The Probabilistic Graphical Model for Multi-Hazard Risk Evaluation of Critical Infrastructure Impairment

Bohdan Sakovych[1], Maryna Zharikova[1,2], Volodymyr Sherstjuk[1]

[1]Kherson National Technical University, Beryslav Road, 24, Kherson, 73008, Ukraine
[2]Bundeswehr University Munich, Neubiberg, 85577, Germany

Abstract

In this paper, the necessity of analysing and classifying the risks of multi-hazard threats by their origin and extent has been investigated. The proposed method of multi-hazard risk evaluation is based on the disposition of the set of valuable objects at critical risk, the set of active threats, and the set of manpower and resources for response operations. The result of applying the method is a categorization of the situations which allows decision-makers and local representatives to timely make adequate decisions in real-time situations.

Keywords

Bayesian network, critical infrastructure, directed acyclic graph, directed graphical model, event, multi-hazard, risk, threat.

1. Introduction

Since the full-scale Russian military troops invaded Ukraine, numerous buildings, bridges, railroads, dams and other critical infrastructure objects have been exposed to numerous risks, impairment, and demolishment, not mentioning the dire aftermath, such as casualties, devastation, uncertainty and refugees. From the very beginning of the invasion, they started spreading havoc and destruction, encroaching not only on military objects but also on residential areas, malls, gas stations and critical infrastructure [1]. The war also exacerbates environmental and ecological problems, such as global warming, drought, numerous wild- and steppe fires, contamination of rivers and lakes, and even poses a serious risk of diseases due to unsanitary conditions and dross. Henceforth, these issues lead to atrocious implications.

Moreover, there are not only physical threats to dissemination. The majority of critical objects and infrastructure are under attack from hackers and blackmailers wanting to disrupt the integrity of the system and outage entire regions and cities. Digital or cyber-threats comprise a type where a criminal combines two or more ways to commit system breakthroughs [2, 3].

CITRisk'2022: 3rd International Workshop on Computational & Information Technologies for Risk-Informed Systems, January 12, 2023, Neubiberg, Germany
EMAIL: 3674150@gmail.com (B.Sakovych); marina.jarikova@gmail.com (M.Zharikova); vgsherstyuk@gmail.com (V.Sherstjuk)
ORCID: 0000-0002-8863-0343 (B.Sakovych); 0000-0001-6144-480X (M.Zharikova); 0000-0002-9096-2582 (V.Sherstjuk)

All the above-mentioned threats are considered multi-hazardous and comprise a major percentile of the global scale. Generally, such threats are concentrated on undermining the defense and integrity of a country. Therefore, the European Union is devising stated risk assessment methods to properly inform aimed forces and representatives about emerging risks of threats. The aim is to evaluate the extent of the multi-hazard risk of threats and forward them to early warning systems and risk assessment mechanisms.

Those threats can be simultaneous and of different kinds, e.g., bombing, cyber-threats and shelling. They are considered destructive forces as they demolish both critical and civil infrastructure [4, 5, 6]. For this reason, it is rather crucial to foresee risks of and preclude upcoming threats by means of prevention, mitigation and preparedness through to disaster response, object recovery and restoration.

Nevertheless, when there is a risk of a disaster occurring, it may lead to numerous interwoven disasters causing each other, called domino, or cascading effects, and are explicable through various scientists.

The next section is devoted to analyzing the related research pieces of work. The subsequent section depicts the problem and the solution methods. Accordingly, the fourth section presents the achieved results and a description thereof. Ultimately, the last section comprises the used literature.

2. Related works

The multi-risk assessment and analysis are conducted by numerous scientists, and our local researchers have also performed certain investigations. The paper [3] depicts the problem of multi-hazard risk analysis and management. In this paper, the authors identify some gaps in the existing disaster risk reduction research projects. They used an all-new approach to multi-hazard risk analysis that considers all the components of multi-hazard risk with a spatial reference. The risk is presented in the form of the following components: hazard characteristics (danger, intensity, area affected by hazard), vulnerable object characteristics (location, vulnerability and speed of recovery), as well as spatio-temporal threat measured in the time it takes for the hazard to reach the object. It's proposed to present hazard risk in dynamics as passing through the following three stages: potential risk, the risk of threat, and destruction, respectively. Individual risk is presented as a trajectory in the n-dimensional space of its parameters, and multi-risk is assessed using the operation of taking the maximum. The proposed approach to risk analysis allows for diagnosing the situation and making decisions throughout the entire disaster risk management cycle and for early warning and response actions.

The paper [4] presented an event-based spatially distributed dynamic multi-hazard risk model for critical infrastructure objects. The model is based on the three-level spatial model, as well as the dynamic models of the socio-economic system, vulnerability, and event-based scenario model of hazardous process based on using a case-based approach to accumulate and store the scenarios of dynamics of various hazards and multi-hazards, their combination, and chains. Each case can be represented as a sequence of events plunged into a certain context, where each event can initiate scenarios describing the multi-hazard dynamics. The authors stated that the risk for a certain object at a certain time point is a combination of the object state (i), disaster threat (ii), the vulnerability of the object (iii), and potential damage (iv).

The paper [5] states that threats to critical infrastructures can be classified into three categories: natural threats (i), anthropogenic (ii), and technical (iii). Natural threats generally include weather problems; also, geological hazards like earthquakes, tsunamis, land shifting, and volcanic eruptions. Those can greatly affect CI, especially the transportation sector.

The anthropogenic, or human-driven threats are sometimes referred to as terrorism and disobedience. These may be cyber-attacks, explosions, critical infrastructure malfunction or invasion; transportation accidents, failures, and hazardous material accidents (Fig. 1).

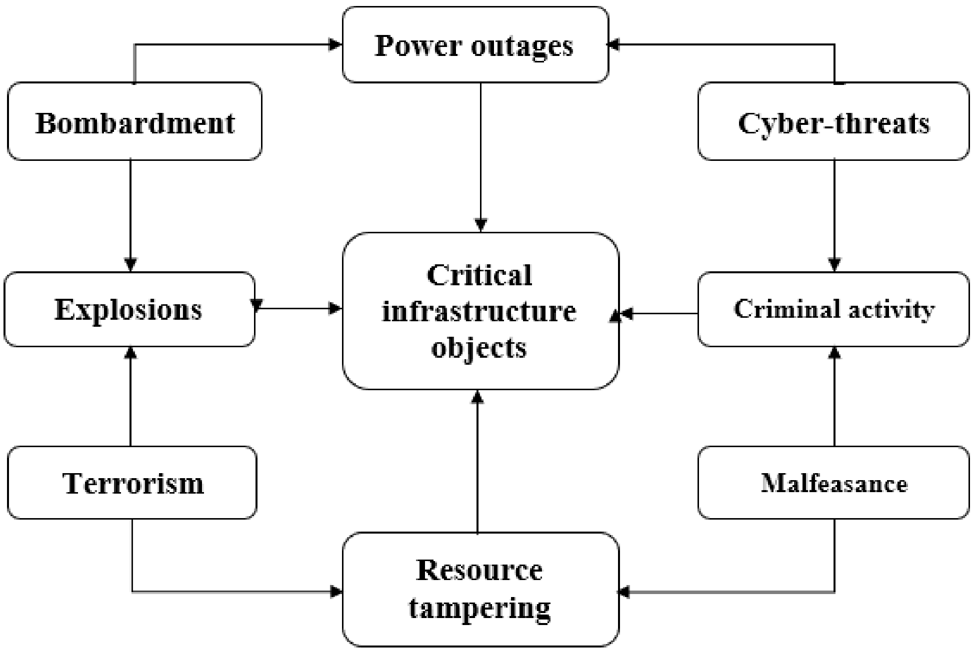

Figure 1: The numerous threats endangering objects of critical infrastructure

Authors of the paper [13] have estimated the multi-hazards of the global port infrastructure at asset levels in light of the numerous dangers, quantifying risks to damaged physical assets and logistics services (port risk) and risks to maritime trade flows (trade risk). The researchers found that nearly 86% of all ports are imposed to more than three hazards. Therefore, the authors have identified a few issues that impede an expansion of the detailed risk analysis to a global scale. First, ports can be damaged by several various hazards that affect the infrastructure and operation of the port, making risk analysis difficult. In addition to affecting the port assets themselves (cranes, terminals), ports are built into local networks of critical infrastructures, such as railways, roads, and electricity damage which can stop the port functions, even if the port is not damaged itself.

Also, in the paper [14] authors have conducted research, in which hazard information can help prompt effective public responses and, consequently, reduce injuries and fatalities by compiling recommendations on how to develop actionable and understandable multi-hazard warning messages. The authors designed various multi-hazard overviews and hazard messages, which were refined during the five virtual workshops we conducted with experts from different fields and surveyed the public to check whether our designs increase people's intention to take action and help them correctly interpret the information presented. In contrast, the hazard overviews with time and action indications significantly increased people's understanding of whether they should take immediate action. Moreover, adding a time- and action-related icon to the hazard messages significantly increased people's intention to take action. For both hazard overviews and messages, people's intention to take action was found to be proportional to the hazard's severity and urgency and influenced by various personal factors, such as past hazard experiences. To conclude, rendering information on multi-hazard platforms more actionable can prompt public responses and, in turn, increase society's resilience toward disasters.

The paper [15] proposes a three-level multi-risk assessment framework that considers possible interactions between threats and risks. The first level represents a flowchart to help users determine whether a multi-threat and multi-risk approach is required. The second level is a semi-quantitative approach to determine whether a more detailed quantitative assessment is necessary. Ultimately, the third level comprises a detailed quantitative analysis of multiple risks based on Bayesian networks.

3. Problem statement

There are a lot of techniques representing interactions and interrelations among hazards. In this paper, we are working on the proper classifier for the potential hybrid risk assessment. Classification is a part of data analysis and pattern recognition that requires a class label for the described instances by a set of attributes and can be implemented in various ways ranging from decision trees, graphs, lists, neural networks, random forests, and k-nearest classifiers.

One of the most efficient classifiers, in the sense that its predictive performance is competitive with state-of-the-art classifiers, is the so-called Naive Bayesian classifier, which learns from the training data, the conditional probability of each attribute A_i with the class label C. Classification is then performed by applying Bayes' rule to calculate the probability of a given C particular instance $A_1, \ldots, A_n$ and then predicting the class with the highest posterior probability. This computation is made feasible by a strong independence assumption: all attributes of A_i are conditionally independent by class value C [7, 8].

Another Bayesian classifier is a Bayesian network (BN) or directed graphical model (DGM) which represents itself as the joint probability distribution of a set of random variables with possible causal relationships. The network consists of nodes representing random variables, edges between pairs of nodes representing the causal relationship and a conditional probability distribution (CPD) at each node. The main purpose of the method is to model the posterior conditional probability distribution of the variable after observing new evidence. Bayesian networks can be built either manually with knowledge of the underlying domain, or automatically from a large dataset using e.g., Python libraries.

Bayesian networks [16-20] are widely used to represent cause-effect relations between hazards. They are statistical models (probabilistic graphical models) that use Bayes' rule to calculate the conditional probability associated with the occurrence of an event. BN can be used in any area where an uncertain reality needs to be modelled involving probabilities, such as risk management, portfolio allocation, insurance, predictions, various system modelling etc. [7, 8]. One of them is monitoring and alerting of hazards and imperilments utilizing cameras, or sensors where data from different sources can be integrated to get an interpretation of the obtained data. For example, to combine the latter from different sensors, angles and resolutions to determine what's in a scene, or industrial sensors can report the condition of the machine and a complete picture only emerges when all the measured values are combined. Frequently, sensor fusion problems must deal with different temporal or spatial resolutions and solve the "correspondence problem" of deciding which events from one sensor correspond to the same events reported by other sensors. BNs are quite robust to missing data, therefore they interweave information meaning each sensor has a finite chance of providing a correct depiction, hence combining the chances of all sensors usually increases the likelihood of a correct interpretation.

A traditional Bayesian network [16-20] consists of a set of variables whose conditional dependencies are represented by a directed acyclic graph (DAG) written as $G = [V, D]$, which is accompanied by a set of conditional probability tables (CPDs). A DAG is a type of directed graph without any directed cycles, where a cycle is a set of directed edges starting at a vertex $v \in V$, and if the arrows are followed in their direction, one will eventually return to the starting vertex. In a BN, each node on the directed graph corresponds to a random variable, and each directed edge implies a statistical dependency. In addition, each node is linked with a conditional probability distribution of the corresponding random variables, which is dependent on its parents in the DAG. Thus, if there is a directed edge from node a to node b in the graph G, node a is a parent of node b.

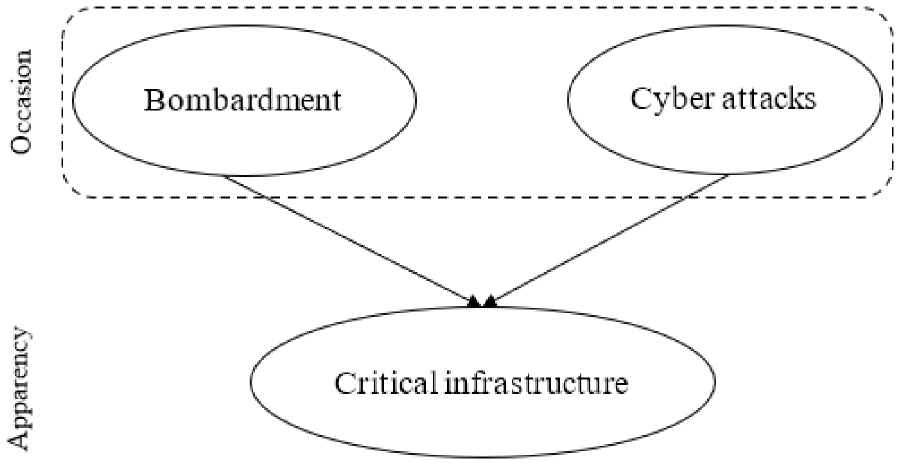

Figure 2: The directed acyclic graph with two destructive activities that lead to critical infrastructure impairment

The two causes in this trivial example are assumed to be independent, i.e., there is no boundary between the two causal nodes, but this assumption is not necessary for the general case. If there is no loop in the graph, Bayesian networks can capture as many causal relationships as are needed to accurately describe a real-life situation. Since a DAG represents a hierarchical structure, here are utilized terms such as "parent", "descendant", "ancestor", "descendant" or just specific nodes. The probability of a random variable of a graph depends on its parent nodes:

$$P(A_1, \dots, A_x) = \prod_{i=1}^{x} P\left(A_i | Par(A_i)\right)$$

The concept of Bayesian networks [16-19] is constructed on Bayes' theorem [16, 17], which assists us with the expression of the conditional probability distribution of a cause given the observed evidence using the inverse conditional probability of the observed evidence below. The Bayes theorem describes the probability of a hypothesis given some observed evidence, in terms of the prior probability of the hypothesis and the likelihood of the evidence under the hypothesis.

4. Solution methodology

The novelty of this work in comparison with the related ones is that the proposed risk analysis covers all three main phases of the crisis management cycle such as pre-crisis, response, and post-crisis. Within each phase, the risk is evaluated differently. As a result, it is divided into potential (for the pre-crisis phase), active (for the response phase), and posterior risk (for the post-crisis phase), which allows decision-makers to make more conformed decisions at every phase of the crisis management cycle.

Hereby, we suggest a crisis management cycle that is divided into three phases: pre-crisis, response, and post-crisis. The main characteristics of risk in the research context imply that it is dynamic and spatially distributed. As for the first one, we presume that for any spatial location, risk will change depending on affecting of multi-hazard threats. For the latter, let us suppose the risk can be evaluated for each area of the territory or for each vulnerable object, which provides its spatial reference. The subject of risk analysis in the proposed model is the evaluation of the chance of losses as a result of the involvement of the target object (here – critical infrastructure objects).

The risk originates from the interaction of multi-hazards and targeted objects, such as infrastructure (including critical), communities and governments affected by that threat. In this regard, risk dimensions include:

1) the probability of threat occurrence which depends on whether the actor has a certain goal and threat potential which depends on the availability of tools used by the actors (if applicable);
2) the characteristics of the targeted object such as object vulnerability, potential damage, and the speed of object restoration;
3) the availability of the object for the actors created the hazard.

Subsequently, multi-hazard risk assessment can be represented as a combination of the following components:

1) evaluation of the probability of a threat occurrence (P_T);
2) availability of tools at the disposal of the actor (threat potential evaluation) (E_T);
3) availability of targeted object for actor (A_O);
4) vulnerability of targeted object (V_O);
5) speed of object recovery (S_O).

Thus, a qualitative multi-hazard risk evaluation for the targeted object at any time moment *t* will be a point or an area in the n-dimensional space of qualitative values of the multi-hazard risk components:

$$R(t) = (P_T, E_T, A_O, D_{O,} V_O, S_O)$$

This risk evaluation is dynamic and can be assigned to each vulnerable object and area of the territory. Next thing, we create a directed graphical model (Fig. 3).

The above model represents bombardment (B), cyber-threats (C), and potential or imposed damage (D) to the infrastructure (I), including critical objects. The probability algorithm for bombardment (B) is constructed below:

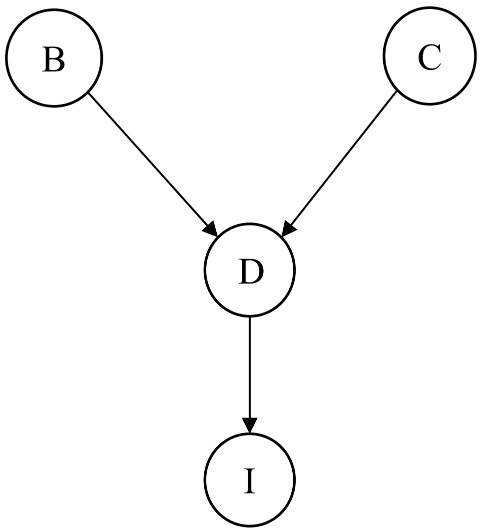

Figure 3: The proposed DGM

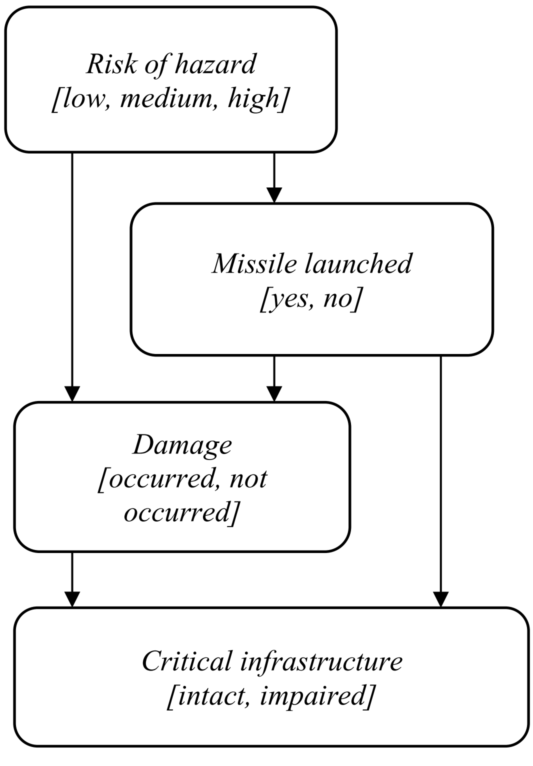

Figure 4: The Bayesian network sketch for bombardment (shelling) event

Let's modelling this with a Bayesian network. Assume that we have two risk levels: low (0-0.5) and high (0.5-1). Our goal is to classify the risks given according to their uprising intensity utilizing the classification method. Let's create the case probability table (see Table 1).

In this case, we can apply the Bayes theorem to model the probability of infrastructure damage (D) given the occurrence of air bombardment (B) and cyber-threats (C). We can express this probability as:

$$P(D|B,C) = \frac{P(B|D)P(C|D)P(D)}{P(B,C)}$$

where *P(D | B, C)* is the posterior probability of *D* given *B* and *C, P(D)* is the prior probability of *D*, *P(B | D)* is the conditional probability of *B* given *D, P(C | D)* is the conditional probability of *C* given *D*, and *P(B, C)* is the joint probability of *B* and *C*.

In the Bayesian network, we can represent these probabilities using conditional probability tables (CPTs) and prior distributions for the variables B, C, and D. The CPTs specify the conditional probabilities of each variable given its parents in the network, while the latter represents the initial probabilities of each variable before any evidence is observed.

Specifically, the Bayesian network for multi-risk critical impairment includes the following components:

- the *B* variable represents the occurrence of bombardment, which has a prior distribution *P(B)* = [0.6, 0.4] for low and high-risk levels;
- the *C* variable represents the occurrence of cyber-threats, which has a prior distribution *P(C)* = [0.7, 0.3] for low and high-risk levels;
- the *D* variable represents the potential damage to infrastructure, which depends on both *B* and *C*.

In particular, the CPT for D given B and C specifies the following probabilities:

This CPT specifies that the probability of infrastructure damage depends on both the levels of bombardment and cyber threats. For example, if both B and C are low, then the probability of D being low is 0.9, and the probability of D being high is 0.1.

Table 1
Damage risk conditional probabilities

B	C	D	P(D|B,C)
Low	Low	Low	0.9
Low	Low	High	0.1
Low	High	Low	0.5
Low	High	High	0.5
High	Low	Low	0.1
High	Low	High	0.9
High	High	Low	0.2
High	High	High	0.8

Using the Bayes theorem, we can compute the posterior probability of *D* given specific values of *B* and *C*, based on the prior probabilities and the conditional probabilities specified in the CPT. For example, if we observe that both *B* and *C* are high-risk, then we can compute the posterior probability of *D* being low-risk as follows:

$$P(D = Low \mid B = High, C = High) = \frac{P(D = Low)P(B = High \mid D = Low)P(C = High \mid D = Low)}{P(B = High, C = High)}$$

Based on the given DAG of the Bayesian network, we can define the joint probability distribution:

$$P(B, C, D) = P(B) * P(C) * P(D \mid B, C)$$

In the expression above, P(B) and P(C) are the marginal probabilities of the nodes B and C, and P(D | B, C) is the conditional probability of D given B and C. We can now represent this using a probability table (probability matrix). Let's assume that each node can take on only two values: 0 or 1, representing the absence or the presence of each event.

$$P(B = 0) = 0.6 \quad P(C = 0) = 0.8$$
$$P(D = 0 \mid B = 0, C = 0) = 0.9, \quad P(D = 1 \mid B = 0, C = 0) = 0.1$$
$$P(D = 0 \mid B = 0, C = 1) = 0.3, \quad P(D = 1 \mid B = 0, C = 1) = 0.7$$
$$P(D = 0 \mid B = 1, C = 0) = 0.2, \quad P(D = 1 \mid B = 1, C = 0) = 0.8$$
$$P(D = 0 \mid B = 1, C = 1) = 0.01, \quad P(D = 1 \mid B = 1, C = 1) = 0.99$$

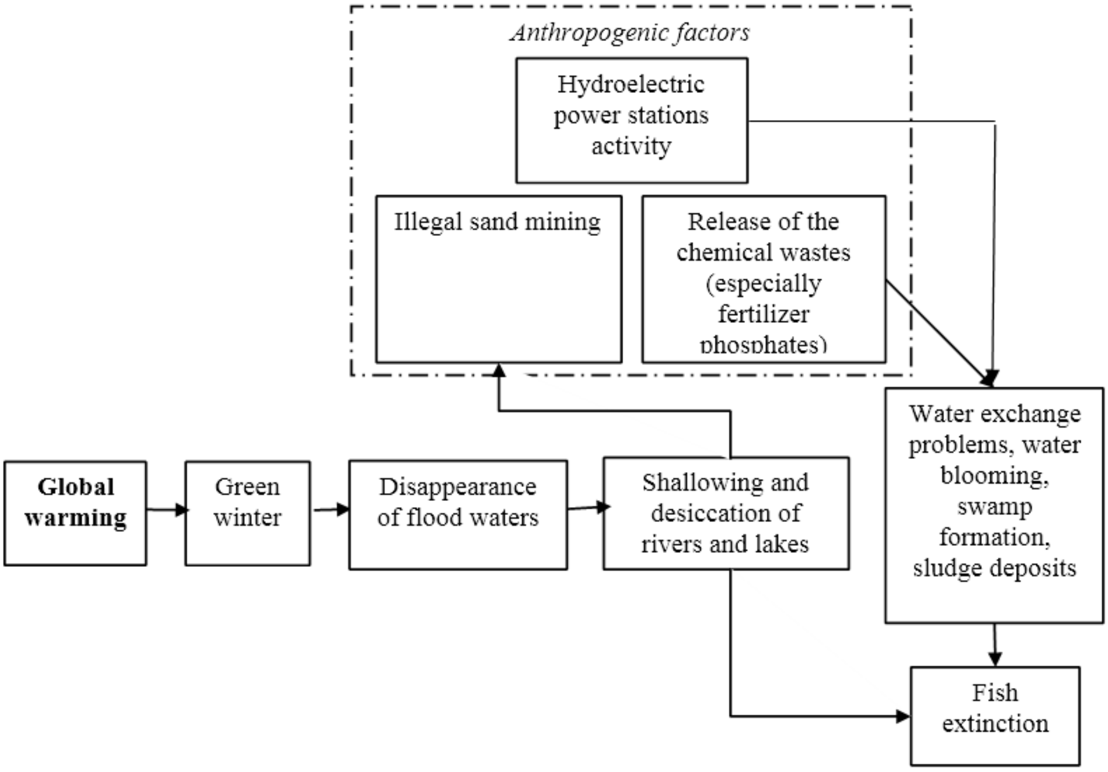

Figure 5: The event tree of river shallowing factors

5. The issues of shallowing the Dnipro River

Global warming leads to snowless winters, which in turn cause a decrease in floodwaters, shallowing the rivers and lakes and thus they desiccate. Moreover, anthropogenic factors also create problems. For instance, such an anthropogenic factor as illegal sand mining leads to the Dnipro River shallowing: the soil moves towards the formed voids, the pits are tightened, but the river channel changes (see Fig. 5).

The next set of issues is tightly associated with industrial, agricultural and domestic wastewater. Phosphates, which enter the Dnipro in unlimited quantities, become the main cause of water bloom. The decomposition products of algae absorb oxygen and evolve into an ideal breeding ground for bacteria and lack of oxygen result in fish extinction.

The normal existence of fish is hindered by obstacles that stand in the way of their migration, which is caused by a change in the chemical composition of the water caused by an increase in its temperature due to a slowdown in its flow due to the corresponding influence of hydroelectric power plants built on the river.

5.1. The deforestation issues

Here is the example of artificial coniferous forests planted around the Lower Dnipro Sands (Oleshky Sands) in the Kherson region, in Southern Ukraine. Those sands sometimes are qualified as a semi-desert. Sands are surrounded by dense coniferous forests planted to prevent dunes from moving. Despite the relatively small areas of the steppes, they are composed mainly of sand, so they often experience sandstorms.

The first reason leading to deforestation is global warming. Another reason is the increasing frequency of forest fires, the scale of which can already be regarded as a global disaster. In addition, forests are prone to insect infestations, which are destroying them at an increasing rate. A completely different reason is that the underground level of water is falling more and more, causing the forests to dry out, which leads to the desolation of forests covering large areas. Such territories gradually turn into sand deserts and causes the movement of sands (Fig. 6).

Unfortunately, in recent years, these processes have acquired a systemic character, significantly changing the natural landscape in many parts of the territory, which causes serious impacts on the ecosystem and affects slowly proceeding climate changes, exacerbating them.

5.2. The shallowing issue

Shallowing the rivers and lakes in Polissya (the northern part of Ukraine, both the part of the territory of Belarus and Poland) gives rise to fires in Chernobyl. Thereby, the ecological danger in the exclusion zone is caused by the presence of nuclear and radiation hazardous objects. Unfortunately, radioactive contamination can spread far beyond this zone, especially as a result of fires.

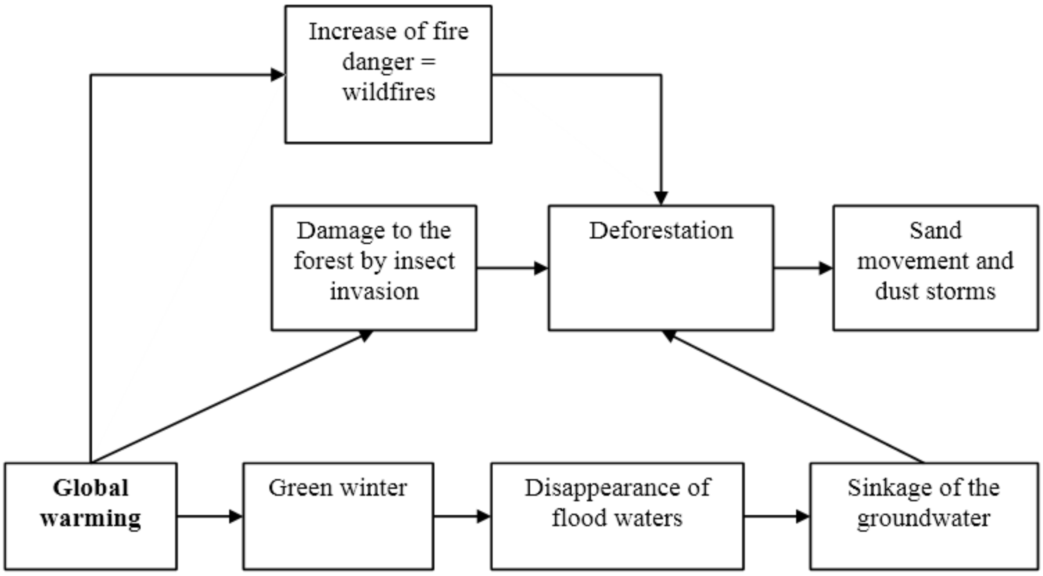

Figure 6: The tree-like primary factors of deforestation

Clearly, the ecosystem of the Kherson region suffers by itself, and, although it causes significant risks to human life, but does not pose an immediate threat to life and health of people. Unlike it, the ecosystem of the Chernobyl exclusive zone is under significant risk of the transfer of radioactive dust that settle down at the forests in this region. The influence of various factors such as strong winds and precipitation during large scale forest fires pose immediate and permanent risk to people health and life (Fig. 7).

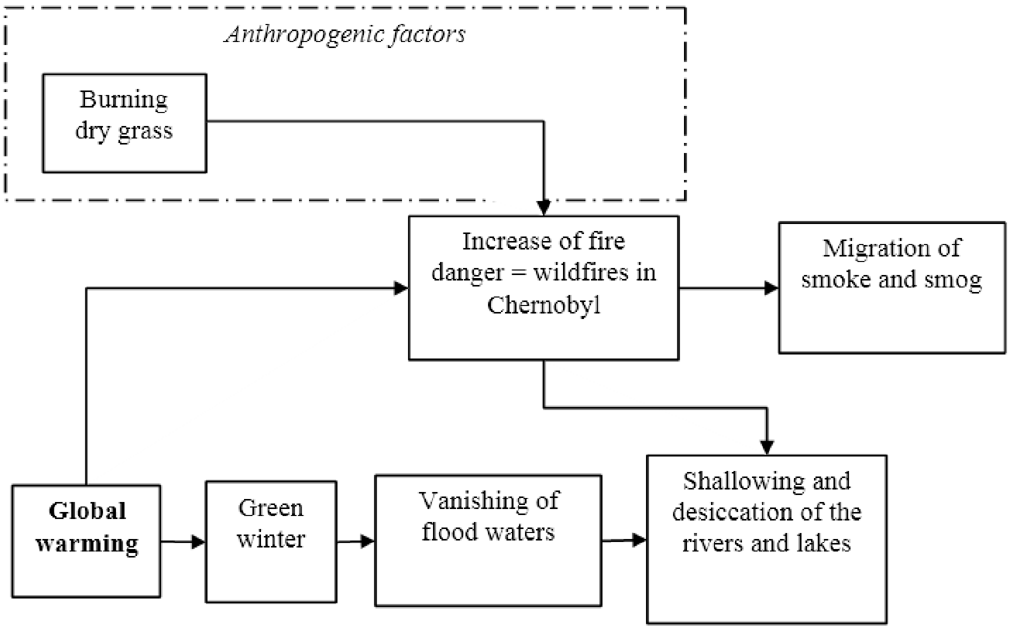

Figure 7: The chain reaction of global warming and anthropogenic factors interference

6. Implementation

The proposed model has been implemented using Visual C++ based on the Free-BN Library and approbated on the simulated area.

The simulation area is the Lower Dnieper Sands (Oleshky Sands) in the Kherson region, in Southern Ukraine. The sands are surrounded by very dense artificial coniferous forests that prevent the sands from moving during strong winds. Global warming leads to the loss of forests in this area. As a result of global warming, we can observe chains of cascading effects. Due to warming, the groundwater levels are decreased, which further increases fire danger, rapid destruction of forests in large areas, desertification of the territory, and the revival of sand movement. Due to warming, forests are also being affected by invasions of insects, and also become more prone to forest fires (Fig. 8).

The results of the conducted simulation show that the proposed model provides enough performance to real-time modeling of a wide range of natural processes from climate change to forest fires and adequate knowledge representation about cascading events taking into account the uncertainty of the observations.

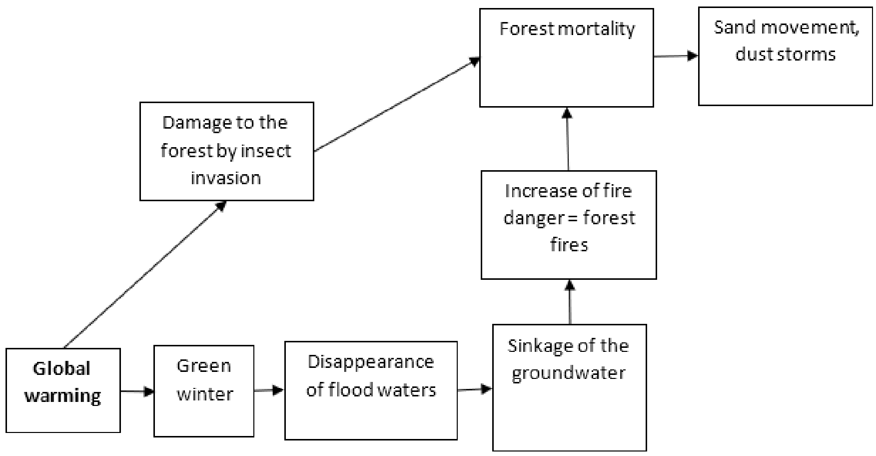

Fig. 8. Cascading chains of events in Kherson Region

The developed software contains a set of functions and procedures that allow defining events, their hierarchies, build DAGs, and assign probabilities transforming the event model into Bayesian networks. The infrastructure hierarchies can also be defined based on the spatially referenced objects' definitions. The developed software is intended for use in the decision support system, which aimed to assess dangers, threats and risk with respect to the pre-defined objects.

The Bayesian Network multi-hazard risk model has been approved and tested within the simulated spatial model of Kherson Area, Ukraine. The simulations of multi-hazard disasters have been carried out to assess dangers, threats and multi-risk posed to various objects within the simulated area by multi-hazard disasters. We evaluate the performance of the decision-support queries directed to assessing multi-risk for the separate objects (buildings), their multitudes (quarters), and the entire areas. Thus, the query response time has been evaluated and averaged. The obtained result of the simulation is represented in Fig. 9.

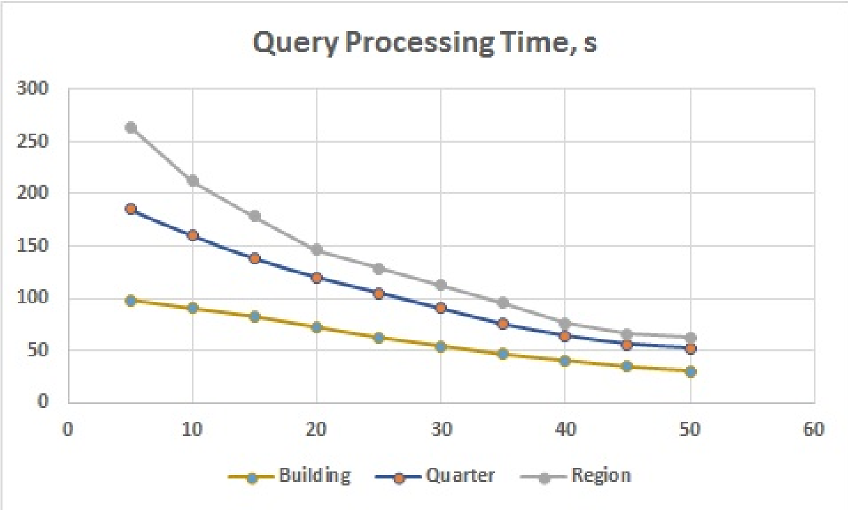

Figure 9: The simulation results

The adequacy of the multi-hazard risk model is confirmed by the above-mentioned experiment. The obtained results allow us to confirm that the developed multi-risk assessment model based on the Bayesian Network provides sufficient performance. Thus, it allows to simulate multi-hazards that contain cascading and triggering effects such as shallowing of Dnipro river and lakes, as well as variety of deforestation issues, dehydration of water sources, etc. Of course, forest fires, tornadoes, sandstorms, and other disasters can be also considered.
Due to the sufficient efficiency of the proposed models, the decision-support system helps decision-maker timely assess threats and risks from emerging events for various infrastructures and objects spatially distributed in an analyzed area of interest.

7. Conclusions

In this paper, the necessity of analysing and classifying the risks of multi-hazard threats by their origin and extent has been investigated. The proposed method of multi-hazard risk evaluation is based on the disposition of the set of valuable objects at critical risk, the set of active threats, and the set of manpower and resources for response operations. The result of applying the method is a categorization of the situations which allows decision-makers and local representatives to timely make adequate decisions in real-time situations.

The crisis management cycle is propped to divide into three phases: pre-crisis, response and post-crisis is presented. The risks according to their uprising intensity utilizing the classification method were sorted. The comprehensive approach of combining relevant tools to prevent, counteract, and recover from the impact of multi-hazards in a coordinated manner to support risk-informed decisions at all phases of the crisis management cycle is depicted. Moreover, the novel method of multi-hazard threat classifying is proffered. As a result, it is divided into potential (for the pre-crisis phase), active (for the response phase), and posterior risk (for the post-crisis phase), which allows decision-makers to make more conformed decisions at every phase of the crisis management cycle.

References

[1] What is a hybrid attack, Security Encyclopedia, HYPR, 2022. URL: https://hypr.com/security-encyclopedia/hybrid-attack

[2] Joint Framework on countering hybrid threats a European Union response, European Commission, Document 52016JC0018, 2018. URL: https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52016JC0018

[3] M.Zharikova, G.Barbeito, M.S.Nistor, S.W.Pickl, Spatially-Distributed Multi-Hazard Risk Analysis, CITRisk, 2021, pp. 83-92

[4] M.Zharikova, V.Sherstjuk, Event-Based Spatially Distributed Multi-Risk Analysis, In: N.Shakhovska, M.O.Medykovskyy (eds) Advances in Intelligent Systems and Computing V.CSIT 2020, Advances in Intelligent Systems and Computing, Springer, Cham, 1293, 2021. DOI: 10.1007/978-3-030-63270-0_55

[5] V.Sherstjuk, M.Zharikova, S.Pickl, M.A.Villota, I.Dorovskaja, D.Chornyi, Modeling Hybrid Attacks and Operations to Assess the Threats in Early Warning Systems, 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, 2022, pp. 39-44. DOI: 10.1109/ACIT54803.2022.9913106

[6] J.Liu, Y.Wang, L.Zha, X.Xie, E.Tian, An event-triggered approach to security control for networked systems using a hybrid attack model, International Journal of Robust and Nonlinear Control, 31, 12, 2021, pp. 5796-5812

[7] Strategic Compass. Council of the European Union, 2022. URL: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

[8] G.Giannopoulos, H.Smith, M.Theocharidou, The Landscape of Hybrid Threats: A conceptual model, Ispra, European Commission, PUBSY, 117280, 2021

[9] S.Haji, Q.Tan, R.Soler Costa, A Hybrid Model for Information Security Risk Assessment, International Journal of Advanced Trends in Computer Science and Engineering, 8, 1.1, 2019, pp. 100–106

[10] F.Aguessy, O.Bettan, G.Blanc, V.Conan, H. Debar, Hybrid Risk Assessment Model based on Bayesian Networks, In Proc. of the 11th International Workshop on Security (IWSEC 2016), Tokyo, Japan, 2016, pp. 21–40

[11] F.Aligne, J.Mattioli, The Role of Context for Crisis Management Cycle, In F. Burstein et al.(eds.), Supporting Real Time Decision-Making, Annals of Information Systems 13, Springer, New York, 2010,pp. 113-132. DOI: 10.1007/978-1-4419-7406-8_6

[12] R.J.Robles, M.K.Choi, E.S.Cho, S.S.Kim, G.Park, J.Lee, Common threats and vulnerabilities of critical infrastructures. International journal of control and automation, 1(1), 2008, pp.17-22

[13] J.Verschuur, E.Koks, S.Li, J.Hall, Multi-Hazard Risk to Global Port Infrastructure and Resulting Trade and Logistics Losses, 2022

[14] I.Dallo, M.Stauffacher, M.Marti, Actionable and understandable? Evidence-based recommendations for the design of (multi-) hazard warning messages, International Journal of Disaster Risk Reduction, 74, 2022, 102917

[15] Z.Liu, F.Nadim, A.G.Aristizabal, A.Mignan, K.Fleming, B.Q.Luna, A three-level framework for multi-risk assessment, Georisk: Assessment and Management of Risk for Engineered Systems and Geohazards, 9:2, 2015, pp. 59-74. DOI: 10.1080/17499518.2015.1041989

[16] Introduction to Artificial Intelligence with Python, CSCI E-80, Harvard Extension School, 2020. URL: https://cs50.harvard.edu/extension/ai/2020/fall/notes/2/

[17] M.Horný, Bayesian networks, Boston University School of Public Health, 17, 2014

[18] A.V.Kolesnyk, S.V.Smelyakov, P.H.Berdnyk, O.I.Kolodyazhnyy, A Bayesian network-based method for assessing the risk of engine failure on an aircraft in flight, collection of scientific papers of the Kharkiv National University of the Air Force, 2(64), 2020, pp. 53-60
[19] N.Ruozzi, Bayesian Networks, Erik Jonsson School of Engineering & Computer Science at the University of Texas at Dallas. URL: https://personal.utdallas.edu/~nrr150130/gmbook/bayes.html C
[20] J.van Westen, S.Greiving, N.R.Dalezios (Ed.), Chapter 2, Multi-hazard risk assessment and decision making, in: Environmental Hazards Methodologies for Risk Assessment and Management, IWA Publishing, 2017, p. 64