UDC 351.74:656.078.5
DOI 10.37772/2309-9275-2024-2(23)-5
JEL classification: G 21, H 56, L 94

RISKS OF CRITICAL INFRASTRUCTURES DURING WAR

Viacheslav BEREZUTSKYI, ORCID 0000-0002-7318-1039, ResearcherID 57204552541[1]
Tetiana TOKHTAMYSH, ORCID 0000-0002-5534-3284, ResearcherID JSL-3854-2023[2]

[1]Department of Occupational and Environmental Safety, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
[2]Department of Economics and Marketing, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine

Corresponding author: Viacheslav Berezutskyi, email: viaberezuc@gmail.com

Abstract. Critical infrastructures becomes one of the main targets during war because of its important role in ensuring the functioning of the state and society. Destruction or damage to critical facilities can have catastrophic consequences for security, the economy, and the lives of citizens. Modern issues related to determining the risk of critical infrastructures during war are considered. ChatGPT is used to determine the probabilities of risks of critical infrastructures. With the help of this chat, a general overview of probabilities was made based on the assumptions made on the basis of the analysis of modern wars in Ukraine and other countries of the world. The obtained results are presented in the form of network diagrams. Shown. that modern wars are more dangerous for the population, due to the desire to destroy critical infrastructures and have a negative impact on the population of countries. Risk in the classic form is considered as a combination of two components, namely the probability of an event and its consequences. This article deals with the first part, that is, the probability of events according to their criticality. The next article will consider the consequences according to their criticality.

Keywords: risks, critical infrastructures, war, population, threat probability.

Author's contribution
The authors made an equal contribution to the article. Together they selected literature, analyzed it and drew common conclusions.

Disclosure statement
The authors have not any competing financial, professional, or personal interests from other parties.

INTRODUCTION

Selection of risk analysis methods based on the use of probability and consequences

The article (Osei-Kyei R., Tam V., Ma M., Mashiri F., 2021) presents approaches to determining the risks of critical infrastructures. In modern society, critical infrastructures (CIs) resilience has become a critical issue in crisis management and CIs protection.a total of 31 threats/hazards are identified, with the most reported threats/hazards being: (1) natural disasters, (2) ageing and decay, (3) cyber threats, (4) terrorist activities, (5) contamination and (6) cascading failure/threat. The findings of this study provide a solid foundation for future research on developing CIs resilience. Additionally, the findings will inform policy makers and government authorities of the salient threats affecting the building of CIs resilience.

European countries are concerned about ensuring that critical infrastructure risks are minimized. While safeguarding critical infrastructure is primarily a national responsibility, the EU and NATO

have stepped up efforts to counter hybrid threats and protect critical infrastructure. The EU and NATO can further increase co-operation in this area through more extensive intelligence sharing and the intensification of joint training and exercises, to better counter hybrid threats (Pillai H., 2023).

In the article (Huth M., Dьerkop S., 2018), the authors focused on the critical logistical infrastructure and develop an evaluation approach for decision makers to support them in channeling risk management activities. The evaluation considers how the limitation or breakdown of any element of the logistical network influences all supply chains that use the network. By calculating risk-induced costs for the supply chains, implications of risk can be quantified and used as a basis for decision making.

THEORETICAL REVIEW

In the article (Dunn M., 2007) the authors pays attention that the terrorist attacks of 11 September 2001 have led to an increased focus on the vulnerability of modern societies in general and the protection of so-called critical infrastructures in particular. however, drafting efficient protection plans has proven to be a challenge: requirements include sophisticated situation analyses, better understanding of vulnerabilities, and a political consensus on how protection measures should be prioritized.

The answer to this question can only be the implementation of a risk-oriented approach.

On 17 February 2017, the United Nations Security Council unanimously adopted Resolution 2341 on Protection of Critical apacities to Prevent Attacks against Critical Infrastructure and called upon Member States to address the danger of terrorist attacks against critical infrastructure. The resolution invites Member States to consider possible preventive measures in developing national strategies and policies. The document (The protection of critical infrastructures, 2018) attests to the threats and risks caused by terrorist attacks on infrastructure facilities and their negative impact on the economies of states. It should be taken into account that the modern war in Ukraine began and continued on the basis of attacks on the infrastructure of Ukraine.

In the article (Heino O., Takala A., Jukarainen P., Kalalahti J., Kekki,T., Verho P., 2019) the authors indicate that functioning and resilience of modern societies have become more and more dependent on critical infrastructures. Severe disturbance to critical infrastructure is likely to reveal chaotic operational conditions, in which infrastructure service providers, emergency services, police, municipalities, and other key stakeholders must act effectively to minimize damages and restore normal operations. This is exactly what was shown in the war in Ukraine.

In the article (Giannopoulos G., Filippini R., Schimmer M., 2012) the authors pays attention on metodology in risk assessment. It is indispensable in order to identify threats, assess vulnerabilities and evaluate the impact on assets, infrastructures or systems taking into account the probability of the occurrence of these threats. This is a critical element that differentiates a risk assessment from a typical impact assessment methodology.

METHODOLOGY

Risk research methodology

Methods to Identify Risks by Comparing the Probability and Consequences of Events Various methods are used to assess risks based on a comparison of probability and consequences of events. Method the Risk Matrix (Johnivan J.R., 2024). One of the most widely used methods. It involves a two-dimensional matrix:

- Probability of an event (low, medium, high, very high);
- Consequences of the event (insignificant, moderate, severe, catastrophic).

By combining these two factors, the risk level is determined. This method provides a clear view of how dangerous a particular event may be. For example, an event with a high probability but low

consequences might be moderate, while an event with low probability but catastrophic consequences might still be deemed severe.

An analysis of other methods that consider risks across probability and consequences has been performed. Method the What-If Analysis (Card A. J., Ward J., P. Clarkson J., 2012). This method involves systematically examining possible events through scenario analysis. It helps identify risks by evaluating the likelihood and consequences based on expert judgment and brainstorming of "what-if" scenarios. Method the Event Tree Analysis (ETA) (Andrews J., Dunnett S.J., 2000). ETA helps analyze the probability and consequences of events by constructing an event tree. This graphical method visualizes all potential scenarios following an initiating event and determines their probabilities and impacts. It is useful for understanding multistep risks. Method the Fault Tree Analysis (FTA) (Bakeli T., Alaoui Hafidi A., 2020). FTA is a logical, graphical method used to identify the causes of an undesirable event. It is also a quantitative risk assessment tool that allows for evaluating the likelihood of critical events based on the probability of contributing factors. Method the SWOT Analysis (Threats and Opportunities) (Sharath Kumar C R, Praveena K.B, 2023). SWOT analysis can be employed to identify internal and external risks and opportunities, combining the data on probability and consequences of threats to develop better risk management plans. Method the Risk Cost Analysis (Cost Risk Analysis, 2024). This method evaluates the potential cost of a risk based on its likelihood and potential consequences. It helps organizations make financial decisions about risk management, taking into account both probability and impact. Method the Business Impact Analysis (BIA) (Taarup J., 2020). BIA assesses the potential financial and operational losses from critical events. It evaluates the likelihood of these events and their consequences on business continuity. Method the Scenario Analysis (Keisle J.M., 2024). Scenario analysis forecasts potential future risks by modeling different event scenarios. It allows the assessment of the probability and impact of each scenario under certain conditions, helping to prepare for future risks.

These methods help systematically evaluate risks by considering both probability and consequences. This supports decision-making in risk management, helping organizations mitigate negative impacts.

RESULTS AND DISCUSSION

Probability Assessment (Defined as Low, Medium, High, Very High). Each critical infrastructure sector's threat level is determined based on probability, which is categorized as:

- Low: Minimal likelihood of disruption.
- Medium: Potential, but not highly likely.
- High: Likely under current circumstances.
- Very High: Almost certain to occur.

Consequences Defined (Insignificant, Moderate, Severe, Catastrophic)

- Insignificant: Minimal impact, easily managed.
- Moderate: Noticeable disruption but can be resolved with time and resources.
- Severe: Substantial impact on services, economic or social function.
- Catastrophic: Systemic collapse or long-term crisis, affecting the entire country or population.

Risk Assessment for Critical Sectors During War

The ChatGPT artificial intelligence program was used in the study (ChatGPT). Risk Assessment for Critical Sectors During War:

1. *Financial Institutions* (Banks). *Probability*: Medium to High (pic.1, Row 1). Financial systems may be targeted for economic destabilization. *Consequences*: Moderate to Severe. Ranging from temporary transaction delays to widespread financial collapse, affecting both local and international markets.

2. *Food Supply* Chains (Stores, Warehouses). *Probability*: Medium to High (pic.1, Row 2). Disruption of logistics and supply chains could lead to shortages. *Consequences*: Moderate to Severe. Depending on duration and geographic impact of disruptions, possibly leading to local famine or food scarcity.

3. Energy Systems (Electric Power, Transmission). *Probability*: High (pic.1, Row 3). Energy infrastructure is a frequent target in warfare to weaken the adversary. *Consequences*: Severe to Catastrophic. As electricity is essential for the functioning of critical services (healthcare, water, communications).

4.Information Systems (Data Centers, Internet). *Probability*: High (pic.1, Row 4). Cyberattacks or physical damage to data centers can disrupt communications and access to information. *Consequences*: Severe. Potentially halting business operations, disrupting communication, and creating national security risks.

5. Space Research and Satellite Communication Centers. *Probability*: Low to Medium (pic.1, Row 5). These are less likely to be immediate targets but could face indirect damage. *Consequences*: Moderate, with disruptions to satellite communications and intelligence services but less direct impact on daily civilian life.

6. Educational Institutions (Schools, Research Centers). *Probability*: Medium (pic.1, Row 6). Schools and universities may be closed or repurposed for other wartime uses. *Consequences*: Moderate to Severe, especially long-term, as disruptions affect future generations' education and research outputs.

7. Logistics (Transport Networks, Fuel Stations). *Probability*: High (pic.1, Row 7). Logistics and transportation systems are essential for military and civilian purposes and are likely targets. *Consequences*: Severe to Catastrophic, with direct impacts on supply chains for food, military resources, and essential services.

8. Communication Systems (Mobile Networks, Radio, TV). *Probability*: High (pic.1, Row 8). Communication systems are critical for both civilian and military operations. *Consequences*: Severe, as disruptions can lead to information blackouts, chaos, and reduced coordination.

9. Water Supply and Sewerage Systems. *Probability*: Medium to High (pic.1, Row 9). Water infrastructure is often targeted to pressure the civilian population. *Consequences*: Severe to Catastrophic, as water supply is crucial for survival and hygiene, potentially leading to public health crises.

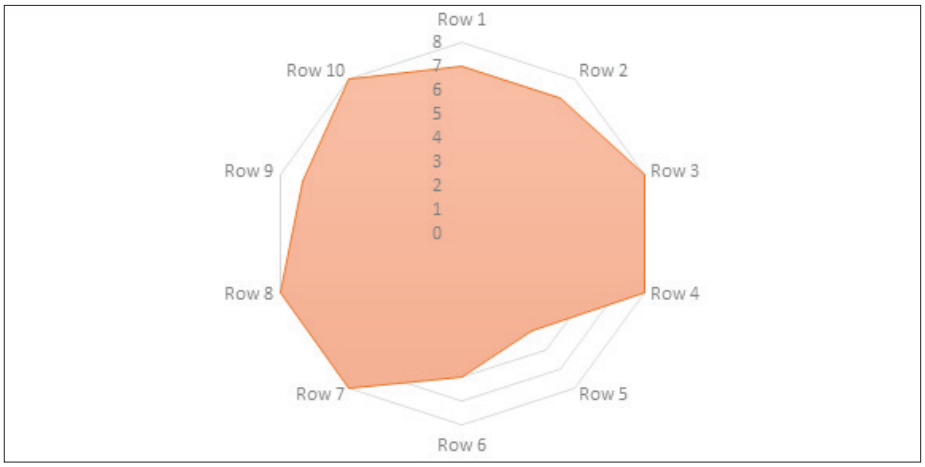
10. Healthcare Systems (Hospitals, Pharmacies). *Probability*: High (pic.1, Row 10). Healthcare is often overwhelmed during wartime due to increased casualties and disruptions in supply chains for medicine. *Consequences*: Catastrophic, as it leads to increased mortality, inability to treat injuries, and public health emergencies.

Based on the above critical infrastructures, in order to apply the Risk Matrix, we will consider the probabilities and consequences for each category of infrastructures. To present the risks graphically, we will divide them according to the point system (Table 1).

Table 1. Probability of Risk and the interval in points

Probability of Risk	**The interval in points (x10-1)**
Very High	9 - 10
High + Very High	8 - 9
High	7 - 8
Medium + High	6 - 7
Medium	5 - 6
Low + Medium	4 - 5
Low	0 - 4

Source: formed by the author

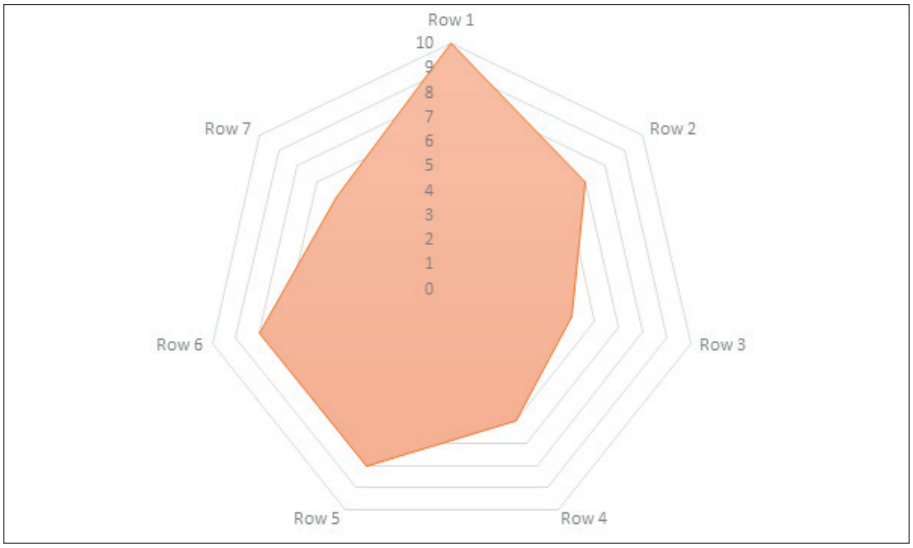


Pic. 1. Probability of Risk Assessment for Critical Sectors During War

Source: formed by the author

Assessing the probability for Critical Sectors During War**:**

1. *Assessing the probability* of a threat to financial critical objects (e.g., central banks, financial markets, stock exchanges, payment systems, etc.) during wartime requires analyzing various factors, including the geopolitical situation, the nature of the conflict, the intent and capabilities of the adversary, and the specific vulnerabilities of the financial sector. Here's an assessment based on typical scenarios: 1. Cyber Threats (e.g., hacking, ransomware attacks, DdoS). *Probability*: Very High (Tabl.1, pic.2, Row 1). 2. Physical Attacks (e.g., bombings, sabotage of financial infrastructure). *Probability*: Medium to High (pic.2, Row 2). 3. Insider Threats (e.g., collusion, sabotage by insiders). *Probability*: Low to Medium (pic.2, Row 3). 4. Disruption of Supply Chains (e.g., supply of essential technology or resources for operations). *Probability*: Medium (pic.2, Row 4). 5. Economic Warfare (e.g., sanctions, currency manipulation). *Probability*: High (pic.2, Row 5). 6. Financial Panic or Loss of Confidence (e.g., runs on banks, market collapses).*Probability*: High. (pic.2, Row 6) 7. Disinformation Campaigns (e.g., spreading false information to trigger market chaos). *Probability*: Medium (pic.2, Row 7).

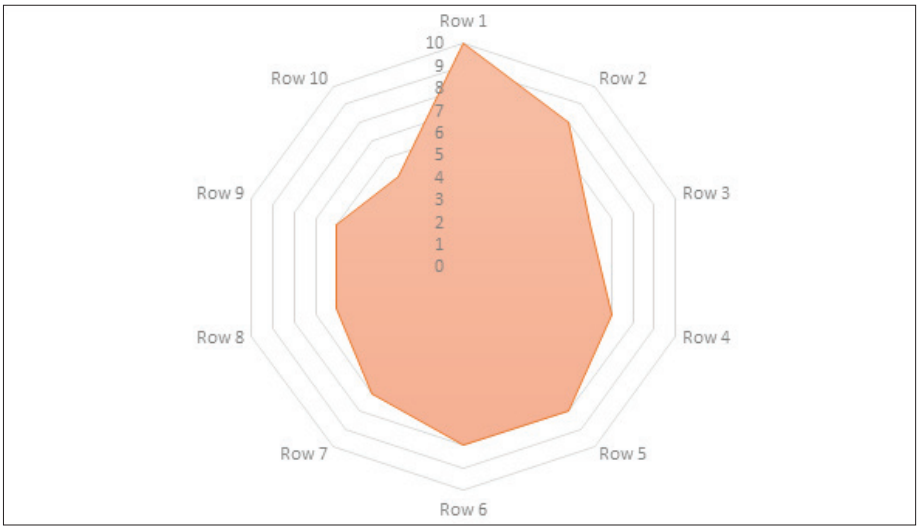


Pic. 2. The probability of a threat to financial critical objects

Source: formed by the author

Overall Risk Assessment – *Probability* of threat: High. Rationale: While not all threats are equally likely, financial systems are attractive targets during wartime due to their centrality to national stability. The likelihood of cyberattacks, economic warfare, and financial panic is particularly high. Physical attacks are less likely but still plausible depending on the war zone and adversaries' capabilities.

2. Assessing the probability of a threat to the operation of food establishments and warehouses (critical objects for food supply during wartime depends on several factors, such as the location of these facilities, the strategic importance of food supplies, and the nature of the conflict. Here's a probability assessment for various potential threats: 1. Supply Chain Disruptions (e.g., transportation routes, fuel shortages). Probability: Very High (pic.3, Row 1). 2. Cyber Threats (e.g., attacks on supply chain management, inventory systems). Probability: High (pic.3, Row 2). 3. Physical Attacks (e.g., bombings, sabotage, raids). Probability: Medium (pic.3. Row 3). 4. Looting and Theft. Probability: Medium to High (pic.3, Row 4). 5. Disruption of Utilities (e.g., power outages, water supply interruptions). Probability: High (pic.3, Row 5). 6. Economic Instability (e.g., inflation, food price spikes, rationing). Probability: High. (pic.3, Row 6). 7. Labor Shortages (e.g., military conscription, displacement of workers). Probability: Medium to High. (pic.3, Row 7). 8. Targeting by Hostile Forces (e.g., to undermine civilian morale or food security). Probability: Medium (pic.3, Row 8). 9. Regulatory Restrictions (e.g., food production controls, rationing policies). Probability: Medium (pic.3, Row 9). 10. Food Contamination Risks (e.g., chemical warfare, biological threats). Probability: Low to Medium (pic.3, Row 10).



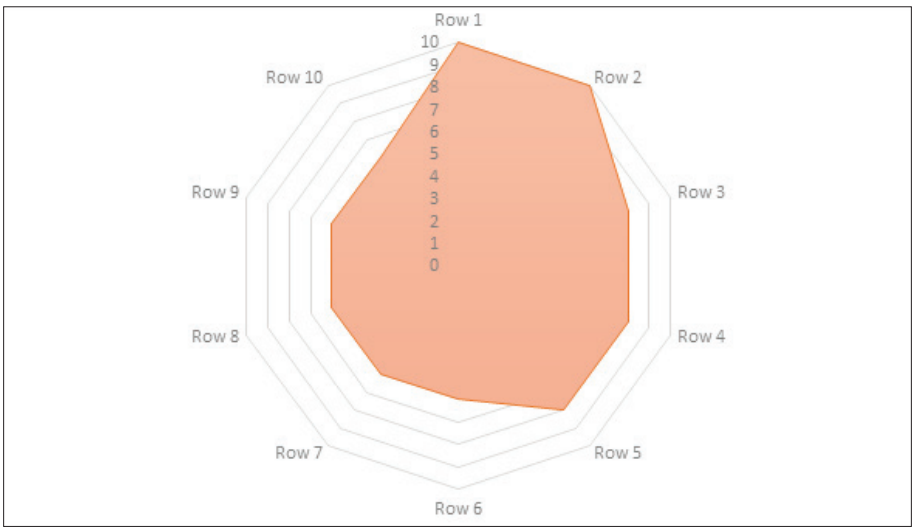
Pic. 3. The probability of a threat to the operation of food establishments and warehouses (critical objects for food supply

Source: formed by the author

Overall Risk Assessment: Probability of threat: High; Rationale: Food establishments and warehouses are vital to civilian and military logistics, making them potential targets in wartime. The most likely threats are supply chain disruptions, utility failures, economic instability, and cyber threats. While direct physical attacks and contamination risks are lower, the overall probability of significant operational threats is high, especially in conflict zones.

3. The probability of threats to the operation of electricity sources (e.g., power plants, renewable energy stations) and the means of transmission (e.g., power grids, substations, transmission lines)

during wartime is significant due to their critical importance for both civilian and military operations. Here's a detailed assessment of potential threats: 1. Physical Attacks on Power Plants and Transmission Infrastructure (e.g., bombings, sabotage). Probability: Very High (pic.4, Row 1). 2. Cyberattacks on the Power Grid (e.g., malware, ransomware, system hacking). Probability: Very High (pic.4, Row 2).. 3. Fuel Supply Disruptions (for non-renewable energy plants, such as gas or coal). Probability: High (pic.4, Row 3). 4. Damage to Transmission Lines and Substations (e.g., artillery, explosions, sabotage). Probability: High (pic.4 Row 4).. 5. Disruption of Maintenance and Repair Operations (e.g., restricted access, safety concerns for workers). Probability: High (pic.4, Row 5).. 6. Utility Workforce Shortages (e.g., conscription, displacement of workers). Probability: Medium (pic.4, Row 6)..7. Damage to Renewable Energy Sources (e.g., wind farms, solar panels). Probability: Medium (pic.4, Row 7). 8. Economic Instability (e.g., funding shortages, inflation). Probability: Medium (pic.4, Row 8).. 9. Natural Environmental Risks Amplified by War (e.g., floods, fires near power stations). Probability: Medium (pic.4, Row 9).10. Targeted Electromagnetic Pulse (EMP) Attacks. Probability: Low to Medium (pic.4, Row 10).



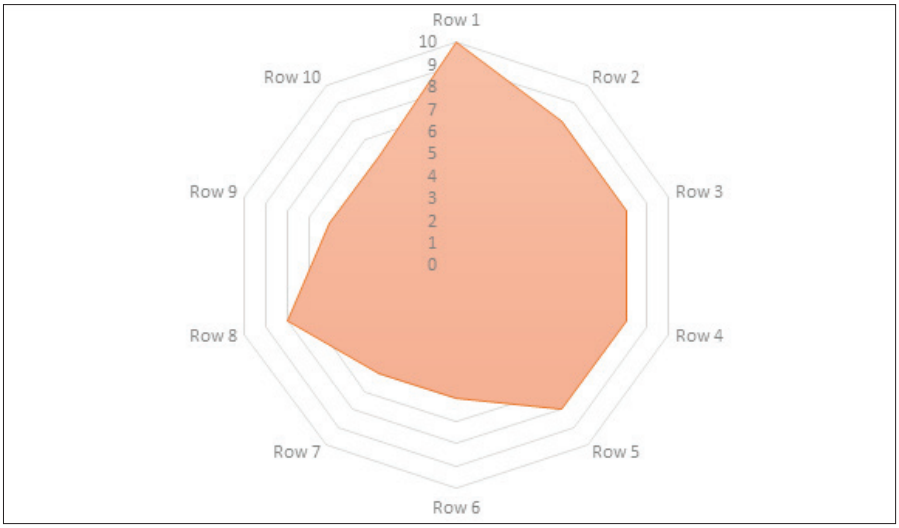
Pic. 4. The probability of threats to the operation of electricity sources

Source: formed by the author

Overall Risk Assessment. Probability of threat: Very High. Rationale: Electricity sources and transmission systems are critical to both military operations and civilian life, making them prime targets in any war. Physical attacks, cyber threats, and fuel supply disruptions are highly likely, given the strategic importance of crippling an adversary's power supply. Maintenance delays, workforce shortages, and economic instability further increase the risk, though they are secondary threats compared to direct attacks. The likelihood of widespread or prolonged outages is very high in active conflict zones.

4. The probability of threats to the operation of information centers and information storage systems (critical for communications, data storage, and command-and-control functions) during wartime is high, as these systems are vital to both military and civilian operations. Here's an assessment of the likelihood of various threats: 1. Cyberattacks (e.g., hacking, ransomware, DDoS attacks). Probability: Very High (pic.5, Row 1). 2. Physical Attacks (e.g., bombings, sabotage, direct strikes). Probability: High (pic.5, Row 2). 3. Power Supply Disruptions (e.g., grid attacks affecting data centers). Probability: High (pic.5, Row 3). 4. Insider Threats (e.g., sabotage by employees, espionage).

Probability: Medium (pic.5, Row 4). 5. Communication Infrastructure Disruptions (e.g., cutting off internet, satellite jamming). Probability: High ((pic.5, Row 5). 6. Denial of Service Due to Overload (e.g., increased demand from military and civilian use). Probability: Medium (pic.5, Row 6). 7. Natural Disasters Exacerbated by War (e.g., fires, floods affecting data centers). Probability: Medium (pic.5, Row 7). 8. Data Corruption or Destruction (e.g., targeted attacks on data integrity). Probability: High (pic.5, Row 8). 9. Legal or Regulatory Disruptions (e.g., restrictions on data sharing, international sanctions). Probability: Medium (pic.5, Row 9). 10. Economic Strain and Resource Shortages (e.g., lack of funds for maintenance or upgrades). Probability: Medium (pic.5, Row 10).



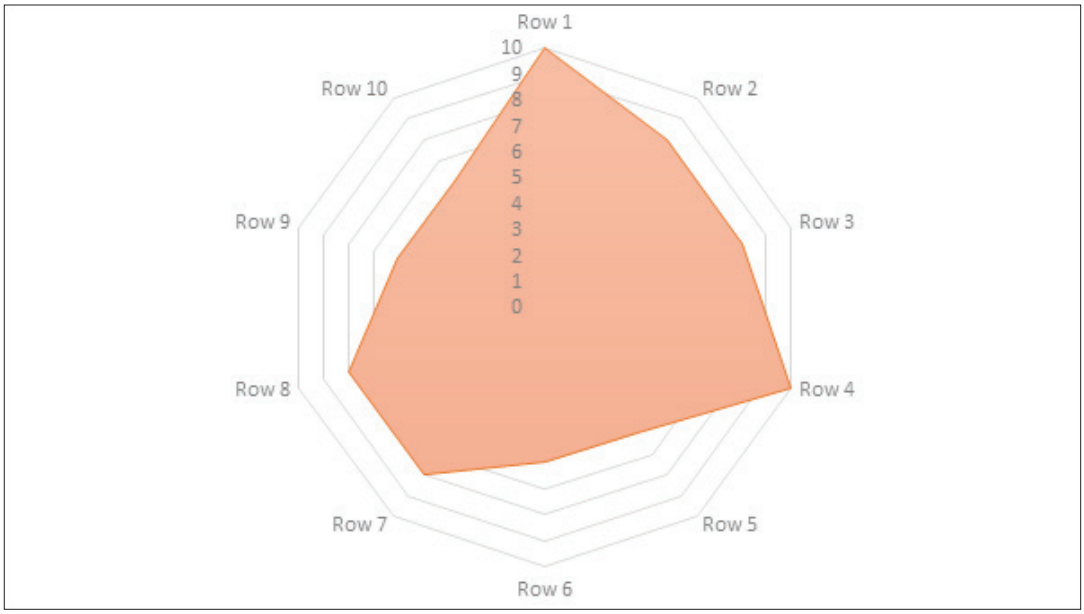
Pic. 5. The probability of threats to the operation of information centers and information storage systems

Source: formed by the author

Overall Risk Assessment. Probability of threat: Very High. Rationale: Information centers and storage systems are critical targets in modern warfare, making them highly vulnerable to cyberattacks, physical strikes, and communication infrastructure disruptions. The risk from cyber threats is particularly high, as these systems are integral to military, governmental, and civilian operations. Redundancies and backup systems provide some mitigation, but the overall probability of threats to these critical objects during wartime is very high due to their strategic importance.

5. The probability of threats to the operation of space centers and space systems (e.g., satellites, launch facilities, communication systems) during wartime is significant due to their crucial role in military, intelligence, and civilian operations. Below is an assessment of the potential threats: 1. Cyberattacks on Space Systems (e.g., hacking, satellite control interference). Probability: Very High (pic.6, Row 1). 2. Anti-Satellite (ASAT) Weapon Attacks (e.g., missile strikes, directed energy weapons). Probability: High (pic.6, Row 2). 3. Physical Attacks on Space Launch Centers and Ground Control Stations (e.g., bombings, sabotage). Probability: High (pic.6, Row 3). 4. Electromagnetic Interference and Jamming (e.g., GPS jamming, satellite signal interference). Probability: Very High (pic.6, Row 4). 5. Kinetic Impact on Satellites (e.g., space debris or intentional collisions). Probability: Medium (pic.6, Row 5). 6. Economic Sanctions and Restrictions on Space Technology (e.g., international trade restrictions on space tech). Probability: Medium (pic.6, Row 6). 7. Power Supply and Infrastructure Disruptions (e.g., energy grid failures affecting ground control centers). Probability: High (pic. 6, Row 7). 8. Space Surveillance and Reconnaissance Disruption (e.g., blinding satellites

with lasers or other countermeasures). Probability: High (pic.6, Row 8). 9. Legal and Regulatory Disruptions (e.g., restrictions on space launches, space activity regulations). Probability: Medium (pic.6, Row 9). 10. Natural Risks Amplified by War (e.g., environmental risks affecting launch sites). Probability: Low to Medium (pic.6, Row 10).

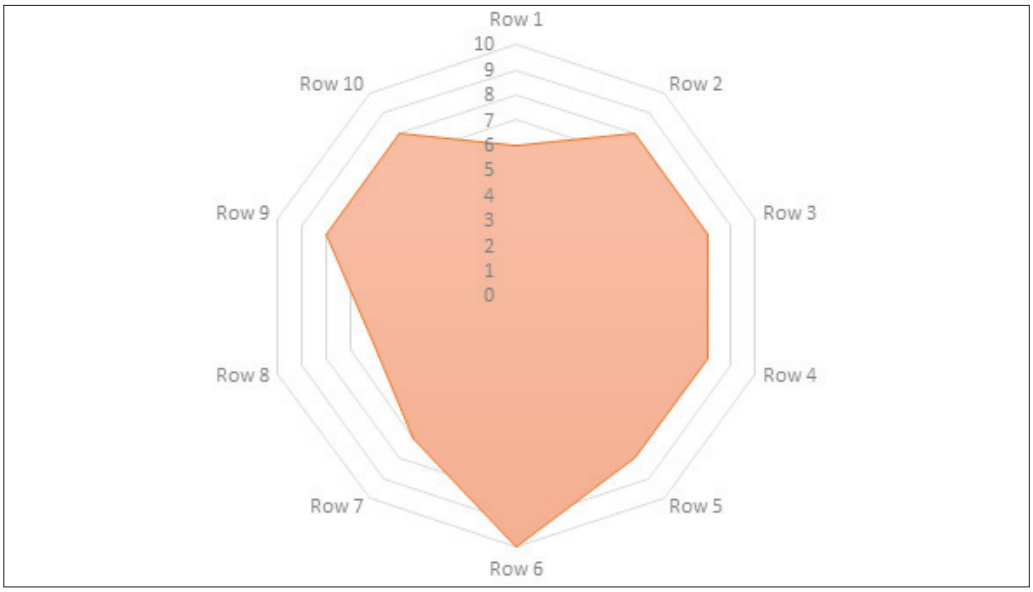


Pic. 6. The probability of threats to the operation of space centers and space systems

Source: formed by the author

Overall Risk Assessment. Probability of threat: Very High. Rationale: Space systems are highly strategic assets in wartime, supporting communication, navigation, intelligence, and military operations. The probability of cyberattacks, electromagnetic interference, and physical attacks on ground stations and satellites is particularly high, making space systems a critical target during conflict. Kinetic and economic risks are less likely but still relevant in some scenarios. The overall risk to space systems and centers is very high due to their essential role in modern warfare and the vulnerability of space assets.

6. The probability of threats to the operation of educational institutions and research centers during wartime is dependent on several factors, including their location, strategic importance, and role in supporting the war effort (e.g., military research). Here's an assessment of potential threats: 1. Physical Attacks on Facilities (e.g., bombings, shelling, sabotage). Probability: Medium (pic.7, Row 1). 2. Cyberattacks (e.g., hacking, data theft, disruption of online learning systems). Probability: High (pic.7, Row 2). 3. Disruption of Communications and Internet Access (e.g., internet blackouts, infrastructure attacks). Probability: High (pic.7, Row 3). 4. Supply Chain Disruptions (e.g., shortages of materials, lab equipment, educational supplies). Probability: High (pic.7, Row 4). 5. Economic Instability and Funding Shortages. Probability: High (pic.7, Row 5). 6. Displacement of Students, Faculty, and Researchers. Probability: Very High (pic.7, Row 6).7. Requisition of Facilities for Military or Civilian Use. Probability: Medium to High (pic.7, Row 7). 8. Intellectual Property Theft or Sabotage (e.g., targeting sensitive research). Probability: Medium (pic.7, Row 8). 9. Faculty and Researcher Shortages (e.g., conscription, reassignment to military projects). Probability: High (pic.7, Row 9). 10. Long-Term Impact on Educational Standards and Research Output. Probability: High (pic.7, Row 10).



Pic. 7. The probability of threats to the operation of educational institutions and research centers

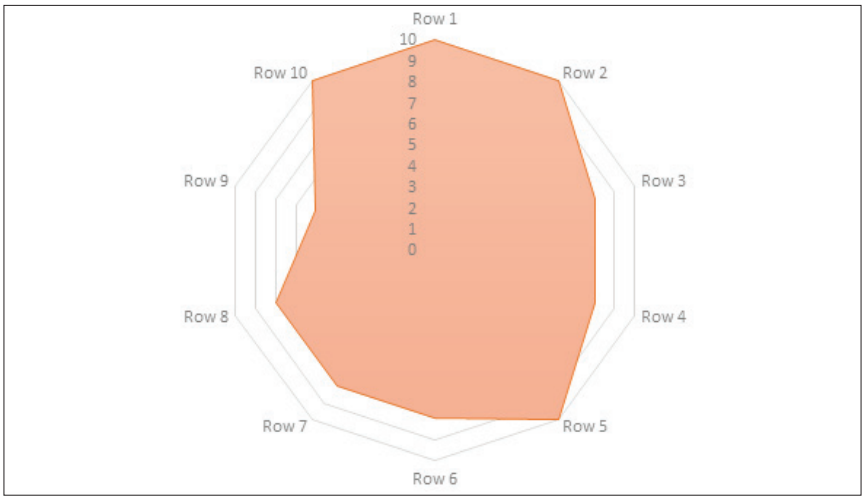
Source: formed by the author

Overall Risk Assessment. Probability of threat: High. Rationale: Educational institutions and research centers face significant threats during wartime, primarily from physical damage, cyberattacks, supply chain disruptions, and the displacement of key personnel. While they are not typically primary military targets, their operations can be severely disrupted by collateral damage, economic strain, and workforce shortages. The most severe impacts are likely to be seen in conflict zones or areas where research is directly related to military or critical infrastructure. Overall, the probability of threats to the operation of these critical objects during war is high.

7. Here is an assessment of the probability of threats to logistic transport networks, service stations, and fuel stations during wartime, with a focus on their importance as critical systems:

1. Physical Attacks on Transport Infrastructure (roads, railways, bridges, ports, etc.). Probability: Very High (pic.8, Row 1). 2. Attacks on Fuel Stations and Depots (e.g., bombings, airstrikes, sabotage). Probability: Very High (pic.8, Row 2). 3. Cyberattacks on Logistics Networks (e.g., disruption of transportation management, fuel distribution systems). Probability: High (pic.8, Row 3). 4. Blockades and Interdiction of Strategic Transport Routes (e.g., ports, railways, highways). Probability: High (pic.8, Row 4).5. Fuel Shortages Due to Supply Chain Disruptions. Probability: Very High (pic.8, Row 5). 6. Attacks on Service Stations and Vehicle Maintenance Facilities. Probability: High (pic.8, Row 6). 7. Economic Sanctions and Supply Restrictions. Probability: High (pic.8, Row 7). 8. Workforce Shortages (e.g., conscription of transport workers, displacement). Probability: High (pic.8, Row 8). 9. Collateral Damage from Nearby Military Targets. Probability: Medium (pic.8, Row 9). 10. Sabotage of Military Convoys and Fuel SuppliesProbability: Very High (pic.8, Row 10).

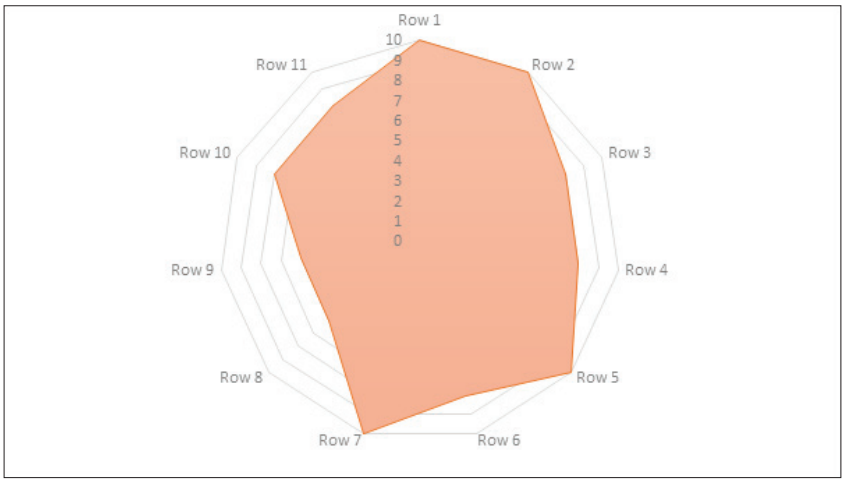
Overall Risk Assessment. Probability of threat: Very High. Rationale: Logistic transport networks, service stations, and fuel stations are highly vulnerable during wartime due to their essential role in supporting military operations and civilian needs. They are likely to face both direct attacks (airstrikes, bombings, sabotage) and indirect disruptions (cyberattacks, fuel shortages, workforce constraints). The critical importance of fuel and transport to both military success and civilian stability makes them high-priority targets, resulting in a very high probability of threats to their operation during war.



Pic. 8. The probability of threats to logistic transport networks, service stations, and fuel stations

Source: formed by the author

8. The probability of threats to the operation of communication systems (mobile networks, radio, and television) during wartime is very high. These systems are critical for disseminating information, maintaining public morale, and coordinating military operations, making them primary targets for disruption. Below is an assessment of the various types of threats: 1. Physical Attacks on Communication Infrastructure (Towers, Stations, Equipment). Probability: Very High (pic.9, Row 1). 2. Cyberattacks on Networks and Systems. Probability: Very High (pic.9, Row 2). 3. Jamming of Radio and Television Signals. Probability: High (pic.9 Row 3). 4. Mobile Network Overload Due to Increased Usage. Probability: High (pic.9, Row 4). 5. Targeted Destruction of Data Centers and Switching Hubs. Probability: Very High (pic.9, Row 5). 6. Internet Shutdowns and State-Imposed Restrictions. Probability: High (pic.9, Row 6). 7. Propaganda and Misinformation Campaigns on TV and Radio. Probability: Very High (pic.9, Row 7). 8. Sabotage by Insider Threats. Probability: Medium (pic.9, Row 8). 9. Use of Electromagnetic Pulse (EMP) Weapons. Probability: Medium (pic.9, Row 9). 10. Dependency on Power Supply Systems. Probability: High (pic.9, Row 10). 11. Disruption of Satellite Communication Links . Probability: High (pic.9, Row 11).

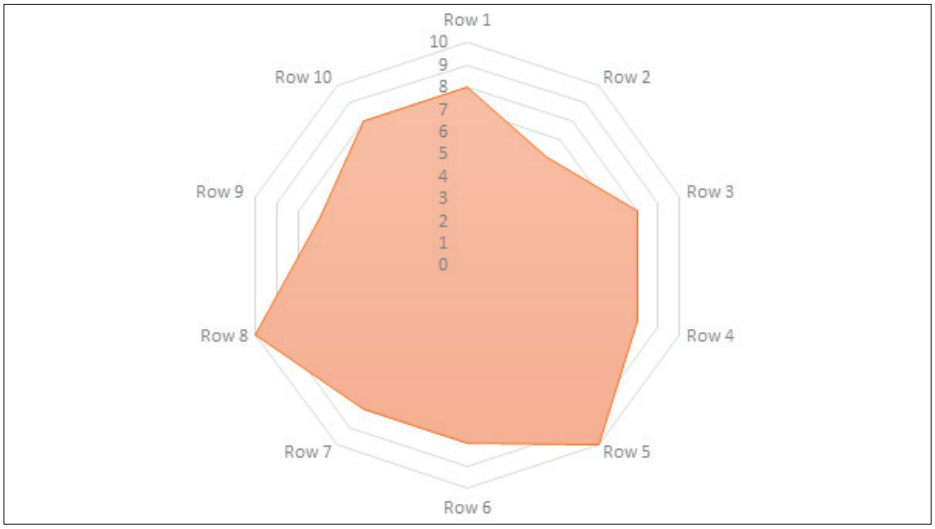


Pic. 9. The probability of threats to the operation of communication systems

Source: formed by the author

Overall Risk Assessment. Probability of Threat: Very High. Rationale: Communication systems (mobile networks, radio, and TV) are vital for civilian and military coordination, making them primary targets in wartime. The most likely threats include physical destruction of infrastructure, cyberattacks, signal jamming, and intentional network overloads. These systems' reliance on power supply and centralized hubs further increases their vulnerability. The overall probability of threats to communication systems during war is very high.

9. The probability of threats to water supply and sewage systems during wartime is high due to their critical role in maintaining public health, sanitation, and general infrastructure stability. Disruption of these systems can have severe consequences for both civilian populations and military operations. Below is an assessment of the probability of various types of threats: 1. Physical Attacks on Water Infrastructure (e.g., water treatment plants, pumping stations, reservoirs). Probability: High (pic.10, Row 1). 2. Contamination of Water Supply (e.g., sabotage, chemical or biological warfare). Probability: Medium (pic.10, Row 2). 3. Cyberattacks on Water Supply Systems (e.g., disruption of control systems, pumps, valves). Probability: High (pic.10, Row 3). 4. Damage to Sewage Treatment Facilities (e.g., bombings, sabotage). Probability: High (pic.10, Row 4). 5. Disruption of Water Supply Due to Damage to Power Grids. Probability: Very High (pic.10, Row 5). 6. Blockades or Siege Tactics Impacting Water Access. Probability: High (pic.10, Row 6). 7. Displacement of Technical Staff and Workforce Shortages. Probability: High (pic.10, Row 7). 8. Destruction of Water Pipelines and Distribution Networks. Probability: Very High (pic.10, Row 8). 9. Pollution of Water Sources Due to Warfare (e.g., industrial pollution, damage to sanitation systems). Probability: Medium to High (pic.10, Row 9). 10. Long-Term Infrastructure Degradation (e.g., lack of maintenance, spare parts shortages). Probability: High (pic.10, Row 10).

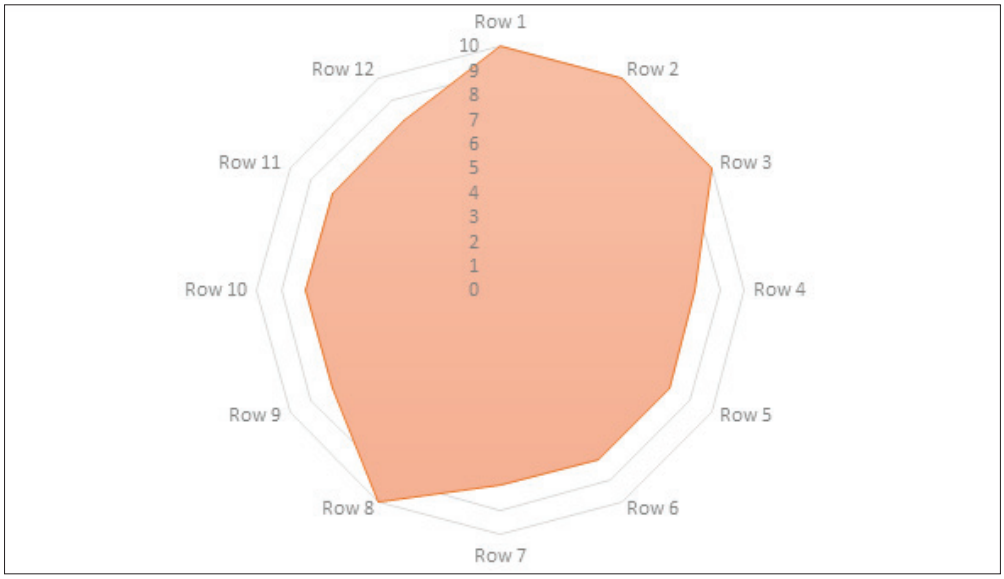


Pic. 10. The probability of threats to water supply and sewage systems

Source: formed by the author

Overall Risk Assessment. Probability of threat: High/ Rationale: Water supply and sewage systems are critical for both civilian populations and military operations, making them high-value targets during wartime. The probability of direct attacks, cyberattacks, and disruptions due to damage to power grids or supply chains is very high. Additionally, the long-term degradation of water and sewage systems due to workforce shortages, lack of maintenance, or siege tactics poses a serious risk. Given the essential role of these systems, the overall threat assessment for their operation during war is high.

10. The probability of threats to the medical system, including pharmacies, polyclinics, and hospitals, during wartime is extremely high due to their critical role in providing healthcare to both military personnel and civilians. Medical facilities are not only essential for treating casualties, but they are also vulnerable to direct and indirect attacks, resource shortages, and infrastructure disruptions. Below is an assessment of the probability of various types of threats: 1. Direct Attacks on Hospitals and Medical Facilities (e.g., airstrikes, bombings, shelling). Probability: High to Very High (pic.11, Row 1). 2. Disruption of Medical Supply Chains (e.g., medications, medical equipment, vaccines). Probability: Very High (pic.11, Row 2). 3. Overloading of Healthcare Systems Due to Increased Casualties. Probability: Very High (pic.11, Row 3). 4. Cyberattacks on Healthcare Information Systems (e.g., patient records, hospital management systems). Probability: High (pic.11, Row 4). 5. Attacks on Pharmacies and Disruption of Pharmaceutical Distribution. Probability: High (pic.11, Row 5). 6. Shortages of Medical Personnel (e.g., displacement, conscription, casualties). Probability: High (pic.11, Row 6). 7. Destruction or Sabotage of Medical Transport and Ambulances. Probability: High (pic.11, Row 7). 8. Contamination of Water and Power Disruptions Affecting Hospitals. Probability: Very High (pic.11, Row 8). 9. Targeted Sabotage or Looting of Medical Supplies. Probability: High (pic.11, Row 9). 10. Spread of Communicable Diseases (e.g., due to overcrowding, poor sanitation). Probability: High (pic.11, Row 10). 11. Economic Sanctions Affecting Import of Medical Supplies and Equipment. Probability: High (pic.11, Row 11). 12. Collateral Damage to Healthcare Infrastructure from Nearby Military Targets. Probability: High (pic.11, Row 12).



Pic. 11. The probability of threats to the medical system, including pharmacies, polyclinics, and hospitals

Source: formed by the author

Overall Risk Assessment. Probability of threat: Very High. Rationale: The medical system, including pharmacies, polyclinics, and hospitals, is extremely vulnerable during wartime due to a combination of direct attacks, resource shortages, and infrastructure damage. The high demand for medical services due to casualties, combined with supply chain disruptions, workforce shortages, and attacks on healthcare facilities, results in a very high probability of threats to the operation of the medical system during war. The critical importance of healthcare for both civilian and military populations makes it a key area of vulnerability in any conflict.

CONCLUSIONS

An analysis of information sources (Osei-Kyei R., Tam V., Ma M., Mashiri F., 2021; Pillai H., 2023; Huth M., Dьerkop S., 2018; Dunn M., 2007; The protection of critical infrastructures, 2018; Heino O., Takala A., Jukarainen P., Kalalahti J., Kekki,T., Verho P., 2019; Giannopoulos G., Filippini R., Schimmer M., 2012) has been carried out, from which it can be concluded that the issue of critical infrastructure risks is an important issue that has received attention only in the last 20 years. At the same time, the risks of critical infrastructures of settlements during the war were not considered at all. Therefore, consideration of this issue in this article is important and relevant.

The use of ChatJPT for the analysis of analytical information that is available on the Internet has proven the effectiveness of such scientific work and the prospects for its development are further explored.

The obtained results of studies of the probability of risks of critical infrastructures proved a high level of probability of threat to these objects, and accordingly, the negative impact that they can cause to the population of countries from the actions of aggressors and terrorists.

REFERENCES

Andrews, J. & Dunnett S. J. (2000). Event-tree analysis using binary decision diagrams. *IEEE Transactions on Reliability*, *49*(2), 230–238. https://www.researchgate.net/publication/3152427_Event-tree_analysis_using_binary_decision_diagrams

Bakeli, T., Alaoui Hafidi, A. (2020). A Fault Tree Analysis (FTA) based Approach for Construction Projects Safety Risk Management. *Proceedings of the 5 th NA International Conference on Industrial Engineering and Operations Management Detroit* (pp. 1889–1901). http://ieomsociety.org/detroit2020/papers/434.pdf

Card, A. J., Ward, J. & Clarkson, P. J. (2012). Beyond FMEA: the structured what-if technique (SWIFT). *Journal of healthcare risk management: the journal of the American Society for Healthcare Risk Management 31*(4), 23–29. https://www.researchgate.net/publication/224821158_Beyond_FMEA_the_structured_what-if_technique_SWIFT

ChatGPT (n.d.). https://chatgpt.com/c/670d6c53-368c-8012-9e4a-f26a60a330e1

Dunn, M. (2007) Critical Infrastructures: Vulnerabilities, threats, responses. *CSS Analyses in Security Policy*, *2*(16). https://www.files.ethz.ch/isn/32592/css_analysen_nr16_e.pdf

FasterCapital. (2024, June 14). *Cost risk analysis: How to identify and mitigate cost risks*. https://fastercapital.com/content/Cost-Risk-Analysis--How-to-Identify-and-Mitigate-Cost-Risks.html

Giannopoulos, G., Filippini, R. & Schimmer, M. (2012). Risk assessment methodologies for Critical Infrastructure Protection. *Part I: A state of the art. Luxembourg: Publications Office of the European Union*. https://www.researchgate.net/publication/368880927_Risk_assessment_methodologies_for_Critical_Infrastructure_Protection_Part_I_A_state_of_the_art

Heino, O., Takala, A., Jukarainen, P., Kalalahti, J., Kekki, T., & Verho, P. (2019). Critical infrastructures: The operational environment in cases of severe disruption. Sustainability, *11*(3), art. 838. https://www.mdpi.com/2071-1050/11/3/838

Huth, M., & Düerkop, S. (2018). Risk management of critical logistical infrastructures: Securing the basis for effective and efficient supply chains. In G. Zsidisin & M. Henke (Eds.), *Revisiting supply chain risk* (pp. 121–135). Springer Series in Supply Chain Management (Vol. 7). https://link.springer.com/chapter/10.1007/978-3-030-03813-7_7

Johnivan, J. R. (2024). *Risk Assessment Matrix: What It Is and How to Use It*. https://project-management.com/risk-assessment-matrix/

Keisle, J. M. (2024). Scenario Analysis. First Online: *25 August 2024*. https://link.springer.com/chapter/10.1007/978-3-031-59353-6_4

Osei-Kyei, R., Tam, V., Ma, M. & Mashiri, F. (2021) Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reduction, 60,* art. 102316. https://www.sciencedirect.com/science/article/abs/pii/S221242092100282X

Pillai, H. (2023). *Protecting Europe's critical infrastructure from Russian hybrid threats*. Centre for European Reform. https://www.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid

Sharath Kumar C. R. & Praveena K. B. (2023). Swot Analysis. *International Journal of Advanced Research 11*(09), 744–748. https://www.researchgate.net/publication/374707908_SWOT_ANALYSIS

Taarup, J. (2020). The business impact analysis. *Working paper No 1. University College Copenhagen, Emergency and Risk management programme*. https://www.researchgate.net/publication/371789651_THE_BUSINESS_IMPACT_ANALYSIS

United Nations Security Council Counter-Terrorism Committee. (2021). *Compendium of good practices: Implementation of Security Council resolution 2396 (2017) addressing the threat posed by foreign terrorist fighters*. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.

РИЗИКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ЧАС ВІЙНИ

Анотація. Критична інфраструктура стає однією з головних мішеней під час війни через її важливу роль у забезпеченні функціонування держави та суспільства. Руйнування або пошкодження критичних об'єктів може мати катастрофічні наслідки для безпеки, економіки та життя громадян.

Розглянуто сучасні питання, пов'язані з визначенням ризику критичної інфраструктури під час війни. Для визначення ймовірностей ризиків об'єктів критичної інфраструктури використовується чат ChatGPT. За допомогою цього чату зроблено загальний огляд ймовірностей на основі припущень, зроблених на основі аналізу сучасних війн в Україні та інших країнах світу.

У статті проведено оцінку ризиків для критично важливих секторів під час війни. До них віднесено: фінансові установи (банки); ланцюги постачання продуктів харчування (магазини, склади); енергетичні системи (електроенергія, передача); інформаційні системи (центри обробки даних, Інтернет); центри космічних досліджень та супутникового зв'язку; навчальні заклади (школи, дослідницькі центри); логістика (транспортні мережі, заправні станції); системи зв'язку (мобільні мережі, радіо, телебачення); системи водопостачання та каналізації; системи охорони здоров'я (лікарні, аптеки).

Отримані результати представлені у вигляді мережевих діаграм. Показано, що сучасні війни є більш небезпечними для населення, що пов'язано з прагненням знищити критично важливі об'єкти інфраструктури та мають негативний вплив на населення країн. Ризик у класичному вигляді розглядається як комбінація двох складових, а саме ймовірності події та її наслідків.

Питання ризиків критичної інфраструктури є важливим питанням, якому почали приділяти увагу лише в останні 20 років. При цьому ризики критичної інфраструктури населених пунктів під час війни взагалі не розглядалися. Тому розгляд цього питання в даній статті є важливим та актуальним.

Використання ChatJPT для аналізу аналітичної інформації, яка доступна в мережі Інтернет, довело ефективність такої наукової роботи та перспективи її подальшого розвитку.

Ключові слова: ризики, критична інфраструктура, війна, населення, ймовірність загрози.

RISKS OF CRITICAL INFRASTRUCTURES DURING WAR

Abstract. Critical infrastructure becomes one of the main targets in times of war because of its important role in ensuring the functioning of the state and society. Destruction or damage to critical facilities can have catastrophic consequences for security, economy, and the lives of citizens.

The article considers current issues related to determining the risk of critical infrastructure in wartime. The ChatGPT chat is used to determine the probability of risks to critical infrastructure facilities. This chat provides a general overview of probabilities based on assumptions made on the analysis of modern wars in Ukraine and other countries.

The article assesses the risks to critical sectors during a war. These include: financial institutions (banks); food supply chains (stores, warehouses); energy systems (electricity, transmission); information systems (data centers, Internet); space research and satellite communications centers; educational institutions (schools, research centers); logistics (transportation networks, gas stations); communication systems (mobile networks, radio, television); water supply and sewage systems; health care systems (hospitals, pharmacies).

The results are presented in the form of network diagrams. It is shown that modern wars are more dangerous for the population, due to the desire to destroy critical infrastructure and have a negative impact on the population of countries. Risk in the classical form is considered as a combination of two components, namely the probability of an event and its consequences.

The issue of critical infrastructure risks is an important issue that has only been paid attention to in the last 20 years. At the same time, the risks of critical infrastructure of settlements during the war were not considered at all. Therefore, the consideration of this issue in this article is important and relevant.

The use of ChatJPT to analyze analytical information available on the Internet has proven the effectiveness of such scientific work and the prospects for its further development.

Keywords: risks, critical infrastructures, war, population, threat probability.

Cite this article: Berezutskyi, V., Tokhtamysh, T. (2024). Risks of critical infrastructures during war. *Law and innovative Society,* 2 (23), 55-70. doi: https://doi.org/10.37772/2309-9275-2024-2(23)-5