METHODOLOGY FOR OPTIMIZING VULNERABILITY OF CRITICAL INFRASTRUCTURE OBJECTS THROUGH SPACE DATA AND ARTIFICIAL INTELLIGENCE USING "COST-BENEFIT" APPROACH

Stefan Hadjitodorov[1], Kamen Iliev[1], Ventsislav Polimenov[2*], Katya Dimitrova[1]

[1] *Center for National Security and Defence Research, Bulgarian Academy of Sciences*
emails: sthadj@cu.bas.bg; kiliev@bas.bg; k.dimitrova@rst-tto.com

[2] *Institute of Mathematics and Informatics, Bulgarian Academy of Sciences*
e-mail: v.polimenov@rst-tto.com

Abstract. Critical infrastructure constitutes the backbone of modern society, encompassing sectors such as energy, transportation, and water supply. Risk assessment of critical infrastructure objects is an important task that helps to identify and analyse the potential threats and vulnerabilities of such objects. In recent years, especially after the outbreak of the war in Ukraine, the importance of space infrastructures (ground and space) has grown and they were included in the list of 11 areas of critical infrastructure in the latest EU directive. On the other hand, space technologies appear in key enablers to support resilient & sustainable Critical Infrastructure. This study examines the novel combination of multispectral satellite images and powerful machine learning algorithms, which together have exceptional prospects for enhancing the effectiveness and precision of evaluating and overseeing crucial infrastructure systems.

Keywords: critical infrastructure, artificial intelligence, space, vulnerability, "cost-benefit" approach.

1. INTRODUCTION

Critical infrastructure constitutes the backbone of modern society, encompassing sectors such as energy, transportation, and water supply. Ensuring the reliability and security of these systems is paramount. The potential for utilizing new technologies to optimise vulnerability should be taken into consideration following the implementation of the requirements of the new Directive

[*] Corresponding author.

http://doi.org/10.7546/EngSci.LXI.24.01.08

(EU) 2022/2557 of the European Parliament and of the Council of December 14, 2022, on the resilience of critical entities and repealing Council Directive 2008/114/EC [1].

Risk assessment of critical infrastructure objects is an important task that helps to identify and analyse the potential threats and vulnerabilities of such objects. This assists responsible organizations and institutions to take measures to prevent incidents and protect the infrastructure in case of all hazards – natural disasters and human actions.

Steps and methodologies used in risk assessment of critical infrastructure objects include some of the following:

1) Identification of critical infrastructure objects: This involves the identification and documentation of all objects that are considered as critical infrastructure. This can include power plants, water supply systems, transportation networks, communication systems, and more.
2) Identification of threats: It can be natural disasters such as earthquakes, floods, storms as well as terrorist attacks, cyber attacks and others.
3) Vulnerability assessment: This could be a lack of physical protection, weak cyber security, limited disaster response, etc.
4) Assessment of the probability of occurrence of threats: This can be done by analysing historical data, expert reports and statistical models.
5) Assessment of the consequences: This includes assessing the impact on society, the economy, the environment and human life.
6) Risk assessment: Once the threat, vulnerability, probability of occurrence and impact assessments have been performed, the risk for each critical infrastructure site should be calculated. This helps to optimise risk cost assessment.
7) Risk reduction measures: Once the risk objects are identified, outline risk reduction measures. This includes physical and cyber security, building emergency plans, training staff, etc.

These steps and methodologies are general guidelines and can be adapted according to the specific needs and context of the risk assessment of critical infrastructure objects. Each organization can apply different methods and tools, depending on its specific requirements and resources.

The emerging discipline of remote sensing and machine learning offers a revolutionary method for enhancing the efficiency and reducing the expenses related to vital infrastructure by minimizing risks. This study examines the novel combination of multispectral satellite images and powerful machine learning algorithms, which together have exceptional prospects for enhancing the effectiveness and precision of evaluating and overseeing crucial infrastruc-

ture systems. For improving (decreasing) the vulnerability of an object the application of the "cost-benefit" approach (also known as "value-effectiveness") is proposed.

2. REVIEW OF EXISTING VULNERABILITIES AND RISK ASSESSMENT METHODOLOGIES

In this chapter, we will review existing vulnerabilities and risk assessment methodologies. Our objective is to provide an insightful overview of the various approaches that have been developed and utilized to evaluate and mitigate risks associated with critical infrastructure. By examining the evolution of these methodologies, their strengths, limitations, and real-world applications, we aim to provide a comprehensive guideline of state-of-the-art methodologies. This guide is designed to assist researchers and practitioners in selecting the most appropriate techniques for their specific needs.

1) CRISRRAM

CRISRRAM is a methodology developed by the European Commission. An all-hazards and systems-of-systems approach is needed, addressing critical infrastructure risks and vulnerabilities at the asset, system, and societal levels. To address the complexity of risk assessments, CRISRRAM adopts a **scenario-based approach** and recommends the assessment of all relevant single and multiple hazard scenarios. Assessments of the possibility of a danger must be conducted in order to choose the suitable scenarios.

2) RAMCAP-Plus

The RAMCAP-Plus methodology was developed by the American Society of Civil. An engineering approach to risk and resilience assessment of all hazards. It covers all infrastructures, taking into account the dual objectives of protection and sustainability. The seven steps in the methodology are: asset characterization; threat characterization; analysis of consequences; vulnerability analysis; threat assessment; risk and resilience assessment; and risk and resilience management. This tool is designed for use by both critical infrastructure operators and decision makers [2] [3].

3) UNITED KINGDOM site prioritisation methodology, intrinsic hazard (safety and environment) and performance.

Prioritization is based on the inherent hazard of the site and its performance in managing major hazard risks. The hazard assessment methodology has two elements [4]:

a) A simple safety ranking scheme assigns numerical values to 'unchanging' features about the site and the surrounding area. The site is given a base score that describes the main activity/type of site, which is then multiplied by a factor that reflects the density of the local population. Where the site presents a high 'societal' risk another multiplying factor is applied.
b) The environmental rating system works in a very similar way: Values are given to the site type and multiplied by 'pathway' and 'sensitivity' factors to provide the 'environmental' ranking score.

4) SWEDEN – site prioritization methodology, intrinsic hazards (safety and environment) and performance.

5) BELGIUM – RRP (Rapid Ranking Technique) methodology for site prioritization, intrinsic hazards (safety and environment) and performance.

3 CRITICAL INFRASTRUCTURE POWERED BY SPACE AND ARTIFICIAL INTELLIGENCE

In recent years, especially after the outbreak of the war in Ukraine, the importance of space infrastructures (ground and space) has grown and they were included in the list of 11 areas of critical infrastructure in the latest EU directive. On the other hand, space technologies appear in key enablers to support resilient & sustainable Critical Infrastructure (CI). Main scope is to identify and analyse technically and economically sustainable space-based services for reducing the vulnerability of Critical Infrastructure and for making such infrastructure "greener". As typical examples can be shown:

- RESILIENT: i) Monitoring of the critical infrastructure from environmental/climate related events (e.g. flooding, earthquake) and from consequences of human actions. ii) Monitoring the structural integrity of the asset itself ; iii) Implementation of cybersecurity; iv) Logistic and maintenance inspection
- SUSTAINABLE: i) Reduce the impact on the environment; ii) Support the development of a new infrastructure; iii) Support the replacement (upgrade) of an existing infrastructure

Four are the main space technologies that can be directly used to assess the vulnerability of CI:

- Satellite Earth Observation (SatEO): i) provide an enhanced operational picture to end users, via data collected by remote sensing satellites in med/high resolution; ii) provide wide coverage for monitoring large assets; iii) change assessment through the analysis of optical and radar time-series images;

- Satellite navigation (SatNav): i) trace and tracking service which are fundamental to know where people and assets are located; ii) for geo-localising in-situ samples;
- Satellite Communications (SatCom): i) increase communication network robustness and communication resilience; ii) back-up solution in case of network failures or cyber-attacks targeting terrestrial communication;
- Space Weather: magnetic storm can cause radiation and geomagnetic spikes which impact on Earth can impact the operation of electricity grids, pipelines, railway signalling, etc.

The additional disruptive technologies as a Big Data analytics, ML, AI, Mega constellations for communication network, 5G, IoT and Crowdsourcing make the space technologies as a powerful tools for: i) Identify, define and assess technically and economically potentially sustainable services; ii) Identify and reduce technical and commercial risks related to the implementation of these services; iii) Consolidate user /customer requirements and engage with relevant customers and other stakeholders for further involvement.

The main national (NASA, CNSA, ISRO, JAXA) and international (NATO, ESA, UNICRI, OSCE, SatCen, etc.) organizations in space, defense, and security have shifted their priorities and urgently launched initiatives in the above-mentioned domains in order to effectively address the vulnerability of critical infrastructure. This involves protecting space infrastructure and utilizing space technologies for other sectors of critical infrastructure, enabling a two-way approach to improving resilience and security.

3.1. Use of Satellite imagery data for risk assessment

Satellite information is characterized by a high frequency of acquisition and spatial resolution and provides an opportunity for prevention, operational monitoring, both during the event and for assessing the consequences.

Satellite technology, particularly remote sensing data, provides a clearer picture of climate and environmental change, and has also become indispensable in measuring progress towards the goals set by the United Nations' 2030 Agenda for Sustainable Development, as well as for the Green Pact proposed by the European Commission. Europe's leadership in Earth observation provides a huge wealth of data for operational monitoring. The Copernicus Emergency Management Service (CEMS) is the service of the European Copernicus program that provides mapping, on request only, of disaster-affected areas.

3.2. Machine Learning and AI

In the pursuit of identifying and mapping critical infrastructure with efficiency and accuracy, the integration of neural network architectures, is paramount. This comprehensive approach encompasses several strategic steps. It commences with the acquisition of high-resolution satellite or aerial imagery, complemented by supplementary data sources, creating a robust foundation for neural network analysis. Subsequent data preprocessing activities encompass cleaning, enhancing, and georeferencing the acquired data, essential for noise reduction, image quality enhancement, and spatial alignment. For training data preparation, annotations are introduced to the imagery, marking the locations and classes of critical infrastructure components, a crucial step that underpins the model's training. This annotated dataset serves as the foundation for training neural networks, enabling them to recognize and classify vital elements within remote sensing data.

Mapping critical infrastructure with remote sensing data is a complex yet essential task, and to address this challenge, three neural network architectures have proven highly effective. Convolutional Neural Networks (CNNs), renowned for their image analysis capabilities [5], are invaluable for recognizing patterns and features in satellite or aerial imagery, making them ideal for identifying critical infrastructure elements such as buildings, roads, and power lines. U-Net and its variants, particularly suited for semantic segmentation, are instrumental for creating precise infrastructure maps by segmenting images into different classes with pixel-level accuracy. For tasks involving time series or sequential data, Recurrent Convolutional Neural Networks (RCNNs) offer a potent combination of spatial understanding and temporal analysis. RCNNs, including ConvLSTM (Convolutional Long Short-Term Memory) and Stacked ConvLSTM, are adept at capturing spatiotemporal relationships in remote sensing sequences, making them suitable for monitoring changes, tracking growth, and detecting anomalies in infrastructure over time. The strategic selection among these neural network architectures aligns with the project's mission of efficiently identifying critical infrastructure components while optimizing available resources and enhancing infrastructure management.

The selection of an appropriate Neural Network architecture is pivotal, with the flexibility to customize and fine-tune models according to the specific infrastructure mapping task [6]. Object detection models are incorporated when precise pinpointing and locating of distinct infrastructure elements is the primary goal. Subsequent model training and validation refine the NN using annotated training data, with continuous evaluation and hyperparameter adjustments enhancing model accuracy. Once refined, the model is deployed

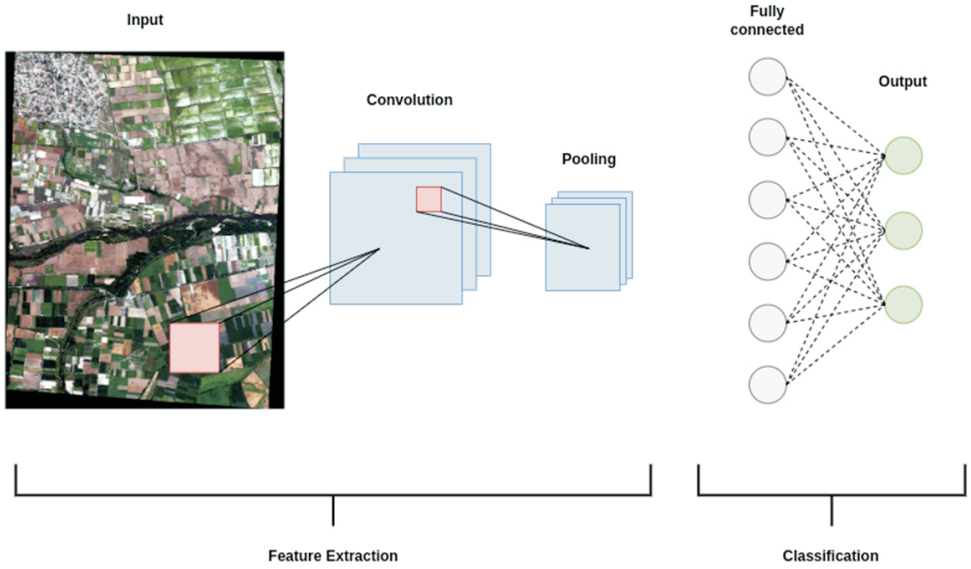

Fig. 1. CNN architecture for Critical Infrastructure mapping

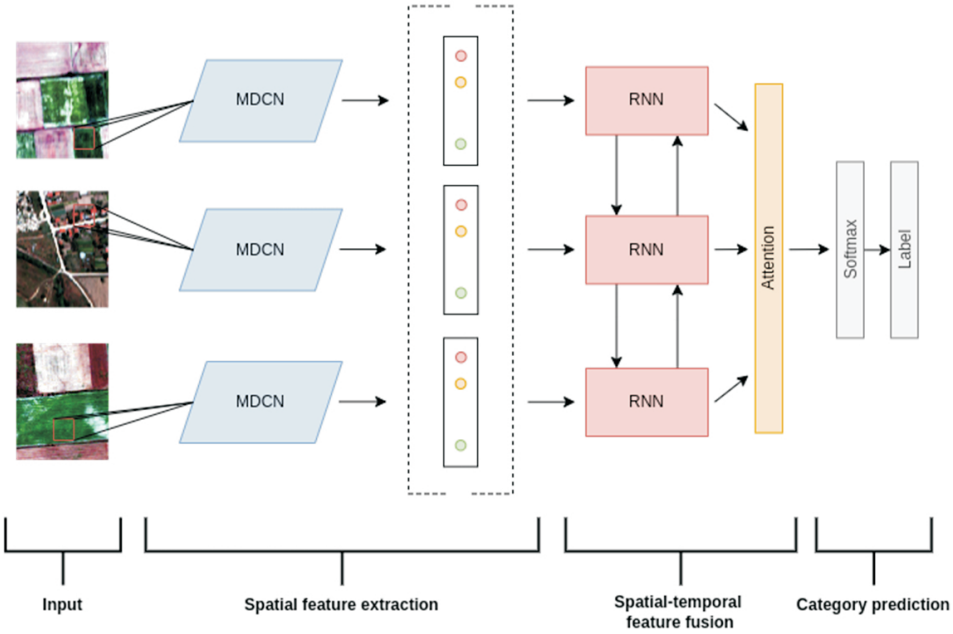

Fig. 2. RCNN architecture for Critical Infrastructure mapping

to analyse new remote sensing data, identifying critical infrastructure components with precision. Post-processing techniques, such as object detection or semantic segmentation, further refine results to create detailed infrastructure maps.

This structured approach not only leverages appropriate neural network architectures but also outlines the systematic implementation steps for efficiently identifying and mapping critical infrastructure. This ultimately improves infrastructure management, supports maintenance planning, and strengthens risk assessment for well-informed decision-making and infrastructure resilience. Considering the above mentioned possibilities of processing satellite data and the information they contain and provide us, their use in the process of assessing the vulnerability and risk of critical infrastructure objects is inevitable [7].

4. METHODOLOGY FOR VULNERABILITIES AND RISK ASSESSMENT FOR A CRITICAL INFRASTRUCTURE OBJECT

This chapter explores the intersection of risk assessment methodologies with the domains of cost optimization and resource allocation.

To ensure the effective protection of a given object within the Critical Infrastructure, it is first essential to evaluate its associated risk level. Consequently, the law in the Republic of Bulgaria mandates the execution of a risk assessment for each individual object within the Critical Infrastructure [7], [8] [9].

Risk rating **R** for these sites is determined by three factors [10, 11]:
– **Threat T** on object. It can be of both natural nature and human activity;
– **Vulnerability V** of object. It represents object's ability to resist a threat;
– **Losses L**, caused by disruption of object's function. These are losses both of the object itself, as well as the subsequent (cascade and public) losses resulting from it, causing population's standard of living to decrease.

$$\boldsymbol{R = Threat \times Vulnerability \times Losses}$$

In the formula above, risk assessment R can only be managed by Vulnerability, since we cannot influence the threat, and losses depend on the magnitude of Vulnerability.

Vulnerability of the objects can be improved by taking measures – organizational and technical, for example [2]:
1. Through organizational measures:
– Optimising management and leadership;

– Creating an alert system for rapid notification and evacuation;
– Relocating technological processes to less dangerous premises;
– Training of composition for action in critical situations;
– Selecting personnel.

2. Through applied technical means to reduce losses, respectively increasing sustainability:

– Constructing water protection walls;
– Making drainage channels;
– Constructing retaining walls against landslides and collapses;
– Reinforcing load-bearing parts of the site (the building);
– Installing fire-resistant partitions;
– Installing fire alarm system;
– Installing an automatic fire extinguishing system;
– Reinforcing electrical insulation in threatened places;
– Moving high voltage systems to a safe distance;
– Moving flammable and explosive materials.

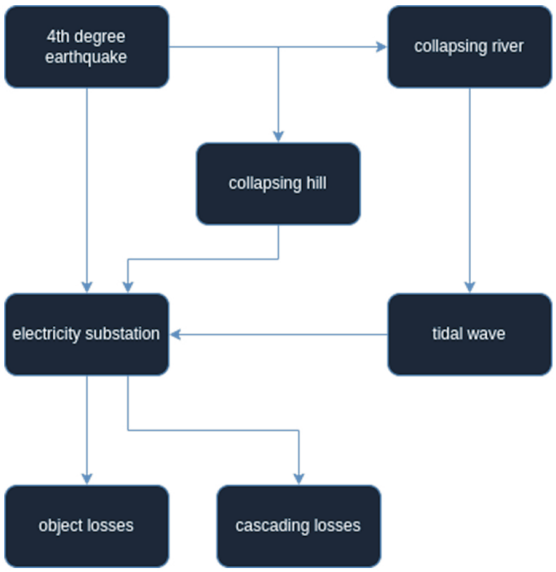

Fig. 3. Schematic of the object and the threats

It is clear that such additional measures can significantly improve (reduce) Vulnerability of a given object. The classic question arises: How much to improve and at what cost? For this purpose, it is appropriate to apply the "cost-benefit" approach, also known as "value-effectiveness".

For example, we will take an **electric substation**, being the only source of power for the neighbouring city and two more settlements in neighbouring areas of the country and as such, being the object of the Critical Infrastructure with the following characteristics:

– The substation is located near a river, in its flood zone, and is separated by a wall;
– On the other side is a hill, with the danger of collapses;
– Around the station there is a 50-year-old poplar grove;
– Road with a tunnel passes through the bay, above the substation;
– A 440 kV high-voltage line enters the substation.

Threat T is a magnitude five earthquake. It causes damage to the station, as well as a collapse from the bay, which also damages the station. During the earthquake, the river was blocked, the water broke through and the substation was flooded by a two-meter shock wave. This is shown schematically in Fig. 3.

Apart from the various methods that have been documented in the literature for calculating vulnerability, the following procedure is used to optimize vulnerability for a particular object:

1. Calculate how much of the financial costs will be spent for implementing organizational and technical measures in order to improve Vulnerability. Four options are considered, and for each of them costs and Vulnerability are calculated, shown in Fig. 4. Naturally, as costs increase, Vulnerability decreases (improves).

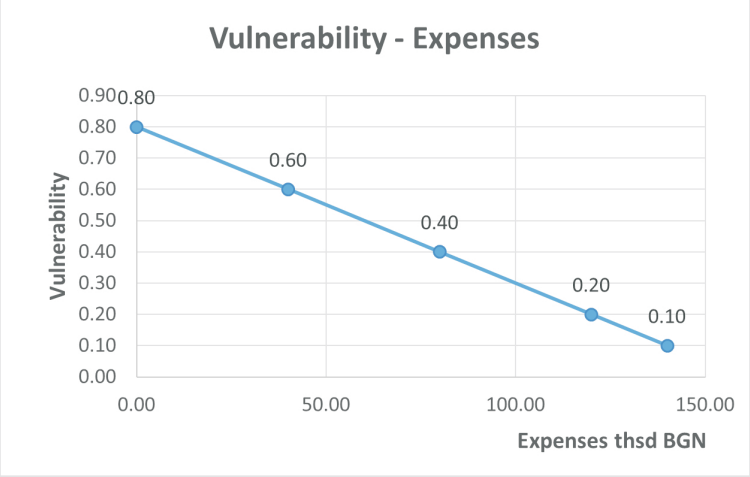

Fig. 4. Necessary financial costs to reduce Vulnerability

Please note that the line presented here is approximate. In reality, it is broken, but it follows the drawn course.

2. For each of the Vulnerability points Losses are also calculated, including cascading and public ones, and "Vulnerability – Losses" graph is constructed, Fig. 5.
3. Risk assessment R is calculated depending on Threat, Vulnerability and Losses.

Fig. 5. Dependency between object vulnerability and subsequent losses

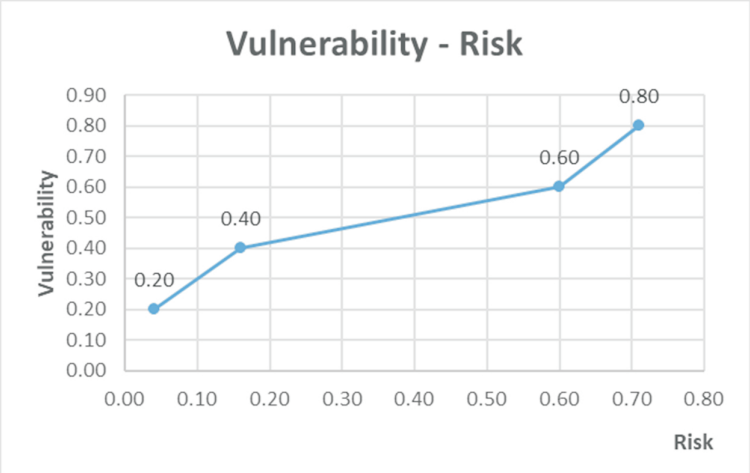

Fig. 6. Dependency between site vulnerability and risk assessment

Calculation is done for the four points and Vulnerability – Risk graph is plotted, shown in Fig. 6.

Depending on the acceptable risk assessment, Fig. 6 determines the minimum acceptable vulnerability. Let the minimum acceptable risk be R = 0.30. Then the minimum acceptable Vulnerability is 0.46. In order to achieve this vulnerability, additional financial costs of BGN 70,000 are necessary.

In this way, the Vulnerability of the object is optimized.

5. DISCUSSION

As outlined, in the previous chapter, the Vulnerability is a transitional element in the scheme of Risk. The acceptable Vulnerability is defined based on the minimal permitted Risk, which in turn determines the minimum required financial expenditures.

It is necessary to take into account the brokenness of "Vulnerability – Costs" graph, which may lead to higher costs for achieving acceptable risk.

The graphs "Vulnerability – Costs" and "Vulnerability – Losses" are thoroughly analysed and compared. If determined that loss reduction is more important than financial cost of improving Vulnerability of an object, Vulnerability can be "strengthened" in the interest of population, i.e. to invest more funds in a given object to significantly improve its vulnerability, in order to significantly reduce cascading losses.

Since cascading losses can hardly be calculated accurately, we consider the following practical recommendation to be appropriate: Accept 80% of the calculated value as an acceptable Vulnerability.

All the calculations are based on expert assessments. This is the R risk assessment scheme, thus competent specialists who are well-versed in their field should be included throughout the entire procedure. They must be able to estimate with good accuracy what the losses will be for the object and what activities to undertake in/for it, respectively – what financial means they will cost. Since it is a matter of objects of the critical infrastructure, it is necessary to precisely determine the losses for the population, which can be caused by both the object itself and by disrupting the activity of other related objects, i.e. cascading losses.

Widely used "cost-benefit" method can be upgraded by the proposed methodology of using satellite images and Neural Networks to efficiently identify critical infrastructure components while optimizing available resources and enhancing infrastructure management.

6. CONCLUSIONS

In this paper, a review of the existing state-of-the-art risk assessment methodologies, presenting different approaches and pros and cons, to highlight the importance of selecting the most appropriate one, is done.

The "cost-benefit" ("value-effectiveness") method is efficient, effective and recommended for optimizing the Vulnerability of Critical Infrastructure objects. This work provides an understanding of how effective data from Space in combination with deep learning techniques for CI analysis.

Disruptive technologies as a Big Data analytics, ML, AI, advantage the space technologies as a powerful tool for identification, definition and assessment the vulnerability of the CI. The possibility, satellite data processing and the obtained information though ML and AI techniques used in the process of assessing the vulnerability and risk of critical infrastructure objects, is inevitable.

Expansion of this work would include concrete application of the methodology on satellite imagery using ML and AI to provide mapping and risk assessment on the CI.

ACKNOWLEDGEMENTS

This work was partially supported by the Bulgarian Ministry of Education and Science under the National Research Programme "Young scientists and postdoctoral students-2" approved by DCM 206/07.04.2022 and under the National Research Programme "Protection of the Environment and Reduction of the Risk of Adverse Events and Natural Disasters", Agreement № Д01-230/06.12.2018.

REFERENCES

[1] 2008/114/EC, Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive.

[2] G. Giannopoulos, R. Filippini and M. Schimmer, Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. EUR 25286 EN, Publications Office of the European Union, Luxembourg (2012).

[3] M. Theocharidou and G. Giannopoulos, Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. EUR 27332, Publications Office of the European Union, Luxembourg (2015).

[4] A. Ahmed, V. Santos M. Sales Dias and A. N. Mahmoud, A hybrid model of self-organizing map and deep learning with genetic algorithm for managing energy consumption in public buildings, *Journal of Cleaner Production* (2024) **434** (14), https://doi.org/10.1016/j.jclepro.2023.140040.

[5] S. Kamoji, M. Kalla and I. Shamshi, A Framework for Flood Extent Mapping using CNN Transfer Learning, *International Journal of Intelligent Systems and Applications in Engineering* (2022) **10** (3s), https://doi.org/10.17762/ijisae.v10i3S.2426.

[6] Y. Zou, H. Weinacker and B. Koch, Towards urban scene semantic segmentation with deep learning from lidar point clouds: A case study in Baden-Württemberg, Germany, *Remote Sensing* (2021) **13** (16), https://doi.org/10.3390/rs13163220.

[7] Council of Ministers, Council of Ministers, REGULATION No. 256 of October 17, 2012, on the adoption of an ordinance on the order, manner and competent authorities for establishing critical infrastructures and their sites and risk assessment, Council of Ministers, Bulgaria (2012), (in Bulgarian).

[8] JRC Scientific and Policy Reports. An Overview of Methodologies for Hazard Rating of Industrial Sites, (2016).

[9] Risk assessment methodology for established critical infrastructures and their sites in the "defense" sector in the Republic of Bulgaria – SOFIA, MD, (2017) Sofia (in Bulgarian).

[10] A methodology for modeling, analyzing critical infrastructure, identifying interdependencies, assessing vulnerabilities and risk, and planning defense capabilities, CNSDR-BAS, (2005) Sofia, (in Bulgarian).

[11] Methodology for the assessment of critical infrastructure sites at the national level and the risks for their sustainability, CNSDR-BAS, Sofia, 2023 (in Bulgarian).

Received February 07, 2024