THE CONCEPT OF RESILIENCE AND PROTECTION OF CRYTICAL INFRASTRUCTURE AGAINST NATURAL AND MAN-MADE DISASTERS IN REPUBLIC OF MACEDONIA

By
Metodi Hadji-Janev and Vlatko Jovanovski

Abstract:

With this paper we analyze the concept of resilience in context of protection of critical infrastructure in Republic of Macedonia. Our starting hypothesis is that in this moment there is absence of national consensus of what resilience means which reflects negatively on actual protection of critical infrastructure against all types of hazards in Republic of Macedonia. In the first part of the paper we identify the concept of resilience as seen by different branches of science and we examine that in Macedonian context. In the second part we analyze how the concept of critical infrastructure protection against all types of hazards is in placed in Macedonia and what does it mean to have unified/centralized approach towards this issue. With the third part of the paper we question the resilience of the system for disaster/crisis management itself if there is no coherent state strategy towards protection of critical infrastructure. We end the paper with possible recommendations' for the future.

Key words: resilience, critical infrastructure, protection, disaster risk reduction

Introduction

At the last UN Special Thematic Session on Water and Disasters held in New York on the 13th of March, Japanese Crown Prince Nahurito used the term resilience in context of creating synergies of the old and the new approaches towards disaster risk reduction:
"If we combine available means such as early warning systems, education and governance with lessons from history, we can create a society more resilient to disasters (Hasan, 2013).
Misha Hussain from the Guardian identifies the term resilience as the newest sexiest word in international development. Having in mind that there is no universally accepted definition of the word resilience he is rightfully asking the question is it just a new buzz word or a development solution (The Guardian, 2013).
With the Sendai Report from 2012 the World Bank commits itself for the years to come to better understand and design long term disaster resilience in the most vulnerable areas on Earth. Additionally in this particular Report we can also see some other definitions currently used for the concept of resilience:
"The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner" – United Nations International Strategy for Disaster Reduction.

"The ability of a social or ecological system to absorb disturbances while retaining the same basic structure and ways of functioning, the capacity for self-organization, and the capacity to adapt to stress and change" – Intergovernmental Panel for Climate Change.
"The ability of countries, communities and households to manage change, by maintaining or transforming living standards in the face of shocks or stresses - such as earthquakes, drought or violent conflict - without compromising their long-term prospects." – Department for International Development, United Kingdom".
So, crowned princes, journalists, governments and international organizations are using the word resilience in their own search for better solutions in reducing risks from natural and manmade disasters. But what does it mean exactly? Can or should the world unify the meaning of resilience? This paper represents our joint contribution to this debate this time connected with the issue of protection of critical infrastructure in Republic of Macedonia. In the first chapter of the article we examine the term resilience, its origins and definitions. By choosing one of them and translating it in Macedonian context we show in practice that resilience can be a catchy phrase but it can also mean something more, driver of change. In the second chapter we introduce the term critical infrastructure in relation to disaster risk reduction and crisis management. With this chapter we are aiming to stress the importance of the interconnected relations between resilience and critical infrastructure protection. In the third chapter we go in depth of how is actually critical infrastructure protection organized in Republic of Macedonia, by identifying the legal framework and the variety of different authorities dealing with this issue. With the fourth chapter we are identifying gaps in the area of managing the process of critical infrastructure protection in Macedonia and we identify possible elements of that process that need to be improved. Our concrete proposals for improvement are given in the final chapter five.
The method that is used during writing this article is a combination of policy analysis and literature review.

1. Understanding resilience

The word resilience comes from Latin *resilīre* with meaning to spring back. Usually it is used as an adjective describing someone's (system or individual) characteristic of returning to the original form or position after being bent, compressed, or stretched or recovering readily from illness, depression, adversity, or the like. It entered the world of psychology with Victor Frankls' "Men's searching for meaning" in 1946 (Korstanje, 2011). Victor Frankl was a psychologist, survivor of the Nazi camps, and spent his entire professional life exploring the ability of the human brain to withstand hard times and survive by giving personal meaning to the events. Even when he was in the concentration camp he was curious in finding the reason why do some people survive and others don't. He explains that is not due to pure physical health, because the conditions in the camps were horrible but due to the will of the soul to survive by projection of a goal and a reason to live. For some of the fellow prisoners' survivors he found out that the mental projections are their families and the dream of reunion. For him personally it was the idea to become professor in psychology and to teach students about the resilience of human nature in

stress situations. Surveying the science campus of ecology the term resilience is used in correlation of stability and ability of a system to withstand a disturbance and adapt to changed circumstances (Gunderson, 2000). Civil engineers understand it as a capacity of an element or a system to face and absorb the impacts produced by a stressing factor by rapidly reestablishing balance (Salat and Bourdic,2012).

If I would search for one element in the above mentioned definitions that unites all of them, it would definitely have to do something with "change management". There has to be a change caused by external or internal factors and that change needs to be managed in order the system to preserve its core functions. Accordingly, psychology recognizes the stress factor from the outside environment and by successful management of the changes that are caused we judge if a system is resilient or not. Civil engineers are measuring the level of endurance of system from the outside pressures up to the breaking point in order to manage those circumstances so that the system prevails. Ecologists are adapting the system to the new conditions and in that sense adaptation equals conducting techniques for change management. So the common denominator for various resilience definitions would be change management.

In order to narrow down my hypothesis I will focus my attention on resilience to natural and manmade disasters and the changes that need to be managed caused by these events. If we understand disaster management phases as a continuum process, showed in Figure 1, we can easily relate prevention, mitigation, preparedness, response and recovery with the process of withstanding, absorbing, adapting to the new environment and bouncing back, all of them core elements of resilience.

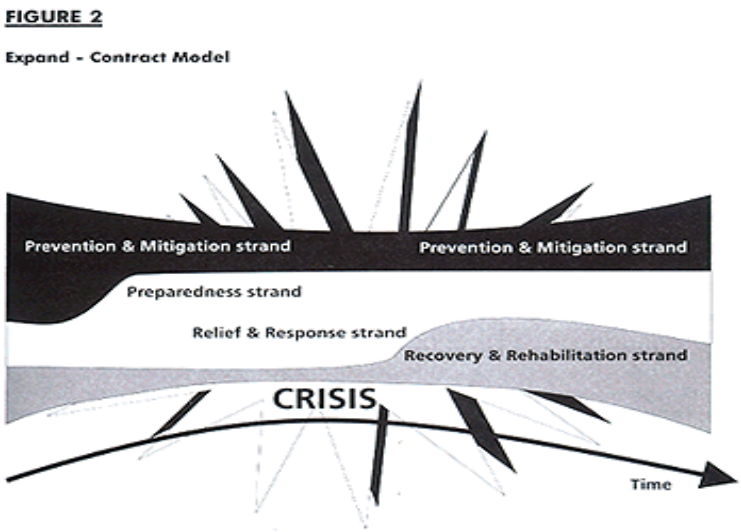

Figure 1. Disaster management phases
Source: Green paper of disaster management, available at http://www.polity.org.za/polity/govdocs/green_papers/disaster/gpdm2-3.html

Having said this there are two strands that can be noticed in disaster management policies when we speak about resilience. The first one is called engineered resilience and is focused mainly on the time that is needed for a system to bounce back from an external shock. In that way we judge

systems as resilient to disasters if the system spends less time to recover from the event. This approach has its foundation in the understanding of systems as highly organized entities with complicated parts but with predicted relations. If we understood the parts of the system and if we enforce the appropriate action we will receive an expected outcome. One of the traps that are hidden in this approach is narrowing down the focus on the trigger event and advice for structural measures only to deter external shocks. By focusing only on the speed of "bouncing back" or "normalization" we might replicate the same structures that caused the disaster in the first place. Restoring normal conditions of life after a disturbance (natural disaster) implies the question what is normal and normal according to whom?

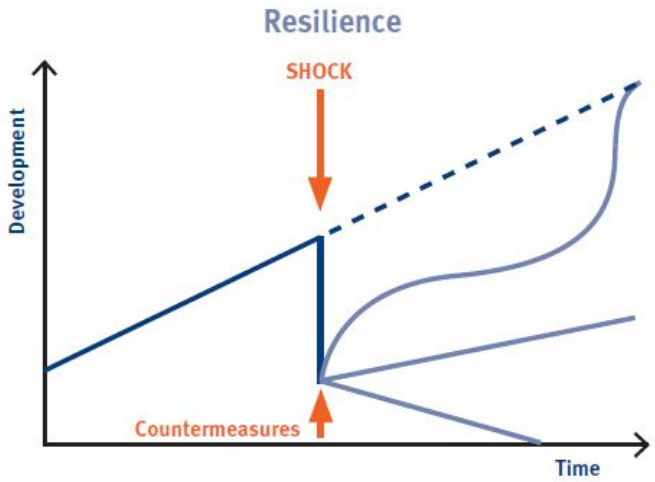

Figure 2. Impacts of shocks and recovery
Source: modified from Conway at al.,2010

Figure 2 represents how shocks (disasters) might influence on our social systems and affect the level of development. The thick vertical line will go down proportionally to the vulnerability of the system and in that way it might give us a rough picture of the level of resilience of the system. After the shock the recovery process might go up again with the same line and the system will bounce back in very short period of time but it will create the same vulnerabilities that caused the disaster in the first place. Additionally the author of the model is giving us three other options for the recovery process to continue. The first one is never to achieve the same level of development and the other two are slowly progressing in what we call "building back better". These two lines of the graph are connected with the second strand in disaster management towards understanding of resilience. It is a combination of preparedness thinking and complexity theories. (add reference) calls it evolutionary resilience. It means that systems change due to external shocks (disasters) and trough internal evolutionary path. According to (add reference) when a system achieves maturity the level of resilience is at its lowest level leading to change that will open a window of opportunity for another loop of growing and maturity. The key of this strand is to actually manage the process of change that inevitably happens to a system. Therefore resilience should be understood as a proactive approach towards

disaster management and in all of its phases (prevention, mitigation, preparedness, response and recovery). Having said this resilience should be seen more as a constant process of creating safer communities rather than an outcome that we need to measure. Finally bouncing back as one of the catchy phrases explaining resilience should be replaced with bouncing forward.

We can easily explain this with the case of Macedonia and our national efforts in disaster risk reduction. Macedonian system for disaster management is far from being perfect. We have unique design in the world where two national institutions are claiming the right to lead this process within the country. The first one is Protection and Rescue Directorate which has operational capacities for first response in case of natural and manmade disasters, jurisdiction in preparedness planning, prevention and mitigation activities. The second one, Crisis Management Center, coordinates all the actors in order to prevent possible crisis to happen (caused not only by natural and manmade disasters but also by criminal activities, acts of terrorism, civil unrests etc.), to coordinate the response of the state if a crisis is declared by the Government and in normal times to manage the national early warning system and the upcoming establishment of the E-112 number. In the mean time almost every year in spring time we have flesh floods and during summer time wild fires. These small scale disasters that we are experiencing almost on yearly basis are extremely costly for our national economy and they did took few human lives which makes them even more serious. In summer of 2012 we've lost four lives due to the wild fires and this year one man was drowned in the floods. Despite this the system for disaster management persists to be rigid and changes are few and usually reactive rather than proactive. I found it very hard to explain how it is possible that today in 2013 in Macedonia with all the technology that the national hydro-meteorological service possesses, with vast coverage of wireless and communication network across the country, with free media existing and two institutions responsible for disaster management in place, there are testimonies of the flood survivors saying: "We woke up this morning and everything around us was flooded". It is rightfully to ask what happens with the early warning system and where were the risk assessments and the contingency plans of the municipalities and the state for these types of scenarios. The main dilemma addressed with this article is have we proven as resilient in this last case with the flesh floods or not? Using the engineering approach toward resilience the answer will be YES. The system experienced external shock, the Government and the municipalities reacted upon it, mechanisms for damage compensation were activated, we have lost only one live and in couple of days the system restored its normal functions. On the other hand if we follow up the approach towards resilience as change management the answer in this particular case will be NO. We have bounced back to our old vulnerabilities and now we are waiting for the new season to come and repeat the same mistakes. There is no media attention in the moment, there is no public pressure and nobody is asking for responsibility of the absence of early warning systems and risk communication in Macedonia. There is no progression in formulating detailed risk assessment and develop better contingency plans and therefore no management of change has happened. We are back in the old days when disasters were explained only as acts of God and we are helpless to do anything about it.

This recent example, among many other, raises the question whether or not Macedonia has appropriate strategy of how to bounce forward, i.e. (effectively prevent, mitigate, respond adequately with appropriate preparedness and recover). In other words do we have appropriate approach in protecting what is critical or at least what so far has proven to be critical in order to boost these infrastructures resilience or not?
The reason for such question also comes from international experience where many countries recently have increased focus on the concept of resilience and all hazard protection. Macedonian concept is similar to these countries' experience. Nonetheless in applying strategies for comprehensive protection focused on all hazard approach and resilience these countries have identified critical infrastructures to their national security. Macedonia so far has done little in such identification. Thus before we address the issue of protection critical infrastructure in Macedonian as a part of the "all hazards" approach under current disaster risk reduction concept and crisis management we will briefly explain the logic behind this approach.

2. Linking resilience and critical infrastructure protection

Critical infrastructure protection (CIP) is currently seen as an essential part of national security in numerous countries around the world. Center for Security Studies from Zurich in its two focal reports for 2008 and 2009 on CIP have identified several trends in this area (Crisis and Risk Network Report, 2008 and 2009).

First, many countries pay increasing attention to the concepts of resilience and all-hazard Approaches;
Second, this has direct implications for how CIP is organized: A move towards the centralization of responsibility in this policy domain can be observed;
Third, there is continued or even growing attention to the cyber-dimension of the issue, linked to the growing awareness that the globally connected information and communication technologies have become a particularly vulnerable part of every country's national infrastructures (often also discussed under the heading of "cyberwar"); (Crisis and Risk Network Report, 2008, p.2)
Fourth, energy infrastructure protection: expanding governance and international cooperation and
Fifth, public-private partnerships: new relationships and challenges, (Crisis and Risk Network Report, 2009, p.5).

Governments that follow this approach believe that ability of one's system to withstand, absorb, adapt to the new situation and to bounce back would be best achieve through identified critical infrastructures that need to be protected. As a result broad range of political and administrative initiatives and efforts to improve the security of these infrastructures are underway in the US, in Europe as well in other parts of the world.

Three other reasons also urge countries that apply comprehensive all hazard approach and resilience in their national security strategies to identify critical infrastructures that need protection. First it is more practical (for the operational level). Second technical reason (i.e. achieving necessary standardization) and finally, financial reasons (it is les costly). (Crisis and Risk Network Report, 2008, p.6)

International trends and experience in this area also show that in general countries are using two models of prioritization (i.e. identification of critical infrastructure). First model, countries distinguish between critical infrastructures that deserve a greater level of attention. Second, countries identify vital points within a critical infrastructure.

The benefit of applying "all-hazards" approach is that it enables the country to develop comprehensive protection regardless of the threat. The main focus here is on the system's capability to respond to a whole spectrum of unanticipated events. To achieve such capacities all stakeholders (public and private) need to develop their security systems to a point where the system is able to recover from adversity, to restore it either to its original state or to a modified state based on new requirements. In other words as we have already mentioned above to create greater resilience. However it is worth mentioning here that these capacities (that ensure grater resilience) are build under different approach that is distinguished from just defensive oriented measures (understood as in classic conventional defense systems).

Although protection is integral part of the resilience of the system, greater resilience is usually achieved through commonly embedded processes inside and out side the system. These processes are established on the synergies between the various stakeholders not just in side the country's security system but also between stakeholder on regional level or global through different organizations (such as NATO, EU for example).

Additional important benefit that this approach ensures is that it protects each-stakeholder interest. Giving that modern threats that come from terrorism, organized crime and recently potentially from state actors are critical infrastructure oriented and that natural disasters could severely endanger our safety and security by endangering critical infrastructure that ensure our everyday lives, protecting these infrastructure becomes crucial. It ensures our wellbeing through protection of systems and services that they provide, but at the same time through this protection it ensures business efficiencies and continuity. Therefore improving resilience of critical infrastructure is in each stakeholder's interest.

Macedonia so far has experienced both devastating natural disasters and terrorist attack. Skopje earthquake in (1963) forever changed the image of the city. In addition flesh floods, and wild fires represent constant challenge each year causing significant material costs and irreparable damage to the environment. On the other hand recent trends of global terrorist threat seem that did not overcome Macedonia. Although many have argued that radical Islam is present in the South East Europe, Jasharevic's attack on US embassy in Bosnia, attack at so called Smilkovci Lake in Macedonia and the attack on the Israeli tourists in Bulgaria, clearly confirmed that the threat from radical Islamists ready to commit terrorist attacks is real (Hadji-Janev, 2012). Both of these attacks were on direct infrastructure that could be considered as critical in a narrow context

(U.S. embassy in Sarajevo-Jasarevic case and ground transportation system at Bulgarian airport) or critical in a broader context (endangering public safety by executing civilians-fishermen randomly picked up by the suspect terrorist) (Hadji-Janev, 2012). Hence importance of protecting critical infrastructure in Macedonia is undoubtedly top priority.

3. Protecting critical infrastructure in Macedonia

Closer look at Macedonian crisis management system (including national defense, internal security and civil protection - their relations and functions) will show a significant shortfall when it comes to critical infrastructure protection. Precisely there is absence of systematic lists of objects, condition or infrastructures marked or identified as a critical for the purpose of their protection. However this does not mean that disaster risk reduction concept could not be applied in conducting system analyses in order for one to come out with conclusions and accordingly to provide recommendations.

Giving that Macedonia follows all hazards approach in resilience building one could still determine the quality of resilience to man made and natural disasters crises. More or less in previous discussion we have emphasized the link between resilience in all hazards approach (concept embedded under disaster risk reduction concept) and CIP. Thus it is clear that still one could analyze the system of CIP in Macedonia. To understand how CIP is organized and function one should take a closer look in to Macedonian legislation for critical infrastructure protection (if there is any), operational design built under the institutional context (stakeholders and their role), and how emergency response, preparedness and recovery are transferred in to practice.

3.1. Macedonian legal framework for critical infrastructure protection

Using analogy of how other states “pump” their resilience under the all hazards approach strategies through CIP it is clear that this analysis should look in several existing laws. Macedonian legislation explained under disaster risk and reduction management approach gravitates over the, Crisis Management Center (The Official Gazette of RM” No. 29/05), Ministry of Interior (The Official Gazette of R.M no.92/09), Protection and Rescue Directorate (Official Gazette of RM”, No. 36/04,49/04,86/08,18/11), Ministry of Defense (The Official Gazette of R.M no.5/03, 06 and 08), Ministry of Transport and Communication (The Official Gazette of RM, No. 40/07), Directorate for Protection of Classified Information (The Official Gazette of RM”, No.9/04), Ministry of Environment and Spatial Planning (The Official Gazette of R.M No. 48/10, 124/10 and 51/11).

Since there is no clear dedicated list of critical infrastructure further legal segmentation follows regarding the anticipated roles and service support for successful CIP. However, all of these documents include acts defining the responsibilities of the government authorities in case of emergencies as well as legislation dealing with issues - such as technical IT security for example,

(The Official Gazette of RM", No.9/04). Some laws or regulations also contain responsibilities for private stake holders on a local level as well. International legislation further facilitates legal background for CIP in Macedonia. This is understandable since cyber-security and environmental protection are on the security agenda in most of the international organizations to whom Macedonia is party.

One could observe this legislative in two directions. First, obligations incorporated from Macedonian's membership of these organizations (or willingness to join). In this context further legislative support comes from the fact that almost all critical infrastructures rely on energy and telecommunications for support. Second, most of the services that provide this support in Macedonia are owned or operated on a commercial basis (foreign private enterprises). Consequently, all bilateral and multilateral agreements in this regards have to be considered. Since these corporations in Macedonia run their security based on Macedonian private security agencies from legal point of view, one should also take into account the Act for security of property and personnel.

In sum, Macedonian legislation for CIP does not centralize responsibility only in one governmental authority. It consists of both, provisions that directly locate responsibility and the leading role of specific agency (we will also refer to this later), and provisions that imply responsibility (regarding the bilateral business agreements and corporate security). Speaking in terms of Penal code act CIP's regulations have also preventive role. Nevertheless, it could be argued that legal basis for CIP in Macedonia more or less, draws the organizational structure of governmental authorities involved in this process.

Macedonian institutional context for CIP is also highly influenced by regional and international organizations' initiatives and their respective documentations. Many international organizations are dealing with this challenge and have taken steps to raise awareness, establish international partnerships, and agree on common rules and practices. European Union (EU), the Forum of Incident Response and Security Teams (FIRST), the G8 Group, NATO, the OECD, the United Nations (UN), and the World Bank Group are just some of these organizations that have influence which institutions will design national institutional context for CIP. In its resolution UN Resolution 57/239 from December 2002 the UN General Assembly outlined elements for creating a global culture of cyber-security, inviting member states and all relevant international organizations to take account of them in their preparations for the summit (UN Resolution 57/239 of December 2002). In December 2003, UN Resolution 58/199 further emphasized the promotion of a global culture of cyber-security and the protection of critical information infrastructures (UN Resolution 58/199 of December 2003).

Over the past decade, some important projects have been initiated in support of strengthening disaster risk reduction actions across South East Europe, which eventually affected Macedonian national institutional context for CIP. In 2000, the Stability Pact for South East Europe launched the *Disaster Preparedness and Prevention Initiative* (Stability Pact for South East Europe, 1999; DPPI SEE, 2010). Support to DPPI has also been acknowledged by the World Bank. In 2007, World Bank with European National Platforms for disaster risk reduction and Hyogo Framework

for Action (HFA) national focal points, in partnership with the World Meteorological Organization (WMO), initiated the South East Europe Disaster Risk Management Initiative - SEEDRMI (South Eastern Europe Disaster Risk Mitigation Initiative, 2007). In 2007 another initiative from the World Bank, the WMO and the United Nations, through the International Strategy for Disaster Reduction (UNISDR), initiated the South Eastern Europe Disaster Risk Mitigation and Adaptation Programme – SEEDRMAP (South Eastern Europe Disaster Risk Mitigation and Adaptation Program, 2008).

3.2. Institutional context of Critical Infrastructure Protection in The Republic of Macedonia

Crisis Management Center (CMC), Protection and Rescue Directorate (PRD), Directorate for Protection of Classified Information (DPCI), Ministry of Interior (MOI), Ministry of Defense (MOD), Ministry of Transport and Communication (MOTC) and Ministry of Environment and Spatial Planning (MOESP) build the list of governmental authorities directly involved in Macedonian CIP. There is no single leading governmental authority in Macedonia in this process. Which government authority will lead the overall process in CIP process (i.e. control and coordination) is situation-dependable.

Since 2009 Macedonia is 11th country that has established National Platform for Disaster Risk Reduction (NPDRR) under the Hyogo framework for action (United Nations, 2005). From security point of view the basis for NPDRR is also supported by the National conception for defense and security (2003) and the National security strategy of Republic of Macedonia (2008). As a nationally owned and led forum of all risk reduction stakeholders NPDRR provides coordination, analysis and can give proposals for priority actions'. It requires concentrated activity, through the coordination and active involvement processes of the competent authorities. NPDRR covers competent crisis management state institutions, scientific and academic institutions, NGOs, the Red Cross as well as the business community. Thus NPDRR is crucial in Macedonian CIP since it identify, assess and monitor disaster risks and enhance early warning coordination. Responsible for preparation planning and organizing all of the activities necessary for crisis is Crisis Management Center (CMC). It maintains close relationships with MOI, DPCI, PRD and MOTC.

MOI covers most of the CIP in ordinary situation. Although it is not stipulated by the law (The Official Gazette of R.M no.92/09, art. 5), virtually MOI is leading governmental authority for CIP in Macedonia during ordinary-peace time situation. Operating under the MOI, Directorate for security and counter-intelligence covers not just most of the organized crime and terrorism issues, but also other issues regarding the CIP. As a result of the recent crime trend regarding the money transport issue, as additional implied task for MOI is to provide security for money transport even for the private corporation (Stargoski, D, 2010). The two most important agencies that fully support the MOI's role in CIP in Macedonia are Protection and rescue directorate and Ministry of transport and communication.

Leading governmental institution for transport CIP is Ministry of transport and communications (MOTC). In defining the transport critical infrastructure in Macedonia MOTC follows NATO's definition. Beside railway, and all ground transport infrastructure MOTC is leading governmental agency in air and water transport CIP too. MOTC approach in defining transport CIP goes beyond the transport infrastructure of goods and people. It also recognizes energy transport infrastructure (gas and gasoline) and telecommunication and internet infrastructure. MOTC practice this responsibility in coordinated support manner. MOI and MOD provide main assistance and enable MOTC successfully to coordinate transport CIP. However, information CIP and coordination for transport CIP with private sector is also highly involved in MOTC planning of transport CIP.

In the area of environmental protection and prevention of industrial accidents the lead is by the Ministry of Environment and Spatial Planing(MOESP) mainly trough implementation of the EU SEVESO Directive and the Convention for cross border effects of industrial hazards.

Protection of the information is crucial part of the overall CIP in Macedonia. Leading governmental agency for information protection (including critical information) is Directorate for protection of classified information (DPCI) (The Official Gazette of RM", No.9/04, art. 4). MOI's Directorate for security and counter-intelligence is in close relation with the DPCI and provide crucial data and efforts to DPCI for successful information protection (The Official Gazette of RM", No.9/04, art. 50). As specific part of the overall defense, Ministry of Defense (MOD) and Intelligence agency play pivotal role in information protection too. All of the military information protection is run by Military service for security and intelligence. Inside the MOD Army of the Republic of Macedonia plan and conduct information operation (IO). DPCI also has close coordination with these MOD's bodies that support DPCI objectives. Macedonian Intelligence agency is in close relation with MOI's Directorate for security and counter-intelligence and thus contributes to the overall information protection. Ministry of transport and communication (MOTC) also has significant role in information protection. MOTC manages telecommunication and internet provider sector and has crucial role for coordination with the private corporate that run telecommunications and internet. In the context of the industry information protection DPCI coordinate all of the activities within the industry sector. These activities are vigorously coordinated with private sector involved in industry sector in Macedonia.

If a crisis is declared, than by the law, situation rapidly changes (The Official Gazette of RM, No. 29/05). During the crisis the Prime minister designate the leading person from the standing Steering committee accordingly (The Official Gazette of RM" No. 29/05,art 13-14). During declared national state of emergency or war, Macedonian Armed forces will take the lead. Armed forces are also responsible for providing protection for designated military and defense infrastructure even in peace time. However, Armed forces' role in CIP is also crucial during declared crisis or during international military operations. During declared crisis Army of the Republic of Macedonia declares units that should support civilian crisis management. International military operations have also brought relatively new role of the armed forces in the

context of the CIP. This basically includes infrastructure that is used for conducting military operations abroad (The Official Gazette of RM" No. 36/10, art. 199-202).
From all of the above it won't be that difficult to conclude that the organizational structure for CIP in Macedonia is highly decentralized and based cross-governmentally trough the agencies (institutions). This network of institutions consists of institutions with legislative, executive, and judiciary powers, infrastructure facilities of energy supply companies, information and communication technologies, infrastructure facilities that ensure the provision of vital goods, transport and traffic infrastructures.

4. General analyses of how emergency response, preparedness and recovery are transferred in to practice for Critical infrastructure protection

So far there was no actual response that could serve as a case example for effective analyses of the CIP in Macedonia. Therefore analysis that follows will be fictional and oriented toward recent practices. Several examples that could point positive and negative practices of existing disaster risk and reduction concept that Macedonia follows and that is base for CIP show that main challenges that could affect effective CIP are based over discrepancy between legislation and organizational design and operational reality, effective and coherent risk assessment methodology and clearly defined strategy and accountability between central and local stakeholders.

4.1. Discrepancy between legislation and organizational design and operational reality as a challenge for effective Critical infrastructure Protection

At first glance legislation is clear and decisive. It dedicates specific role to specific actors from the public sector in different situation. This is quite understandable since disaster risk reduction concept is all hazards oriented. Arguably in such situations centralized planning is needed. One could argue that NPDRR as a nationally owned and led forum for risk reduction provides coordination, analysis and proposals for actions' priority. Furthermore as we described above, NPDRR should enable assessment and monitoring of disaster risks and further enhance early warning coordination. Leading authority that organizes all of these processes is the CMC. However given the capacities that CMC possesses and given the different security concepts and approaches that other stakeholders that need to coordinate facilitate and lead in specific situation follow, serious issues challenge effective CIP.
Namely, CMC has little capacities to run CIP alone. It is true that under the NPDRR CMC is just a leading body that coordinates disaster risk reduction. But it is also true that supporting bodies (MOI and MOD) follow different security concepts. For example MOI follows EU approach in dealing with security issues while MOD follows NATO concepts and standardization. In fact, since NATO and EU does not see the threats with the same eyes and does not have the same approach to deal with it the two most important supporter in CIP does not "speak the same

language" on the ground. For example EU has its own guidance for CIP (EU Commission, 2007) and NATO has its own too (NATO, December 10, 2012). That logically reflects to organization, chain of commands, standardization (including development of standard operative procedures) and last but not least logistics and communications. The issue became even more alarming when CMC adopted UN led concept for disaster risk reduction. This means that although three concepts are well developed and could in fact provide effective CIP, even if there are well designed coordination procedures there still will be issues. The limited budgets push all of three supporting institutions to apply or coordinate funding and support in the area of narrow security concepts that each one of them is following (i.e. EU, NATO and although rarely UN, respectively).

Furthermore, although NPDRR was envisioned in good manner so far the reality is alarming. According to the NPDRR there must be plans for joint exercises and cooperation and coordination. So far these plans have seen the light at ministerial level but not on the ground. There are some partial cooperation on the executive level (such as for example between the Armed forces and PRD units for mountain search and rescue) but this is way beyond the necessary level for effective CIP.

Clear prove for the above mentioned issues are several cases of severe fires where response units were not able to establish communications with the equipment that they posses. Usually thanks to the tactical and operational enthusiasm of the personal involved in the operations these issues were bridged. In the case of the fire suppression in one of our oldest monasteries this winter (Treskavec Monastery, build in the XIV century), the question that we ask is about the effectiveness of the coordination procedures between the armed forces and the civilian structures for disaster management in real time operations for protecting CIP. From one hand there are speculations that the chief of the Armed forces did not employ near by units due to the legal barrier (i.e. according to the defense law only the President could employ the Armed forces). And from the other hand CMC local authorities issued *open panic requests to all citizens* with of-road vehicles to approach for help, creating problems to the ongoing operations that were already in place by the municipal firefighting service (Utrinski, February 04, 2013).

Similarly one might ask the question about the private stakeholders' role in CIP. Many important infrastructure coming from energy and communications sectors are owned and operated by private stake holders. Consequently although there are responsibilities that they need to follow, everyday security and information gathering for early warning still resides on private stakeholders' capacities and abilities. Additionally different security concepts among stakeholders that need to cooperate under the NPDRR brings us to another significant issue i.e. effective and coherent risk assessment methodology.

4.2. Issues with the risk assessment methodology

The essence of the risk assessment process is designed by the Law on rescue and protection. In that sense Article 11 prescribes the responsibility to all public and private organizations to

prepare a plan for protection and rescue against natural and other disasters *based* on valid *hazard* assessment. How the hazard assessment should be done is given by the Methodology for *hazard* assessment and the content of the plan for rescue and protection adopted by the Government in 2006. Based on this Methodology in 2007 the Government adopted the National Hazard Assessment against natural and other disasters. The first discrepancy that we can see in the title and the content of our strategic documents is the inconsistent use of the terms "risk" and "hazard". According to the Methodology from 2006 with the National Hazard Assessment we have identified the hazards that can cause possible disasters by type and location. But this is just the first step in doing the risk assessment (Coppola,2011,p.38). Hazards are part of the equation that explains what is risk in context of disaster management: R(risk) = H(hazard) x V(vulnerability). Unfortunately the current Methodology doesn't lead disaster planers to the next level of answering the three crucial questions that every risk assessment should address:

- What can happen?
- How likely is that to happen?
- What will be the consequences?

The answer of these questions should give a solid foundation for disaster planners for future activities in preventing risks or preparing the system for effective response. In order to reach this end data collection and information shearing between first of all governmental institutions is a must. We have mentioned before the lack of valid data base for critical infrastructure facilities or elements within those facilities. This problem reflects also on the risk assessment process as well. In this moment there is no system in placed that will track history of disasters and their effects (victims, damages, costs etc.), which creates problems for the planers on all levels but it creates problems for the scientist as well willing to do research in this area.
The terrain in Macedonia for a paradigm shift in the area of disaster management in general is more than ready. Having said this, the overall responsibility to lead this process lies with the national top level organizations. They have to create understanding what do we want to achieve, to develop flexible frameworks and to offer valid tools to the levels bellow so that we can achieve results. Centralized planning doesn't have to mean diminishing local initiatives and creativity. If put in placed properly in the way that gives clear instructions about the goals that need to be achieved and support the process with flexible frameworks it can boost local development and lead to excellent solutions.

4.3. Clearly defined strategy and accountability between central and local stakeholders

Effective CIP require clearly defined strategy. So far Macedonia lacks such document. Given that in the age of globalization and technological advance the nature of the threat has changed and the way that security is perceived has also changed protecting critical infrastructure emerged

as an essential task for many security agencies (Hadji-Janev, 2013, p. 93-95). New asymmetric threats that come from non state actors are unconventional and critical infrastructure focused.
Attacks in Bali, Madrid, London, Moscow, but also attack in Sarajevo, or in Bulgaria attest the above view. These attacks were on systems and services that they provide and on which our modern live depends upon. On the other hand security response requires comprehensive and carefully designed approach due to the evolution of democratic perceptions and approaches to security. Today it is clear that protection of human rights with excessive use of force causing mass casualties and material damage could be endangered easily due to the development of technology. Thus confronting asymmetric threats that come from non-state actors practicing terrorism require skillful well organized security forces ready to cope with these threats but at the same time ready to protect human rights and democratic values. Although identifying potential infrastructure that could be target is not an easy job so far has proved as a useful approach in contributing toward greater security while maintaining democratic standards.
Developing strategies for protecting this infrastructure is quite helpful to confront challenges that come from natural disasters as well. Although we could do little to confront actual natural disaster we could do much more to reduce the reasons that cause it or to mitigate and manage the consequences with identifying critical infrastructure. Thus working on prevention and on mitigation we build resilience of the system and thus reduce the consequences from natural disaster.
The strategy for critical infrastructure protection will also help to designate specific roles for all stakeholders, since all of them as we have mentioned above, have the necessity for protection, but not the capacities for doing it alone. Therefore future strategy must consider all stakeholders from public and private sectors. This will serve as a background for future role that each stakeholder will have in providing such protection.

5. Recommendation for the future

From all of the above it became clear that Macedonia has quite well designed platform that could easily be adopted to serve for development of effective CIP. However, from the discussion above it also became clear that there are some challenges that require greater attention if we are about to develop resilient based CIP. Therefore we will provide some recommendation that could serve as a starter but also as a platform for future more detail research on this topic.

5.1. Recommendation regarding the legislation and institutional context of critical infrastructure protection in the Republic of Macedonia

Authorities must identify critical infrastructures in the Republic of Macedonia. This has to be done with official document and in accordance with security threats, and current and existing concept for disaster risk reduction having the all hazard approach. Accordingly there has to be

official bylaws that will facilitate ministerial support for critical infrastructure protection through respective sectors functioning in accordance of administrative laws.

Legislation should mandate clarification of roles and responsibilities for CIP at national and local communities' level. In addition it should be bared in mind that systems and services that they provide are connected interlinked on regional level. On the other hand today security requires regional and international cooperation. Therefore one could not achieve effective CIP without improving regional cooperation and designate stakeholders that will be responsible for cooperation and collaboration and improving communication between all relevant sectors and agencies responsible for CIP.

To be effective CIP requires efficient and prioritized allocation of financial and human resources. This needs to be done in the context of existing disaster risk reduction policies, or in accordance with the EU guidance for CIP or NATO based approach and guidance for CIP. Again there must be leading agency or body without leaving room for falling in to gap where "when two or three stakeholders are responsible no one is responsible". We are aware that this will require sacrifice due to the power sharing and funds and budgets, nonetheless we are also aware that national interest highly overruns these considerations too.

Consequently responsible stakeholders must develop standardized cross-ministerial and cross sector agreed criteria for CIP. Since the analyses about recent practice under the NPDRR clearly showed that there is discrepancy between strategic and executive application of current crisis management developed under the all hazards approach there must be a controlling mechanisms. These mechanisms should ensure that responsible stakeholders have established appropriate programmes, plans and essential task lists accordingly.

Controlling mechanism should be also developed to ensure periodical joint exercises with rigorous analyses of conducted joint activities and exercises with the focus on the best practices lessons learned from regional global experiences. These controlling mechanisms should also consider budget planning for CIP, achieved level of expertise among dedicated personnel for CIP from respective stakeholders (private and public) with recommendation for future improvement and reevaluation of the achieved improvement.

Finally one thing that is lacking in the security sector in Macedonia and consequently will reflect to the CIP is the absence of relevant researches in the area. Thus we believe that if Macedonia is about to build resilience through CIP it definitely needs to consider building resilience through knowledge advocacy and research. Later could also serve as a crucial factor in development of appropriate risk assessment methodology for CIP.

5.2. Recommendation for better risk assessment methodology for critical infrastructure protection

One could not achieve effective CIP in the environment where many stakeholders need to contribute and when all of these stakeholders have different perception about the threat. Therefore for effective CIP Macedonia needs to formalize protocols and unifies methodology

and institutional capacities for integrated collection, analysis and dissemination of hazards, vulnerabilities and loss data at the national and local level. Accordingly this will lead to development of standardized approaches, tools, methods and information management systems (with focus on information sharing sentiments) to facilitate comprehensive multi-hazard risk assessments, through implementation of the existing security documents and in compliance with chosen guidelines (EU, NATO or UN). Hence comparable multi-hazard risk profiles should be developed in line with (chosen guidelines) considering the regional trends as well. These guidelines regularly need to be updated, easily available and to include assessments from and for key sectors (with specific regard to urban settlements and vulnerable communities). However, without allocation of sufficient funds and guarantee that there will be regular investments to support the development of technical and institutional capacities to identify, assess and monitor potential threats.

5.3. Recommendation for future strategy for critical infrastructure protection

For effective CIP Macedonia needs strategy that will ensure centralized planning and decentralized execution. No matter how expensive it might be, Macedonia needs centralized approach in managing the planning process in CIP. In fact, Macedonia needs to fulfill the gap between theory and practice. This will also help to analyze and further improve existing legislative, organizational structure, mechanisms and methodology in CIP approach. Recent fatality of terrorist attacks and natural disasters and their aftermath consequences overrun the costs of preventive approach to protect critical infrastructure.

In order to be effective in this centralized planning process Macedonian government needs to coordinate, facilitate and stimulate all the authorities (especially private corporate) that directly or indirectly build security network in CIP. In terms of coordination recent practice shows that many governments in fact have established cross-sector advisory boards for CIP (The National Infrastructure Advisory Council in the United States; the Critical Infrastructure Advisory Council (CIAC) in Australia; or the Association of Italian Experts for Critical Infrastructures (AIIC). Since centralized planning is not new in Macedonian security tradition existing platforms of this kind (like for crisis management) could serve as well designed base for CIP Former security was actually organized in similar manner. It was based on central planning and central execution. Central planning is crucial for private sector involvement in this process. Existing Steering committee for crisis management is good background to expand on. However, for steering the networks indirectly one must have a good knowledge about the structures and tasks of very different networks in CIP. The most difficult part probably consists of monitoring all the different networks. The goal of facilitation should be support of the specific elements of the security network (especially private corporate) and enable them to work efficiently by creating a network-friendly environment. Governments can promote the networks, advise them (e.g., by creating general frameworks for interaction or by developing model agreements), and sometimes they even have to grant exemptions for networks from laws that impede private collaboration.

An example for such a case is the exemption for Information Sharing and Analysis Centers (ISACs) from the Freedom of Information Act (FOIA) in the United States (Thibodeau, Patrick, Julay 24, 2002). Stimulation of the network is crucial. Sometimes private companies will have specific concerns with participating in the CIP network which strategy also needs to consider (Esther and Anindya, 2005, p. 186–208).
From all of the above it would not be hard to conclude that Macedonia is on a right way in CIP. Nevertheless, specific challenges should be address immediately before it is too late.

Conclusion

The concept of resilience put in context of disaster risk reduction gives different motion to the overall activities. It is a proactive approach and much more than just simple bouncing back or restoring normality after a disaster or a crisis. In every socio-economic and political system there are functions that must be protected in order the system to preserve its core functions. We build resilience of those core functions by identifying them, assessing the risks towards them and formulating clear procedures for their prevalence in times of crisis. In order this approach to be successful the national Government needs to speak with one voice and have appropriate strategy towards the issue. With showing the case of Macedonia in this regards we think that further enhancement of the legal framework which will result with centralized planning but with decentralized execution should be the way of creating resilient critical infrastructure.

References:

Conway,G.,Waage,J.K.,Delaney,S.(2010)*Science and Innovation for Development*.UK Collaborative on Development Science. UKCDS: Hampshire, UK

Coppola,D., (2011), Introduction to international disaster management, Elsevier Inc, Burlington USA

Crisis and Risk Network Report, (2008), *Focal report-1 Critical Infrastructure Protection*, Center for Security Studies, Zurich Switzerland;

Crisis and Risk Network Report, (2009), *Focal report-2 Critical Infrastructure Protection*, Center for Security Studies, Zurich Switzerland;

_____, "Disaster Preparedness and Prevention Initiative-DPPI SEE", 2010, retrieved March 14,2013, from at: http://www.dppi.info/content/about-us;

EU Commission, (2007), "European Programme for Critical Infrastructure Protection", European Union Official Journal, 2007, retrieved 25 March 2013, from: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm;

Gal-Or, E. and Ghose A., (2005), "The Economic Incentives for Sharing Security Information", Information System Research 16 (2)

Gunderson, L.H,(2000), Ecological Resilience – In Theory and Application, Annual Review of Ecology and Systematics, Vol.31, pp.425-439
Hadji-janev, Metodi (2012), "Managing the consequences of terrorist attacks: The Case of Macedonia", in: Chaleta D. & Shemella P. (Eds.) Managing the Consequences of Terrorist Acts - Efficiency and Coordination Challenges, Ljubljana;
Hadji-Janev, M. (2013), "Threats to the Critical Information Infrastructure Protection (CIIP) Posed by Modern Terrorism", In: Théron, P., & Bologna, S., *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, IGI Global, USA
Hasan, M. (2013), 800-year-old lesson from Japan, UNISDR New York UNHQ Liaison Office, available at www.unisdr.org/archive/31667
Hussain, M. (2013), Resilience: meaningless jargon or development solution?, The Guardian available at www.guardian.co.uk/global-development-professionals-network/2013/mar/05/resilience-development-buzzwords
Korstanje, M.E.,(2011), Reconnecting with poverty: new challenges of disaster management, International Journal of Disaster Resilience in the Built Environment, Vol. 2 No. 2, pp. 165-177
NATO Parliamentary Assembly, (2007), "The Protection Of Critical Infrastructures", 162 CDS 07 E rev. 1, Annul Session, retrieved March 10, 2013, from: http://www.nato-pa.int/default.asp?SHORTCUT=1165;
NATO (Dcemebr, 2012), "Protecting Critical Infrastructure", retrieved: 25 March 2013, from: http://www.nato.int/cps/en/natolive/news_92793.htm;
_____, "South Eastern Europe Disaster Risk Mitigation Initiative", 2007, retrieved March 3, 2013 from: http://www.unisdr.org/europe/eu-publications/SEEDRMI.pdf;
Salat,S.,Bourdic,L.,(2012), Systematic resilience of urban complex systems, TeMa Journal of land use, mobility and environment 2, pp.55-68
Stability Pact for South east Europe, 1999, available at: http://www.stabilitypact.org/default.asp;
Stargoski, D, 2010, *450.000 Euros stolen from vehicle of Stopanska Banka Bitola*, A1, retrieved March 03, 2011, from: http://www.a1.com.mk/vesti/default.aspx?VestID=118410;
The Official Gazette of RM No.5/03, 06 and 08, "Law of Defense" and Law for changes and addition of Law of Defense", Republic of Macedonia;
The Official Gazette of RM", No. 36/04,49/04,86/08,18/11, The Law on Rescue and Protection", Republic of Macedonia;
The Official Gazette of RM, No.9/04, "The law of classified information"
The Official Gazette of RM, No. 29/05, "Law on Crisis Management", Republic of Macedonia;
The Official Gazette of RM, No. 40/07, "Law of Security in railway traffic"
The Official Gazette of RM No.92/09, "Law on Iinternal Affairs", Republic of Macedonia;
The Official Gazette of RM No. 48/10, 124/10 and 51/11, "Ministry of Environment and Spatial Planning", Republic of Macedonia;
Thibodeau, Patrick, (Julay 24, 2002), "House Panel Jousts over information sharing bill", Computerworld, retrieved March 17, 2013 from:

http://www.computerworld.com/s/article/72962/House_panel_jousts_over_information_sharing_bill;
UN Resolution 57/239 of December 2002;
UN Resolution 58/199 of December 2003;
United Nations, (2005), "International Strategy For Disaster Reduction (UN ISDR)", Brought under Hyogo framework for action, available at: http://www.unbrussels.org/agencies/unisdr.html;
_____, Utrinski, February 04, 2013, "The Monastery Treskavec near Prilep burned out", retrieved 25 March, 2013, from:
http://www.utrinski.com.mk/?ItemID=E300C5B24014A441823C71B29134232A.
World Bank, GFDRR, Government of Japan, (2012), The Sendai Report, International Bank for Reconstruction and Development/International Development Association of the World Bank, Washington DC

About the authors:

Metodi Hadji-Janev (PhD) was borne 15 June 1976 in Stip Macedonia. Lieutenant Colonel Metodi Hadji-Janev (PhD) had spent almost 12 years of service as Special Forces officer in Macedonian Special Forces. In 2003 LtC Metodi Hadji-Janev (PhD) was deployed as commander of Macedonian Special task forces in Iraq. He is the author of the book "Iraqi Freedom: The Road to Babylon" and author of numerous articles related to the International law, organized crime and international terrorism. Since January 2011 Hadji-Janev (PhD) has been assigned as the head of Social science department at the Military Academy in Skopje and Co-director of Intelligence sharing course in NATO Center of excellence-Defense Against Terrorism in Ankara Turkey.

Vlatko Jovanovski (MDMa) was born 7 September 1978 in Sveti Nikole, Macedonia. He has a Bachelor degree in law from the University St.Cyril and Methodius –Skopje since October 2002. In 2004, successfully completes the qualification and specialization for Officers for legal service with the land forces of the Army of Republic of Macedonia at the national Military Academy. In 2006 he started working for the Protection and Rescue Directorate of Republic of Macedonia and that is his current working environment. In 2012 he earned his Masters in Disaster Management from the University of Copenhagen – School of Global Health.