

PROTECTION OF CRITICAL NATIONAL INFRASTRUCTURE: CHALLENGES FOR THE PRIVATE SECURITY SECTOR

Branko Mihaljević

University of Applied Sciences Velika Gorica, Croatia

Abstract

The world in the new decade comes with heavy baggage from the previous periods. It is important to emphasize that these events opened a number of important new safety trends worldwide which will be facing us in the future: the emergence of new urban violence, rising food prices and an increase in hunger worldwide, an increase in migration processes from areas of endangerment and low resources towards those rich in resources, an increase in intolerance and ethnic violence in developed societies, the development of various movements and activities which create new security challenges for modern states, but also the human community as a whole, more frequent natural disasters, threats to critical infrastructure, and similar occurrences. It seems that in the future we will be facing the challenges that have arisen in the past, but for which we have not found a solution to reduce or eliminate them, and new challenges that could significantly jeopardize the many forms of modern life. One of the negative consequences of such a development could be our feeling that the challenges are becoming more complex and our political institutions do not have enough power to deal with them, which could initiate a search for new answers that do not necessarily have to mean progress but rather the opposite. If we add intense terrorist attacks and threats out of control even in traditionally resilient societies to all of the above, then the times in which we live show an ever greater need for the involvement of the private security sector in the protection of critical infrastructure, people, assets and operations at all levels of the societal organization. The solution lies in the good communication and cooperation between the public and private security sector, where the private security serves only a preventive role.

Keywords: protection, critical infrastructure, private security.

Address for correspondence: Branko Mihaljević, University of Applied Sciences Velika Gorica, Zagrebačka c. 5, Velika Gorica, Croatia, e-mail: branko.mihaljevic@vvg.hr.

1. INTRODUCTION

1.1. Identification and description of the research problem

The protection of critical infrastructure is complex and is increasingly becoming a topic in the Republic of Croatia. The need for a strategic, dynamic and proactive approach is needed primarily in the process of planning critical infrastructure protection in the conditions of various and numerous forms of crisis and emergency situations. In the late 1980s, the term “infrastructure” was a reference point for the creators of public policy and security. Today, the phrase “critical infrastructure” has become a special subject of interest in numerous analyses relating to terrorism and internal security of nation states.

The complexity of crisis and emergency situations, especially the recognition that their emergence could endanger and jeopardize some critical capacities that are irreplaceable in the regular state and society functioning process, have obliged most countries to develop and establish various measures and activities to protect critical infrastructure. In that sense, the Republic of Croatia adopted the Critical Infrastructures Act in 2013, and the government of the Republic of Croatia adopted the Decision on the designation of sectors from which the central state administration bodies identify national critical infrastructures, and the list determining the order of critical infrastructure sectors. Under the aforementioned law, the National Protection and Rescue Directorate in 2013 adopted the Ordinance on Risk Assessment

Methodology for Critical Infrastructure Protection. The Republic of Croatia has taken over the *acquis communautaire* contained in Council Directive 2008/1/114 / EC of 8 December 2008 on the identification and definition of European Critical Infrastructures and the assessment of the need to improve their protection. Although these normative acts represent a good foundation for the establishment of various measures and activities of critical infrastructure protection in the Republic of Croatia, it has not yet established an integral protection system, due to the inertia of state institutions. Additionally, due to the lack of systematic research into critical infrastructure protection issues in Croatia and among the security experts as their stakeholders, there are no publicly available insights into the current problem of systematic critical infrastructure protection as a basic prerequisite for its development. Therefore, the following research problem can be justified:

- Lack of up-to-date knowledge regarding the current state of affairs, and the needs and possibilities of enhancing the protection and establishment of the national critical infrastructure protection system, as well as the role played by the private sector in the security system.

1.2. Research objectives

The aim of the preliminary research on the challenges of the private security sector in the protection of critical national infrastructure is to determine the up-to-date understanding of the current state of affairs, and the needs and possibilities for enhancing critical infrastructure protection based on the analysis of available documents combined with the opinions of experts on the theoretical and practical business issues related to critical infrastructure protection and the role of the private security sector in the critical infrastructure protection system.

1.3. Research hypothesis

As this is the first and preliminary study dealing with the protection of national critical infra-

structure and the challenges facing the private security sector during its protection in the Republic of Croatia, no pre-defined research hypothesis will be set.

2. DEFINITION OF CRITICAL INFRASTRUCTURE

Immediately after the terrorist attacks in September 2001, critical infrastructure has become an important and essential part of national security, and its protection is one of the priorities of each country.

There are many critical infrastructure definitions, but all of them, in principle, refer to assets and facilities which are crucial to the continuous functioning of the economy and society. For the purposes of this paper we have selected several definitions.

The United States: "Critical Infrastructure and Basic Resources is a term that refers to the wide range of assets and facilities needed for the day-to-day functioning of the social, economic, political and cultural systems in the United States. Any break in the critical infrastructure elements poses a serious threat to the overall functioning of these systems and can lead to property damage, human casualties and significant economic losses"[1].

Australia: "Critical Infrastructure represents those physical objects, supply chains, IT sectors and communications networks that would be severely affected or severely disabled for a long time, which could subsequently have a significant impact on the nation's social or economic well-being, or affect Australia's ability to maintain national defense and provide national security"[2].

The European Union: "Critical Infrastructure - ECI" implies a critical infrastructure located in the territory of a Member State whose disturbance or destruction would have a significant impact on at least two Member States. The significance of the disruption in the functioning of the critical infrastructure elements is assessed on the basis of interdependence criteria. This implies the effects

of cross-sector dependence on other types of infrastructure“ [3].

Generally speaking, definitions of the critical infrastructure framework in many countries vary and depend on a variety of specific conditions, ranging from political circumstances to geographic locations.

Nowadays, the world economy is still undergoing major financial challenges, but in the field of national and public security within the context of critical infrastructure protection, large assets are

invested with a steady growth trend, which denotes the crucial importance of critical infrastructure. Table 1 shows the consumption of some countries worldwide regarding critical infrastructure protection with projections for 2018 in billions of dollars [4].

The latest JP Freeman’s market research estimates that 38% of integrated systems are based on network technologies. This trend intensified the recession and the desire to rationalize the system, as well as improve the functional aspects of security.

Table 1. Consumption regarding Critical Infrastructure Protection (\$ Mr)

Country	Consumption for 2008	Projection for 2018
USA	707.7	993.3
China	86.5	183.4
UK	87.1	112.3
France	81.1	104.5
Germany	67.3	90.1
Saudi Arabia	45.3	84.5
Japan	61.6	80.4
India	34.1	70.7
North Korea	35.2	54.4
Turkey	23.1	47.7
Italy	38.2	46.9
Australia	31.6	45.8
Canada	24.8	33.9

3. CRITICAL INFRASTRUCTURE PROTECTION – THE USA AND THE EU EXPERIENCE

Both in the United States and the EU there were different attitudes regarding the risks and threats that could endanger the general security of nations and critical national goods. But regardless of such attitudes, a two-tiered standpoint was soon formed:

- Which resources represent a critical infrastructure?
- What measures are needed to protect them?

In the United States, the resources identified as critical infrastructure mainly include: electricity

supply system, financial and banking system, telecommunications, storage and transportation of gas and petroleum products, water supply system, transportation sector, industry, emergency services, police, fire brigade, and the sector responsible for the continuity of government functioning [5].

The second systematization is focused on 11 sectors, including water, agro-industry and food, emergency services, public health, industry, energy, telecommunications, transport, finance and banking, chemical and other hazardous substances, postal services and delivery [6].

In the National Strategy for the Protection of Critical Infrastructure and Key US Material Go-

ods, the basic elements of infrastructure are identified which need to be protected in various types of crisis situations.

Key assets include national cultural goods, nuclear power plants and embankments and levees. In addition, fundamental ministries have also been identified which have to assume responsibilities for the protection of national assets. The Ministry of Homeland Security, the Ministry of Defense and the Ministry of the Interior are the main competent authorities, but the Ministries of Energy, Justice, State Administration, Agriculture, Health, Finance and the Environmental Protection Agency likewise have their responsibilities [7].

The EU has also made significant efforts in analyzing critical resources and has taken appropriate measures in their protection.

Historically, on 24 June 2004, the Council of Europe asked the Commission to prepare a comprehensive strategy for critical infrastructure protection. In its response, on 20 September 2004, the Commission adopted a document dealing with terrorism as a potential threat. The document also received its official title "Protecting Critical Infrastructure in Combating Terrorism" which suggests clear guidelines on what would improve prevention, readiness and response to terrorist attacks affecting the critical infrastructure in Europe.

The Council accepted the Commission's intention to propose the European Critical Infrastructure Protection Program - EPZKI / EPCIP, and agreed on the establishment of the Critical Infrastructure Intelligence Information Commission - IMUKI / CIWIN.

In October 2005, the Commission adopted the Green Paper on the European Critical Infrastructure Protection Program, which outlines its political views on the establishment of protection programs.

The 2005 Commission's Decision on the Judiciary and Internal Affairs Council called for a draft of the European Critical Infrastructure Protection Program.

In the following years, the Council of Europe Directive and the EU Internal Protection Strategy were adopted. During 2012 the programme and a revision of the directive were also drafted.

The aim of European policy in this area is to ensure an adequate and equal level of protection for the installations of selected critical infrastructure. This is only enforceable on the basis of a common European framework for critical infrastructure protection. The EU's concern for the critical infrastructure of the member states stems from the danger that destruction or disruption of some critical infrastructure in a single EU country could directly affect other Member States. In such cases, protective measures are as powerful as is their weakest link.

In this sense, the EU defines European Critical Infrastructure as an infrastructure consisting of physical resources, services, devices, IT sector, network security and infrastructure, economic and social values of: 1) two or more member states, 2) three or more member states.

The European Commission has also identified crucial areas of critical infrastructure: energy, IT, water, food, finance, public order and security, transportation safety, chemical and nuclear facilities, space and scientific research.

4. PUBLIC-PRIVATE PARTNERSHIP IN THE SECURITY SYSTEM

Contemporary security threats and hazards have new features that are subject to change and adaptation to new conditions, changing forms and instruments of activity and are difficult to foresee. Given these properties, it is very difficult to develop responses that guarantee effective protection, which is a major challenge for modern societies. The struggle against such threats is a primary challenge for modern societies. However, if we take into consideration all of their features that are constantly evolving in contemporary conditions, it is clear that the state can not lead an effective struggle without including all elements of national power, without the help of the private sector and its citizens [8].

The model of co-operation between the state and the security sector in combating modern security threats can be developed through a form of public-private partnership that gains more and more importance. For the development of effective instruments to combat modern security threats and hazards, the key contribution and joint action of all these factors - the private sector and the citizens - are crucial.

4.1. The importance of public and private security partnerships

The protection of critical infrastructure is one of the most optimal areas for establishing partnerships between the public and private sectors, given their very often public - national or local character, which can be translated into public ownership or public management or public goals. It is unacceptable to continue to distinguish between the public and private security sector because the private security sector is often given the “commercial” moniker, since its services are paid for. Public sector security services are also being charged and are more expensive than the private sector. This is however less visible to the general public, as those expenses run through the state budget.

In the European Union there are trends regarding the redistribution of the public sector’s responsibilities in favor of the private security sector, which undoubtedly represents the directions for further development of the private security sector. The fact is that in every single European country there is an ever-growing presence of private security companies in the public protection services. The case studies that will be presented in this paper clearly show that well-defined, efficiently managed and well-controlled partnerships between the public and private entities without any doubt increase the security of critical infrastructure.

The experience of public-private partnerships in the field of security in the EU countries shows that, for the sake of efficiency, these partnerships must be based on the following principles:

- Open dialogue between the competent public institutions and private security providers.
- Clear guidelines on the role of each partner individually.
- Clear legal and contractual framework of cooperation.
- Communication mode for the exchange of relevant information.
- Regular process moments and necessary corrections and improvements whenever and wherever they may be needed.

It is important to emphasize that there must be constant interaction within the formally mandatory common structures that are specifically established in the context of the partnership.

For the fulfillment of all the criteria, optimal success and efficiency of the partnership between the public and private security sector in the field of critical infrastructure protection, it is vitally important for every partner to fully understand their role, responsibility and limitations. Due to the lack of knowledge of these elements, the partnership between the public and private sector in the field of critical infrastructure protection throughout the EU is still not sufficiently developed and is not used to maximize its potential [9].

4.2. Examples of good practice of police and private security partnerships

In all countries of the world, the security sector is fairly specific, often wrapped in “secrecy” and largely operates out of the public eye. Governmental structures today still find it difficult to relinquish a centuries-old monopoly over the use of force, regardless of the important changes in the society, which necessarily require the redistribution of competencies between the public and private sector, especially in the security sector. In the early 2000s, the London City District Police Department, responsible for securing the financial institutions in the capital of the United Kingdom, which were constantly a potential target for terrorists, established the Griffin project. The project

consists of four key activities:

- Days to raise awareness of private security sector officials organized by the local police. They focus on questions on how to identify, respond, and report suspicious activities such as terrorist reconnaissance of potential targets for an attack.
- Internet education for knowledge acquisition that keeps the sufficiently high levels of interest and training among the participants in order to obtain official accreditations.
- Regular communication between the police and private security officers, whether through videoconferencing, SMS messages or electronic mail, to ensure that intelligence and accident reports are timely forwarded.

Almost half of the private sector security sector in the UK, especially in seaports and airports, has completed the Griffin project and now has special security engagements. The project has also attracted attention in the United States, Australia and Singapore.

In numerous German cities, private security companies have united with the local police in terms of shared information they then subsequently supply to the police force. While driving the city streets and performing their daily activities, members of private security companies can detect suspicious persons or vehicles or see any other illegal activity, and such information is immediately forwarded to the control center of their company, which then forwards this information to the police forces for further assessment and possible dealing with. Such projects have proved to be very efficient and are very much accepted by the police forces in Germany. Through the involvement of private mobile patrols, the number of surveillance vehicles on the streets has doubled overnight in relation to the number of police patrol vehicles in some German cities.

In Spain, the police recognized that private security officials are valuable resources. That is the reason why all contracts signed between the private security companies and their clients have to be re-

gistered with police authorities, including the data pertaining to the number of staff involved in the provision of services. The police also established an open telephone line to enable them to communicate quickly with private security companies.

The public-private partnership in Belgium is formalized, regulated by official laws and regulations and if a change in government occurs, only the political priorities in the national security system are altered and adapted to new policies. Exchange of information is systematically organized and works at a high level. Both sectors obtain information from a single operations-communications center of the federal police. Reductions to public spending imposed the need to integrate the private sector and redistribute jurisdiction, so the private security sector was also engaged in the following activities: nuclear power plant security, embassies, protection of public buildings, and patrols in critical zones, money transfer and similar operations. Unlike the Anglo-Saxon model, prerequisites for private security sector engagement are much more rigorous. The process of integrating the private security sector into police affairs has taken a step by step approach, however, a conclusion can be drawn that the public-private partnership is an actual need of the state, and does not depend upon the good will of the police structures. The results of this co-operation, their efficiency and effectiveness are visible and have a significant impact on the increase in the citizens' security, although a certain part of the police hierarchy still expresses a certain amount of distrust in the public-private partnership.

The security sector has been experiencing a sort of evolution in the Republic of Croatia over the past two decades. Since its very beginnings, when the protection of persons and property mainly involved the simplest guard duties, nowadays certain segments of private protection represent a highly developed activity. This is primarily the case with the operations related to technical protection, which develop on a daily basis following the development of various technologies, which is evident above all when it comes to the protection of

financial institutions and the transfer of money and other valuables. Security guards, their employers, trade unions, and the guild of security guards need to agree on the establishment of the Chamber as much as possible, since the law foresees the founding of the Chamber, but nothing practical has been done about it.

The activity of the Chamber should be regulated by additional regulations. In certain ways, this has been left to the professionals themselves. In proportion with the development of private protection as a professional activity, its role and importance within the security sector are likewise growing. Today, in line with current security trends and standards of airport security worldwide and in the EU, the internal security services of airports or external security companies take full responsibility for some very sensitive operations which have been previously done by the police, such as the control and prevention of unauthorized access to safety-sensitive and protected areas of the airport, as well as the security checks of travellers' luggage and things, and security checks of passengers and their hand luggage. The Ministry of the Interior considers security guards to be a very important part of the overall security sector. Since private security activities protect those goods whose protection is not provided by the state, i.e. they fall outside the purview of the state; the importance and the role of this business activity are obvious. Regarding the status of private security as a professional activity, despite the ubiquitous economic problems that affect the entire economy, including the sector of private protection, which is primarily reflected in the low salaries of security guards, it is necessary to continuously implement the measures to improve the activities of security in order to realize the highest possible amount of general social security. The private security sector strengthens its capacities every day. The numbers of licensed security guards are impressive and open up opportunities for establishing different models of co-operation. The Ministry of the Interior has an important task in helping and directing the overall system of protec-

tion, and in particular encouraging closer cooperation in this area.

5. PRIVATE SECURITY IN CRITICAL INFRASTRUCTURE PROTECTION IN THE REPUBLIC OF CROATIA

Critical infrastructure protection is one of the key national security priorities and serves to protect the core values of society. Extensive attention has to be paid to the protection itself, which is extremely difficult because it is impossible to devote time and efforts to the protection and preservation of critical infrastructure without analyzing the role and contribution of the private security sector, which is a fundamental element in the protection and preservation of critical infrastructure. By joining the European Union, the Republic of Croatia has been obliged to align the security sector, with an emphasis on the need for the harmonization of Croatian legislation with the European regulations concerning the issues of critical infrastructure protection. This is a term that has not been used in Croatia for a very long time, although it covers essentially what we consider to be "objects of significance for defense".

When it comes to securing critical infrastructure facilities, it is essential to create a detailed protection plan based on previous safety analyses and risk assessments. The purpose of security is the protection of critical infrastructure where it is necessary to ensure the functionality, business continuity and uninterrupted distribution of a particular service or commodity, and in particular to prevent any disruption of critical infrastructure, either through targeted activity or by accident. Critical infrastructure is thus protected through its own security systems, private security systems and the employees of the Ministry of Interior and their joint cooperation. In extreme cases of particular threats to critical infrastructure, the protection activities may include the military [10].

Unfortunately, the security needs of critical infrastructure and the present state of affairs differ greatly from the professionalism and total security

when it comes to a large number of critical infrastructure facilities. In most cases, critical infrastructure security is provided by the organization itself, mostly involving guards with quickly completed or little training, who have neither the qualities needed to perform their professional duties, nor the motivation or the feeling for proper conduct, often failing to act in accordance with mandatory actions, which subsequently results in criminal offences or misdemeanors on critical infrastructure facilities. They also do not alert the police officers in time, which is why the aforementioned criminal offenses or misdemeanours become the black hole of criminality as there is no possibility of capturing and prosecuting perpetrators, meaning that there is an extremely large possibility of a direct threat to the country's national security occurring [11].

Furthermore, in a large number of facilities no security system has been established at all, and the security is provided through occasional rounds made by the organization's employees and occasional police officers' visits, meaning that there is an even greater chance of an adverse event [12].

Likewise, for unknown reasons there is still some intolerance and stereotypes in a particular group of senior police officers and private security employees, whereby they refuse to share information and work together, leading to a bleak outlook regarding the security of critical infrastructure facilities, but also in other cases where joint cooperation is necessary.

Due to all this, it is important to raise the awareness regarding critical infrastructure security to the highest level, both for the head of the facility, as well as for the guards, security officers, police officers, employees of the organization and other citizens, and consider this to be a priority in the normal functioning and maintaining of the overall national security of the state.

Every private security officer should apply the powers within the scope of his or her duties, i. e. at a given moment assess the threat and use their competence in accordance with the type of the

threat, which would enable them to successfully accomplish the goal. In such a case, their authority is used in accordance with the Private Security Act and the authority as such must be proportionate to their need, while the employees of private security companies are obliged to respect the fundamental human rights guaranteed by the Constitution of the Republic of Croatia.

The professional standpoint is that the protection of space, facilities, property and persons should be carried out by professional security companies which train and educate their employees in accordance with the rules of their profession, taking into account their professionalism and expertise. The most important thing is that such security companies educate and train their employees on a daily basis, in compliance with the needs of private security sector, new trends in security systems and operational methodology, as well as providing security and protection services using able and qualified personnel at all times [13].

The current state of affairs is such that the market dictates the trends, so the demand is still the greatest for those security companies that will provide perimeter security utilizing the lowest possible resources, with no regard for their competence and quality. The private security sector in the Republic of Croatia is a relatively new field and the struggle between security companies regarding the takeover and domination in the security systems occurs on a daily basis.

6. CONCLUSION

The Republic of Croatia has systematically established a public - private partnership in the security sector. The field of private security has been legally regulated, and in the recent years there has been a lot of strenuous, systematic and organized effort by the Guild of Security Guards and the Ministry of Interior on the study of foreign experiences and their implementation into national regulations and standards. However, so far this has only been a very good precondition for the faster professionalization of this activity and an increase

in the quality of services. While all this is not dependent only on the employers and employees in the private security sector, the greatest responsibility for training and licencing lies with them since the state has de facto completed their own part of the bargain – it adopted legislative acts, issued training authorizations, it has examination committees and it has fulfilled other conditions. The extant normative – legal framework in the Republic of Croatia represents a good foundation for a more active involvement of the private security sector in all emergency situations.

By researching this topic, the author has shown the close links between critical infrastructure and private security employees, whereby it is apparent that the critical infrastructure protection system is not able to function normally, or even function at all without the private security sector.

Although underrated and underestimated in most cases, the employees of private security companies have become the cornerstone and the foundation of security sector's functioning, bearing heavy responsibility and concern for the national security of the Republic of Croatia and its citizens. The shortcomings are numerous and a lot of time will pass before the status of private security is raised to the level it has in more developed countries, as we need to be aware this is a longterm process which needs to go hand in hand with the modernisation, innovations and other trends. Taking into account all aspects of the issues we analysed in this paper, we can draw a uniform conclusion that critical infrastructure can be adequately protected only if private security sector is incorporated into the protection system alongside state institutions.

7. REFERENCES

1. Murray, A.T, Grubestic, T.H. (2012). Critical infrastructure protection: The vulnerability conundrum, *Telematics and Informatics*, 29 (1).
2. Moteff, J. (2005). Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences, Congressional Research Service, Washington, DC.
3. Mihaljević, B. et.al. (2013). Impact of Critical Infrastructure Ownership on the National Security of the Republic of Croatia, National critical infrastructure protection – regional perspective. Zoran Keković, (ur.). - Beograd : University of Belgrade - Faculty of Security Studies, 155-166.
4. Radvanovsky, R. (2006). Critical Infrastructure – Homeland Security and Emergency Preparedness. New York, Taylor & Francis Group.
5. Critical Infrastructure Emergency Risk, Management and Assurance, Emergency Management Australia, A Division of The Attorney General's Department, (2003).
6. National Strategy for the Physical Protection of Critical Infrastructure etnes and Key, URL: <https://www.hsdl.org/?view&did=1041>.
7. Cvrtila, V. and Perešin, A, (2013). Razvijanje novih modela sigurnosnog djelovanja. *Glasnik AKD zaštite*, 7/8 (8): 7-11.
8. Hamidović, H. (2012). Objektivne opasnosti – subjektivna mjerila, *Open Info Trend*, Zagreb, accessed 27 March 2017, URL: <http://www.infotrend.hr/clanak/2012/>.
9. Kulišić, D. (2008). Mjere sigurnosti od terorističkih i inih zlonamjernih ugroza kritične infrastrukture (II. dio). *Sigurnost*, 50 (4): 343-364.
10. Matika, D., Poljanec-Borić, S. (2009). Kritična infrastruktura u Hrvatskoj/prema novom sustavu sigurnosti i zaštite – Zagreb. Institut za istraživanje i razvoj obrambenih sustava Ministarstva obrane RH- a, Institut društvenih znanosti "Ivo Pilar".
11. Palačić, D. (2010). Zaštita osoba i imovine. Zagreb: IPROZ.
12. Krajčak, I. (2014). Zaštitarstvo je važan dio mozaika sektora sigurnosti, *Zaštita*, 4/14.
13. Zakon o kritičnim infrastrukturama, NN, 56/13. – Critical Infrastructure Act, OG 56/13

ZAŠTITA KRITIČNE NACIONALNE INFRASTRUKTURE: IZAZOVI ZA PRIVATNI SEKTOR SIGURNOSTI

Sažetak

Svijet u novo desetljeće ulazi s mnogobrojnim opterećenjima koja su nastala u prethodnim razdobljima. Važno je naglasiti kako su ti događaji otvorili nekoliko važnih novih sigurnosnih trendova u svijetu s kojima ćemo se suočavati u budućnosti: pojava novog urbanog nasilja, porast cijena hrane i porast gladi u svijetu, porast migrativnih procesa iz područja ugroženih resursa prema područjima koja njima obiluju, porast netolerancije i etničkog nasilja u razvijenim društvima, razvoj različitih pokreta i aktivnosti koji na različite načine stvaraju nove sigurnosne izazove suvremenim državama, ali i ljudskoj zajednici u cjelini, sve učestalije prirodne nepogode, ugrožavanje kritičnih infrastruktura i sl. Čini se kako ćemo se u budućnosti suočavati s mnogobrojnim izazovima koji su nastali u prošlosti, ali nismo pronašli rješenje za njihovo smanjivanje i eliminaciju te s novim izazovima koji bi značajno mogli ugroziti mnoge oblike suvremenog života. Jedna od negativnih posljedica takvog razvoja mogao bi biti naš osjećaj da su izazovi sve složeniji, a da naše političke institucije nemaju dovoljno moći za njihovo rješavanje, što bi moglo pokrenuti traženje nekih novih odgovora koji nužno ne moraju značiti napredak. Upravo suprotno. Ako se svemu navedenom dodaju i sve intenzivniji teroristički napadi i prijetnje koje izmiču kontroli čak i tradicionalno otpornim društvima, onda se u vremenu u kojem živimo više nego ikada nameće potreba većeg uključivanja privatnog sektora sigurnosti u zaštitu kritične infrastrukture, osoba, imovine i poslovanja na svim razinama organizacije društva. Rješenje je u dobroj komunikaciji i suradnji javnog i privatnog.

Ključne riječi: zaštita, kritična infrastruktura, privatna sigurnost.