PIECES OF A LARGER PUZZLE: THE ALMOST IMPOSSIBLE TASK OF PROTECTING CRITICAL INFRASTRUCTURES

Veerle Pashley[1], Marc Cools[2]

'A man who discovers his pants are on fire

tends to have very little time to worry

about somebody else's box of matches'

(Dexter in Jeff Lindsay, 2005, 75).

Preface

Writing an article on critical infrastructure protection is quite challenging. Scientifically speaking, we ascertain a serious lack of

1 Veerle Pashley is a PhD student in criminology and social & military sciences at the Free University of Brussels and the Royal Military Academy.

2 Marc Cools is a Professor in Criminology at the Free University of Brussels and Ghent University.

research. A possible explanation could be the fact that in studying critical infrastructure protection one must be able to integrate a multidisciplinary scope. The changing landscape of security (Crawford, 2012) and prevention requires a scientific viewpoint that implements segments coming from several disciplines, i.e. economy, technology, governance, law, sociology and criminology. Evidently, this means a challenge for researchers. Taking these transitions into account, this paper aims at better understanding of critical infrastructure protection. First, we will discuss the conceptualisation of the concepts 'infrastructures', 'critical' and 'protection'. Each word entails a different connotation. We will also focus on the European dimension. Considering the fact that a clarifying definition is currently difficult to realise, we will explore the underlying characteristics and give ideas for new directions. This paper will also reflect on the role of intelligence and private security. Last, we will present criminological reflections regarding the changing landscape of security and its effect on the protection of critical infrastructures. The recent focus on resilience gives an interesting alternative for the encountered challenges.

Introduction: critical infrastructure protection and the underlying challenges

The protection of critical infrastructures, such as water, energy and telecommunications, is of the utmost importance. If these assets are at risk or destroyed, it will have an impact on the economy, psychology and pride of a nation or society (Lewis, 2006, 1). Technological progress and economic shifts emphasizes the

importance of information, telecommunication and knowledge infrastructures (Thissen & Herder, 2003). Ever since the Cuban Missile Crisis of 1962, the concept of infrastructure security has been evolving. Former President of the United States of America, Kennedy, and former Prime Minister of the Soviet Union, Khrushchev, had troubles with inadequate telecommunication technology. It was the first sector to be defined as 'critical' (Lewis, 2006, 2). Since the nineties, critical infrastructure protection became a main focus of security strategies.

Citizens rely on the proper functioning of certain organisations, e.g. water, energy, telecommunications... If critical infrastructures fail, it can compromise the functioning of society. Today, we ascertain some important technological and institutional changes, which have an impact on critical infrastructures. Also, systems are becoming more and more complex. Our global society obliges us to consider trans-boundary dependencies and an increasing service quality (Thissen & Herder, 2003). These transitions illustrate that the protection of critical infrastructures is a security strategy, which is far from clear.

A first problem scientists and practitioners encounter is the difficulty of formulating an efficient conceptualisation. Both theoretically and practically, current understandings of critical infrastructures are very vague, broad and uncertain. It seems almost impossible to fully understand the underlying structures and meaning of the concept. Subsequently, a second problem arises. In order to protect companies, organisations, sectors and/or key resources, three important aspects are

necessary: risk planning, risk management and risk leadership. Yet, critical infrastructures can be huge in size and our global society challenges us to act locally and internationally. The eruption of the Icelandic Eyjafjallajökull volcano in 2010 illustrates how a local nature disaster can have an enormous effect on technology (non functioning air traffic) and the economy in several countries. Therefore, critical infrastructures can be interdependent. As a result, prevention and repression strategies are extremely difficult because it questions the very aim of security. More specific, what does 'security' of critical infrastructures means and how can we respond to threats or disasters if multiple sectors are involved? This question entails a third problem. In order to protect critical infrastructures we need to have adequate protection strategies that focus on prevention. Moreover, we must reflect on threats or disruptive events that could happen. Considering the changing landscape of security, this almost seems impossible unless we can appeal on our creative thinking. As we will discuss, the focus on resilience (European Commission, 2013) is important and offers another direction in protecting our critical infrastructures.

Managing uncertainties: it's all about Critical Infrastructure Protection (CIP)

In this section of the paper, we will reflect on the conceptualisation of critical infrastructure protection. Considering the reliability of citizens on certain sectors, organisations and key resources, prevention strategies focus on 'uncertain and disruptive events'. This requires a profound system of intelligence in order to know the possible risks.

Critical infrastructure protection: a question of conceptualisation

A good and scientific analysis starts with a closer look at the conceptualisation at hand. The definition of CIP is not easy because of its wide range. This paper examines infrastructures that are critical and need protection. Each word entails a specific connotation and is characterized by several components. First, we have to examine the notion 'infrastructures', which are generally defined as organizational structures that are necessary for the operation of a society or enterprise or the facilities and services that are essential for an economy to function (Lewis, 2006).

The assets are divided into sectors (Lewis, Darke, Mackin & Dudehoeffer in Flammini, 2012, 4). According to the United States' National Infrastructure Protection Plan of 2006, infrastructures and key resources can be divided into eighteen sectors. These infrastructure sectors are agriculture and food protection, drinking water treatment, energy/power, information technology/telecommunications, transportation systems, defence industrial base, public health, banking/finance, postal/shipping and critical manufacturing. Key resources are national monuments/icons, government facilities, chemical facilities, commercial facilities, hydro-electric dams, emergency services and commercial nuclear reactors, materials and waste (United States' National Infrastructure Protection Plan, 2006).

Second, we have to define the notion of 'critical', which is problematic because if we

take a look at the assets, sectors, organisations and key resources we can ascertain that numerous infrastructures are critical. In order to better understand this concept we have to reflect on the reliability of these infrastructures on the functioning of society. Taking a look at the existing literature, we can highlight that critical infrastructures are mostly defined as those assets, systems or functions that can seriously impact national-level public health, the economy, public safety, governance, national security and public confidence (Lewis, Darke, Mackin & Dudehoeffer in Flammini, 2012, 4). Critical infrastructures are *'vital and its incapacity or destruction would have a debilitating impact on our defense and national security. It is a network of independent, often privately owned, systems that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services'* (Lewis, 2006, 3). Therefore, critical infrastructures must ensemble in a reliable way so they provide a critical need (Dynes in Papa & Shenoi, 2008, 3-4).

Third, we have to highlight the concept of 'protection', which is even more problematic. As we can see, the conceptualisation of 'critical' 'infrastructures' is vague and uncertain. This has consequences on how they are protected. Security and protection are focussed on dealing with threats or disruptive events that can vary in context, i.e. crime related, environmental, system failures… As a result, assessing risks becomes (almost) impossible. Most commonly, CIP is examined within a scope of crime related threats. In this light, the protection of critical infrastructures is about strategies and policies that are necessary to prevent and react to

attacks or harms on the aforementioned sectors and key assets (Lewis, 2006, 4).

As mentioned in the introduction, three aspects are important in critical infrastructure protection i.e. risk leadership, risk planning/assessment and risk management. An integrated risk management approach recognizes that both the optimal amount of risk retained and the tools used to achieve a risk level will differ from organisation to organisation. The meaning of integrated is twofold, i.e. integrating risks and integrating ways to manage risks. It emphasizes a systematic approach where risks are evaluated taking into account the multidimensional effects on the organisation coupled with a framework for deciding upon the best implementation strategy (Chew, 2008, 74). Each decision leaders make as well as the integration of both risk planning and assessment means that, in turn, another set of risks emerges (Linkov et al, 2007). Dealing with risks means dealing with never ending uncertainties and strategies. Khatta (2008, 81-82) highlights the need for risk impact analysis. This approach emphasizes decision makers to determine the consequences of possible disruptive events. Scenario building that enables us to reflect on 'things that could happen' is a much wanted tool.

Infrastructures vary in size. The bigger the asset, the more complex its protection gets. Each of the aforementioned sectors is extremely large, complex and open to attack by natural or human actors. Also, there is an interdependency between these infrastructures and key resources, which makes their protection all the more difficult. At the level of the ensemble of critical infrastructures there is a

lack of understanding these interdependencies (Dynes in Papa & Shenoi, 2008, 3-4). Also, its protection is difficult because there is an absence of standardized risk assessment schemes. As a result, we cannot compare the existing risks between regions, industries and divisions. Each sector applies its own methods targeting different aspects of critical infrastructure protection (Lewis, Darke, Mackin & Dudehoeffer in Flammini, 2012, 4). Researchers come to the conclusion that it is practically and economic unrealistic to fully protect every component or sector, let alone all sectors (Lewis, Darke, Mackin & Dudehoeffer in Flammini, 2012, 4). Instead of focussing on the idea that critical infrastructures can be successfully secured as a whole, several authors emphasize the need of a prioritization scheme in order to protect critical infrastructures with limited resources (Flammini, 2012, Lewis, 2006). This means that we must focus on systems instead of sectors and on networks with partners, both publically and privately. In order to prevent supply chain risks or risks due to interdependencies between critical infrastructures, we need better frameworks (Dynes in Papa & Shenoi, 2008, 3-4). Lewis (2006) also emphasizes the necessity of 'asymmetric thinking', which means we have to search for new ways to protect our vast and critical infrastructures from attack, environmental harms and system failures.

Although we have tried to clarify it's meaning, we can see that the conceptualisation of critical infrastructure protection remains challenging because of its size and its multidisciplinary components. Our focus is too much aimed at the 'protection' of 'uncertain events' that could happen to 'all critical infrastructures'. In chapter

4 we will highlight another possible approach, which has become a strategy in Europe and can diminish some of the encountered difficulties.

Critical infrastructure protection in Europe

In 1999, the Treaty of Amsterdam emphasized the European Union's role in security strategies against terrorism (Van Nevel, 2010, 35). Post 9/11, the European Council approved an action plan, which highlights the importance of freedom and security for citizens. Therefore, acts of terrorism should be prevented and tackled. As a result, he European Union created the counter terrorism strategy in 2005 that focuses on prevention and protection.

In 2007, the European Union created a programme called *'Prevention, preparedness and consequence management of terrorism'*, a project with a time limit of six years. The aim is to protect citizens and critical infrastructures within the scope of freedom and security (European Union, 2007) in supporting Member States. Although countries are individually responsible for the protection of critical infrastructures, it is important to have transnational guidelines because of the aforementioned interdependence between certain sectors and organisations. The EU also wishes to support its Member States.

In 2004, the European Commission launched a communication with the idea of creating a European Programme for Critical Infrastructures (EPCIP). The aim is to support companies and governments in the EU in their security strategies. It seeks to provide an all-

hazards cross-sectoral approach[3]. In 2005, the EPCIP emphasized the need for creating better networks. The Critical Infrastructure Warning Information Network (CIWIN) brings together specialists from the EU to assist the European Commission in establishing networks programmes to facilitate information exchange on threats, vulnerabilities, measures and strategies (Van Nevel, 2010, 37). EPCIP Contact Point meetings are organized in order to exchange information between Member States of the EU (www.ec.europa.eu). They also fund and execute multiple studies in order to identify the needs of an adequate critical infrastructure protection.

In 2008, there was an important transition when the EU launched a Directive called *'On the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection'*. Considering the fact that the EU highlights the freedom of each Member State to protect critical infrastructures, the Directive makes a clear distinction between Critical Infrastructures and European Critical Infrastructures. Article 2 of the Directive (2008) defines a critical infrastructure as *'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'*. A European Critical Infrastructure, on the other hand, has a different connotation. It is a critical infrastructure

3 www.ec.europa.eu

that is located in the EU and its disruption of destruction must have a significant impact on at least two Member States. Article 2 of the Directive (2008) states that the impact must be assessed in terms of *cross-cutting criteria* (interdependencies infrastructures). This means that when critical infrastructures have essential or vital services in several countries of the EU, security strategies obtain a European dimension.

In 2012, the European Commission launched a staff-working document *called 'On the review of the European Programme for Critical Infrastructures Protection (EPCIP)'*. Based upon research results, they highlight several conclusions on critical infrastructure protection. All Member States have legally implemented the Directive of 2008 and have identified European Critical Infrastructures. Also, they underlined that even though the Directive seeks to improve a better protection, there is no indication that the security of energy and transport sectors is improved. Another viewpoint of the staff-working document is the fact that European strategies should focus on systems instead of sectors (critical infrastructures are often too huge and complex). We also need a European Forum for decision-making and a critical infrastructure risk management policy with more specific guidelines and recommendations (European Commission, 2012, 18-19).

In 2013, a very important document was launched that has new and interesting insights on the protection of critical infrastructures. The European Commission staff-working *document 'A new approach to the European Programme for Critical Infrastructure Protection: making*

European critical infrastructures more secure' (2013) highlights alternative directions. The interdependency between organisations, the variety and complexity of certain sectors as well as the uncertainties of transnational security strategies were points of discussion, which advocated the need of other focal points. The document stimulates the need of resilient critical infrastructures (we will discuss this in chapter 4) and interdependent systems. Furthermore, a new approach will be implemented. In order to have a more focussed approach EPCIP selected four critical infrastructures that have a European dimension in order to optimise their protection and resilience. These sectors are Eurocontrol (EU Air Traffic Management Network Manager), Galileo (global satellite navigation system), the Electricity Transmission Grid and the European Gas Transmission Network (European Commission, 2013, 7-8). The selection was based on their cross-border dimension, representativeness and interest in piloting and sharing best practices. The aim is to set up tools for prevention (risk management and risk assessment), preparedness (increasing consideration for resilience and preparation) and response (long-term recovery of critical services).

If we compare this document to other papers of the European Commission, we ascertain an increasing focus on specific strategies. The uncertainties of disruptive events made it quite clear that strategies should focus more on resilience and preparedness. This strategic shift offers opportunities to execute studies, which are much more focussed on certain particularities.

Intelligence, private security and critical infrastructure protection

Protecting critical infrastructures is an important core business in the framework of protecting the economic potential (Cools, Dassen, Libert, 2005). Intelligence services play a vital role in security strategies regarding CIP.

Intelligence is a process consisting of three characteristics (Shulsky & Schmitt, 2002). First, it is about gathering information regarding actual and potential threats. Second, it evolves around activities that focus on gathering, analysing and processing information as well as countering threats. Third, the organisation of intelligence is important. Often forgotten in literature is the fact that intelligence is also about networking. If you want information about actual and potential threats, you need to have contacts. Intelligence is, as a process, extremely complex. Information is necessary to obtain knowledge on situations, events and changes in society. Intelligence is also about assessing and evaluating risks. This means one must have solid networks and be able to estimate transition of a social, political, economic and technological nature.

The protection of critical infrastructures is an important task for intelligence services, since they provide advice and analysis regarding crime related threats (e.g. terrorism, sabotage). Collecting information regarding risks and possible disruptive events is challenging. We live in a world were a lot of information is available. Intelligence or knowledge gathering must make a distinction between relevant data and irrelevant data. Subsequently, information can also be insufficient, undetermined and

uncertain (Richards, 2010, 40). How can one determine which intelligence must be further explored or not? Protecting critical infrastructures means that scenario's must be created based on reliable information, especially since most problems are linked with indirect risks and immeasurable threats. In order to create efficient scenarios, networking (both privately and publically) is important. Collaboration strategies are important to protect our economic potential. Steenlant and Ven (2005, 324-328) stress out that international commitments as well as meetings with companies are a necessity.

The security and safety of critical infrastructures is the responsibility of the owner of the company or organisation (Van Nevel, 2010). On this level another important partner emerges, i.e. the private security sector. Their input is foremost the provision of training. When organizations or installations, which have a vital impact on the continuous functioning of public authorities, the market and society, are facing disruptive events or emergencies, it is of the utmost importance to safeguard and secure these critical infrastructures. Since critical infrastructures can be threatened, e.g. terrorist attacks, technological failures and natural disasters, the added value of private security is targeted in specialisation that is aimed at developing sector specific knowhow and market segments (CoESS, 2013, 17; Müller, 2012). Training is an important focal point for private security. Companies and their personnel have to obtain a certification from government authorities and follow training if they want to deliver private security (CoESS, 2011). In most European countries, critical infrastructure protection is evaluated as an important task for

private security. Subsequently, the protection of critical infrastructures is generally seen (Davidovic, Kesetovic & Pavicevic, 2012) as a responsibility that must be organized between the public and private sector.

Private security takes part in larger security strategies, which is mostly explained as 'governance of security'. This theory focuses on the pluralisation of security in certain areas or 'nodes' and examines how these 'nodes' relate to one another (Johnston & Shearing, 2003). However, a very recent study conducted by Adam White (2011) sheds new light on the matter. He claims that a broader interdisciplinary scope is needed, i.e. the integration of the 'new political economy'. His main critique of contemporary studies on private security is that they fail to integrate both the administrative context and the economic context (White, 2011). Indeed, scientists in general and criminologists in particular often overlook to integrate both pillars in security research. However, contemporary studies need to find a way to implement both the administrative and the economic context. This would allow us to fully understand the underlying process and practical organisation of security related private – public collaboration strategies.

We already discussed the conceptualisation of critical infrastructure protection and the role of intelligence. The question arises: what is the role of private security companies in critical infrastructure protection? In order to give an appropriate answer we must take a look at the field and consult existing working documents. The Confederation of European Security Services (CoESS), which is the representative

organisation for private security services, has created interesting white papers and guidelines that give a general overview of the current situation. Considering the aim of this paper, it is necessary to discuss certain aspects of these documents. The sector emphasizes the *'explicit allocation of roles and responsibilities for protection along with common standards of risk assessment to be adopted so that best practice is used to apply appropriate levels of security'* (CoESS, 2012a, 4). Taking into account the importance of accountability and responsible decision-making (Davidovic, Kesetovic & Pavicevic, 2012: 70) the private security sector advocates the need of a special license regarding critical infrastructure protection (CoESS, 2012a).

The main issue of contemporary public – private partnerships in security strategies is that private security is often called upon as an afterthought. As a result, the effectiveness of such a collaboration is somewhat eroded. In order to improve effective partnerships, the private security sector should be included from the beginning, i.e. in the design (conceptualisation of approaches) and the operation (possible as well as applied strategies) of critical infrastructure protection (CoESS, 2012a). Considering the fact that the private security industry consists of corporations, the sector is more than familiar with the structural components of risk assessment, identifying security threats and sector specific training.

New directions in thinking about Critical Infrastructure Protection: the introduction of resilience

The new European focus on resilience is quite exciting because it narrows the gap in critical infrastructure protection. But what does this precisely mean? Taking a look at other international documents, we conclude that this shift is detectible in other regions as well. In the United States of America, the 'National Infrastructure Advisory Council' or NIAC supplies advise concerning the aforementioned eighteen critical infrastructure sectors and key resources. They also give feedback to lead Federal agencies having responsibilities regarding CIP and industry coordinating mechanisms. Their aim is twofold. First, they want to search for strategies which enhance public-private cooperation. Second, they encourage the private industry to frequently perform risk assessments of critical information and telecommunication systems[4].

In 2009, the NIAC released a study report called 'Critical Infrastructure Partnership Strategic Assessment Study',which highlighted some interesting results. It focuses on the importance of resilience for the public and private sector in creating their risk assessment strategies. Infrastructure resilience is *'the ability to reduce the magnitude, impact and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to and/or rapidly recover from a potentially disruptive happening'* (NIAC, 2009,

4 http://www.dhs.gov/national-infrastructure-advisory-council

8). Risk management should therefore focus on the resilience of a critical infrastructure.

Resilience aims at the enhancement of three capacities. The absorptive capacity is the ability of the system to endure a disruption without significant deviation from a normal operating performance. The adaptive capacity is the ability of systems to adapt to a shock to normal operating systems. Recoverability is the ability of a system to quickly recover from disruptive events (NIAC, 2009).

Three features characterize critical infrastructure resilience (NIAC, 2009). These features are robustness (maintain operations and functions in the face of a crisis), resourcefulness (prepare for, respond to and manage a crisis or disruption as it unfolds) and rapid recovery (return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption).

Important to stress out are some of the recommendations of the NIAC report (2009), since they are specific and coherent with scientific research on critical infrastructure protection. A first focus should be on further exploring the conceptualisation of critical infrastructure protection and resilience. As other studies highlight (Goetz & Shenoi, 2010; Flammini, 2012; Hokstad, Utne & Vatne, 2012), our current knowledge remains very general and there are many difficulties in clarifying the main focal point. The main problem is the fact that several infrastructure sectors can be viewed as ‘critical’. Also, the possibility of a ‘chain reaction’ if a disruptive event occurs is a vast reality. E.g. the effects of the Eyjafjallajökull volcano in Iceland impacted the

economy, technology... Risk management is often restricted to specific sectors and organisations. The interdependency between critical infrastructures, nationally and internationally, challenges an integrated approach. Therefore, public – private cooperation strategies are of the utmost importance. As scientific research emphasizes (Goetz & Shenoi, 2010), the roles and responsibilities of critical infrastructure partners should be clarified and implemented in risk management. Since the protection of critical infrastructures challenges partners to 'think about the unthinkable' (Gosselin, Leysen & Verbeke, 2007) we must focus on alternative viewpoints and working procedures. In this scope, the focus on resilience should be encouraged because it is the first step towards an adequate protection. As mentioned, private – public collaboration strategies are of the utmost importance. This focus was made very clear in the NIAC report. Europe's strategy is somewhat comparable with the US.

Three main strategies are linked with the European viewpoint on critical infrastructure resilience, i.e. prevention, preparedness and response (European Commission, 2013, 8-9). The aim of the European Commission is to work on each of these characteristics. Prevention will be aimed at the creation of tools for risk assessment and risk management. In doing this, the private sector should be included more profoundly. The idea is to create best practices on a European level, which highlight several recommendations, scenario scenes and guidelines. Considering the fact that intelligence plays a vital role, the EU Intelligence Analysis Centre (INTCEN) will also be included in further planning. The preparedness and response

strategy is aimed at training, awareness and exercises.

In our opinion, what is missing in the document is the vital role of risk leadership and coordination. Since European Critical Infrastructures are crosscutting and interdependent, how will these strategies be coordinated? This remains unclear and since a multitude of partners are involved, a profound risk coordination scheme is of the utmost importance.

Although these transitions are interesting, several questions still remain unanswered. First, the importance of preparedness is still very vague. As mentioned, disruptive events that can threaten critical infrastructures are uncertain. All things considered, numerous threats could occur. Also, we do not now if and when such events will take place. We have to deal with a lot of uncertainties. We can apply the same question for the factor 'response'. How can we prepare an efficient recovery if we do not know what could happen? Scientifically speaking, there are several challenges tangible and we lack a proper theoretical framework that could clarify the underlying difficulties. Criminological research produced several security studies that focus on strategies and governance. They mostly focussed on direct threats. However, we lack insight that deals with uncertain events. Following chapter will provide a criminological framework that will highlight these uncertainties more profoundly.

Challenges for the criminological researcher: thinking about uncertainties and vague events that could happen

As mentioned, scientific studies regarding critical infrastructure protection and resilience are not common. A possible explanation for the current lack of research could be the difficulty of an alternative scope and the wide range of critical infrastructures. Therefore, it is important for scientists to focus on two realities.

First, we have to be able to study uncertain threats, i.e. disruptive events that have not occurred but could happen. This means we have to be able to widen our theoretical framework, both nationally and internationally. Subsequently, the concept of 'risk management' should be integrated in security studies. Second, we must take into account the changing landscape of 'security'. Critical infrastructure protection is not a 'new' phenomenon, however the actual conceptualisation is. This is mainly due to societal transitions and the changing landscape of 'security'.

If we take a look at literature regarding security and thinking about the unthinkable (Gosselin, Leysen & Verbeke, 2007), we can conclude that most ideas are formulated from a perspective of criminal threats such as terrorism and war. Critical infrastructure protection is therefore mainly studied within this scope. Intelligence and security services are also focused on these threats. However, environmental events and technological failures can also have disastrous effects on infrastructures. Subsequently, 'thinking about the unthinkable' for organisations, firms and society has never been so challenging. Especially since we live in a

global society where boundaries are becoming more and more blurring.

The focus on resilience offers new opportunities. Also, the importance of systems instead of entire sectors offers more hand-on working procedures. Gosselin, Leysen & Verbeke (2007) conducted research related to the question 'What can threaten our prosperity?' In answering this question we must study our weaknesses. Culture, institutions and democracy have an important position among intangible assets (e.g. corporate culture, ethics, consultation…) of highly developed industrial countries (Kay, 2004, 37; Gosselin, Leysen & Verbeke, 2007, 4). This means that several invisible characteristics are associated with protection our economic potential and the protection of critical infrastructures. This knowledge is often overlooked. Nevertheless, if the interdependency between infrastructures is a priority, these elements should also be included.

Let us examine the different aspects of security, which will clarify the difficulties critical infrastructures are facing. Our society faces potential and existing threats that can be characterized on several levels (Crawford, 2012). First, we emphasize crime-related risks and threats. These can be acts of terrorism, organised crime … Second, technological threats are becoming more and more apparent. Third, economic risks are a vast reality. Fourth, environmental threats often remind us of our vulnerability. Fifth, we are also facing scientific risks, since certain inventions and study results can be much wanted items. All these events occur both locally and globally.

The problem of this changing landscape of security is that criminology studies mostly focus on the first characteristic. However, we can ascertain blurring boundaries between all these levels. The 9/11 terrorist attacks are a perfect example of how all these security facets can be intertwined. Criminologists should ask themselves two important questions: 'Is our knowledge of security still applicable in this global and multidimensional reality?' and 'Shouldn't we be focussing more on this changing landscape and aim at multidisciplinary security studies that focus on an evaluation of disruptive events, both global and local?'

In our opinion these questions should be discussed amongst scientists and practitioners. If we want to search for new directions, an interplay between empiric science and applied science is of the utmost importance.

Conclusion

If we want to increase our knowledge on critical infrastructure protection, we need to increase academic research. The concepts of critical infrastructures, protection, resilience, preparedness and response need to be further defined. We must also focus on alternative methodologies (Pashley & Cools, 2013) in order to examine the underlying characteristics of uncertain disruptive events. Subsequently, a theoretical framework should be developed, based upon empirical studies. Security and protection in the 21st century requires an alternative and broad scope. Uncertainties can seem unmanageable. However, creative thinking can help to change old directions into new opportunities.

References

1. *Chew, D.H. (ed.) (2008). 'Corporate Risk Management', Journal of Applied Corporate Finance (Book Edition). Columbia, Columbia University Press.*
2. *Coess – Aproser (2013). The socio-economic value of private security services in Europe. Fourth White Paper on Private Security, Wemmel, CoESS.*
3. *COESS (2012a). Critical infrastructure security and protection: the public-private opportunity, White Paper and guidelines by CoESS and its working committee. Wemmel, CoESS.*
4. *COESS (2012b). Critical infrastructure private guarding company requirements checklist,Wemmel, CoESS.*
5. *COESS (2011). Private security services in Europe: facts and figures, Wemmel, CoESS.*
6. *Cools, M., Dassen, K. Libert, R., Ponsaers, P. (eds.) (2005). De Staatsveiligheid: essays over 175 Veiligheid van de Staat, Brussel, Politeia.*
7. *Crawford, A. (2012). The evolving concept of security: mapping the dynamics of security in Europe, Leeds, unpublished document.*
8. *Davidovic, D. Kesetovic, Z., Pavicevic, O. (2012). National critical infrastructure protection in Serbia: the role of private security, Journal of Physical Security 6, n°1, 59-72.*
9. *EUROPEAN COMMISSION STAFF WORKING DOCUMENT (2013). A new approach to the European Programme for Critical Infrastructure Protection: making*

European critical infrastructures more secure, Brussels, (28.08.2013).

10. *EUROPEAN COMMISSION STAFF WORKING DOCUMENT (2012). On the review of the European Programme for Critical Infrastructures Protection (EPCIP), Brussels,(22.06.2012).*
11. *EUROPEAN COMMISSION (2013), 'Critical Infrastructures'. URL: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm.(20.06.2013).*
12. *EUROPEAN UNION COUNCIL DIRECTIVE (2008). 'On the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection', Official Journal of the European Union,(23.12.2008).*
13. *EUROPEAN UNION, Counter-Terrorism Strategy (Brussels 30th November 2005). URL: http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf. (20.06.2013)*
14. *EUROPEAN UNION (2007-2013). Specific programme: prevention, preparedness and consequence management of terrorism. URL: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33262_en.htm. (20.06.2013)*
15. *Flammini, F. (ed.) (2012). Critical infrastructure security: assessment, prevention, detection, response,Billerica, WIT Press.*
16. *Goetz, E., Shenoi, S. (2010). Critical infrastructure protection,New York, Springer.*
17. *Gosselin, P.G., Leysen, J., Verbeke, T. (2007). 'Protecting a nation's economic*

potential: proposal for a scientific research agenda',European Journal of Intelligence Studies, N°1, 3-21.

18. *Hokstad, P., Utne, I., Vatne, J. (eds.) (2012). Risks and interdependencies in critical infrastructure protection,London, Spinger-Verlag.*
19. *HOMELAND SECURITY, 'National Infrastructure Advisory Council'. URL: http://www.dhs.gov/national-infrastructure-advisory-council.(20.02.2013)*
20. *Johnston, L., Shearing, C.D. (2003). Governing Security: Explorations in policing and Justice, Londen, Routledge.*
21. *Kahn, H. (1980). Thinking about the unthinkable in the 1980s,New York, Hudson.*
22. *Khatta, R.S. (2008). Risk Management,New Delhi, Global India Publications Pvt Ltd.*
23. *Kay, J. (2004). The truth about markets: why some nations are rich but most remain poor, London, Penguin Books.*
24. *Lavoy, P.R., Saga, S.D., Wirtz, J.J. (2000). Planning the unthinkable, Cornell, Cornell University Press.*
25. *Lewis, T.G. (2006). Critical infrastructure protection in Homeland Security: defending a networked nation,New Jersey, Wiley Interscience.*
26. *Lindsay, J. (2005). Dearly Devoted Dexter, New York, Doubleday.*
27. *Linkov, I., Wenning, R.J., Kiher, G.A. (eds.) (2007). Managing Critical Infrastructure Risks, Dordrecht, Springer.*
28. *Lopez, J., Setola, R., Wolthusen, S.D. (eds.) (2012). Critical infrastructure protection: information infrastructure models, analysis and defence,Berlin Heidelberg, Springer-Verlag.*

29. *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.*
30. *NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (2009). Critical Infrastructure Resilienc, Research Report, USA.*
31. *Papa, M., Shenoi, S. (red.) (2008). Critical infrastructure protection 2, New York, Springer.*
32. *Pashley, V., Cools, M. (2013).'Breaking boundaries. Collapsing the dark side of researching criminology',in: Beyens, K., Christiaens, J. et al (Eds), The Pains of Doing Criminological Research, Criminological Studies, Brussels, VUBPress, 161-180.*
33. *PRESIDENTIAL POLICY DIRECTIVE (2013). 'Critical Infrastructure Security and Resilience'. URL: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.(21.06.2013)*
34. *Richards, J. (2010). The art and science of intelligence analysis, Oxford, Oxford University Press.*
35. *Shulsky, A.N., Schmitt, G.J. (2002). Silent Warfare: understanding the world of intelligence, Virginia, Potomac Books.*
36. *Steenlant, J., Ven, C. (2005). 'Het belang van de inlichtingendiensten voor de bescherming van het economisch potentieel van onze bedrijven', in: Cools, M., Dassen, K., Libert, R., Ponsaers, P. (eds.) (2005). De Staatsveiligheid: essays*

over 175 Veiligheid van de Staat, Brussel, Politeia.

37. *Thissen, W.A.H., Herder, P.M. (2003). Critical infrastructures: state of the art in research and application, Kluwer's International Series: Operations Research & Management Science, Dordrecht, Kluwer.*
38. *HOMELAND SECURITY (2006). 'United States' National Infrastructure Protection Plan 2006'. URL: http://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf. (15.09.2013)*
39. *Van Nevel, H. (2010). De bescherming van kritieke infrastructuren: een publieke of overheidstaak? Een casestudy in de Zeebrugse Haven. Master Dissertation. Ghent University. Unpublished Document.*
40. *White, A. (2011). 'The new political economy of private security'. Theoretical Criminology 16, n°85, 85-101.*
41. *White, A. (2010). The Politics of Private Security: Regulation, Reform and Re-legitimation, New York, Palgrave Macmillan.*