KEY QUALITY CRITERIA FOR PRIVATE SECURITY IN THE PROTECTION AND RESILIENCE OF CRITICAL ENTITIES

Sanja Kermetchieva

Abstract

Security is a key concern in societies worldwide. Moreover, societies are dependent on the continual operation of critical infrastructure i.e., critical entities (sectors: energy; transport; banking and finance; water; health; digital infrastructure; food; public administration; space) that are key and vital for national security, economic vitality, and public health and safety, and relevant regionally and globally, due to its physical, cyber, geographic, and logical interdependency. However, in the dynamic security context, there are risks and threats to critical infrastructure with potential cross-sectoral or cross-border nature, including accidents, natural disasters, public health emergencies, such as a pandemic, and hybrid threats, including terrorist offences, criminal infiltration, and sabotage. Hence, strengthening the security and resilience of critical infrastructure is high on the agenda of authorities.

Private security companies are part of the security continuum and have always complimented state security efforts. Moreover, the increasing security risks to critical infrastructure driven by natural and geopolitical events have increased the role of private security services, and security companies and personnel are an integral part of Critical Infrastructure Protection. The main tendency of this paper will be to elaborate on the EU Directive on the resilience of critical entities 2022/2557 of 14 December 2022. The theoretical explication will cover the wider critical infrastructure protection and resilience concept. The main focus will be to analyze the role of private security in critical infrastructure protection. Furthermore, this paper will elaborate on the sector-specific Standard EN 17483, Private security services -Protection of critical infrastructure, which illustrates requirements for quality in organizations, processes, personnel and management. The final goal will be to systematize the body of knowledge about the key quality criteria of private security in the protection and resilience of critical entities.

Keywords: critical infrastructure protection and resilience, private security, quality

1. MEGA TRENDS, CHALLENGES, THREATS, AND HAZARDS SHAPING THE MODERN SECURITY LANDSCAPE

The world in the 21st century is witnessing key global trends that are affecting economic, social, political, environmental, and cultural aspects of life, causing fundamental changes in humanity. There is an evident remake of (geo)politics, and a completely different political and strategic context. Euromonitor International had outlined some of the latest geo-political realities, such as the pandemic of COVID-19, the war in Ukraine; the surge of oil and gas prices (first due to the post-pandemic global economic recovery, and then supply shocks coming from Russia’s invasion of Ukraine); multi-decade high inflation; escalating
tensions between the two largest economies, US and China, etc. (Hofer et al., 2023). At the same time, globalization remains to be one of the key mega trends, together with the growing urbanization trend. Starting from 2008 more than 50% of the world’s population lives in urban areas and in Europe this figure is close to 75% and the trend is expected to continue (Baker and Broughton, 2018). Demographic transformation with considerably increased life expectancy, shrinking working-age population, migration on a large scale and regional/local migration are changing the workforce. Not only the people’s movement but also the movement of capital/money are reflecting the dynamic and continually changing environment. The world is experiencing a third (non)industrial revolution, with emerging technologies and innovation, digitalization, and artificial intelligence, that are marking a new era of transformation. Moreover, the advances in genetics, biotechnology, nanotechnology, robotization and computerization are shaping a new global reality and are considered the pillars of the new economic paradigm. At the same time, climate change remains a defining issue of the 21st century and one of the most dramatic stressors impacting nature and people’s health with global scope and unprecedented scale.

In this complex world, all the key mega trends are bringing both opportunities and challenges for societies and are creating a dynamic threat landscape. New challenges facing societies nowadays are the rise of the digital economy, fragmentation of the internal markets, the growing impact of climate change, security threats, etc. And all together, the contemporary trends and challenges create an ambience for the development of new threats and hazards to humanity.

The US Department for Homeland Security had identified threats and hazards, both natural and man-made (deliberate or accidental), specific to a country, or region, or with a global influence, such as: climatological, hydrological, meteorological events (extreme temperatures, floods, tropical cyclones, storms); geophysical events (earthquakes, tsunamis); pandemics; technological and industrial accidents (industrial fires, chemical spills); unscheduled disruptions (large scale power outages); criminal incidents and terrorist attacks; cyber incidents; supply chain attacks and foreign influence operations (to spread misinformation or undermine democratic processes), etc. At the same time, the European Union has accepted an all-hazards approach, referring to natural or man-made, accidental, or intentional, such as: natural disasters, climate change and evolving hybrid and terrorist threats. Moreover, at the EU level, it is emphasized that terrorist activity is increasing and becoming more diffuse, with attacks that are simple, opportunistic, or complex and well organized.

This ambience is affecting the life of people and societies and is dramatically shaping the security architecture around the world. Hence, security has been, is, and continues to be one of the concerns of greatest importance in societies worldwide. Furthermore, the highest priority of societies is the security of vital assets, systems, facilities, networks, and other elements of the society that provide lifeline functions of the society and of its citizens, identified as critical infrastructure.

2. CRITICAL INFRASTRUCTURE PROTECTION, THE NEW APPROACH TO IMPROVEMENT OF SECURITY AND RESILIENCE

Critical infrastructure represents a medium of national and international importance whose destruction, temporary or permanent disruption in process activities, would seriously endanger or weaken national and public safety, economic and social prosperity (Perinic and Mikac, 2015). Critical infrastructures are those physical and virtual systems that are essential to the minimum operation and function of social life, economy, and government. These
include but are not limited to the following areas: telecommunications; energy; banking and finance; transportation; water systems (Nadal and Padanyi, 2016). From the citizen’s perspective, the critical infrastructure would be reflected in the degree of security of key resources, such as providing drinking water, electricity, transportation, communication, health system, etc. and from the state’s perspective it would be reflected in all capacities that are of vital interest for the state.

Historically, the concept of critical infrastructure protection has arisen earlier in 1962, during the Cuban Missile Crisis when US President Kennedy and the President of the Soviet Union Khrushchev experienced difficulties in communication, due to inappropriate telecommunication technology, thus the telecommunication was identified as one, but not the only sector of vital importance for the national security and state in general and considered as critical infrastructure (Lewis, 2006). The term “critical infrastructure protection” has been first used by US President Bill Clinton in his presidential directive issued on 22 May 1998. A formal legal framework for critical infrastructure was defined by NATO in 2001, followed by USA acts in 2003, and EU acts in 2004. To be more precise, The EU established the European Program for Critical Infrastructure Protection (EPCIP) in 2006 and adopted the European Critical Infrastructure (ECI) Directive in 2008, which applies to the energy and transport sectors.

At the World Economic Forum 2022 in Davos it was clearly emphasized that despite more than two decades of experience critical infrastructure protection still is a challenge, referring to the recent Colonial Pipeline attack that had paralyzed the gas supply on the east coast of the US, similar impacts witnessed as a result of the Amsterdam-Rotterdam-Antwerp attack in February 2022, and the Florida water plant incident in February 2021.

Furthermore, in the recent couple of years the world and Europe faced numerous political and technical developments, an increasingly complex risk environment, with high-impact, low-probability events, such as the COVID-19 pandemic, terrorist attacks (Brussels, Zavantem airport, Maelbeek metro attack), the war in Ukraine, the sabotage of the Nord Stream pipelines in the Baltic Sea, hybrid threats targeting democratic states’ decision-making processes etc. As the European Commission acknowledged, this environment rendered the ECI Directive outdated for purpose. Hence, in 2019 the European Commission initiated an evaluation of the ECI Directive and found that the existing measures do not provide adequate and sufficient preparedness and response to address the variety of new risks that the world and Europe were facing.

In this context, a new Critical Entities Resilience Directive (CER) was created and published in the Official Journal of the European Union as Directive (EU) 2022/2557 and entered into force on 16.1.2023. The new CER Directive is expected to provide strengthen the resilience of critical infrastructure with an overarching framework with respect to all hazards, to a range of threats, including natural or man-made, accidental, or intentional hazards, terrorist attacks, insider threats, or sabotage. However, the major novelty is that the CER Directive will extend the scope of covered sectors, from 2 sectors (energy and transport) to 11 sectors: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space, and food.

Moreover, member states are obligated to have a strategy for ensuring the resilience of critical entities, carry out a national risk assessment and, on this basis, identify critical entities. Critical entities are required to carry out risk assessments of their own and take technical, security and organizational measures that are appropriate and proportionate to the risks they face to prevent, protect, respond, resist, mitigate, absorb, accommodate, and
recover from an incident. Each critical entity will have to designate a liaison officer or equivalent as a point of contact with the competent authorities.

Generally, the new CER Directive introduces a shift in focus, from protection to resilience. In other words, the Directive reflects not only the ability to protect against incidents but also to bounce back into full operation afterward. Rather than being limited to the physical assets and infrastructure, the emphasis is on the entities making use of the infrastructure, as well as on its supply chains and processes.

2.1. Macedonian regulation for critical infrastructure protection

In the Republic of North Macedonia, there is no existing specific law or regulation for the identification and protection of critical infrastructure. According to the Law on private security (article 44) the Government with a special act regulates which entities have to organize mandatory security, which may be considered as an identification of those entities that are of vital interest to the state. Those entities are identified according to their core activity if it is related to the handling of radioactive substances or other substances dangerous for people and the environment, objects of particular cultural and historical significance, as well as in other cases when it is in the interest of security and defense of the Republic of North Macedonia.

However, the Government of North Macedonia acknowledges that due to the latest technological developments, global environmental changes, and natural disasters, there is an evident need to reconsider the regulation and protection of critical infrastructure in terms of new, modern risks and threats, such as natural disasters, terrorism, espionage etc. Thus, in the second half of 2022, the Ministry of Defense created a Draft Law for Critical Infrastructure, that was transparently and publicly discussed by the relevant officials, experts and academia, and uploaded to the Unique national electronic register of regulations of the Republic of North Macedonia (Ener), in December 2022.

This Draft Law for Critical Infrastructure follows the new CER Directive general structure and recommendations in terms of creating a national strategy for the resilience of critical entities, identification of critical entities, carrying out a risk assessment, physical protection, appointing liaison officers etc. The Draft Law for Critical Infrastructure identifies 9 national critical infrastructure sectors: energy, transport, banking systems and infrastructures and financial markets, health, water, food, hazardous materials, public service and digital infrastructure, communication, and information technologies. A specific novelty will be the obligation for the critical entities to appoint a liaison security officer, who will be certified by the Chamber of the Republic of North Macedonia for private security and will have to obtain a certificate for classified information. The liaison security officer will be responsible for continual communication for security issues between the owner/operator and the respective sectoral Ministry and with the coordinative center at the Ministry of Defense. However, along with the responsibility for communication, the liaison security officer will be responsible for a continual overview of the security risks and threats for the critical entity and will adequately update security plans for the resilience and protection of the critical infrastructure.

Moreover, the new regulation for critical infrastructure protection, both, the CER Directive on a European level, and the Macedonian National Draft Law for Critical Infrastructure introduce a new, coherent approach to critical infrastructure protection with three priority areas: preparedness, response and international cooperation. Furthermore, there is an evident, clear aim to reduce the vulnerabilities and strengthen the physical
resilience of critical entities to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage.

3. THE ROLE OF PRIVATE SECURITY IN THE PROTECTION OF CRITICAL INFRASTRUCTURE

Nowadays private security is worldwide recognized as an active stakeholder in providing security to people, corporations, and the state. It conducts public powers delegated by the state and plays a vital role in crime prevention, protection of critical infrastructure and protection of the everyday life of people. We witness private security officers working at airports, public transportation hubs, energy facilities, banks, commercial facilities, shopping malls, hospitals, schools, universities, residential buildings, sports events, concerts and almost in every aspect of people’s life. Moreover, in the last period according to the International labor organization the role of private security services, vis à vis state security has increased due to the increasing security risks driven by natural and geopolitical calamities (ILO, 2022:3). Geneva Center for Security Sector Governance, DCAF not only that identifies the increased demand for private security services in the last decades, but additionally emphasizes that private security services employees outnumber public security forces in a significant number of countries, offering security guards protection, regulating access to property, supplementing state security providers, such as police in crowd control at large events, guarding critical infrastructure etc. (DCAF, 2020:72)

During the COVID-19 pandemic, private security officers supported law enforcement and the ranks of frontline workers to uphold public safety and economic activity. The European Commission officially recognized private security as an “essential service” or “critical occupation” at the beginning of the COVID-19 situation. According to CoESS, in those challenging times, private security had provided continued protection of land, air and maritime supply chains, and was essential, particularly to uphold the transport of medical supplies, food and cash. CoESS outlines that around 25% of private security guaranteed business continuity at Critical Infrastructures, and around 25% of private security officers were called in to implement infection prevention and control (IPC) measures at hospitals, social care facilities and supermarkets.

4. IDENTIFYING QUALITY IN PRIVATE SECURITY

Private security constitutes a part of the state’s security system and is essential for safety and security in many different locations, and especially important in critical infrastructure protection, as above already illustrated. Thus, it is crucial to discuss the need to define quality and argue criteria that will provide quality and will guarantee a high level of competence and professionalism in carrying out public powers for the broad scope of activities of private security.

Globally, the legal framework for private security outlines the minimum or optimal mandatory criteria for the profession. There is no harmonisation of the legal acts and there are existing, minimalistic systems or comprehensive legal frameworks that regulate the work of private security, providing a narrower or wider focus on the range of sectors, entrance for firms and individuals, levels of training, licensing conditions, and so on.

The review of the private security regulation indicates that rarely does exist the basic regulation that outlines a set of specific criteria for the quality of the private security sector. However, that does not necessarily denote a vacuum of relevant work in this regard. European Association of Private Security employers CoESS together with the European
Organization of Workers Uni Europa have acknowledged the need to address the issue of private security quality and in 2016 published a document “Buying quality private security services” that outlines specific aspects of the private security work that indicate quality.

For the purpose of identifying a clear set of criteria for the quality of private security, grounded on the above-noted document defined by both, the workers’ and employees’ organizations we have created a system of 5 key elements that are interrelated and coherently organized: (1) Private security employees; (2) Security management; (3) Professional capacities of the company for providing private security; (4) Broader legal framework and special regulations; (5) Social responsibility.

Moreover, those key elements address and reflect both the public interest for (private) security and the corporate interest of the private security companies that offer security services and that have in-house security as corporations. Thus, the structure of the quality system and quality elements (criteria) aims to reflect the accountability of private security to all stakeholders, the client, the state, and the general community.

The identified 5 key elements in terms of key fields of work of private security may be further divided into several interdisciplinary subcategories that define and support each of the key fields. Private security employees as quality element/criteria are defined with several key factors, such as training and upskilling employees, improvement of skills and professional competencies, employment procedure and conditions of employment. Accordingly, the security management field (or quality element/criteria) is determined by the skills and competences of the management team in terms of higher, management knowledge and practices implemented in day-to-day work, clearly indicated standards of professional communication with employees, clients, authorities, the training of the security managers, but also with deontological code of conduct which is applied by the management team etc. The first two elements of quality refer to the human resources of the private security sector, the employees, and the managers. The third element considers the professional capacities of the company to carry out private security public powers and it refers to both the private security companies that offer security services and to companies that have in-house security sectors. This aspect takes into consideration two sub-criteria: standard operating procedures (SOPs) and quality control. Regarding the private security industry, the standard operating procedures are defined by having an operational working plan with several necessary elements, such as: performance monitoring; mandatory reports; clear methodology for job rotation; capacity to change a worker due to dismissal, illness, or other reasons, etc. Additionally, the company should guarantee its professional capacities for private security with: Schedule of duties; Mobilization and support plan; Transition plan; Performance monitoring assessment; Training plan/exercises; Reversibility plan; Accountability systems/structures; Disaster recovery/business continuity; Management model etc. (Kermetcieva, S and Mileska Stefanovska V, 2023). The quality control for private security companies from the perspective of this quality criteria should be on an external and internal level. The external quality control should be carried out by a third party and should refer to the implementation of standards in private security operations. Internal control may be determined by the internal acts of the company. The fourth element of the quality system for private security should confirm that the company works according to all relevant acts that regulate some aspect of the private security work, such as: the Law on Weapons, the Law on Personal Data Protection, in terms of video surveillance regulation etc., General Data Protection Regulation (GDPR), the Law on Police, the Law on Internal Affairs etc. And finally, private security companies are closely related to the society where they operate, private security companies fulfill the needs of society and society provides the
companies with resources and safe and secure society is capable of maintaining its vital functions (Kermetcieva, S. and Mileska Stefanovska, V., 2023). Hence, private security companies should manage their processes to produce an overall positive impact on society, nurturing relations with relevant stakeholders, such as the authorities, customers, suppliers, employees, media, residents etc.

When we review the relevant regulation for critical infrastructure, regarding the above-illustrated quality elements for private security, we outline that both, the CER Directive and the Macedonian draft law on critical infrastructure indicate that critical entities should ensure adequate training of personnel of critical entities, additionally, critical entities should ensure employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information. The security management in those regulations also considers appropriate training requirements and qualifications, and a background check. Also, the regulation indicates that each critical entity must designate a liaison officer or equivalent as the point of contact with the competent authorities, who need to be adequately trained and certified. Hence, there is no dilemma that critical infrastructure protection is one of the most significant fields of work in the private security sector. Therefore, identification of quality and further implementation in practice is important and it is necessary that it is recognized in a specific regulation.

5. EUROPEAN STANDARD EN 17483: PRIVATE SECURITY SERVICES-PROTECTION OF CRITICAL INFRASTRUCTURE

The European standard EN 17483 was approved on 23 May 2021, and implemented by the national standards organizations from 34 European countries, among which North Macedonia.

The standard lays down quality criteria for private security both when provided for public or private owners or operators of critical entities. The quality is identified for the organization, processes, personnel, and management of the company that provides private security services and is set on several fundamental elements, such as management systems, human resources policies, operating procedures, communication etc.

Precisely, the standard outlines that companies providing private security at critical entities should have the following management systems implemented: a management system such as EN ISO 9001 or similar; a risk management system (e.g., EN ISO 22301[6] or ISO 31000[9]); a structured occupational health and safety management system [e.g. ISO 45001[12]); IT Security management system such as EN ISO/IEC 27001[7].

Additionally, the standard EN 17483 implies several company policies that are important to serve as clearly written documents that will reflect the quality of critical infrastructure protection. One of the most significant policies is the human resources management policy that according to the standard EN 17483 will need to include accurate information on the number and structure of staff, job description, retention of staff, career development, training, staff performance, staff motivation etc. Another important policy indicated with the standard is the business continuity policy with operational contingency plans, which will need to identify the significant risks with regard to operational processes and procedures and technologies used together with the definition of the suitable measures for risk minimization (further information and examples are given in e.g. EN ISO 22301[6]). Furthermore, the security company will need to demonstrate a structured corporate governance policy providing evidence of several aspects of the company, such as a code of
conduct for directors and employees, internal and external control procedures and audits, and reporting arrangements - financial and operational.

This standard puts special emphasis on the employees in terms of identification, selection and recruitment of personnel, necessary interpersonal skills of workers etc. And finally, the standard EN 17483 highlights the training for critical infrastructure protection in terms that it shall cover: legally mandatory specific training; introductory and on-the-job training; critical infrastructure specific training; site-specific training with a particular reference to health and safety, emergency plans and environment management where applicable; refresher training; enhanced training as required; and management training as required.

To sum up, the European standard EN 17483 - Private security services - Protection of critical infrastructure is not a mandatory requirement for companies that carry out security at critical entities. Private security companies may have implemented some of the indicated quality standards, and, they may have imposed several internal acts or policies, however, there is a lack of research on the implementation of this standard.

We are aware that the new CER Directive indicates that “Member States should, where useful, encourage the use of European and international standards and technical specifications relevant to the security and resilience measures applicable to critical entities.” However, it will be up to the member states transposing the Directive to make the decision on the legal requirements for mandatory implementation of the European standard EN 17483.

6. CONCLUDING REMARKS

We may all agree that societies are dependent on the smooth functioning of large and interdependent Critical Infrastructure systems (Savolainen, 2019:8). However, in the latest changing and challenging environment, the existing security risks have an existential impact on businesses and everyday life of people, thus, states must take decisive steps towards strengthening the protection of critical infrastructure in terms of implementation of a reshaped, remodeled concept of security and resilience.

The European regulation for private security and protection is not harmonized in terms of the existing differences regarding the training hours for employees, entry conditions for companies, control etc. However, the new Critical infrastructure directive aims at unifying the criteria for protection and resilience using accepted standards. Member countries are expected to tailor the respective national regulation for critical entities with a structure that will provide wide acceptance of mandatory standards for protection and resilience, and among others also the European standard EN 17483 - Private security services - Protection of critical infrastructure. Additionally, there is an evident need to address the quality of private security from a regulatory perspective and to initiate a comprehensive process of definition of quality and identification of quality criteria for the private security sector. This will not only provide unified criteria for the quality of critical infrastructure protection but will guarantee enhanced accountability of the private security sector generally.
REFERENCES:

3. Gerasimoski, S.,
10. Kermetchieva, S and Mileska Stefanovska, V, 2023, “Quality criteria for the private security companies and challenges for their implementation in the contemporary environment”, Security dialogues
15. Niemi, A., and Torres, F., 2022, Evaluation of the proposed European Commission directive on critical entities resilience and its potential to consolidate the resilience terminology, Proceedings of the 32nd European Safety and Reliable Conference (ESREL 2022)
17. Savolainen, J., 2019, Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?, Hybrid CoE
Documents, regulation:

Buying quality private security services, 2016, Confederation of European Security Services
Decision on the determination of legal entities that are obligated to have private security (Official gazette of RM nr.106/2013)
Law on private security (Official gazette of RM Pavlovaite, I., et all, 2020, Intel:Skills Intelligence for the Private Security Services, Confederation of European Security Services, Uni-Europa
Physical protection of critical infrastructure against terrorist attacs, 2017, CTED Trends Report, United nations Security Council
Standard EN 17483, Private security services - Protection of critical infrastructure
The global security market, Annual and Sustainability Report 2022