Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 511-518

Critical Infrastructure Risk Assessment Approach

Zarko I. Zdravkov
Rakovski National Defence College
Defence Advanced Research Institute
Sofia, Bulgaria
z.zdravkov@rndc.bg

Ivo G. Radulov
Rakovski National Defence College
Defence Advanced Research Institute
Sofia, Bulgaria
i.radulov@rndc.bg

***Abstract*—The paper focuses on the activities for improving protection of critical infrastructures and in particular a methodology for the risk assessment of CI assets of the Ministry of Defence (MoD) of the Republic of Bulgaria is presented. It defines the stages through which this process takes place and proposes a mathematical apparatus including analytical expressions for risk assessment. The methodology reveals how experts can measure, document and report risk in this area. It uses universal mathematical models for risk assessment based on adapted scientific theories and methods making it applicable to risk assessment for other CI assets in Bulgaria.**

Keywords—critical infrastructure, risk, risk management

I. INTRODUCTION

Effective risk management requires the application of a systematic approach related to the identification, assessment and mitigation of potential threats to critical infrastructure assets in Bulgaria. This includes the development of strategies to prevent the occurrence of risk events, prepare for crisis response, and identify activities to restore damage after these events occur. Establishing a unified risk management methodology will allow organizations whose responsibilities are related to this topic to implement best practices and procedures for protecting critical infrastructure assets.

The proposed methodology into this article has been developed for the purposes of the Ministry of Defence (MoD) of the Republic of Bulgaria. It has been successfully approbated since 2017. It is original, with a low degree of complexity, which is a prerequisite for its successful application in practice. Into the methodology have been applied universal mathematical models for risk assessment based on adapted scientific theories and methods which makes it applicable to all CI assets in the Republic of Bulgaria.

II. MATERIALS AND METHODS

By definition, risk is a function of the probability of a risk event occurring and its consequences. To make the result more accurate, another component is added to this function in this methodology - the influence of the vulnerabilities of the CI assets. Thus, the risk score becomes the product of the probability (P) of a risk event occurring, the influence of the vulnerabilities (V) of the CI assets and the impact (I) of the risk event occurring for each individual asset.

$$R = P.\ V.\ I \tag{1}$$

The assessment of the probability of a risk event occurring is done in linguistic qualitative terms with the help of experts. The coding of probabilities with numerical values is given in Table 2.

The other necessary component for risk assessment in the identified CI-s and their assets is their vulnerability to occurrence of the identified risk event. The assessment of the vulnerabilities for a given CI site is performed by experts with experience in the relevant field. For their convenience, a questionnaire can be prepared to list the vulnerabilities. For each vulnerability, countermeasures shall be listed, if any. Where countermeasures are available for existing vulnerabilities, the experts assess their aggregate effectiveness in the range of 0 to 100%.

The next main component of the risk assessment is the consequences of a risk event. This is done by assessing losses through qualitative measures that are translated into quantitative (monetary) ones. Losses are classified according to a material loss classification scale (see Table 4).

Risk is a function of the elements listed above and is calculated as the product of the three values. The result is a rank number derived from the conditionally separated intervals for the five risk levels for each individual risk event (see Table 5).

Figure 1, Stage 2 illustrates the general sequence of steps required by the risk management process. (ISO 31000:2018 - Risk management)

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.23

III. Results and Discussion

A. Assumptions and constraints

In mathematical modelling it is almost always necessary to make simplifying propositions. The presented Methodology has been carried out under assumptions and constraints imposed by the specificity of the subject matter and by the lack of sufficient information on certain controllable and/or independent variables and parameters as well as on the interactions between them.

In order to achieve the objective of the Methodology, the following assumptions have been made:

- Critical infrastructures and their assets are identified a priori by experts in accordance with the established procedure in the Ordinance on the Procedure, Method and Competent Authorities for the Identification of CIs and their assets and Risk Assessment, in force since 23 Oct. 2012, adopted by Council of Ministers Decree No. 256 of 17 Oct. 2012 [2] [3];
- the possible risk events for a critical infrastructure asset are:

1. disasters - fire (forest, field); flood; earthquake; landslide and collapse; snow and ice; fire caused by an accident at the site; explosion and/or nuclear, chemical and bacteriological event caused by an accident at and/or outside the site by the CI;

2. acts of terrorism, as well as individual acts of organized crime that directly threaten the security of citizens and critical infrastructure [4].

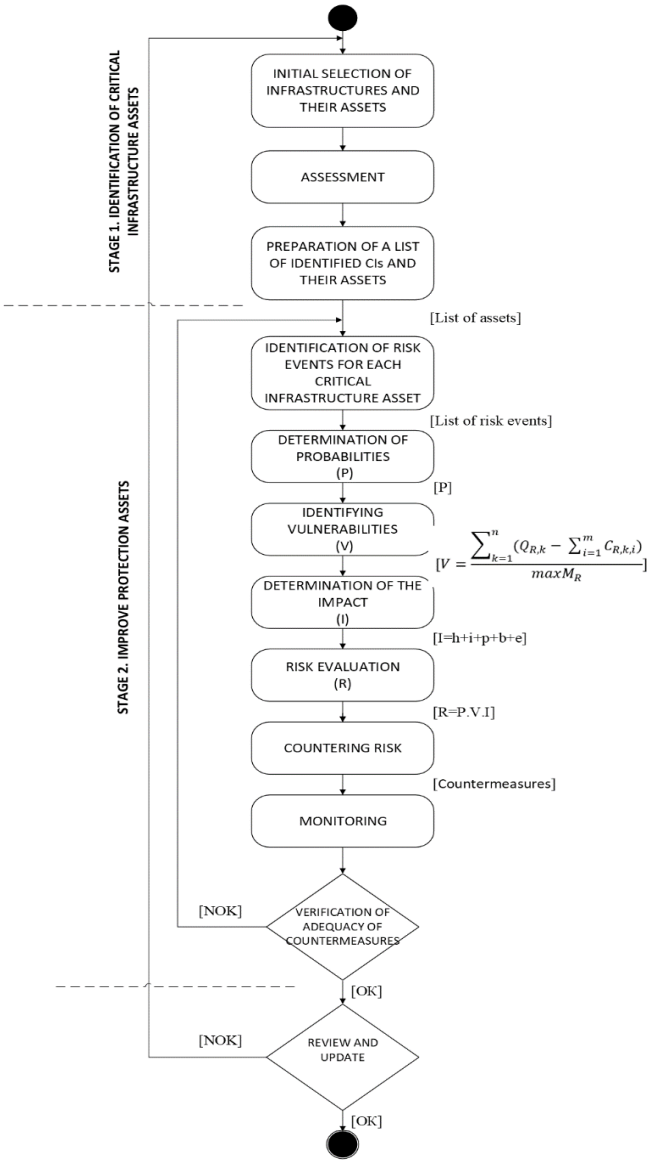

Fig. 1. Model for risk management of Critical Infrastructure.

Constraints:

- Connectivity of assets in a common infrastructure is not taken into account. Indirect damages caused by direct or indirect action of the CI site are not valued;
- A risk assessment model without risk accumulation is used. Risks are assessed individually and not in combination, i.e. it is not considered that a single risk may lead to the occurrence of a second risk, which in turn leads to the occurrence of a third risk, and so on, until set objectives fail;
- The following risks are not considered: 1) disasters caused by drought, violent winds, tornadoes, dust storms, hailstorms, sea storms, outbreaks of contagious diseases and epidemics in humans, animals and plants; 2) space, aviation, rail, road, vessel and unintentional accidents [4].

B. Risk events identification

Optimally, risk identification should take into account all possible hazards, their probability of occurrence and their likely impact, but such a complex approach is difficult to achieve in practice.

In order to simplify the process of identifying risk events, this Methodology presents scenario development questions relating to the occurrence of the identified risk events. This limits the number of situations and determines which risk to analyze in the next steps. This is a cyclical process and if additional risks are subsequently identified, they must be taken into account for further analysis [5].

Using clarifying questions, Table 1 presents several scenarios to identify possible risk events. The questions are answered with YES or NO, thus forming the list of risk events. Only those events are taken into account for which the answer to the question about the scenario coming true is affirmative.

TABLE I. QUESTIONS TO IDENTIFY RISK EVENTS

№	..... (Name of critical infrastructure facility)	
	Scenarios for the occurrence of potential risk events (Clarifying question to identify them)	***Response***
Disasters		
1.	Fire (forest, field): Is it possible that a CI fire at the site could be caused by the ignition of a field, belt or woodland in the vicinity?	YES/NO
2.	Flood: Is flooding of the CI site possible due to being in the catchment area of a river or other water body?	YES/NO
3.	Earthquake: Are there possible consequences/damages to the CI site due to being located in a seismic hazard area?	YES/NO
4.	Landslide: Are there possible consequences/damages to the CI site the due to being in a landslide area?	YES/NO
5.	Snow and Ice: Is it possible to disrupt the CI site's performance due to its location within areas covered in snow and ice?	YES/NO
6.	Nuclear, chemical and bacteriological event due to off-site accident: Are there possible impacts to the CI site due to being in the contamination source area?	YES/NO
7.	Fire arising from an accident: Is a fire likely to occur at the CI site as a result of the presence of flammable and combustible substances and materials?	YES/NO
8.	Explosion caused by accident: Are there possible consequences/damage to the CI site as a result of an accident with explosive materials present?	YES/NO
9.	Nuclear, Chemical and Bacteriological Event arising from an accident at the Site: Are there possible consequences/damages to the CI site arising from the handling of nuclear, chemical and bacteriological materials?	YES/NO
Terrorist acts		
10.	**Internal:** Are there internal contradictions that could lead to a terrorist attack?	YES/NO
11.	**External:** Are there external socio-political contradictions that could lead to a terrorist attack?	YES/NO

C. Probabilities determination

Determining the probability (P) of a risk event occurring is done in linguistic qualitative terms through expert judgment. An exponential distribution was used to determine the probability scale. The estimation of probabilities is coded using Table 2.

TABLE II. PROBABILITY CODING

Ratio	Description of probability (Expert scale)	Interval
0,2	Practically impossible	$[0 \div 10^{-4}]$
0,5	Unlikely	$(10^{-4} \div 10^{-2}]$
1,0	Possible in certain cases	(10-2 ÷ 0,10]
3,0	Below average	(0,10 ÷ 0,20]
5,0	Medium	(0,20 ÷ 0,35]
7,0	Above average	(0,35 ÷ 0,55]
10,0	High	(0,55 ÷ 1,00]

D. Identifying vulnerabilities

TABLE III. DETERMINATION OF VULNERABILITIES AND PERFORMANCE MEASURES

In this stage, the vulnerabilities associated with the identified risk event for the specific asset are recorded. A "cross-section" of vulnerabilities with potential threats is made. Given a lack of relationship between a potential hazard and existing asset vulnerability, no risk is assessed, i.e. it is not possible for such a hazard to affect the performance of the asset. A questionnaire is developed for each of the recorded potential risk sources. Answering a specific question determines the potential vulnerabilities of the identified risk events for each specific CI site.

……. **(Risk event name)**								
	Vulnerability		Countermeasure effectiveness C_R (%)				$\sum_{i=1}^{m} C_{R,k,i}$	$Q_{R,k} - \sum_{i=1}^{m} C_{R,k,i}$
	Question	Value						
1.	$Q_{R,1}$	0 or 1	$C_{R,1,1}$					
2.	$Q_{R,2}$	0 or 1	$C_{R,2,1}$	$C_{R,2,2}$	$C_{R,2,3}$			
3.	$Q_{R,3}$	0 or 1						
	……							
k.	$Q_{R,k}$	0 or 1						
Number of vulnerabilities		$maxM_R$						$M_R = \sum_{k=1}^{n} (Q_{R,k} - \sum_{i=1}^{m} C_{R,k,i})$
Prerequisite for the risk event								

The following analytical expression is used to calculate the impact of existing vulnerabilities (VR) and their countermeasures against the probability of the risk event occurring:

$$V_R = (\frac{M_R}{maxM_R}) \quad (2)$$

where: index *R* denotes the specific risk event;

M_R - prerequisite for the occurrence of the R^{-th} risk event;

$maxM_R$ - maximum value of vulnerabilities defined by questions for occurrence of the R^{-th} risk event.

For each risk event, M_R and $maxM_R$ are calculated. The premise for the occurrence of *R* (M_R) is defined as the difference between the value of each vulnerability and the effectiveness of the measures applied to mitigate it.

Vulnerability is calculated by answering each question regarding a risk event with either YES or NO. The purpose of each question is to determine the presence of vulnerability. For the purposes of the Methodology, the following is assumed:

- If YES, the question is assigned a value of 1 (vulnerability exists);
- If NO, the question is assigned a value of 0 (no vulnerability).

The prerequisite for the occurrence of the R^{-th} risk event M_R is calculated using the formula:

$$M_R = \sum_{k=1}^{n} (Q_{R,k} - \sum_{i=1}^{m} C_{R,k,i}) \quad (3)$$

where: *n* - number of questions directed at the R^{-th} risk event;

m - number of countermeasures against a vulnerability defined by n^{-th} question;

$Q_{R,k}$ - question that detects a vulnerability (takes the value 1 or 0 depending on the answer for the k_1^{-st} question);

$C_{R,k,i}$ - effectiveness of the i^{-th} countermeasure against the vulnerability from the k^{-th} question (evaluated in percentage);

$\sum_{i=1}^{m} C_{Rki}$ - aggregated effectiveness of complementary *i* number of measures for this vulnerability (assumes a value from 0 to 100%).

Effectiveness values for complementary measures (where there is more than one measure for the same risk event) are distributed up to 100%. The resulting parameters are transferred in Table 3.

Note: Aggregated efficiency ($\sum_{i=1}^{m} C_{Rki}$) of complementary *i* number of measures for each vulnerability assumes a value from 0 to 100%.

$maxM_R$ is a function of vulnerability detection issues:

$$maxM_R = n, \quad (4)$$

where: *n* – number of YES questions

E. Determination of the impact

The negative consequences of the occurrence of risk events are calculated on the basis of a valuation of the losses when critical assets of the objects are affected, namely [6]:

- human losses (*h*);

- information (*i*);
- processes (functions) (*p*);
- buildings and structures (*b*);
- machinery and equipment (*e*).

The valuation of losses is entered for each asset affected as the total is calculated through the following formula:

$$I=h+i+p+b+e \quad (5)$$

The human losses (*h*) are calculated by the formula:

$$h = t(\sum_{k1=1}^{n}(h1_{k1} + h2_{k1}) + \sum_{k2=1}^{m} h3_{k2}) \quad (6)$$

where: *n* - number of dead;

m - number of injured;

t - coefficient of loss of public confidence;

$h1_{k1}$ - financial means of compensation for the death of the $k^{1\text{-}st}$ victim;

$h2_{k1}$ - financial resources for the selection and training of an officer to replace the $k^{1\text{-}st}$ victim (to be entered only when the deceased is an employee of the establishment concerned);

$h3_{k2}$ - financial resources for treatment and recovery.

The loss of public confidence in human casualties is captured by the loss of public confidence factor (*t*). Using the following semi-quantitative scales, it can take the following values: (1) limited/not significant, (2) minor/significant, (3) moderate/serious, (4) significant/very serious, and (5) catastrophic/disastrous. Most common value of "t" is 2.

The information loss (*i*) is calculated by the formula:

$$i = \sum_{k1=1}^{n} i1_{k1} + t\sum_{k2=1}^{m} i2_{k2} \quad (7)$$

where: *n* - number of destroyed information units[1];

m - number of information units with breached confidentiality;

t - coefficient of loss of public trust;

$i1_{k1}$ - financial means for the recovery of the $k1^{\text{-st}}$ information unit;

$i2_{k2}$ - financial means to recover the $k2^{\text{-nd}}$ information with breached confidentiality.

Similarly, to the previous case, the decrease in public trust upon loss of confidentiality is accounted for by multiplying the resulting value by a factor of 2.

The process loss *(p)* is calculated using the formula**:**

$$p = \sum_{k=1}^{n} p_k \quad (8)$$

where: *n* - number of disrupted processes;

p_k - lost financial resources from lost benefits of the $k^{\text{-}th}$ function.

Losses (damages) to buildings and structures *(b)* are calculated using the formula:

$$b = \sum_{k=1}^{n}(b1 + b2)_k \quad (9)$$

where: *n* - number of buildings and structures affected;

b_{1k} - financial resources lost from damage to the building or facility;

b_{2k} - financial resources for reconstruction of the $k^{\text{-}th}$ building or facility.

The loss of machinery and equipment *(f)* is calculated by the formula:

$$e = \sum_{k=1}^{n} e_k \quad (10)$$

where: *n* - number of destroyed and/or damaged machinery and equipment;

e_k - financial resources for the purchase, delivery and installation of the machinery and/or equipment or financial resources for repairs.

After finding the losses (*I*) as the sum of the additives in formula (5), a classification of the amount of material losses is made based on their position on the limiting interval of the scale in Table 4. The relevant coefficient from Table 4 is substituted into the risk calculation formula. The result is a dimensionless rank number.

TABLE IV. CLASSIFICATION OF MATERIAL LOSSES

Ratio	Description of the losses	Amount of losses (Million Euro)
1,0	Small	[0 - 3,5]
3,0	Significant	(3,5 - 12]
7,0	Serious	(12 - 48]
15,0	Hazardous	(48 - 100]
40,0	Catastrophic	above 100

F. Risk evaluation

A risk evaluation is made for each CI asset using formula (1).

Risk evaluation is a specific type of activity in which the results of the analysis are compared with the risk criteria to determine whether the risk is acceptable or unacceptable. Risk evaluation is also concerned with the grading of risks to determine their importance and priority. The grading and prioritization of risks is carried out in accordance with the

[1] Valuable information

scale adopted in Table 5, thus concluding which of the identified risks should be managed [7].

TABLE V. CODING OF RISK LEVELS

Grade	Rank	Description
I	(0 - 2]	Negligible, too limited- no attention needed
II	(2 - 5)	Acceptable - attention needed
III	[5 - 35)	Moderate - measures needed to reduce it
IV	[35 - 200]	Serious - measures should be taken immediately
V	> 200	High - cessation of activity until the risk is eliminated

The rank number obtained from formula (1) is coded into five levels of importance. For the first two levels of risk (negligible and acceptable) no special measures are needed. The III level, signifying a moderate risk, is marked in yellow, meaning measures are needed to reduce it. The last two levels of risk (serious and high) are visualized in red and demand special attention to be addressed.

When substituted with the possible probability, vulnerability and consequence values, the risk matrix appears in the format shown in Figures 2 to 6.

V / *P*	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,2	0,02	0,04	0,06	0,08	0,10	0,12	0,14	0,16	0,18	0,20
0,5	0,05	0,10	0,15	0,20	0,25	0,30	0,35	0,40	0,45	0,50
1	0,10	0,20	0,30	0,40	0,50	0,60	0,70	0,80	0,90	1,00
3	0,30	0,60	0,90	1,20	1,50	1,80	2,10	2,40	2,70	3,00
5	0,50	1,00	1,50	2,00	2,50	3,00	3,50	4,00	4,50	5,00
7	0,70	1,40	2,10	2,80	3,50	4,20	4,90	5,60	6,30	7,00
10	1,00	2,00	3,00	4,00	5,00	6,00	7,00	8,00	9,00	10,00

Fig. 2. Risk rank numbers calculated for impacts = 1 (small), probabilities (*P*) from 0.2 to 10 (by row), and vulnerabilities (*V*) from 10 to 100% (by column)

V / *P*	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,2	0,06	0,12	0,18	0,24	0,30	0,36	0,42	0,48	0,54	0,60
0,5	0,15	0,30	0,45	0,60	0,75	0,90	1,05	1,20	1,35	1,50
1	0,30	0,60	0,90	1,20	1,50	1,80	2,10	2,40	2,70	3,00
3	0,90	1,80	2,70	3,60	4,50	5,40	6,30	7,20	8,10	9,00
5	1,50	3,00	4,50	6,00	7,50	9,00	10,5	12,0	13,5	15,00
7	2,10	4,20	6,30	8,40	10,5	12,6	14,7	16,8	18,9	21,00
10	3,00	6,00	9,00	12,0	15,0	18,0	21,0	24,0	27,0	30,00

Fig. 3. Risk rank numbers calculated for impacts = 3 (significant), probabilities (*P*) from 0.2 to 10 (by row) and vulnerabilities (*V*) from 10 to 100% (by column)

V / *P*	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,2	0,14	0,28	0,42	0,56	0,70	0,84	0,98	1,12	1,26	1,40
0,5	0,35	0,70	1,05	1,40	1,75	2,10	2,45	2,80	3,15	3,50
1	0,70	1,40	2,10	2,80	3,50	4,20	4,90	5,60	6,30	7,00
3	2,10	4,20	6,30	8,40	10,5	12,6	14,7	16,8	18,9	21,00
5	3,50	7,00	10,5	14,0	17,5	21,0	24,5	28,0	31,5	35,00
7	4,90	9,80	14,7	19,6	24,5	29,4	34,3	39,2	44,1	49,00
10	7,00	14,0	21,0	28,0	35,0	42,0	49,0	56,0	63,0	70,00

Fig. 4. Risk rank numbers calculated for impacts = 7 (severe), probabilities from 0.2 to 10 (by row) and vulnerabilities from 10 to 100% (by column)

V / *P*	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,2	0,30	0,60	0,90	1,20	1,50	1,80	2,10	2,40	2,70	3,00
0,5	0,75	1,50	2,25	3,00	3,75	4,50	5,25	6,00	6,75	7,50
1	1,50	3,00	4,50	6,00	7,50	9,00	10,5	12,0	13,5	15,00
3	4,50	9,00	13,5	18,0	22,5	27,0	31,5	36,0	40,5	45,00
5	7,50	15,0	22,5	30,0	37,5	45,0	52,5	60,0	67,5	75,00
7	10,5	21,0	31,5	42,0	52,5	63,0	73,5	84,0	94,5	105,0
10	15,0	30,0	45,0	60,0	75,0	90,0	105	120	135	150,0

Fig. 5. Risk rank numbers calculated for impacts = 15 (hazardous), probabilities (*P*) from 0.2 to 10 (by row) and vulnerabilities (*V*) from 10 to 100% (by column)

V / *P*	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
0,2	0,80	1,60	2,40	3,20	4,00	4,80	5,60	6,40	7,20	8,00
0,5	2,00	4,00	6,00	8,00	10,0	12,0	14,0	16,0	18,0	20,0
1	4,00	8,00	12,0	16,0	20,0	24,0	28,0	32,0	36,0	40,0
3	12,0	24,0	36,0	48,0	60,0	72,0	84,0	96,0	108	120,0
5	20,0	40,0	60,0	80,0	100	120	140	160	180	200,0
7	28,0	56,0	84,0	112	140	168	196	224	252	280,0
10	40,0	80,0	120	160	200	240	280	320	360	400,0

Fig. 6. Risk rank numbers calculated for impacts I = 40 (catastrophic), probabilities (*P*) 0.2 to 10 (by row) and vulnerabilities (*V*) 10 to 100% (by column)

The matrix is used as a means of visualizing risks in order to classify them. Each risk event is classified for itself. The values obtained from the risk evaluations for each of the identified risk events are not to be added up together and then compared according to the classification indicated. Averaging their values is also prohibited.

Prioritization of risks is necessary due to the limited resources available for the implementation of the activities for the protection of assets from CI and for the management of the associated risks. For this reason, it is not possible to take effective measures to reduce the impact of all identified risks. The significance of the different risks changes during the course of the activities under the influence of internal and external factors. Therefore, it is important to know the significant risks at any time to develop countermeasures against them [7, 8]. There are four cases in which the assessed risks may not be mitigated:

- with a negligible probability of the risks occurring;
- where the impact of the risks is unrelated to the implementation of the activity;
- where the magnitude of the expected impacts is insignificant for the CI site;
- where the sources of risk are beyond the scope and extent of the specific activity.

G. Mitigating risk

Mitigating risks to CI assets is the process of selecting and implementing measures to reduce a particular risk to specified acceptable levels. This process defines the exact content of the countermeasures, the time necessary to implement them, the persons involved in the processes and their functions [9].

Countermeasures can be aimed at reducing the probability of a risk occurring, reducing vulnerabilities, limiting the magnitude of expected consequences or at all three simultaneously.

The development of risk countermeasures may require collaboration and cooperation with various internal and external to the organization entities.

A key requirement for risk countermeasures is that they are cost-effective, efficient and efficacious. Measures are specific to each CI site and each risk event associated with it. They must be appropriate to the risk countermeasure strategy adopted by the organization.

H. Monitoring

To achieve the desired effectiveness of the risk management process, ongoing and periodic monitoring and reporting of identified risks and actions taken to minimize (mitigate) them are required. CI site managers should review the entire risk register once a year. Particular risks may also be reviewed more frequently (monthly) due to their specificity and level of importance. The risk register may be updated on an ad hoc basis if changes in the environment occur.

The risk analysis and assessment information are formed as a risk management report.

IV. CONCLUSION

This paper is the second in a series that describes the Model for risk management of Critical Infrastructure (CI) of the Republic of Bulgaria. The first one [1] focuses on activities of developing rules and proposing a mathematical apparatus for identifying critical infrastructures and their assets.

Into this paper is proposed Methodology sets out the general approach to risk management for identified critical infrastructures and their assets. The stages through which this process takes place are defined. A mathematical apparatus that includes analytical expressions for risk assessment is proposed. In this way, the theoretical foundations of risk management are linked to the practical application aspects of the Methodology.

The Methodology reveals how experts can measure, document and report risk in this area.

The success of risk management for critical infrastructures and their assets depends heavily on the adaptation of the proposed methods in practice.

The Methodology overcomes the lack of a risk management toolkit for critical infrastructures and their assets. It incorporates the best existing practices in the field, making it applicable to users beyond the scope of the intended target group. This is what determines its relevance, and its usefulness will hopefully be appreciated by all those interested in this subject.

Based on the proposed methodology, a software application MORis® has been developed to automate the risk assessment and management process for the identified critical infrastructures and their sites in the defence sector.

ACKNOWLEDGMENT

The document was developed under the National Scientific Programme "Security and Defence", funded by the Ministry of Education and Science of the Republic of Bulgaria in implementation of the National Strategy for the Development of Scientific Research 2017-2030, adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

REFERENCES

[1] Radulov I., Dimitrov T., Zdravkov Z., Petrov Zh., "Model for risk management of Critical Infrastructure of the Republic of Bulgaria", DIGILIENCE 2024-ISIJ 55: Open Source Intelligence, Artificial Intelligence, and Human-centered Approaches to Cybersecurity and Countering Disinformation (2024): 44-54, ISSN 0861-5160, e-ISSN 1314-2119,
Available: https://www.researchgate.net/publication/385578897_Model_for_Risk_Management_of_Critical_Infrastructures_of_the_Republic_of_Bulgaria [last viewed: 27 May 2026].

[2] Ordinance on the Procedure, Method and Competent Authorities for the Identification of CIs and their assets and Risk Assessment, in force since 23 Oct. 2012, adopted by Council of Ministers Decree No. 256 of 17 Oct. 2012.

[3] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114 [last viewed: 04 September 2024].

[4] Shalamanov, V., et al. "Study for the analysis and evaluation of the system for population protection and emergency response.

White Paper on Civil Protection of the Republic of Bulgaria", Research Project No. 12 under the 2004 working program of the Standing Committee on Protection of the Population from Disasters, Accidents and Catastrophes, Available: https://www.scribd.com/document/22546642/Analysis-and-assessment-of-the-civil-protection-system-BG-2004 [last viewed: 27 May 2026].

[5] Risk Assessment and Mapping Guidelines for Disaster Management. SEC(2010)1626 final, EUROPEAN COMMISSION, Brussels, 21.12.2010.

Tagarev T., Pavlov N., "Planning Measures and Capabilities for Protection of Critical Infrastructures", Information & Security: An International Journal, 22, (2007): 38-48. Available: https://www.researchgate.net/publication/269834426_Planning_Measures_and_Capabilities_for_Protection_of_Critical_Infrastructures [last viewed: 27 May 2026].

[6] A Complete Guide to Risk Prioritization Matrix. Best Practices, Tools, and More, July 23rd, 2024, Available: https://www.6sigma.us/six-sigma-in-focus/risk-prioritization-matrix/ [last viewed: 17 September 2024].

[7] Stoyanov, V., Zlateva, P., Kirov, G., Stoyanov, K. "Application of fuzzy logic in forecasting potential losses from natural disasters". Second National Scientific and Practical Conference on Emergency Management and Population Protection, BAS, Sofia, 2007.

[8] Georgiev, V., Risk Management as a Tool of Program Management. Sofia, Military Journal, 2005.