International Journal for Quality Research 19(1) 281-296
ISSN 1800-6450

Georgi Pavlov [1]
Teodora Gechkova
Tiana Kaleeva

Article info:
Received 20.03.2024.
Accepted 16.09.2024.

DOI – 10.24874/IJQR19.01-18

CRITICAL INFRASTRUCTURE PROTECTION – STRATEGIC OPPORTUNITIES

Abstract: *The scope of the current article is regarding the critical infrastructure protection. The goal of the scientific research is to present strategic opportunities for protection of the critical infrastructure's facilities, through outlining and overcoming the critical infrastructure's vulnerabilities. That is achieved based on a conducted survey on the critical infrastructure's vulnerability and outlined strategic mechanisms and activities for improving the critical infrastructure protection, including the introduction of behavioral analysis. The research is accomplished through the application of documentary analysis, comparative analysis and a survey among competent specialists in the researched area.*

Keywords: *Critical Infrastructure, Security, Protection, Strategic management*

1. Introduction

The critical infrastructure is a system of elements and facilities that are part of any modern and rapidly developing society. They are characterized by a high degree of dependence and interdependence, which are usually not equal. The critical infrastructure's facilities supply goods and services of essential importance for the normal functioning of the society. Disruption in their normal functioning would result in significant financial losses, as well as human losses in some cases. Many examples exist regarding accidents and incidents that have occurred as a result of various risks and threats.

In mid-2021, the United States of America (USA) declared a state of emergency as a result of a cyberattack on the country's largest fuel pipeline, which serves over 50 million consumers. The work of the country's strategic facility has been suspended due to the attack that encrypted the information systems for the purpose of demanding a ransom.

The total damages, including the critical infrastructure, from the biggest earthquake in Turkey from 2023 were estimated to more than 34.2 billion dollars, equivalent to 4 % of the country's GDP for 2021 (Ankara. The World Bank, 2023).

The presented examples outline the relevance of the studied issues and the lack of sufficient effectiveness in the undertaken protective measures and programs. The risks and threats to the security of the facilities within the critical infrastructure are constantly evolving, which is a result of the dynamic and unpredictable security environment.

The authors of the research aim to highlight several strategic mechanisms for overcoming the degree of vulnerability in the critical infrastructure's facilities. The goal of the scientific study is supported by the implementation of more than a few main

[1] Corresponding author: Georgi Pavlov
Email: gpavlov@unwe.bg

tasks:

- Development of a survey and its application among specialists in the security field. Its results visualize the degree of vulnerability in the different sectors of the national critical infrastructure, which are of strategic importance for the normal functioning of the economy and the society in general;
- Identification of strategic risks to the critical infrastructure security that reveal the necessity of priority protection measures;
- Development of a risk matrix, consisting of strategic risks, probability of their occurrence and defined degree of influence;
- Development of an exemplary structure of a "goal tree" for the protection of critical infrastructure in Republic of Bulgaria, comprising three hierarchical levels – main objectives, baseline objectives and key measures.

The thesis of the scientific study is related to the scientific team's understanding that the strategic prioritization of the mechanisms for critical infrastructure protection is related to a preliminary planning and practical implementation of appropriate approaches leading to an increased security of the critical infrastructure's facilities.

The scientific article is limited to researching the vulnerability of four strategically important sectors in terms of ensuring the normal functioning of the society to various risks and threats, both at district and national level.

Identifying strategic activities and mechanisms to enhance the security of the critical infrastructure and introducing behavioral analysis as an instrument to decrease the vulnerability to various anthropogenic risks are considered to be the main contributions of the scientific research. This has been achieved with the application of a variety of research approaches, such as:

- systematic approach;
- problem-oriented approach;
- process approach;
- documentary approach;
- interdisciplinary approach.

The applied methodology includes:

- documentary analysis;
- comparative analysis;
- survey.

2. Research methodology

For efficient conduction of the current scientific research a specific set of approaches are applied in order to be achieved the main goal – to outline the critical infrastructure's vulnerabilities and to present strategic opportunities for protection of the critical infrastructure's facilities. Among those approaches are the following:

Systematic approach – the scientific research regarding the critical infrastructure provides a diverse information concerning the different categories of strategic facilities, as well as their vulnerability and protection mechanisms. The achievement of the main research goal is facilitated through documentary and comparative analysis, both aiming to reveal possible alternatives for appropriate solutions in connection to the problematic area of the article. The effective application of the systematic approach provides an opportunity for continuous researches in the current scientific area, thus outlining prospects for improvement in the process of protecting the critical infrastructure;

Problem-oriented approach – the researched topic requires the application of a critical thinking in analysing strategic mechanisms for protection of the critical infrastructure. That is especially relevant, when the goal of the research is concentrated on formulating suggestions and opportunities for improvements, such as is the aim of the current article. The conduction of problem-oriented approach is chosen for the needs of this research since it is expected to provide

knowledge and information about important scientific facts, broaden the authors' experience and qualification in the field of the critical infrastructure, and outline relevant conclusions and solutions;

Process approach – the critical infrastructure protection is a continuous and long-lasting process with numerous dependent and interdependent activities, necessary for the achievement of the desired results in protecting its entities and related facilities. Based on this approach, opportunities are provided for improvement of that process, affecting the strategic mechanisms for protection;

Documentary approach – this approach is carried out by applying bibliographic research of specialized scientific information, public and statistical data and other relevant materials in the field of critical infrastructure, security and defence, strategic management, social sciences and others. The approach is based on fundamental criteria such as relevance, reliability, accuracy, credibility, etc. All of which are necessary for the successful conduction of the current scientific research;

Interdisciplinary approach – the research is achieved through an interdisciplinary approach which includes an application of a complex of scientific methods and techniques. The interdisciplinary approach in the science outlines opportunities for researching and analysing the problematic area through a set of scientific prospective in order to increase the interest and awareness towards the results and proposed solutions.

In conducting the scientific research, specific methods are applied in order to reveal and analyse the state of the examined area and to support the process of providing opportunities for overcoming the challenges in the protection of the critical infrastructure's facilities. The applied methods are as follows:

Documentary analysis – a qualitative research method based on systematic approach for analysing documented evidence, aiming to acquire empirical knowledge about the researched areas – critical infrastructure, security and defence, strategic management, protection and others. The method requires reviewing, researching and interpreting the provided information in order to obtain the necessary for the studied area knowledge (Frey, 2018). For the purposes of the current research, various information sources are examined and analysed, including:

- Laws and regulations;
- Strategic and management documents;
- Public accessed data and records;
- Bibliographic monitoring of similar scientific researches in the field;
- and others, related to the topic of the problematic area.

Comparative analysis – this method aims at systematically studying and analysing two or more research areas or objects in terms of their similar and different features in order to formulate common conclusions (Azarian, 2011). This method involves understanding of various types of policies, systems and structures by comparing them with one another. As well as that, it provides access to a wide range of alternative options and solutions to issues and challenges and in that way could facilitate the process of overcoming them (Esser & Vliegenthart, 2017). Hence, it could improve the understanding and raise awareness towards the improvement of the critical infrastructure protection and outline the possible challenges regarding it. For the purposes of the current research the comparative analysis is conducted on three levels – firstly, examining the bibliographic data of established specialists in the field; secondly, analysing the normative base, concerning the topic of the research; and thirdly, comparing the results arising from the conducted survey;

Survey – an effective quantitative method of data collection which is suitable for studying and analyzing a various type of issues. The

advantages of the survey are related to: allowing the surveying of a significant number of persons simultaneously and through that the obtaining of supplementary statistical data; conducting it anonymously and predisposing respondents to engage in this process by giving impartial and honest answers; obtaining and processing the data relatively straightforwardly as a process, etc. For the purposes of the scientific research a survey was conducted among experts from the "National and Regional Security" Department and the Center for Strategic Security and Defense Studies at the University of National and World Economy (Sofia, Republic of Bulgaria).

3. Literature review

In general terms the critical infrastructure is an asset, system or groups of any, which role is fundamental for providing and maintaining crucial functions of the contemporarily societal well-being (Botev, 2013). In regards to that, the disruption or destruction of the critical infrastructure or its elements due to natural or malicious acts could cause significant negative outcome for a particular country and its citizens (Stanchev, 2019).

The concept of infrastructure was coined in the 19th century by the Swiss military theorist Antwan-Henry Jomini, who emphasized its strategic and operational importance for the direction of combat operations. Until the middle of the 20th century, it was a military term used to refer to the territorial organization of the army's system of maintenance and operation. Gradually, the term "infrastructure" began to be used in the economic and management theory. It is currently widely applied in the field of computer science, economic geography and in the field of security research (Hadjitodorov, 2007).

According to the new European Union's Directive 2557 of 2022 the critical entities provide essential services and through that take indispensable role in the maintenance of the economic activities and crucial functions of the society and the whole Union. The directive presents a definition of critical infrastructure – "an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service" (EU. European Parliament, 2022). In an Annex to the directive are outlined the sectors, subsectors and categories of entities which are considered critical for the European Union (EU). The main sectors and subsectors are as follows:

- Energy – electricity, district heating and cooling, oil, gas, hydrogen;
- Transport – air, rail, water, road, public transport;
- Banking;
- Financial market infrastructure;
- Health;
- Drinking water;
- Waste water;
- Digital infrastructure;
- Public administration;
- Space;
- Production, processing and distribution of food (EU. European Parliament, 2022).

Another group of facilities included in the composition of the critical infrastructure exists – a group of facilities that are assigned to the so-called "symbolic criterion". These are all facilities that do not constitute infrastructure, but are with a symbolic meaning – historical places, natural landmarks, cultural monuments, etc. (Drakalieva & Ivanov, 2010).

The complexity of the critical infrastructure makes it vulnerable to a various set of risks and threats to its normal functioning, which implies the necessity of enhancing its resilience (Lazarov, 2019). Hence, the EU's Member States should adopt a strategy in relations to that. It shall set strategic measures for "achieving and maintaining a high level of resilience on the part of critical

entities and covering at least the sectors set out in the Annex" (EU. European Parliament, 2022).

Common to that is the attitude of other countries, outside of the EU, in relations to defining and protecting the critical sectors. For instance, USA formulates similar definition – "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (USA. Congress, 2001). There are 16 critical infrastructure sectors in the country, amongst which: Chemical; Commercial facilities; Communications; Critical manufacturing; Dams; Defense industrial base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government facilities; Healthcare and Public health; Information technology; Nuclear reactors, materials and waste; Transportation systems; Water and Wastewater systems (USA. Cybersecurity & Infrastructure Security Agency, n.d.).

Other countries focus on the one main for their society sector. For instance, Israel defines as crucial and critical the cyberspace of the country, emphasizing on enhancing its sustainability (Tabansky, 2011).

The necessity of developing a model for the formulation of a national security strategy is of a significant importance. It includes the assessment of the security environment on global, regional and domestic level, the analysis and formulation of a national ideal, national interests, goals and means to achieve them. Of particular importance for the successful formulation of the strategy is the participation of all parliamentary political forces and the guarantee of political consensus (Angelov, 2022).

The risk analysis of critical infrastructure in disasters and accidents in the country is a key element of the protection of the national security. The issues and requirements in relations to the analysis of the systems for monitoring of the critical infrastructure in natural disasters and crises might have an effect of the whole national security (Getsov et al., 2022).

4. Critical infrastructure – risks for its facilities

The critical infrastructure is exposed to numerous and different in its intensity threats and risks for its normal functioning, hence imposing the necessity of introducing adequate mechanisms for their overcoming and protection of the facilities of the critical infrastructure. The security and safety on the territory of its facilities is of upmost importance for the whole well-being of the country, region or union.

Conduction of a research regarding the critical infrastructure's security risks involves identifying, analyzing, assessing, interpreting and taking specific measures to reduce and / or neutralize them. Potential risks are most often associated with the occurrence of unexpected changes, complicated situations, dangerous events, negative trends, etc.

As strategic security risks for the critical infrastructure could be identified:

- Anthropogenic risks (anthropogenic incidents, hazards, threats, etc.);
- Cyber risks (cyber disruptions, incidents, interventions, attacks, etc.) (Choraś et al., 2017);
- Natural risks (natural disasters, hazards, cataclysms, etc.);
- Terrorist risks (terrorist attacks, sabotages, malicious acts, etc.);
- Technical risks (technical disruptions, failures, etc.);
- Human risks (human errors, accidents, incidents, etc.);
- Technogenic risks (technogenic accidents, catastrophes, etc.);
- Criminal risks (criminal attacks, thefts, unlawful activities, etc.).

When analyzing the critical infrastructure's risks a proper assessment according to the

likelihood of their occurrence and the degree of impact exerted should be applied. Relating to that the risks might be categorized with high, moderate or low levels. In accordance to that a risk matrix could be formulated, assessing the type of risks, their occurrence probability and the influence degree. Table 1 presents a hypothetical example of such matrix.

Table 1. Risk matrix example

Strategic risks	Occurrence probability	Degree of influence
Anthropogenic risks	Moderate	Moderate
Cyber risks	Moderate	High
Natural risks	High	High
Terrorist risks	High	High
Technical risks	Moderate	High
Human risks	High	Moderate
Technogenic risks	Moderate	Moderate
Criminal risks	High	High

The strategic analysis and research of the security risks of the critical infrastructure reveal the need to identify priority measures to successfully overcome them considering the occurrence frequency and the negative consequences.

5. Case study results

The form of the survey regards the specialist's assessment in determining the levels of vulnerability for the critical infrastructure at national and district level regarding the Republic of Bulgaria. The respondents determine as most serious vulnerability that might affect the critical infrastructure on national level the danger of human actions. On the opposite side, the specialists assessed the natural causes as most vulnerable for the critical infrastructure on the district level. The country's threats analysis reflects its specific characteristics, such as geographical location, economic state, political stability, technical progress, etc.

The strategic analysis of the level of vulnerability of the critical infrastructure of the Republic of Bulgaria is aimed at revealing the degree of its protection, security, reliability, etc. It is performed on national and district level only and does not involve any regional or international assessments. It considers the negative impact of both natural factors (floods, earthquakes, wind storms, wildfires, rainfalls, blizzards, etc.) and human factors (accidents, incidents, sabotages, terrorist attacks, criminal acts, etc.). The assessment information is based on collected data by surveying the experts and asking them to use the scale of between 1 to 10, where 1 is lowest level of vulnerability and 10 is the highest.

The first part of the survey focuses on assessing the vulnerability on national level in regards to natural causes and human actions. The second part is concerning the same factors but on district level. Comparison between them is conducted and certain conclusions are outlined. The third part of the survey is focused on assessing the vulnerability among different critical infrastructure sectors of Republic of Bulgaria regardless of the factors affecting them. The results are accompanied by specific conclusions as well.

Regarding the first part of the survey the analyzed results concerning the level of vulnerability of critical infrastructure's facilities at national level to natural causes are graphically presented in Figure 1.

According to the surveyed experts the critical infrastructure's entities and the facilities related to them are most vulnerable to natural events caused by: floods (7,6); fires (7,2) and earthquakes (7,0). The level of vulnerability to natural hazards is lowest regarding storms (6,67) and extensive rainfalls (6,47). In general terms the average assessment of the critical infrastructure's vulnerability to natural causes on national level is near 7 (6.98). That result outlines this type of vulnerability as relatively high.

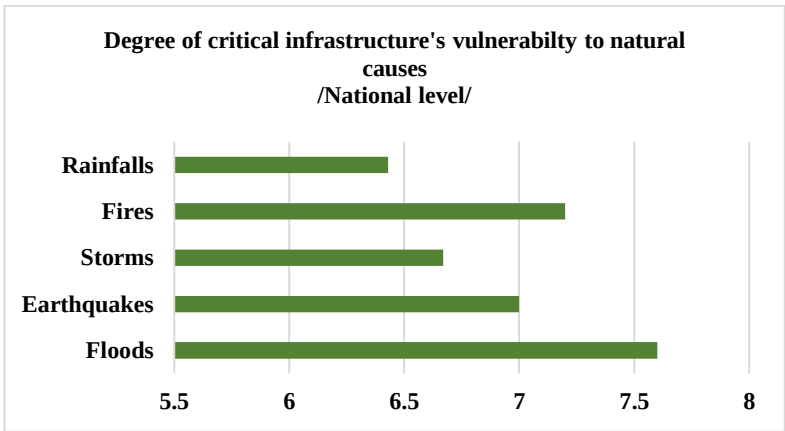

Figure 1. Vulnerability to natural causes /National level/

Afterwards, the surveyed experts are asked to evaluate the critical infrastructure's vulnerability to various of events caused by human actions, again on national level. The summarized results are presented in Figure 2.

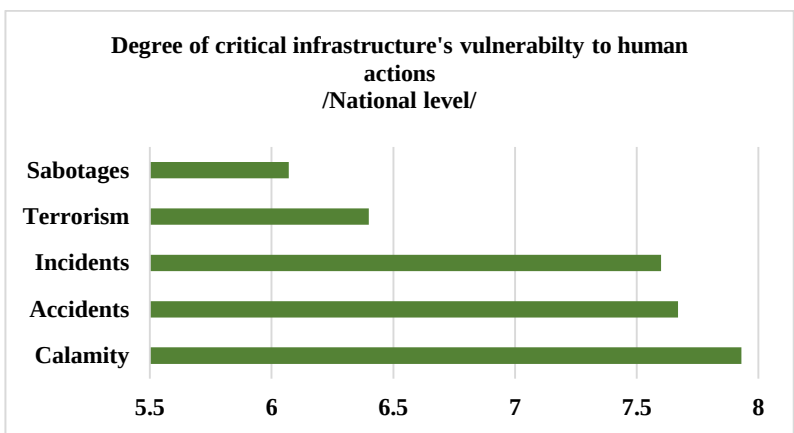

Figure 2. Vulnerability to human actions /National level/

The surveyed experts consider the national critical infrastructure's entities and their facilities as most vulnerable to events of calamities (7,93), accidents (7,67) and incidents (7,6) caused by human actions. The potential vulnerability to acts of terrorism and sabotage is seen as relatively lower, respectively 6,4 for terrorism and 6,07 for sabotages. In general terms the average assessment of the critical infrastructure's vulnerability to human actions on national level is 7,13. Compared to the natural causes the result is slightly higher, outlining is as relatively more challenging for the critical infrastructure.

Regarding the second part on the survey the experts' assessment concerning the level of vulnerability of critical infrastructure's facilities at district level to natural causes is graphically presented in Figure 3.

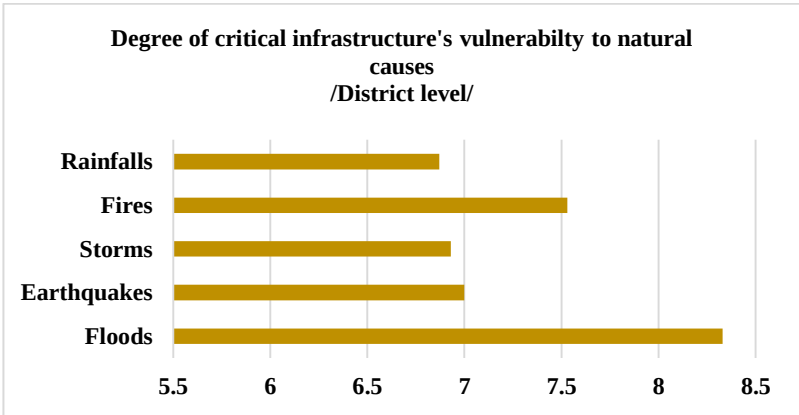

Figure 3. Vulnerability to natural causes /District level/

According to the surveyed experts the critical infrastructure's entities and related facilities at district level are mostly vulnerable to flooding (8,33). Fires (7,53) and earthquakes (7,0) are also causing serious vulnerability. The lowest result is noted regarding storms (6,93) and extensive rainfalls (6,87). In general terms the average assessment of the critical infrastructure vulnerability to natural causes on district level is 7,33. This result outlines that the vulnerability of natural causes on district level is significant.

Differences could also be observed in the assessment on the critical infrastructure's vulnerability to events caused by human actions on district level. The summarized results are presented in Figure 4.

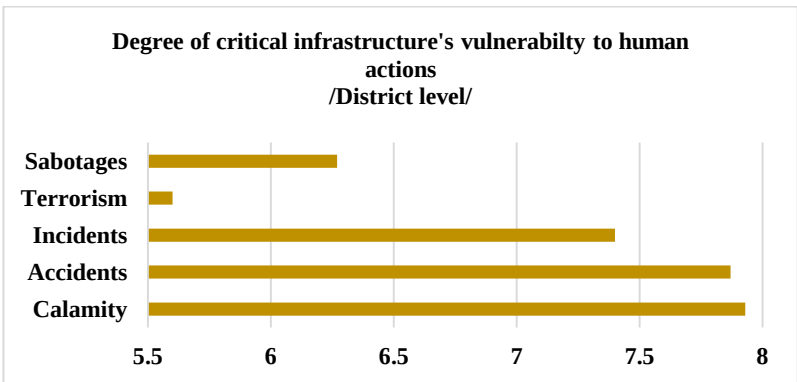

Figure 4. Vulnerability to human actions /District level/

According to the survey the critical infrastructure's facilities at district level are mainly threatened by potential calamities (7,93) and accidents (7,87) caused by human actions. The possible incidents are also indicated with a high result (7,4). Relatively low is the vulnerability to sabotages (6,27), while the one regarding terrorist acts is significantly low (5.6). The average vulnerability to the critical infrastructure on district level that is caused by human actions is estimated at 7,01. Compared to the natural causes this result is lower with 0,32, outlining the factors regarding the human activities as less problematic for the facilities of the critical infrastructure.

In order to compare the evaluation concerning the natural causes and human actions on both national and district level the authors illustrate the results in Figure 5 and Figure 6.

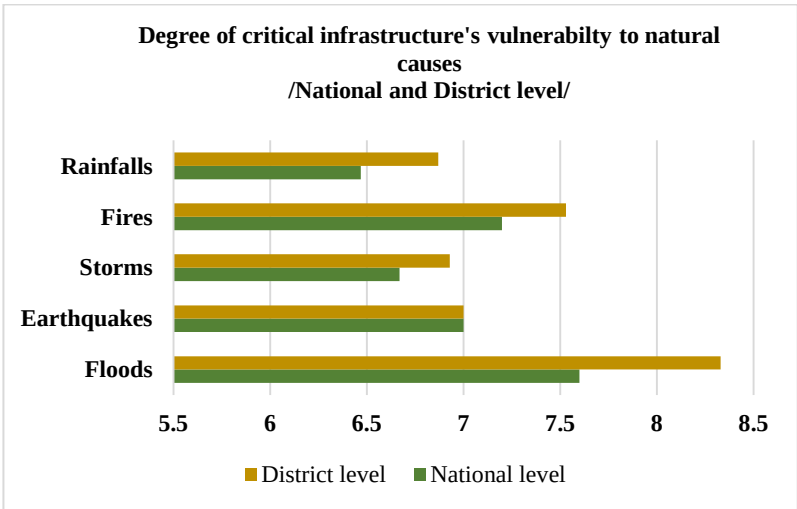

Figure 5. Vulnerability to natural causes /National and District level/

The results show that for both the National and District critical infrastructure the highest level of vulnerability regarding the natural causes is observed for the floods while the lowest is for the rainfalls. With exception to the earthquakes, every other natural hazard is presented with a difference in the results based on national and district level. The most significant is the one concerning the floods. According the survey the average assessment of the critical infrastructure's vulnerability to natural causes on district level is higher than the one on national level by 0,35.

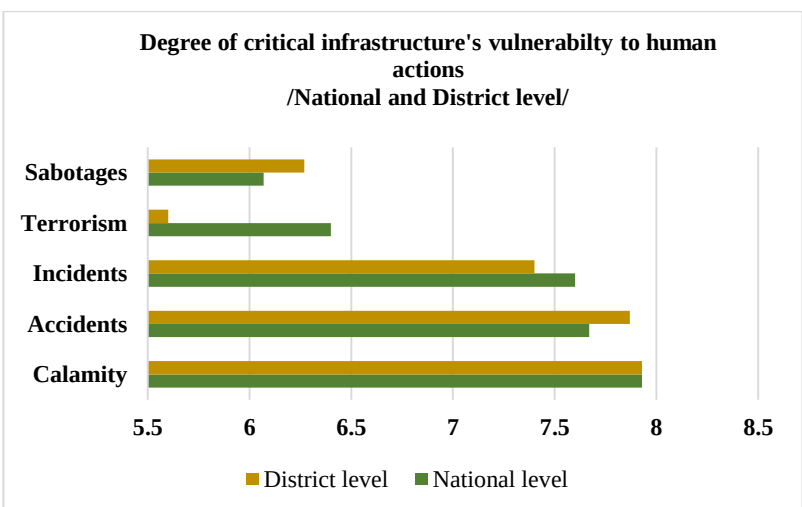

Figure 6. Vulnerability to human actions /National and District level/

The results show that for both the National and District critical infrastructure the highest level of vulnerability regarding the human actions is registered for the calamities while the lowest is for terrorism, when it comes to the district critical infrastructure, and sabotages to national one. Similarly, to the previous indicators, the comparison here shows that there are differences to the evaluation of the factors regarding human actions on national and district level. Nevertheless, they are in the same direction, excepting the sabotage and terrorism variances. According the survey the average assessment of the critical infrastructure's vulnerability to human actions on district level is lower than the one on national level by 0,12.

As a final part of the survey, the experts are asked to assess the vulnerability among different critical infrastructure sectors of Republic of Bulgaria regardless of the factors (natural or human) which are affecting them. The summarized results are graphically presented in Figure 7.

The obtained results indicate that the critical infrastructure's facilities in the considered sectors are potentially vulnerable and require additional and strategic protection. The received assessment are very similar and close as results – "Telecommunication" (8,0); "Energy" (7,93); "Transport" (7,7) and "Water Resources" (7,8). The conducted survey and its results outline the existence of similar challenges in the protection of the critical infrastructure in the strategic sectors of Republic of Bulgaria.

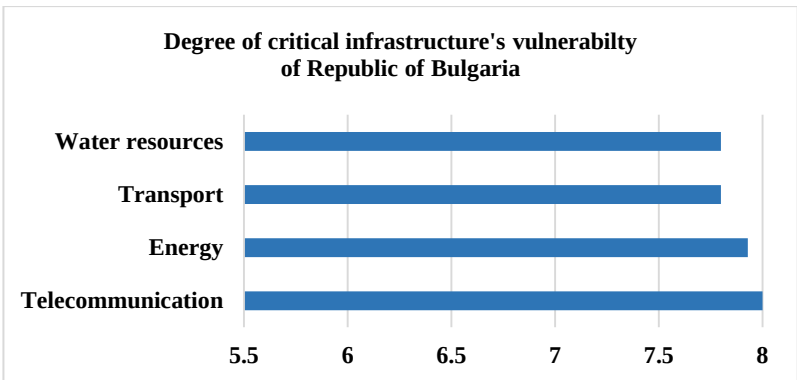

Figure 7. Critical infrastructure's vulnerability of Republic of Bulgaria

6. Discussion

The strategic prioritization of the mechanisms for protecting the critical infrastructure is associated with the preliminary planning and practical implementation of appropriate approaches. It requires appropriate systematization and efficient directing in formulating the priorities adequately. The setting of objectives is an irrevocable and important part of the planning process. It could be abstract or more focused, regarding the levels of government.

The preliminary defined priorities provide the opportunity to determine the immediate connection between the planned objectives and the required resources. Initiatives with a higher priority should respectively receive more resources compared to those with a lower priority. This allows the proper allocation of limited resources in national or institutional level.

Defining in advance the top priorities in decision making could be performed by applying a tree of objectives. It involves a hierarchical system of related elements at different levels. That might be a set of

normative goals, responsibilities, initiatives, measures, etc. It is systematically depicted by a tree structure, consisting of individual vertices and corresponding branches. It could present alternative solutions, issues, situations, scenarioizes, etc.

The structure of the tree for critical infrastructure protection in our country is presented in Table 2. It contains three hierarchical levels at which the main objective, baseline objectives and key measures are represented.

Table 2. Tree of objectives for the critical infrastructure in Republic of Bulgaria

Main Objective	
1.0	To enhance the protection of the critical infrastructure
Baseline objectives	
2.1	To ensure the security of the critical infrastructure
2.2	To increase the resilience of the critical infrastructure
2.3	To increase the stability of the critical infrastructure
Key measures	
3.1	Key measures for the construction of the critical infrastructure
3.2	Key measures to protect the critical infrastructure
3.3	Key measures to maintain the critical infrastructure
3.4	Key measures to strengthen the critical infrastructure
3.5	Key measures for the critical infrastructure rebuilding

The improvement of critical infrastructure protection in the Republic of Bulgaria refers to its continuous development and enduring improvement. The security provides greater safety and defense. Resilience of protection requires higher reliability and resistance. The stability of the protection is connected to the relevant maintenance and strengthening of the critical infrastructure's entities and related facilities.

Based on the conducted research, the authors categorize several main activities to increase the security of the critical infrastructure of the country:

Developing a network of partnerships between the state and the private sector – apart from the security information concepts, the public and private sectors, jointly with the non-profit organizations and the Academia, work together on the preparation of a number of recommendations, plans and programs with a practical focus to ensure the sustainability of the critical infrastructure (such are all practical guidelines for risk analysis and assessment and emergency management, concepts for the protection of humanitarian organizations, social associations, hospitals, etc., all of which are based and guided by the principle and role of strategic planning in the process of protecting the facilities and systems of the critical infrastructure of a particular country);

Determining the main priorities of the country's state policy – determining the state interests that require the development and implementation of priority protection plans and programs. As an example could be presented the process of ensuring the provision of supplies of essential goods and services, which could be legally secured as private transport companies are legally obliged to provide a secured and reliable supply network. Quality control could be carried out using periodic technical inspections and monitoring reports;

Protection of the telecommunications services – Figure 7 of the conducted survey shows the high degree of vulnerability of this sector at national level. Supplies in the telecommunication sector of the national critical infrastructure are also subject to legal regulations, aiming to prevent unauthorized access and / or deliberate interruption of supplies. In addition, operators of telecommunications and information systems should be obliged to identify threats that could be expected. That requires a process of planning and undertaken of various protective measures;

Defining the protection of critical infrastructure as a key element of the national security of the country – the indicated in Figure 7 sectors of the national critical infrastructure are both dependent and interdependent. Disruption in the normal functioning of one of the sectors has a negative impact on the others. In recent years, almost all spheres of public life of the country are characterized by interconnectedness and interdependence. These are issues which determine the actions of protecting the critical infrastructure. Therefore, all aspects of the security express an important role in every one of the respected areas. In that regard, addressing cross-cutting issues is essential for the effective management of the sector, part of the system, carried out by the relevant line ministries and agencies;

Technical support – it is an essential part in overcoming the threats related to accidents and incidents at both national and district level. Figure 6 outlines the vulnerability of the critical infrastructure's facilities from the point of view of the human factor – poor technical maintenance or its lack thereof, which would further increase the vulnerability of the facilities. The development and implementation of various analyses, plans and programs for research and threat assessment aimed at increasing the resilience of critical infrastructure. This is a comprehensive model of partnership at national level, applied to increase the security of the elements and facilities of the national critical infrastructure system;

Taking initiatives and implementing a various set of measures to enhance information security, which could be presented as follows: comprehensive preventive measures taken by the government, government agencies and businesses to address issues concerning the data protection. The measures aim to ensure the compatibility and compliance of the information technologies with all computer-based infrastructures. The legal framework defines all concepts and precise measures to deal with the above-mentioned issue, as the identified instruments are applied cooperatively with the business entities and the stakeholders;

Organizing and conducting training seminars and scientific events – various measures and practical orientations for crisis management are discussed, which are developed and proposed by government and private partners, focusing on the effectiveness of the crisis response system on national level. As a result of the joint exercises is enhanced the mutual trust and cooperation between the different stakeholders, based on the perception that the crisis management process, which is an integral part of the critical infrastructure protection, could only be sufficiently effective through the implementation of joint actions at all levels of government;

In order to ensure the security of the critical infrastructure, which is fully dependent on the constantly changing and evolving risks and threats in the surrounding environment, and to increase the sustainability of the facilities, preventive, anticipatory measures are implemented, taking into an account the potential of the new technologies. In cooperation with the academic community, the industrial sector and the owners / operators of the critical infrastructure's facilities of the country, several innovative solutions might be developed, ensuring the security of the society;

The country's critical infrastructure is characterized by an important feature in terms of ownership – most of the infrastructure's entities and facilities are not state-owned, but are managed and controlled by private organizations or investors. This also applies to the public services' provision. As a result of this trend, responsibility for the security and reliability of the critical infrastructure is increasingly assumed by the private sector, and in separate cases shared with the state. Thus, the functions, assigned to the state and / or the private sector, are mainly aimed at developing preventive

provisions or mechanisms for protecting and controlling the goods and services supply in the event of disaster or other emergency, when normal market mechanisms are not functioning. Therefore, as a preemptive measure to manage the severe crises and accidents is the implementation of an institutional approach, based on cooperation between the state, the business and the industrial sector, within the framework of established partnerships to achieve higher national security.

In the process of protecting the critical infrastructure, in addition to the threats of terrorism, attention should be paid to the threats arising from extreme climate change (Figure 6). They are characterized by no smaller scale, frequency of repetition (if in the past century natural disasters were observed every few years, even decades, today they are a daily occurrence) and the losses amount (both human and / or economic). Significant damages to the critical infrastructure's facilities could be caused by severe storms or floodings. Global climate change and its effects, which are increasingly observed, will gradually engage the global community in the future Therefore, the attention of the state and society in ensuring the security of the critical infrastructure must be focused on the threat of terrorist attacks, on the one hand, and, on the other hand, on the threats of natural disasters. Nevertheless, other threats, such as those arising from systematic and human errors, should also not be ignored, since they could cause damage to the systems as well.

Of similar importance are the risks and threats to the information infrastructure (Figure 6).

Criminal acts, technical malfunction or human error are only a small part of the threats that determine the security and normal functioning of the infrastructure. Any society, in its technological development, will be increasingly sensitive to disturbances in the functioning of this infrastructure. This requires the development and implementation of high standards of security and safety of supply. This strong social dependence on the normal functioning of the goods and services supply is called the "paradox of vulnerability" – the more the susceptibility of society to failures in the delivery process decreases, the more serious the impact of a truly destructive incident will be. This paradox is constantly increasing due to the growing dependence of almost all sectors of the national economy on guaranteeing the supply of electricity, telecommunication, information products, etc. Therefore, the state policy of the country is especially important in this area. In order to ensure the security of the critical infrastructure, it is necessary to develop the so-called "strategically subobjectives" that will be defined and implemented using a range of concepts, plans and programs. In the field of information technology, security is guaranteed by the National Plan for the Protection of Information Infrastructure.

Human factors possess threats both as external and internal factors. For one critical organization an attack from the inside could have a negative influence at the same or higher level as an attack from the outside. Malicious acts caused by the human factors led to a serious vulnerability for the particular facility.

Behavioral analysis might be an effective instrument for mitigating the critical infrastructure's vulnerability. It is based on the concept of analyzing the external expression of person's emotional state and is commonly popular and used regarding social relations. However, its scope provides an opportunity to be applied in a wide range of social issues, including security and defense.

Since the critical infrastructure, in general, is fundamental for the normal functioning of all aspects of the society and the wellbeing of its citizens, its protection is of significant importance. That involves mainly physical safety and security. Failure to achieve that could negatively affect the maintaining of

crucial strategic activities and inevitably result in economic, political and social challenges. In order that to be achieved, diversity of instruments and approaches should be implemented. Behavioral analysis could be one of them.

Its main advantages are based on its main role – to analyze person's behavior and detect (if any) the existence of suspicious or dangerous traits (Ekman, 2011). Generally, that could be defined by the term "hostile" behavior. It is believed that those people would express different behavioral traits than those who are not hostile. It is based on the fact that their emotional state is preoccupied by feelings like stress, guilt, anger, irritation, even confusion (Reiman, 2007). All that trigger certain nonverbal indicators which commonly are in contrast of the verbal ones. For instance, a person could claim he / she is "fine" but at the same time his / her demeanor shows signs of aggression (Navarro, 2018).

According to specialists in the field behavioral analysis could be conducted analyzing different body parts and facial expressions. That is achieved through subjectively dividing the observed individual into 6 levels – face, head, shoulders, hands, legs, walking posture (Nierrenberg et al., 2019). The focus should be applied on the: head position and movements; facial expressions and mimics; shoulder position and movements; hands position and gestures; legs position and movements; and posture and walking pace.

The development and introduction of monitoring programs and systems based on the applied behavioral analysis could be beneficial for the contemporary security systems, including those of the critical infrastructure. They provide the ability to monitor a significant number of individuals simultaneously and detect those who are suspicious or dangerous. In that matter, the detection of those individuals might timely and adequately prevent the occurrence of illegal or terrorist acts, presenting a helpful instrument for the safety and security of the critical infrastructure and enhancing its protection.

7. Conclusion

The conducted scientific research fulfilled the preliminary set goal in outlining the critical infrastructure's vulnerabilities and in presenting strategic opportunities for protection of its facilities. The conducted survey, among specialists in the field, outlines as most serious vulnerability on national level the danger of human actions and the natural causes as the most significant vulnerability on the district level. The enhancement of the critical infrastructure protection requires the introduction of appropriate mechanisms. The strategic prioritization of these mechanisms is related to the preliminary planning and practical implementation of proper approaches. It requires appropriate systematization and efficient directing in formulating the priorities adequately. Last but not least, the research outlines a set of strategic activities, including the implementation of new approaches (behavioral analysis), for improving the critical infrastructure protection.

Acknowledgment: We would like to express our gratitude to all specialists who took part in our survey, as well as to our colleagues at the UNWE's Department of "National and Regional Security" for the provided support.

This article is part of the university project "BG05M2OP001-2.016-0004-C01 – ECONOMIC EDUCATION IN BULGARIA 2030", subsidized by the Operational Programme "Science and Education for Smart Growth" and EU through the European structures and investment funds.

References:

Angelov, Gr. (2022). Model for developing a strategy for the protection of national security. Law and Education, 46-52. Retrieved from http://research.bfu.bg:8080/jspui/bitstream/123456789/1652/1/46_52jur_sbornik_2022.pdf

Ankara. The World Bank. (2023). Earthquake damage in Turkey estimated to exceed $34 billion: World bank assessment report. Retrieved from https://www.worldbank.org/en/news/press-release/2023/02/27/earthquake-damage-in-turkiye-estimated-to-exceed-34-billion-world-bank-disaster-assessment-report

Azarian, R. (2011). Potentials and limitations of comparative method in social science. Research gate, 8-9. Retrieved from https://www.researchgate.net/profile/Reza-Azarian/publication/281269760_Potentials_and_Limitations_of_Comparative_Method_in_Social_Science/links/55dd953d08ae3ab722b1d865/Potentials-and-Limitations-of-Comparative-Method-in-Social-Science.pdf

Botev, G. (2013). Critical infrastructure protection. Sofia: Academy of the Ministry of Interior.

Choraś, M., Kozik, R., Flizikowski, A., Hołubowicz, W., & Renk, R. (2016). Cyber threats impacting critical infrastructures. *Managing the complexity of critical infrastructures: A modelling and simulation approach*, 139-161. Retrieved from https://link.springer.com/chapter/10.1007/978-3-319-51043-9_7

Drakalieva, P., & Ivanov, I. (2010). Syvremenna koncepciya za zashtita na kritichnata infrastruktura – genezis, celi, metodologiya, problemni zoni [Modern concept of the critical infrastructure protection – genesis, goals, methodology, problem areas]. Sofia: Economy

Ekman, P. (2011). Izlazhi me, ako mozhesh [Lie me, if you can]. Sofia: Zhanua ’98.

Esser, F., & Vliegenthart, R. (2017). Comparative research methods. The International Encyclopedia of Communication Research Methods. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118901731.iecrm0035

EU. European Parliament. (2022). Directive 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557#:~:text=(20)%20Directive%20(EU),the%20security%20of%20network%20and

Frey, B. (2018). The SAGE Encyclopaedia of educational research, measurement and evaluation. Education. Retrieved from https://methods.sagepub.com/reference/the-sage-encyclopedia-of-educational-research-measurement-and-evaluation/i7603.xml

Getsov, P., Rangelov, B., Mardirosyan, G., Sotirov, G., Nedyalkov, D, Zafirov, D., …, Zagorski, N. (2022). Analysis of the risk and threats to the critical infrastructure during natural disasters, accidents and crises on the territory of the Republic of Bulgaria. Eighteenth International Scientific Conference Space, Ecology, Safety, 251-260. Retrieved from http://space.bas.bg/SES/archive/SES%202022_DOKLADI/4_Ecology/1_Getsov.pdf

Hadjitodorov, St. (2007). Protection of the critical infrastructure in the national framework of Republic of Bulgaria. Analysis edition – international politics and security. Retrieved from https://www.expert-bdd.com/index.php?option=com_content&view=article&id=745:----------&catid=20:--&Itemid=38

Lazarov, Vl. (2019). Uyazvimost na kritichnata infrastruktura [Critical infrastructure’s vulnerability]. Sofia: About the letters.

Navarro, J. (2018). Rechnik na ezika na tyaloto - prakticheskо rakovodstvo za talkuvane na choveshkoto povedenie [Body language dictionary – a practical guide for interpreting of human behaviour]. Sofia: Iztok-Zapad.

Nierrenberg, G., Calero, H., & Greyson, G. (2019). *How to read a person like a book*. New York: Square One Publishers.

Reiman, T. (2007). Ezikat krie, tyaloto razkriva [The tongue hides, the body reveals]. Sofia: Ergon.

Stanchev, M. (2019). Organizaciya na zashtitata na obekti of kritichnata infrastruktura [Organization for protection of the critical infrastructure's facilities]. Sofia: Academy of the Ministry of Interior.

Tabansky, L. (2011). Critical infrastructure protection against cyber threat. *Military and Strategic Affairs*, *3*(2), 61-78. Retrieved from https://www.inss.org.il/wp-content/uploads/2017/02/FILE1326273687-1.pdf

USA. Congress. (2001). Critical infrastructure protection act. Retrieved from https://www.law.cornell.edu/uscode/text/42/5195c#e

USA. Cybersecurity & Infrastructure Security Agency. (n.d.). Critical Infrastructure Sectors. Retrieved from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Georgi Pavlov
Department "National and Regional Security", University of National and World Economy
Sofia,
Bulgaria
gpavlov@unwe.bg
ORCID 0009-0008-5389-7575

Teodora Gechkova
Department "National and Regional Security", University of National and World Economy
Sofia,
Bulgaria
tgechkova@unwe.bg
ORCID 0009-0004-3101-9983

Tiana Kaleeva
Department "National and Regional Security", University of National and World Economy
Sofia,
Bulgaria
tianakaleeva@gmail.com
ORCID 0000-0002-4472-2959