedish Defense Research Agency, 2007, Jarlsvik, H., Castenfors, K., Security and Preparedness in the EU, Stockholm, 2004,
11. Project description: Critical infrastructures, public sector reorganization and societal safety(CISS)https://www.sintef.no/globalassets/project/samrisk/ciss/critical-infrastructures-and-societal-safety.pdf посетена 03/12/2016. О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год.
12. Report on Safety and Security of Society. Report no. 17 to the Storting (2001-2002). Government Norway: https://www.regjeringen.no/en/dokumenter/Statement-on-Safety-and-Security-of-Soci/id420173/ посетена на 6/12/2016. О. Бакревски, Т. Милошевска, Ѓ. Алчески - Заштита на критична инфраструктура Скопје 2017год.

13. Secrétariat Général de la Défense et de la Sécurité Nationale: http://www.sgdsn.gouv.fr/site_rubrique70.html, посетена 06.12.2016.

14. International jurnal of mathematical models and methods in applied sciences - Measures for critical infrastructure protection – Ludek Lucas, Lubos Necesal – Issue 7, Volume 5, 2011.

15. Zakon o kritičnim infrastrukturama, (Narodne novine 56/2013).

16. Odluku o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura, (Narodne novine 108/2013).

17. Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura, (Narodne novine 128/2013).

18. http://www.asadria.com/index.php/teme/kolumne/276-kriticna-infrastruktura-i-znacaj-osiguravanja-njenog-neprekidnog-djelovanja - Denis Caleta - Kritična infrastruktura i značaj osiguravanja njenog neprekidnog djelovanja, Превземено на 17.09.2015г.

19. Presidential Policy Directive -- Critical Infrastructure Security and Resilience The White House

20. Office of the Press Secretary February 12, 2013