351.824.11:327(510)
https://doi.org/10.18485/fb_bri_se.2019.ch12

Petar Stanojevic
Faculty of Security Studies, University of Belgrade

Zoran Jeftic
Faculty of Security Studies, University of Belgrade

Goran Mandic
Faculty of Security Studies, University of Belgrade

Critical Infrastructure Continuity in the Belt and Road Initiative*

Abstract

Critical infrastructure (CI) protection is considered to be an intersection between natural hazards, politics, business, technology and risks. 'One Belt, One Road' initiative develops connections between the spaces and states from Asia (China), through Africa and Europe including numerous ports, railways and roads, dams, telecommunication facilities, oil and gas pipelines, electricity network lines, powerplants and many other different enterprises. Risks connected to the facilities are both external (theorists, natural hazards, cyber-attacks etc.) and internal (technological accidents, human errors, pollution, occupational health and safety issues etc.). In order to obtain maximal benefits and return on investments, new endeavours need continuity, stability and operational excellence in their business operations. Unfortunately, disruptions can be massive and can be caused by different sources and motives. For example, one of the latest cases, which involves many players is Venezuela and its electricity supply system.

Almost all of the countries involved in 'One Belt, One Road' initiative are classified as developing countries, so their abilities and resources, when it comes to treating potential hazards, are more or less limited. At the same time, some of them are EU members, where CI protection and HSE (Health, Safety and Environment as the business function), are developed or, at least, heavily regulated. 'One Belt, One Road' initiative connects countries, infrastructure and companies and gives

* This paper is a part of the research on the project III 47029, MESTD of RS

complete benefits only if all the parts are fully operating. Since protective measures are only as strong as their weakest link, there is a need for the Comprehensive Approach development.

The Comprehensive Approach should include countries, private entities, all governmental and supranational stakeholders, private business and safety & security and science & academia organizations in CI protection. It should have a proactive and preventative, but also an improved resilience role. At the same time, protection from both external and internal hazards is needed. External protection requires a new model which includes the involvement of military power, private intelligence, police, private security and civil protection companies. On the companies' level, new enhanced HSE models and operations are needed in order to obtain synergy.

Constructive cooperation, based on common regulative environment standards, mutual trust, training, research and development, information tools, shared measures and coordinated action should be key factors in reducing the risk of endangering the security of CI and enhancing it, so as to achieve the Comprehensive Approach.

This paper deals with the need to develop the Comprehensive Approach in CI protection within the 'One Belt, One Road' initiative, and gives special attention to particular needs and possible ways of establishment. The establishment of permanent bodies, with the task to explore opportunities and options, should be the first step in enhancing cooperation. The EU model in CI protection is also of interest, in the sense of establishing a regulatory framework.

Key words:

Critical Infrastructure, Business Continuity, "One Belt and One Road" initative, Comprehensive Approach

1. INTRODUCTION

Critical Infrastructure (CI) protection is a contemporary need and paradigm. At the moment, we can see a slight difference between countries when it comes to their definition and list of critical infrastructure sectors, but a vast majority of them takes into consideration the following: energy, transportation, agriculture and food, water, public health and safety, emergency services, government, defense industry, information and telecommunications, banking and finance, environmental protection, industry/manufacturing and also science. In the case of the "Belt and Road" project, the ports, airports, railroads, highways, electric power generation and distribution, gas and oil infrastructure are of utmost importance, even though there are also numerous production-oriented developments.

All countries are aware of the CI protection importance and despite different interpretations of it, there is a group of issues linked to the lack of resources and abilities. Regulations are not similar and do not ask for the

same requirements as far as the applicability is concerned in the modern world. Apart from those differences, the regulations have serious lacks in some cases. This problem occurs most often in developing countries. A vast majority of the countries participating in the "Belt and Road" initiative belong to that very group. Contrary to them, there are also the EU members participating in the project with highly developed regulatory systems.

The infrastructure development is predominantly financed through loans or through direct investments. Minor disruptions in the establishments' work may reduce the system's performance and cause large economic losses. Developing countries are especially vulnerable and sensitive regarding potential financial gaps. The most recent example is the state of Montenegro with the ongoing public discussion about possible state bankruptcy due to a loan taken from China in order to build a highway [27]. Having in mind that expensive infrastructure projects are not immediately cost-effective, and that they do become cost-effective in the long run, additional disruptions can bring not only economic but also political problems. One of the examples is the Belgrade-Budapest railroad, which can be justified in economic terms only as a significant traffic boost, visible after a longer period of time.

The main CI problem is high dependence among the sectors. For example, if a sector, such as an energy one, is under attack, that would have consequences on all the other sectors. Interdependence among the sectors of CI should be taken into account when establishing the protective programs. It should be understood as a multilevel or domino effect. The primary task is consequently creating the secondary effect, the secondary is creating the third, etc. Eventually, many of them are involved. The actualization of asymmetric forms of endangering state and CI security should, also, not be overlooked. The latest example of Venezuela, when the electricity supply system was interrupted, had tremendous consequences for the whole society. The multilevel or domino effect always requires additional measures and resources, which cannot come from a single company (CI) and, hence, requires the engagement of external, predominantly governmental forces.

The malicious actions are not the only cause of accidents. Natural disasters can also happen together with accidents caused by gaps in business management or technology glitches.

Risk management is one of the key management roles. Owners (public or private) and managers have the task to provide business stability and continuity and to provide safe work conditions for their employees, and to protect the environment. Developing countries, characterized by weak institutions, lack of competence, financial aid, legislative rules and good economy, need to provide better public services and to improve their socio-economic conditions. These countries promote a public-private partnership,

apart from a strictly public (state) and private ownership and professional management at CI.

In order to resist the contemporary global threats and hazards and improve the security situation, an intensive level of integration and interaction between the national and supra-national security structure and the interdependence of national, regional and multilateral bodies should be reached. However, the state's role as a security entity, in international relations, is crucial and indispensable.

2. INTERNATIONALLY ACCEPTED APPROACHES AND REGULATIONS

The United States has a National Infrastructure Protection Plan from 2006 [1], where infrastructures and key resources are divided into eighteen sectors. Some of these infrastructure sectors are the following: the agriculture and food protection, treatment of drinking water, energy/power, information technology/telecommunications, transportation systems, defense industrial base, public health, banking/finance, postal/shipping and critical manufacturing. National monuments/icons, government facilities, chemical facilities, commercial facilities, hydro-electric dams, emergency services and commercial nuclear reactors, materials and waste, are key resources. The transport resources alone, which are very diverse, contain 5.000 public airports, 120.000 miles of major roads, 590.000 bridges, 2.000.000 mile of pipelines, 300 ports, and 500 major, urban and public crossings. This undoubtedly resembles the "One Belt and One Road" initiative and its magnitude.

From 2004, the European Commission (EC) has been building the "European approach" with the idea of creating a European Program for Critical Infrastructures (EPCIP) [2, 3, 4, 5, 6, and 7]. The aim is to support companies and governments in the EU as far as their security strategies are concerned. It seeks to provide an all-hazards cross-sectoral approach (www.ec.europa.eu). The regulation makes a clear distinction between Critical Infrastructures of the member countries and the European Critical Infrastructures (the infrastructure important for at least two countries). The corresponding EC Directives are key elements in the creation of the common legislative framework. EPCIP Contact Point meetings are organized in order to exchange information between the Member States of the EU (www.ec.europa.eu). The EU fund is needed in many conducted studies, in order to identify the needs of an adequate critical infrastructure protection.

Article 2 of the Directive (2008) states that the impact must be assessed in terms of cross-cutting criteria (the interdependence of various infrastructures). This refers to the European dimension the security strategies reach when critical infrastructures have essential or vital services in several countries of the EU. The current approach is that the European strategies should focus on systems instead of sectors (critical infrastructures are often too large and more complex). EPCIP is divided into four critical infrastructures, which have a European dimension, in order to optimize their protection and resilience. These sectors are the Euro control (EU Air Traffic Management Network Manager), Galileo (global satellite navigation system), the Electricity Transmission Grid and the European Gas Transmission Network. It's important to consider the latest approach (cross border or multilateral) to the most of the endeavors in the "One Belt and One Road" initiative, which are predominately international and develop the transportation systems.

One of the most interesting establishments in the EU is the Critical Infrastructure Warning Information Network (CIWIN), which gathers experts from the EU to assist the European Commission in establishing network programs which could facilitate information exchange when it comes to threats, vulnerabilities, measures and strategies [8]. One idea was to create a knowledge base, on a European level, with the best practices which would contain recommendations, what-if scenarios and guidelines.

The EU has three main strategies based on the critical infrastructure resilience, i.e. prevention, preparedness and response [2]. Prevention is aimed towards the creation of tools for risk assessment and risk management. The private sector should participate to a profound extent. Considering the fact that intelligence plays a vital role, the EU Intelligence Analysis Centre (INTCEN) is included. The strategies of preparedness and response both rely on gathering the equipment, providing adequate training, raising awareness and conducting exercises.

In terms of critical infrastructure protection measures, all countries, including the Republic of Serbia, must: a) identify CI, b) create CI maps, c) determine an information, hierarchy and content exchange network, d) train the personnel who takes part in the CI jobs and tasks, e) train the CI personnel for an event of a crisis or an emergency, f) establish liaison officers in the CI and g) develop security (protection) plans.

It should be underlined that, as far as the industrial practice is concerned, the EU has introduced an integrated approach, represented through a number of directives, among which the most important are the Integrated pollution prevention and control (IPPC) directive (Directive 2008/1/EC of 15 January 2008, concerned with integrated pollution

prevention and control) and the Council Directive 96/82/EC of 9 December 1996, on the control of major-accident hazards involving dangerous substances (also known as the Seveso II Directive) [9, 10]. Out of the few dozen other directives, ATEX and PED are maybe the most important. This set of regulations aims to reduce the probability of accidents and to improve resilience. Prevention, preparedness, response, documented approach, public and expert verification involvement are all in the basis of this model. Ownership does not hold special significance; every party should execute its legal obligations. The above-mentioned directives have expert and regulatory bodies all over the EU, where at least all member states participate. All risks should be covered by documented protection and emergency plans.

3. THE MILITARY, POLICE, PRIVATE INTELLIGENCE, CIVIL AND PRIVATE PROTECTION AND THE CRITICAL INFRASTRUCTURE PROTECTION

By protecting the critical infrastructure, the economic potential is protected as well. The safety and security of CI is the responsibility of the company owner, prescribed by the public laws and driven by the real need not to allow unnecessary losses. Company's safety and security structures are focused on specific protection tasks and develop specific know-how, abilities and resources. Since critical infrastructures can be threatened, by more or less common threats like terrorist attacks, technological failures and natural disasters, the extra value of private security lies in its specialization and targeting sector, more precisely in its know-how and, consequently, specific market segments [11] which would decrease costs for operating companies, due to a higher specialization and better resource use.

In most European countries, critical infrastructure protection is understood as an important task for private security. Subsequently, the protection of critical infrastructures is generally seen [12] as a responsibility which should be organized between the public and private sector. Companies and their personnel must obtain a certification from government authorities and go through a training program if they want to provide private security [13, 14, and 15].

In order to create an effective partnership with different companies, the private security sector should be included from the beginning, i.e. in the design itself (the conceptualization of approaches) and the operation

of critical infrastructure protection [13]. The fact that the private security industry consists of various corporations should not be taken lightly, as the private sector has high competences in risk assessment, security threats identification and has developed specific training for this sector.

Intelligence services play a vital role in planning and executing security strategies regarding the CI. The CI protection is an important task for intelligence services, as they provide advice and all sorts of analysis regarding related threats (e.g. terrorism, treason and also organized crime).

Contemporary military services perform the following five basic tasks [16]:

1. Protecting the state's independence, sovereignty, territorial integrity, and, in the broader context, its citizens;
2. Preserving peace in international relations or peace enforcement;
3. Providing humanitarian assistance in case of natural disasters;
4. Fulfilling the tasks of Homeland Security and
5. Participating in building the nation.

Generally speaking, these are internal and external tasks, or as some would call them, non-traditional and traditional tasks. The Geneva Centre for the Democratic Control of Armed Forces (DCAF), conducted a research in 2012, in 15 consolidated Western democracies[1], on internal roles of the Armed Forces. The results showed that 20 different roles were identified, and 10 of them can be included in the broader category of law-enforcement-related tasks. Location and personnel security is among those tasks. Only Luxemburg, Spain and Germany don't have this task assigned to its military. The conclusion was that each country is involved in providing aid with military help, in case of natural disasters. It is truly important to underline that the protection of the CI is not an exclusive task of the military forces. Armed forces are, in fact, often considered as a last resort, after a request made by the civil authorities [17].

In Eastern Europe[2] civil defense capacities are seriously disabled due to the lack of financial support and the change of the strategic orientation. The capacity of military forces is also significantly lower, for the same two reasons. In many countries, like Serbia, the police overtook the responsibility regarding all emergency situations, including fires. The police and new established government departments are struggling to

---

1 Austria, Belgium, Denmark, Finland, France, Germany, Italy, Luxemburg, the Netherlands, Norway, Spain, Sweden and the United Kingdom, along with the United State and Canada.

2 Almost all Eastern European countries take part in the 16+ project and the "Belt and Road" initiative lead by China.

reach required capacities and competences. Switching responsibility from one governmental department to another and attributing them different roles caused dangerous misunderstandings and reduced the already disproportionate capacities. At the same time, the probability and quantity of possible accidents within the CI has not decreased, but, on the contrary, has increased due to new infrastructure and industrial developments.

New threats, like Cyber security, require new kinds of highly sophisticated and trained resources. All governmental services and most of the companies lack such capacities.

Everything mentioned previously leads to a logical conclusion that all available forces should be included in dealing with accidents related to CI. The military force is the only government service which could gain a surplus of the capacities. The reason behind that is, for the most part, the fact that most of the military forces have been preparing for a large-scale war during the Cold War era. The military force is traditionally a source of highly trained and motivated personnel as well. New tasks which had been given to the military organization, require a new organization model which is easily adaptable for all kinds of possible tasks, like the one presented in [18].

It is worth mentioning that generally known roles of military forces, as far as the new age is concerned, like defeating the enemies, maintaining peace and helping the local and global hazard operations, are usually opposed to the military tactical capabilities design, organization and technology use, if uncovered as joint requirements. This urges the defense planners, especially for land and joint forces, to leave behind the tactical twentieth century military organizations, and to recognize a new approach in military engagement.

Sharing and exploiting internationally crucial resources and infrastructures, within the homeland area, have colossal international risks, especially in the form of asymmetric or terrorist warfare actions. The question of military capacity implementation in the prevention process and potential asymmetric threatening situations should be considered as national and international military defense tasks. At this very moment, the majority of military forces belonging to small countries do not have appropriate capacity, technologies or organization flexibility, so as to be included effectively in different missions, along with any civil emergencies or infrastructure protection risk operations.

Low budgets burden the military, other governmental agencies and institutions, and ultimately ask the national economies to develop joint, civil and military emergency capacities so as to share responsibility when it comes to the defense, peace and security protection in risk variable tasks.

This refers to the appropriate participation of military forces, joined together with other civil (armed) and not armed forces, such as civil protection, gendarmerie, police, Special Forces, private homeland or international security units.

Encompassing abilities of civil governmental and non-governmental agencies and participants in joint military formations, based on various situational bases, represent beneficial and prominent practices in a large-scale homeland hazard disaster and can, also, be expected in an international mitigation or peace keeping missions. Also, civil hazards can help integrate required resources, in comprehensively planned operations for the military forces and can be a part of modular constituents of the battle teams.

Military organizations, like NATO, have the aim to protect energy supply lines. NATO's role in energy security was first defined in 2008 at the Bucharest Summit and has only been strengthened since [26].

According to [19]: "In the Persian Gulf area and Israel, concepts have been developed which, along with the responsibility of companies themselves, offer cooperation to the government in the interest of security. Generally speaking, the Police and the Armed Forces can be hired to protect gas pipelines. In those instances when the military power or the police cannot take care of the gas pipelines security, for whatever reason, private companies could be put to work. Companies, i.e. owners of gas pipelines, should be responsible to their partners, customers and investors. Some of the tasks private security companies have are to lead strategic consultations, to assess existing risks and to defend those facilities and employees.

The Baku – Tbilisi – Ceyhan oil pipeline security system may serve as an excellent example of a modern approach to pipeline security. The oil pipeline will be in its entire length situated in the ground; there will be only terminals and compressor stations on the surface. Apart from that, additional security measures will be taken so as to protect the installation from theft and any damage. The oil pipeline will be fully covered by the security personnel, even cavalry will be used, while modern techniques and technologies will also be applied (such as optical and similar cables).

According to the "Gazprom" standards, compressor stations should be lined with a two-meter high metal fence on the top of which there should be three barbed wires on both sides. It should be 2 meters and 50 cm tall overall. In order to protect from or prevent any unlawful interference when it comes to compressor station functioning, as linear pipeline management, a security service must be hired. Objective judgment, group discussions and following commands of the security service will provide safety to the security compressor stations, along with the linear parts of the gas pipeline. The personnel of the security service should be trained in a special way,

licensed to do that sort of job, and most importantly, they should have adequate equipment. Compressor stations should be secured round the clock, by armed personnel who is set up on guard posts, and appropriate equipment for signalization should be set up (alarms, cameras, etc.)."

So as to protect the "South Stream" gas pipeline, it was planned to engage the Sector for Emergency Situations of Serbia's Ministry of Interior, Center for Emergency Situations from Niš and Serbian Armed Forces.

Some examples of non-traditional military engagement are: a) in 2008, when around 1.000 soldiers were sent to guard high-profile public places, such as train stations and St Peter's Cathedral in Rome, and b) when more than 3.000 Italian military officers were deployed to support police patrols in their fight against crime in 2008 [17].

All of the above mentioned examples justify the need to employ all source resources in CI protection. This is much more important when it comes to complex endeavors like the „One Belt one Road" initiative, where participating countries do not have a plethora of resources and competences.

4. NEW DIRECTIONS IN CRITICAL INFRASTRUCTURE PROTECTION: THE INTRODUCTION OF RESILIENCE

In 2009, the NIAC released a study [20] called 'Critical Infrastructure Partnership Strategic Assessment Study', which highlighted some interesting results. It focused on the importance of resilience, for the public and private sector, when it came to creating their risk assessment strategies. Infrastructure resilience is 'the ability to reduce the magnitude, the impact and/or the duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends on its ability to anticipate, absorb, adapt to and/or rapidly recover from a potentially disruptive occurrence'. Risk management should, therefore, focus on the resilience of a critical infrastructure.

Three features alone characterize critical infrastructure resilience [20]. They are robustness (the ability to maintain operations and functions in the middle of a crisis), resourcefulness (the ability to prepare for, respond to and manage a crisis or disruption as it unfolds) and rapid recovery (the ability to return to and/or reconstitute normal operations as quickly and as efficiently as possible after a disruption).

The above-mentioned approach is what the developing countries should develop, in order to improve the cost and effectiveness of their CI protection systems.

5. CORPORATE SAFETY AND SECURITY MANAGEMENT (HSSE MANAGEMENT)

Corporate Safety and Security management systems (also known as Health Safety Security and Environment – HSSE) have as their main goal to systematically identify failures in technological and management activities and monitor management interventions, so as to control risk in companies. Their aim is to see the wider picture, to show relative safety priorities and manage effectiveness of remedial actions.

The HSSE sets out a company's safety and security policy[3] as an integral part of its overall business. Each company should implement a system which works best for them – there is no 'one-size-fits-all' system. Ultimately, HSSE becomes woven into the fabric of the organization and becomes part of its culture. Many of the leading companies have a similar HSSE structure, policies, or techniques based on the management standards like ISO 9001, ISO 14001, ISO 31000, ISO 45001 etc. and an integrated system of safety standards and directives in the EU.

There are numerous elements of safety in a security management system. The main elements could be classified in the following way [21]:

"1. A safety and security policy which would underline the commitment of the organization which is responsible for safety and security;
2. A structure which would assure the commitment to safety and security would be implemented;
3. A training which would equip personnel with adequate knowledge, so as to work safely and without security risks to any third parties or other personnel;
4. In-house security and safety rules which would provide instructions for achieving safety and would manage security objectives;
5. A program of inspection which would identify hazardous conditions and rectify any such conditions at regular intervals or when needed;

[3] The term 'policy', refers to general intentions, approaches and objectives of an organization, along with the criteria and principles which make up the actions and responses. An effective security and safety policy would set a clear direction for an organisation to follow. It would contribute to all aspects of business performance, as a part of an apparent commitment to continuous improvement.

6. A program which would identify hazardous exposure or risk such exposure has for the workers and any third parties and would provide suitable protective equipment, as the last resort, where engineering control methods are not as feasible;
7. An investigation of any accident or incident which would discover the cause and would develop prompt arrangements in order to prevent recurrence;
8. Emergency preparedness which would develop, communicate and follow through with plans which are prescribing effective management of emergency situations;
9. Evaluation, selection and control of sub-contractors which would ensure that sub-contractors are fully aware of their safety obligations and are in fact meeting them;
10. Safety committees;
11. An evaluation of hazards related to work process or potential hazards, and development of safety and security procedures;
12. A promotion, development and maintenance of safety and security awareness;
13. A program for accident control and hazard elimination, especially when it comes to the personnel's and third parties' exposure to any risk;
14. A program which would protect workers from occupational health hazards."

Companies' HSSE systems are an inseparable part of the overall CI safety and security system. If this system functions in the best possible manner, it then decreases possibilities and consequences of the unwanted events. By doing so, it relives a significant part of an always scarce state, which has created the resources and costs. That is exactly why improvements on the company level have to be an inseparable part of any CI protection system/organization.

5. A COMPREHENSIVE APPROACH TO THE PROTECTION OF THE "ONE BELT AND ONE ROAD" CI

The protection of the CI is itself a very complex and demanding activity. Having in mind the abundance of critical infrastructures, especially in such large-scale projects as the „Belt and Road" initiative, significant challenges in the CI protection can appear, such as [22]:

- The creation of complex critical infrastructure sectors, because it would be impossible to protect an entire critical infrastructure and its components, for example, in the transportation sector it would be almost impossible to protect numerous kilometer-long communication lines, a large number of airports, sea ports, numerous bridges and similar structures.
- The lack of supervision and responsibility in a sector where several public and private institutions work together.
- Not sharing enough information between institutions which are working together, which would lead to a new vulnerability and impact the response-efficiency when it comes to the CI protection.
- The creation of complex knowledge which should include a large quantity of special skills.
- The creation of a strong interdependence of individual sectors of the CI and between its sectors.
- The creation of flawed tools for the CI and its vulnerability analysis.
- The occurrence of asymmetric conflicts, as an especially efficient form which could affect the CI vulnerability.

There is also a misunderstanding between the public and private sector when it comes to the perception of vulnerability and efficiency, as the main aim of the private one is efficiency conditioned by market activity, while vulnerability is only considered if the situation compels them to it.

Additional problems lie in a) the rapid change in incident sources or nature which would impede with investigations regarding creating counter-measures, b) a strong political influence, as incidents can affect the domestic and international political environment, c) an unpredictable environment as not all causes or consequences can be foreseen. Therefore, CI protection must be examined to such an extent that it can have a multidisciplinary scope. The changing landscape of prevention of and protection from accidents would require a scientific standpoint which would implement segments from several disciplines, i.e. the science of resolving conflicts, defense studies, economy, technology, governance, law, sociology, criminology, etc.

The asymmetric nature of modern day risks and threats for the CI asks for undisputed and conditional comprehensive security measures. Having in mind the complex character of the endeavors and participants included in the 'One Belt, One Road' initiative, the aim of the approach can also be defined as creating procedures and practices for the purpose of strengthening the resilience of the CI and its readiness for prevention,

mitigation, response and recovery (similar to the Canadian National Strategy for the CI [23]).

The achievement of the goal can be reached only through a Comprehensive approach which should include at least:

- The identification of national, regional or sectoral CIs which would be connected to the sustainable functioning of the "Belt and Road" initiative and its auxiliary structures,
- The identification of national, regional or sectoral risks and hazards for the CI;
- The examination of the risks, hazards or gaps in protection plans for the CI,
- Establishing the stakeholders and interested parties,
- Building partnerships among the stakeholders,
- Implementing an all-hazards risk management approach,
- Establishing the minimum criteria when it comes to joint regulations and resources,
- Developing the business continuity practice,
- Establishing the coordination bodies,
- Improving and establishing the academic and scientific cooperation and its capacities,
- Developing procedures which would address intentional and accidental incidents, both within the homeland area and internationally,
- Training and developing the resources together,
- Enabling information sharing with the stakeholders in due time,
- Managing all the planning and documentation in an urgent manner,
- Establishing appropriate systems for early warning,
- Enhancing communication about risk among the states, companies, citizens and the general public,
- Obtaining greater commitment from governmental bodies and participants in regards to incident prevention and management,
- Monitoring progress,
- Constantly analyzing and improving the approach.

The approach should cover all accidents, despite the nature of their causes: 1) natural disasters, 2) errors (technical failure or human error), and 3) organized violence activities (terrorism, crime, war) etc. [24].

All the improvements in conducting the approach would be seen in higher rates of competitiveness, productivity and cost-effectiveness, but also higher social responsibility when it comes to the operation of the CI.

Responsibility for national and general security is, above all else, in the hands of each nation-state. States are obliged to provide a systematic

framework when it comes to responding to various types of crisis in the field of critical infrastructure. A large number of and many types of CI indicate that all levels of government should take part in the CI protection. Companies should use all their required resources as well, as accident occurrence is, luckily, not a permanent and every day kind of situation, so it would not be rational to establish and maintain preventive measures and resources separately. Merging resources, sharing information and knowledge are the best and the most sustainable ways to use the resources in terms of effectiveness and cost. That's precisely why the CI protection within the "Belt and Road" initiative must rely on cooperation between the involved states, on the national and subnational level, on the PPP, private entities, resources and information sharing.

6. ESTABLISHING A COMPREHENSIVE APPROACH

In order to secure a sustainable, safe and cost/effective CI protection system, it should have the following features:

- shared values,
- understanding of the situation and common aims,
- coordination mechanisms,
- an information sharing mechanism,
- structures for development and planning,
- structures for monitoring and detecting early warning signs,
- Pre-established relationships and multilateral understanding through common education, values, training, analysis and response planning in case of potential CI crisis.

Traditionally limited by time and put in the framework of the well-known "modus operandi", people often forget about the wide range of possibilities when cooperation is achieved. Infrastructure and regulations often represent a serious obstacle as well.

Coordination mechanisms and bodies are necessary in order to erase any gaps in system functioning, deal with the lack of resources or knowledge, or even to decrease the respond time. Those coordination bodies have to be permanent. Establishing permanent bodies, which would have the goal to explore opportunities and options, would be the first step in improving cooperation and resolving issues in:

- Mitigating different issues among countries and finding common ground,
- Taking advantage of synergies,

- Determining the cooperation policy when it comes to two options a) whether to be a part of a highly structured organization like the EU or b) to have "freedom" and a less structured coordination mechanism.
- Resolving the first steps in determining the stakeholders, the CI, sharing information and knowledge etc.

A good example to follow is the one from 2016, when China and the Arab countries signed the "China's Arab Policy Paper" [25]. This mentioned document established the basic principles of cooperation and coordination on multilateral bases.

By using this or a similar approach countries can:

- gradually 'expand' their development model and avoid sharp changes,
- choose a dynamic and efficient approach and position themselves in transition for long-term survival,
- find balance between the wait-and-watch strategy and an active reaction,
- mutually develop strategies to be flexible and able to evolve quickly in response to anticipated changes,
- Set up goals and priorities when it comes to the investment in, operation, research or development of future technologies.

7. CONCLUSION

Critical infrastructure (CI) protection is in the meeting point between natural hazards, politics, business, technology and risks. The 'One Belt, One Road' initiative should develop connections between the states from Asia (China) through Africa, all the way to Europe, including numerous ports, railways and roads, dams, telecommunication facilities, oil and gas pipelines, electricity network lines, power plants and many other different enterprises. Risks connected to the facilities can be both external (terrorists, natural hazards, cyber-attacks etc.) and internal (technological accidents, human errors, pollution, occupational health and safety issues etc.). In order to gain maximum benefits, new endeavors need continuity, stability and excellence in their business operations. Unfortunately, disruptions can be massive and can come from different sources and have different motives. Venezuela and its electricity supply system are just the latest example which involved many participants.

Almost all of the countries which are involved in the 'One Belt, One Road' initiative are classified as developing countries, so their abilities

and resources when it comes to treating potential hazards are more or less limited. At the same time, some of them are EU members, where CI protection and the HSE (Health, Safety and Environment as the business function) are either developed or heavily regulated. The 'One Belt, One Road' initiative aims to connect countries, infrastructures and companies, and to offer various benefits, if all the parts are fully operational. Since protective measures are as strong as their weakest link, a Comprehensive Approach should be developed.

A Comprehensive Approach has to include countries, private entities, all governmental and supranational stakeholders, private businesses, safety and security, scientific and academic organizations in CI protection. It should have a proactive and preventive, but also an improved resilience role. At the same time, protection from both external and internal hazards is needed. External protection needs a new model of joint involvement of military power, intelligence, police, private security and civil protection companies. On the company level, a new and enhanced HSSE model and new operations are needed in order to reach synergy and rationalize the use of public resources.

In order to carry out a Comprehensive Approach, constructive cooperation based on common regulative environment, standards, mutual trust, training, research and development, information, tools and measures sharing, along with coordinated action, should all be key factors in reducing the risk of and improving the security of the CI.

Development of a Comprehensive Approach in CI protection inside the 'One Belt, One Road' initiative is an obvious need and can significantly improve the abilities of all of the involved countries in CI protection. Establishing permanent bodies which have the goal to explore opportunities and options should just be the first step in improving cooperation. The EU model in CI protection is also of utmost importance when it comes to establishing a regulatory framework.

China and other involved countries should have an interest in the protection of the "Belt and Road" initiative and its relation to CI, since their goods would be moved through the developed infrastructure and improve the security of energy supply, increase and speed up the communication channels. Better CI protection would secure economic efficiency as far as investments are concerned and it would cut down on unnecessary losses.

BIBLIOGRAPHY

1. United States' National Infrastructure Protection Plan 2006.
2. European Commission Staff Working Document. A new approach to the European Programme for Critical Infrastructure Protection: making European critical infrastructures more secure. Brussels. 28/08/2013.
3. European Commission Staff Working Document. On the review of the European Programme for Critical Infrastructures Protection (EPCIP). Brussels. 22/06/2012.
4. European Commission, Critical Infrastructures, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm, 20/06/2013.
5. European Union Council Directive. 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. 23/12/2008.
6. European Union Counter-Terrorism Strategy, Brussels 30th November 2005, http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf, 20/06/2013, 16h55.
7. European Union (2007–2013). Specific programme: prevention, preparedness and consequence management of terrorism (2007-2013), http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33262_en.htm, 20/06/2013, 17h15.
8. Van Nevel Hannes (2010). De bescherming van kritieke infrastructuren: een publieke of overheidstaak? Een casestudy in de Zeebrugse Haven. Master Dissertation. Ghent University.
9. Directive 2008/1/EC of 15 January 2008 concerning integrated pollution prevention and control – IPPC
10. Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances (Seveso II Directive).
11. Müller, J. (2012). Schutz kritischer Infrastrukturen. In: Stober, R., Olschok, H., Gundel, S. & Buhl, M. (eds.). Managementhandbuch: Sicherheitswirtschaft und Unternehmenssicherheit. Stuttgart: Richard Boorberg Verlag, 366–375.
12. Davidovic, D. Kesetovic, Z. & Pavicevic, O. (2012). National critical infrastructure protection in Serbia: the role of private security. Journal of Physical Security 6(1). 59–72.
13. CoESS – APROSER (2013). The socio-economic value of private security services in Europe. Fourth White Paper on Private Security. Wemmel: CoESS.

14. CoESS (2012a). Critical infrastructure security and protection: the public-private opportunity. White Paper and guidelines by CoESS and its working committee. Wemmel: CoESS.
15. CoESS (2012b). Critical infrastructure private guarding company requirements checklist. Wemmel: CoESS.
16. Žugić B.R. (2007), Civilna kontrola vojske, VIZ, Beograd, p.21
17. Schnabel A. and M. Krupanski (2012), Mapping Evolving Internal Roles of the Armed Forces, DCAF, SSR Paper 7
18. Milinović M. Jeftic Z. (2013), Challenges of National Defense in International State and Private Corporative Management of Infrastructure Protection, National Critical Infrastructure Protection-Regional Perspective, International Scientific Conference, Belgrade: University of Belgrade- Faculty of Security Studies and Institute for Corporative Security Studies Ljubljana, p. 119–131.
19. Mitar Kovač, Nenad Dimitrijević, Brankica Potkonjak-Lukić; Security aspects of the "South stream" as a critical infrastructure element of the Republic of Serbia, Challenges of National Defence in International State and Private Corporative Management of Infrastructure Protection, National Critical Infrastructure Protection-Regional Perspective, International Scientific Conference, Belgrade: University of Belgrade- Faculty of Security Studies and Institute for Corporative Security Studies Ljubljana
20. National Infrastructure Advisory Council (2009). Critical Infrastructure Resilience. Research Report. USA.
21. Hong Kong Labour Department, Occupational Safety and Health Branch. (April, 2002). Code of Practice on Safety Management First ed. Retrieved from http://www.info.gov.hk/labour/public/index.htm
22. Prezelj, I., Konceptualna opredelitev kritične infrastrukture, FDV, Ljubljana, 2008. str. 13.
23. Canadian government, (2009), National Strategy for Critical Infrastructure, Her Majesty the Queening Right of Canada.
24. Federal Republic of Germany, Federal Ministry of the Interior, (2009), National Strategy for Critical Infrastructure Protection (CIP Strategy).
25. "China's Arab Policy Paper," 2016; https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1331683.shtml
26. Bucharest Summit Declaration, https://www.nato.int/cps/us/natohq/official_texts_8443.htm
27. https://www.blic.rs/biznis/vesti/opasan-projekat-crne-gore-ako-kini-ne-vrate-kredit-za-autoput-beograd-bar-ostaju-bez/b8pjkxz?utm_source=blic_kat_kultura_sidebar&utm_medium=sidebar_najnovije_info