THE CONCEPT OF A METHOD FOR PREDICTING THE CASCADE EFFECT UNDER CONDITIONS OF HYBRID WARFARE

Wojciech WRÓBLEWSKI[a)], Michał WIŚNIEWSKI[b)]

[a)] The Fire University, POLAND
e-mail: wwroblewski@apoz.edu.pl, ORCID: 0000-0003-3415-9485
[b)] Warsaw University of Technology, Faculty of Management, POLAND
e-mail: michal.wisniewski@pw.edu.pl, ORCID: 0000-0003-3435-3114

Abstract: The changing nature of conflicts is creating new challenges in civilian protection. Features of hybrid warfare, such as multidimensionality, synergistic effects, blurring of boundaries, or asymmetricity, force practitioners and scholars to consider new threats. The article examines how the characteristics of hybrid warfare affect the emergence of cascade effects. We conducted research on examples of the war in Ukraine and the Israeli-Palestinian war. The concept of a method for predicting the cascade effect under conditions of hybrid war is proposed. The concept involves using the Six Ways to Die method to take areas affecting the health and life of the civilian population and define a network of object dependencies on which proper functioning of the State in these areas depends. Using complementary tools such as process analysis, risk assessment, Petri nets, and Bayesian network in the form of the Critical Infrastructure Security Situational Management methodology, the authors provide a comprehensive solution for modeling how to protect the life and health of the civilian population. To the author's knowledge, this is the first holistic study in this issue.

Keywords: hybrid warfare, civil protection, cascade effect, threats.

JEL Classification: H56, H76.

1 Introduction

Conflicts have accompanied humanity since dawn, generating negative consequences primarily for civilians. Many of them have a traditional framework. However, hybrid warfare is an increasingly common phenomenon. Hybrid warfare is a broad, complex, and adaptive combination of conventional and unconventional means, overt and covert military, paramilitary, and civilian actions, used in a highly integrated manner by state and non-state actors seeking to achieve their goals (North Atlantic Council, 2016). According to the Global Conflict Tracker report, 30 conflicts and wars are currently happening in the world (CFR, 2024). Against this background, the war in Ukraine and the war between Israel and Hamas stand out, the course of which is widely reported in academic literature and the media. Both conflicts are seen as hybrid wars.

Media reports of attacks by parties to conflicts indicate that the threats used in hybrid tactics create unique and hard-to-identify complex networks with cascading effects, to which an initial disruption in one political, economic, social, or other system triggers a series of further related disruptions in different systems. These disruptions build up and spread, affecting further sectors and areas, which can lead to complex and difficult-to-predict effects on a broader scale (Zwęglinski, et al., 2020).

The available literature addresses the problem of predicting the cascading effect in the context of hybrid warfare. The available papers in the Scopus and Web of Science Core Collection (WoS CC) database published after 2014 on this topic refer to the issues of ecology (Gaynor, et al., 2021), medicine (Linebarger, 2021), physical protection (Landucci, et al., 2020), and protection of selected groups of industrial facilities (Landucci, et al., 2017; Linebarger, 2021). The available literature indicates that the problem of occurrence of the cascade effect in the context of hybrid warfare has been noted. However, the available knowledge has to be more holistic and provide solutions to narrowly defined problems.

Tools developed within the framework of critical infrastructure security management can provide a solution to the observed problem of how to holistically address the issue of predicting cascading effects in the context of civilian protection. Tools such as process analysis (Krupa and Wisniewski, 2015), risk assessment (Zio, 2018), Petri nets (Kabir and Papadopoulos, 2019), and Bayesian networks (Hosseini, et al., 2016) provide comprehensive solutions for modeling how to deliver added value to protect the lives and health of civilians.

This paper aims to analyze the feasibility of using the Six Ways to Die model in protecting civilians under conditions of hybrid warfare in the context of identifying network conditions that cause a cascading effect. The model defines the essential areas, the provision of which will allow the civilian population to survive the period of conflict. The model also provides a tool for defining the sequence of activities that must be performed to deliver the service or product under consideration. The authors, assuming that each activity requires the availability and proper functioning of specific resources that need to be protected from threats, prove that it is possible to develop a model of the interdependence of facilities involved in providing goods and services that protect the life and health of the civilian population during a conflict. Analysis of the interdependence model will make it possible to predict the consequences of the materialization of threats and, consequently, will provide decision-makers with analytical material that will enable the implementation of preventive measures or contingency plans that reduce the cascading effect.

The paper is organized as follows. The next section presents the method of research. The section "Background" describes the concept of hybrid warfare, identifying its features with particular attention to the issue of complexity and the cascading effect. This procedure was done to indicate the research gap and to explain how this study complements previous research. Then, an analysis is presented indicating the consequences of hybrid warfare for civilians using selected conflicts as an example. In the discussion of the results section, the link between the Six Ways to Die method, the observed effects of hybrid warfare, and the effect of hybrid warfare on the civilian population are discussed. Also indicated is a model process that defines the goals of protecting the civilian population, methods of their attainment, and anticipation of threats to the actions taken. Limitations of the study and suggestions for future research are discussed in the conclusion.

2 Research method

The study used the desk research method. Desk research is an example of the so-called nonreactive methods, that is, methods that enable the study of social behavior without interfering with that behavior (Babbie, 2005). It is a method of studying found data and establishing the current state of knowledge in the field under study. Analysis, inference, and synthesis were used as complementary methods.

There are many concepts for applying this method. The study adopted the procedure presented in Fig. 1.

As defined in the section "Introduction" of the article, the research area is concerned with the possibility of predicting the cascade effect caused by the threats arising from hybrid warfare, which affects the health and lives of civilians.

The problem is the possibility of using the Six Ways to Die model to help shape strategies for protecting civilians in hybrid wars.

The search for the source was conducted using two scientific databases: Web of Science Core Collection (WoS CC) and Scopus. The databases were chosen because they are the most commonly used in literature searches and are the leading databases with significant scientific impact (Joshi, 2017; Visser, van Eck and Waltman, 2021). These databases are considered the two most important multidisciplinary bibliometric databases. Complementary sources of data focusing on media reports on the conflicts under analysis are the PAP (Polish Press Agency) and Defence-24 portals.

The collected source data were used to discuss the concept and features of hybrid warfare. The analyses made it possible to define the essential areas that hurt the lives and health of the civilian population. Defining these areas made it possible to link the Six Ways to Die model to the considered problem of the occurrence of the cascading effect caused by threats generated by hybrid conflicts.

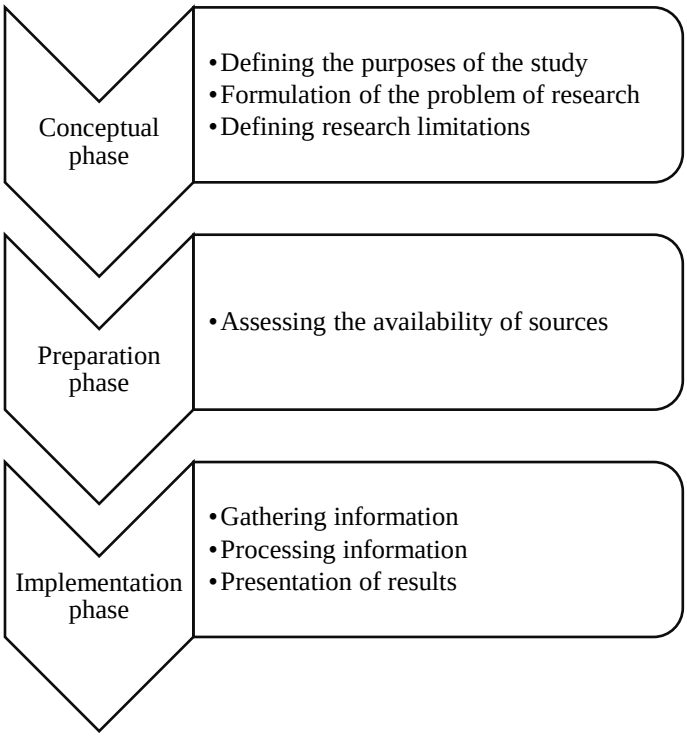

Figure 1. Desk research study procedure
(*Source:* Authors' concept)

It discusses the use of the Six Ways to Die model in predicting the course of the cascading effect and, consequently, formulating preventive actions and adopting contingency plans.

3 Background

3.1 The hybrid war

Hybrid warfare is widely debated and, at the same time, challenging to define in a one-dimensional way. This is due to the nature of this type of strategy, which generally aims to achieve strategic political, military, and economic goals that might be more difficult to achieve through traditional forms of armed conflict.

In the academic literature, the dominant concept is hybrid warfare, authored by Frank Hoffman. Hoffman (2007) analyzed various previous theories, including Fourth Generation Warfare, Complex Warfare, and Unlimited War. Hoffman defined hybrid wars as combining a full spectrum of different methods of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts involving unlimited violence and coercion, and criminality. According to Hoffman, what distinguishes hybrid wars from previous forms of conflict is the blurring of their boundaries, even at lower tactical levels (Hoffman, 2007).

In Amos C. Fox's assessment, although Frank Hoffman's concept serves as a valuable reference point, his definition of hybrid warfare proves insufficient, mainly due to its focus on terrorist acts and criminal disorder (Fox, 2017). Fox presents an alternative definition of hybrid warfare, developed by Robert Leonhard, which emphasizes that hybrid warfare and its accompanying operations are based on the pursuit of asymmetric advantages that enable the achievement of political objectives. It is characterized by undeclared actions, combining conventional and irregular military operations with nonmilitary activities, in a context where the boundary between strategy and tactics is significantly reduced and information plays a crucial role (Leonhard and Philips, 2015, pp. 17-18). Such a perspective, according to Fox, better fits the characteristics of the Russian model of hybrid warfare, while he also noted that many definitions focus only on selected aspects (Fox, 2017).

Fox further extends the discussion by arguing that modern hybrid warfare is a theory of operations based on the definition of force in the information age.

The theory constructs interdependencies between the use of force and domains, levels and elements of force, and between the use of force and time, space, and target. Such a model of operation opens up the possibility of attacking or exploiting multiple vulnerable flanks, allowing operations in one domain to be used to initiate actions in another to create a favorable asymmetry. Hybrid warfare, according to Fox, is thus modeled by its era, reflecting both its capabilities and limitations (Fox, 2017).

Hoffman refined the concept of hybrid warfare, the concept only focuses on operational and tactical levels. Autor admitted that his theory does not include nonhybrid activities such as economic, financial, subversive, information activities, etc. Iskandarov and Gawliczek believe that the holistic feasible concept of hybrid war (Fig. 2) was described by Kaliskan, who, extending Hoffman's concept, pointed out additional categories in hybrid war: economic aspect, social aspect, psychological aspect, diplomatic aspect, and, depending on the context, agricultural aspect. All these areas form the so-called grand strategy (Caliskan, 2019; Iskandarov and Gawliczek, 2020).

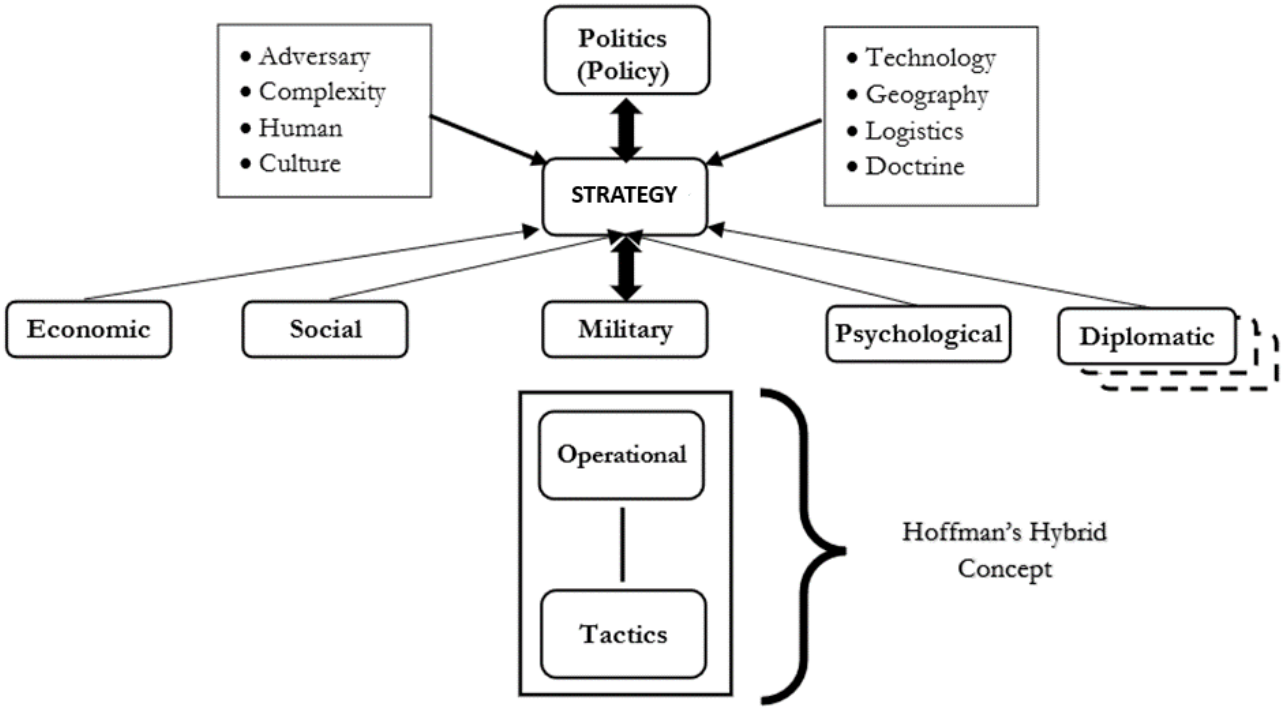

Figure 2. Concept of hybrid warfare in a broader context – grand strategy
(*Source:* Iskandarov and Gawliczek, 2020)

North Atlantic Treaty Organization (NATO)'s definition of hybrid warfare states that it and its supporting tactics can encompass broad, complex, adaptive, opportunistic, and often integrated combinations of conventional and unconventional methods. These activities may be overt or covert, involving military, paramilitary, organized criminal networks, and civilian elements across all spheres of power (Caliskan, 2019).

In discussions about hybrid warfare, understanding the Russian perspective is essential as it significantly influences the international perception of this phenomenon. In the West, it is referred to as hybrid warfare, while in Russia, terms such as new generation warfare, nonlinear warfare, network-centric warfare, and active measures are used interchangeably. Initially, as described by Walecki and Niejełow, the Russian concept of hybrid warfare referred to US actions in Iraq and Afghanistan, characterized as hybrid warfare methods. This theory was later adapted to describe the Russian-Ukrainian conflict (Walecki and Niejełow, 2015). A key element in Russian military doctrine is General Valery Gerasimov's 2013 speech, presenting advanced concepts for planning and conducting military operations, emphasizing the need for scientific anticipation of future challenges. He highlighted the blurred lines between war and peace and the growing importance of nonmilitary

methods as key to modern conflicts (Gerasimov, 2013).

In addition, Evgeny Messner's theories, which describe insurgent wars as prototypes of today's hybrid wars, stress the blurred lines between regular and irregular activities, including sabotage, terrorism, and guerrilla warfare (Banasik, 2015). Furthermore, Hoffman suggests that for Russia, hybrid warfare continues the Cold War practices of combining political, economic, and subversive activities (Hoffman, 2018).

On the international stage, the Chinese approach to hybrid warfare, as described by the Communist Party of China (CPC), involves using all aspects of State power – both physical and intangible – to engage in indirect confrontations with adversaries. This strategy incorporates political, economic, military, and informational means at a strategic level, differentiating it from American concepts that often focus on tactical actions before conflicts (Understanding War, 2021).

Hybrid wars are characterized by multidimensionality, integration of methods and actors, synergy, blurring of boundaries, and asymmetry. The concept of "network-centricity" in hybrid warfare strictly refers to the utilization of network theory, illustrating complex interactions and dependencies within and across networks, facilitating coordinated and dispersed attacks using both traditional and modern tools.

Networking in hybrid warfare is illustrated by structures and dynamics of action based on complex social, organizational, technological, and military networks. These networks enable interaction as well as the sharing of resources and information between different nodes, which facilitates the execution of coordinated and distributed attacks using both traditional warfare methods and modern tools. An example is cyber operations, which are carried out in a distributed manner, but according to a unified strategy, using the resources and skills of distributed groups of hackers. These operations can lead to cascading effects.

Cascading, in the context of hybrid warfare, refers to chain reactions, where one action triggers a series of subsequent, often unpredictable reactions, leading to widespread and multilevel consequences. In practice, an action such as a cyberattack on critical infrastructure can not only disrupt an area, but also trigger a series of further social, economic, and political consequences, compounding the effect of the original attack. Critical infrastructure should be understood in this context as key systems and assets, both physical and virtual, that are so vital to the functioning of the State and its citizens that their failure, malfunction, or destruction would have a negative and destructive impact on State security, including the economy, public safety, and the health and lives of citizens (Itich-Drabarek, et al., 2023).

In the context of civil protection and homeland security, networks:

- change the perception of threats – instead of the traditional hierarchical threat model, network theory highlights the complexity and dynamic nature of threats, which can adapt and evolve rapidly;
- require integrated responses – responding to networked threats requires greater coordination across agencies and sectors, including civilian and military participants, as well as international cooperation; and
- emphasize the importance of monitoring networked threats – effectively countering networked threats requires advanced data collection and analysis tools that can detect and understand complex activity patterns.

However, cascading:

- emphasizes interdependencies – modern societies are characterized by interdependencies in, for example, critical infrastructure, where the failure of one element can affect many others, increasing the potential impact of the original threat);
- forces a thoughtful protection strategy – understanding the potential cascading effects requires the development of more comprehensive population and infrastructure protection strategies that take these interdependencies into account; and
- emphasizes the importance of prevention and preparedness – stresses the need to invest in preventive protection measures and build resilience, especially civilian resilience, to minimize the risk and reduce the potential for cascading effects.

Ensuring security in the context of networked threats and cascading effects in conflict and hybrid warfare is critical to protecting civilians. In the context of civilians, integrated responses at the strategic and operational levels can include rapid relocation, ensuring

access to essential services such as food, water, health care, and shelter, as well as measures to protect against cyberattacks, disinformation, and psychological manipulation. Understanding the cause-and-effect relationships and potential cascading effects allows for earlier identification and mitigation of threats and their effects, which is particularly important in preparation, prevention, and response and provides primary conditions for civilian survival during emergencies.

An analysis of publications collected in the Scopus and WoS CC database, performed on May 08, 2024, identified more than 4659 studies on hybrid wars and conflicts. The studies were identified by query (1). Only six studies addressed the topic of cascading effects and methods of protecting communities from the effects of such threats.

("Hybrid conflict" OR "Irregular conflict" OR "Asymmetric conflict " OR "Conflict in the gray zone" OR "Low-intensity conflict" OR "Subconventional conflict" OR "Subversive actions" OR "Non-standard actions" OR "Conflict below the threshold of war" OR "Mixed actions" OR "Multidimensional conflict") AND PUBYEAR > 2013 AND PUBYEAR < 2025 (1)

The results indicated that the problem of occurrence of the cascade effect in the context of hybrid warfare has been noted. At the same time, the number of studies devoted to this issue indicates an early stage of research that provides solutions to narrowly defined problems. There is an observed lack of holistic works indicating how to protect the population from the effects of hybrid wars.

3.2 The effects of hybrid wars

This study focuses on two hybrid conflicts: the war in Ukraine and Israel's conflict with Hamas. The selection of these cases was based on two key criteria:

- Impact on civilians (indirect and direct). Both wars are characterized by significant impacts on the safety, health, and general living conditions of civilians, making them essential cases for analysis in the context of civilian protection in hybrid warfare (UN, 2024; WHO, 2024).
- Representativeness in scientific literature and public debate. Both conflicts are widely documented and discussed in the academic literature and public debate as examples of hybrid warfare. An analysis of Scopus database resources as of April 29, 2024 for the keyword war in Ukraine and derivatives showed 6074 publications published since 2022. An analogous query on the Israeli-Palestinian conflict returned 147 studies published after 2023.

The consequences of hybrid wars are essentially the consequences for civilians. According to statistics based on a report by the UN Office of the High Commissioner for Refugees (OHCHR) published on February 22, 2024, the war in Ukraine has killed at least 10,582 civilians, including a minimum of 587 children. In addition, 19,875 were wounded, including 1,298 children, and losses on the military side amounted to about 31,000 soldiers. However, these numbers are probably underestimated (Fig. 3).

The April 2, 2024 emergency report shows that 32,975 civilians (Palestinians) were killed as a consequence of the war between Israel and Hamas. Also, 75,577 Palestinians were wounded. On the Israeli side, the losses amounted to 1,200 killed and 5,400 wounded, including 604 soldiers and police officers (Fabian, 2024; WHO, 2024).

The number of Palestinian fighters killed by Israel exceeded 8,000 (Fig. 4).

In modern hybrid wars, various reports emphasize that the direct effects on civilian populations include deaths and injuries mainly caused by large-scale explosive weapons. The long-term effects include limited access to food, water, medical care, and exposure to harsh weather conditions and lack of information, which can lead to lasting health damage or death. These effects are due to both military and nonmilitary threats utilized across several domains (information, economic, legal, cognitive, or energy).

The World Health Organization (WHO)’s report on the humanitarian and health situation in the Gaza Zone from October 2023 to April 2024 indicates that

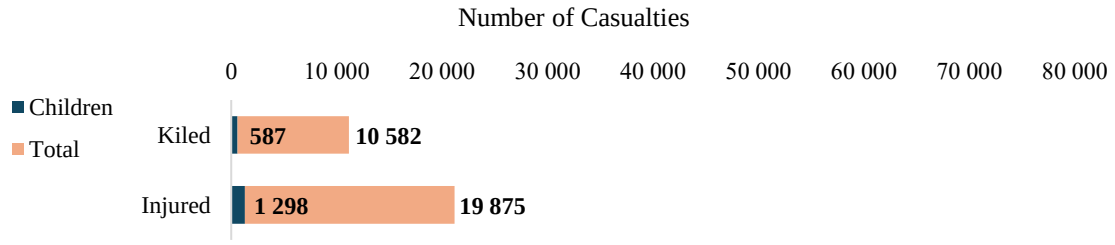

Figure 3. Casualties in the Ukraine conflict (2022-2024)
(*Source:* Own elaboration based on Statista, 2024)

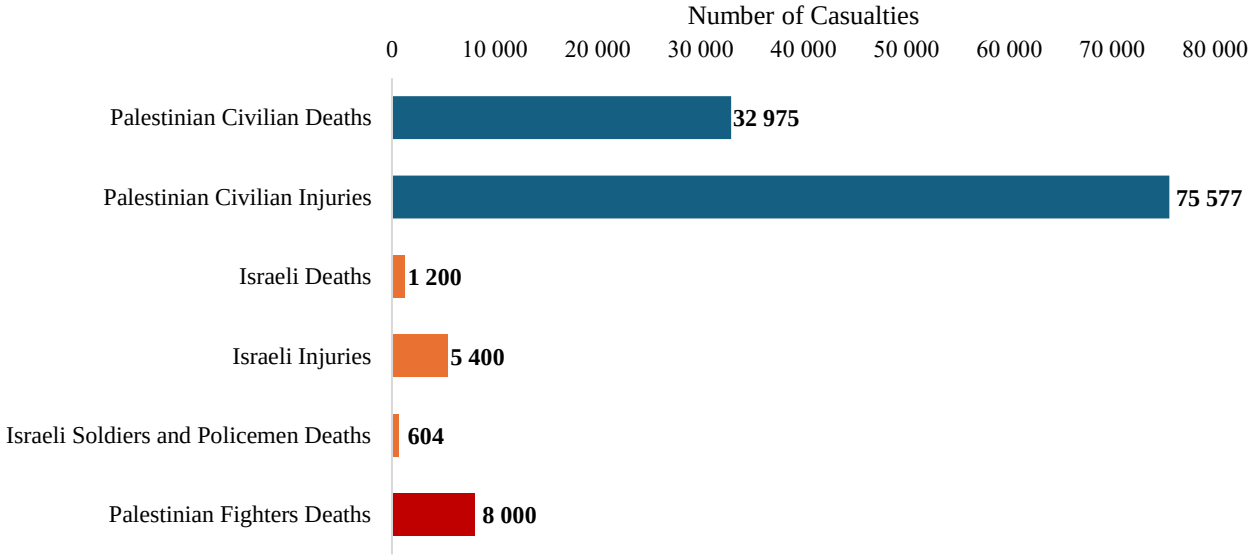

Figure 4. Casualties in Palestine-Israel conflict (2024)
(*Source:* Own elaboration based on Fabian, 2024; VOA, 2024)

75% of the population (1.7 million people) was displaced due to conflict. A total of 7,780 people were reported as missing or buried under rubble. Only 27 of 89 health facilities (30%) are fully functional, and hospital bed occupancy reached 323%. There were 643,254 cases of acute respiratory infections, 345,768 cases of diarrhea, and 47,949 cases of skin rashes. Attacks on health facilities (435 incidents, including the attack on Al-Shifa Hospital) resulted in 722 deaths and 902 injuries. The destruction of infrastructure, lack of access to medicine, medical transport, electricity, and water restricted the health system's operation In addition, food security issues affected about 2.13 million people, and problems with access to electricity and heating exacerbated the difficulties (WHO, 2024). The UN Human Rights Office head emphasizes that the lack of shelter and communication problems further complicate the situation for residents (UNHR, 2024).

The OHCHR report from March 26, 2024 highlights that as a result of military actions in Ukraine, mainly missile attacks, up to 60% of civil infrastructure was destroyed in some regions (UN, 2024). The war also caused mass migration – by February 8, 2024, according to the Polish Border Guard, 18.8 million Ukrainians crossed the Polish-Ukrainian border (PAP, 2024). The civilian population also experiences significant difficulties accessing food and water and basic services in cities such as Mariupol, Irpin, Bucha, Hostomel, and Trostianets (ACLED, 2024).

A significant portion of civilian victims (91%) died or were injured by explosive weapons with a wide range of effects. In addition, deaths or injuries were also caused by small-caliber and light weapons during crossfire, incidents of force escalation, intentional killings, and road accidents involving military or civilian vehicles. Russian forces were responsible for opening fire on civilians attempting to evacuate from endangered areas, resulting in significant casualties

among the population (OHCHR, 2024). OHCHR also documents cases of widespread torture, mutilation, ill-treatment, arbitrary detention of civilians, executions, forced displacements, abductions, and persecution. An example is the filtration process in Mariupol, where civilians were subjected to torture, beatings, electric shocks, and intimidation by executions (OHCHR, 2024).

Evidence from these regions exemplifies the dynamic and networked nature of contemporary warfare, where the effects of military actions are multidimensional and cascading, significantly complicating the security of civilian populations.

4 The concept of predicting the cascade effect

The Six Ways to Die model is a tool for taking the areas that affect the health and life of the civilian population and defining the network of object dependencies on which proper functioning of the State in these areas depends.

The Six Ways to Die model assumes that the primary task of the State is to eliminate factors that can lead to death in six areas (Bennett and Gupta, 2010):

- hunger,
- thirst,
- trauma,
- illness,
- very high temperature, and
- very low temperature.

Eliminating sources of danger should occur at three levels of need: the person, groups of citizens, and the state as an organization. For each level of needs, the conditions for survival can be described by the processes used to achieve them.

An example of a process for ensuring access to food that may be interrupted due to a threat generated by hybrid war is illustrated in Fig. 5.

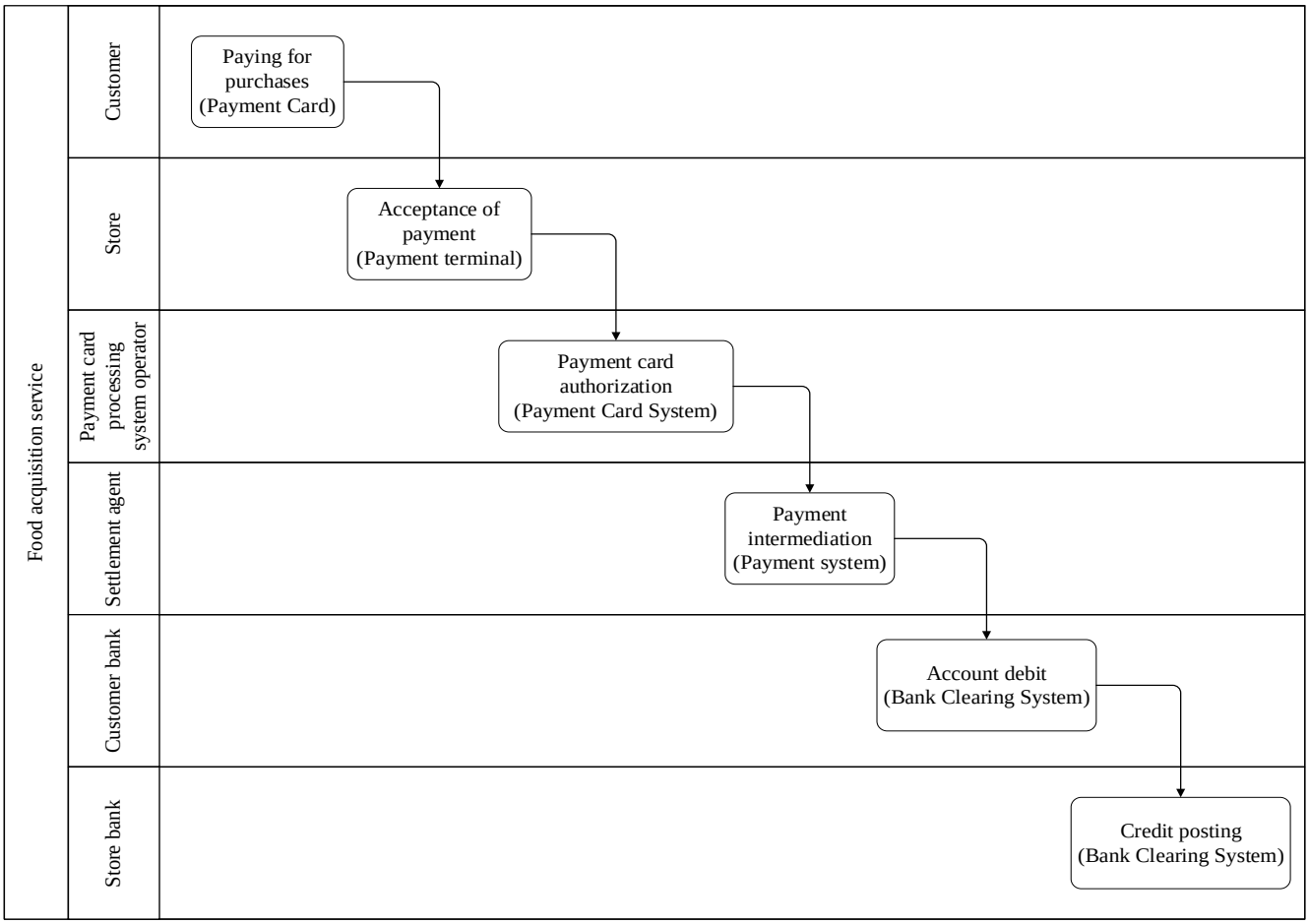

Figure 5. An example of the implementation process of the food acquisition service (*Source:* Own work based on Kisilowski, et al., 2021)

Considering the situation depicted in Fig. 5, a customer wishing to purchase food needs a resource of payment means represented by a payment card. Using a payment card to pay for purchases requires that the store that offers the service of selling goods has a resource in the form of a payment terminal. To debit the customer's account, the payment terminal must have access to a service offered by a clearing agent, which must be certified by one of the payment system operators (e.g., Visa, Mastercard). In addition, the clearing agent must be authorized by the country's Central Bank where it is registered. To complete the transaction, the payment system operator must be able to establish a connection and exchange data with the transaction system of the customer's bank and the bank operating the store. A cyberattack such as DDoS blocking the ability to establish a connection with the payment system operator may result in losing the ability to purchase food. Prolonged unavailability of this service could lead to hunger in the affected area.

An example of cutting off the availability of services to meet basic needs can be seen in the situation described in the article PAP (2022). The article describes the situation of residents of Mariupol, occupied by the Armed Forces of the Russian Federation. Earlier shelling of civilian infrastructure and persecution and forced displacement, combined with the activities of collaborators, led to the restriction of access to drinking water, food, and basic hygiene measures for the civilian population. The situation forced people to feed on pigeon meat. The director of a Mariupol clinic, Oleksandr Lazarenko, points out that eating pigeons poses another threat to the lives of the civilian population by exposing them to diseases. Pigeons are spread of many viral, bacterial, and fungal diseases. As a result, the meat can be infected. One can contract histoplasmosis, encephalitis, ornithosis, toxoplasmosis, and other dangerous diseases, which are dangerous, especially for children and the elderly. With improper treatment of the diseases, some of them can lead to death (PAP, 2022).

The cited article shows how the effects of materialization of one or a group of threats (bombing, persecution, collaboration) can escalate, creating conditions that are conducive to the occurrence of another (risk of infectious diseases). In this case, the destruction of civilian infrastructure resulted in restrictions on access to food, causing famine. The situation forced the civilian population to rely on available food sources, increasing the risk of infectious diseases. In the event of a disease outbreak, the possibility of assistance is limited due to a lack of access to medical care, which can lead to death as a result of illness or injury.

Cybersecurity and Infrastructure Security Agency (CISA) applies the Six Ways to Die methodology at the central level of the US government. CISA defines the critical functions of the State. Then, in creating a table of critical State functions, it successively defines the processes that serve to implement them (Cybersecurity and Infrastructure Security Agency, 2019). Critical government functions are defined as those functions of government and the private sector so vital to USA that their disruption, damage, or destruction would have a detrimental effect on public safety, security of the national economy, national health care, or any combination of these matters (Moteff, Copeland and Fischer, 2003).

The concept presented for the central government level corresponds to the proposal included in the Six Ways to Die methodology. Knowing the critical functions and defining the objectives to be achieved, one can proceed to selecting services and component processes and identifying their operators.

Determining the processes that perform critical services paves the way for identifying the resources that determine the resilience of the service. In this case, resilience is understood as a feature of a system, process, or resource that reduces the level of risk associated with the threat under consideration. Resilience is achieved when it is possible to function or return to functioning at an assumed level within an acceptable time after an incident. Resilience is achieved through the cumulative effect of technical, organizational, educational, etc., undertakings that protect a system, process, or resource from threats (Itich-Drabarnp, et al., 2023).

Actions to secure resources that condition the delivery of an essential service can be determined using the Critical Infrastructure Security Situational Management methodology (Wisniewski, 2020). The Critical Infrastructure Security Situational Management methodology uses a resource situation model, which

determines the state of a resource at a specific point in time. The data characterizing the resource are:

- the functionalities implemented, which can be interpreted as components of an essential service;
- threats to which the resource is susceptible;
- safeguards that are applied as a response to identified threats; and
- the interdependence of resources determined by the organization of the process.

The Critical Infrastructure Situation Model integrates functionalities with resources, which are susceptible to threats whose materialization can damage or destroy the resource and negatively affect the availability of functionality. Threats, in turn, indicate the need for safeguards that condition the proper operation of resources and access to functionality. The data collected in the resource situation model is the input package for further actions:

- Risk value estimation – Based on the risk assessment, the availability of functionality in a specific threat is forecast. If the projected value of functionality does not reach the safety threshold, a decision problem is formulated, taking into account the threats from which the considered risk arises.
- Generation of adverse event scenarios – Data from the resource situation model allows the development of a network of dependencies. Determination of this network makes it possible to identify adverse event scenarios. Determination of adverse event scenarios is based on the probability of a threat and the vulnerability of the resource to that threat. For each scenario, it is possible to determine the risk value associated with the threats included in the scenario. If the risks associated with the scenario do not allow the safety threshold to be reached, a decision problem is formulated for the hazards present in the scenario. Determining the probability of occurrence of a hazard under the condition of materialization of another hazard is achieved using Bayes' theorem (Wiśniewski, et al., 2016).
- Decision problem formulation – The solution to the decision problem is a set of safeguards for each identified threat, allowing the safety threshold to be reached. The decision problem formulation method modifies the Analysis Interconnected Decision Areas (AIDA) method (Krupa and Ostrowska, 2012). The set of safeguards resulting from the solution of the decision problem provides the resource operator with a recommendation for action in response to the risks arising from the threats to which the resource is susceptible.

An analysis of the available literature on hybrid warfare tactics indicates that there is a universal resource necessary for any process to protect civilians from hunger, thirst, injury, disease, excessive heat, and excessive cold. This resource is reliable information directed to the civilian population, especially in an emergency when meeting basic needs is impossible by traditional means. This observation is confirmed by available reports and media reports covering the war in Ukraine and the Israeli-Palestinian conflict. This observation also aligns with the adopted method of analyzing potential cascading effects, where providing services or products to the civilian population requires access to data to enable the launch and proper execution of subsequent planned activities.

Lack of access to information blocks the ability to carry out certain activities and, consequently, the ability to carry out the entire process. The effect of blocking the process of providing essential services or products to the civilian population can expose them to phenomena leading to permanent damage to their health or death due to long-term impact.

A more dangerous phenomenon related to access to information is the lack of data integrity. Only authorized modification of data, even unclassified data, can lead to proper implementation of the accepted process of providing essential goods and services. The process is implemented in this situation, but its effects harm the civilian population. An example of the consequences of violating data integrity can be the modification of records of Emergency Management Plans, which define the evacuation place. Modifying unclassified data in this situation can lead to gathering the civilian population in a place exposed to shelling, for example, instead of directing them to a safe zone.

Blockchain technology may be the answer to the outlined problem of data protection. Applying blockchain technology to protect the population during hybrid warfare can enhance data security, transparency, and resilience. Blockchain has a high level of data security due to its cryptography and decentralized architecture that eliminates single points of failure

(Moosavi, Taherdoost, 2023; Zubaydi, et al., 2023). In hybrid warfare, where cyberattacks are a standard tool, blockchain's ability to resist attacks is invaluable. Data shows that blockchain-based systems are more resistant to typical cyberattacks than traditional databases (Xu, 2016; Benjamin, 2021). Blockchain provides full auditability and transparency of transactions (Hosanagar, 2021; Singh and Kumar, 2021), which is essential in situations where false information and manipulation can lead to confusion and chaos. Every transaction on the blockchain is permanently recorded and publicly verifiable (Tamplin, 2023; The Wall Street Magazine, 2023). Blockchain allows for efficient distribution of data and verification of the sender's identity (Habib, et al., 2022), which is crucial in verifying individuals and entitlements during a crisis.

5 Conclusions

The main goal of protecting the civilian population is to ensure security broadly, including the fundamental values of life and health. The analysis in this study shows that in the reference conflicts and wars described as hybrid, the civilian population has suffered direct and indirect consequences in the form of thousands of victims and casualties. They have also been deprived of primary means of survival like food, water, access to medical and humanitarian aid, electricity and heating, and reliable information.

To minimize the above effects, the Six Ways to Die model is proposed, which allows the setting of strategic goals in the field of civilian protection and the definition of strategies for their implementation. Translating the strategy for achieving the adopted goals into processes makes it possible to identify the resources on which the ability to implement the adopted course of action depends. The data thus obtained feeds the method of situational management of critical infrastructure security, which provides tools for analyzing risks associated with single threats and potential cascading effects. As a result, it is possible to analyze the risks associated with the process under consideration and formulate a decision problem, the solution of which will identify a set of safeguards that reduce the level of risk. The safeguards can be preventive (aimed at preventing the threat from materializing) and reactive (contingency plans). This responds to the need identified in the study's introduction, which concerns the prediction of the course of the cascading effect. At the same time, the proposed method for predicting the cascading effect under conditions of hybrid warfare is the first holistic study in this subject area.

The concept of a method for predicting the cascading effect in hybrid warfare is limited to the features and effects of hybrid war observed in the example of the war in Ukraine and the Israeli-Palestinian conflict. Further research should focus on developing universal features of hybrid warfare and confirming the accepted perception of the safety of civilians (protection from hunger, thirst, injury, disease, too hot and too cold). In addition, it is necessary to empirically test the adopted concept, for example, based on case study and simulation methods. A separate issue is the protection of information from loss and distortion. In this area, modern techniques for ensuring data security can be applied, that is, blockchain.

6 References

[1] ACLED, 2024. *Armed Conflict Location & Event Data (ACLED), Project Ukraine Q&A 2024*. [online] Available at: <https://acleddata.com/acleddatanew/wp-content/uploads/2024/03/Ukraine-QA-2024.pdf>

[2] Babbie, E., 2005. *Badania społeczne w praktyce* (*The Practice of Social Research*). Warszawa: Wydawnictwo Naukowe PWN.

[3] Banasik, M., 2015. How to understand the hybrid war. *Securitologia*, 1(21), pp. 19-34. [online] Available at: <https://www.civitas.edu.pl/wp-content/uploads/2015/03/Securitologia-1-21-2015_019-034.pdf>

[4] Benjamin, N., 2021. How effective is blockchain in cybersecurity? *ISACA Journal*, 4. [online] Available at: <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-4/how-effective-is-blockchain-in-cybersecurity>

[5] Bennett, M. and Gupta, V., 2010. *Dealing in Security: understanding vital services and how they keep you safe*. [online] Available at: <http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf>

[6] Caliskan, M., 2019. Hybrid warfare through the lens of strategy theory. *Defense and Security Analysis*, 35(1), pp. 40-58. https://doi.org/10.1080/14751798.2019.1565364.

[7] Council on Foreign Relations, 2024. *Global Conflict Tracker, Council on Foreign Relations*. [online] Available at: <https://www.cfr.org/global-conflict-tracker> [Accessed 9 October 2023].

[8] Cybersecurity and Infrastructure Security Agency, 2019. *National Critical Functions.* [online] Available at: <https://www.cisa.gov/topics/risk-management/national-critical-functions>

[9] Fabian, E., 2004. *Authorities name 713 soldiers, 66 police officers killed in Gaza war*. The Time of Israel. [online] Available at: <https://www.timesofisrael.com/authorities-name-44-soldiers-30-police-officers-killed-in-hamas-attack/> [Accessed 8 July 2024].

[10] Fox, A.C., 2017. *Hybrid Warfare: The 21st Century Russian of Warfare*. Master's Thesis. https://doi.org/10.13140/ RG.2.2.35922.38086.

[11] Gaynor, K.M., Cherry, M.J., Gilbert, S.L., Kohl, M.T., Larson, C.L., Newsome, T.M., Prugh, L.R., Suraci, J.P., Young, J.K. and Smith, J.A., 2021. An applied ecology of fear framework: linking theory to conservation practice. *Animal Conservation*, 24(3), pp. 308-321. https://doi.org/10.1111/acv.12629.

[12] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S. and Ishfaq, M., 2022. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet*, 14, 341. https://doi.org/10.3390/fi14110341.

[13] Hoffman, F.G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.

[14] Hoffman, F.G., 2018. Examining complex forms of conflict: Gray zone and hybrid challenges. *Prism*, 7(4), pp. 30-47.

[15] Hosanagar, K., 2021. *How the Blockchain Will Impact the financial sector*, Knowledge at Wharton. [online] Available at: <https://knowledge.wharton.upenn.edu>

[16] Hosseini, S., Barker, K. and Ramirez-Marquez, J.E., 2016. A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, 145, pp. 47-61. https://doi.org/10.1016/j.ress.2015.08.006.

[17] Iskandarov, K. and Gawliczek, P., 2023. Hybrid Warfare as a new type of War. The evolution of its conceptual construct. In: M. Banasik, P. Gawliczek and A. Rogozińska, eds. 2020. *The Russian federation and international security*, Poland: Difin, pp. 96-107 <https://www.researchgate.net/publication/373118996_hybrid_warfare_as_a_new_type_of_war_the_evolution_of_its_conceptual_construct>

[18] Itich-Drabarek, I., Misiuk, A., Mitkow, Sz. and Bryczek-Wróbel, P., 2023. *Encyklopedia Bezpieczeństwa Narodowego (Encyclopedia of National Security)*. Warszawa: Dom Wydawniczy ELIPSI. [online] Available at: <https://encyklopedia.revite.pl/>

[19] Joshi A., 2017. Comparison between Scopus & ISI Web of science. *Journal Global Values*, 7(1), pp. 1-11.

[20] Kabir, S. and Papadopoulos, Y., 2019. Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: A review. *Safety science*, 115, pp. 154-175. https://doi.org/10.1016/j.ssci.2019.02.009

[21] Kisilowski, M., Skomra, W., Smagowicz, J., Wiśniewski, M. and Szwarc, K, 2021. *Zarządzanie bezpieczeństwem infrastruktury krytycznej i ciągłością usług kluczowych państwa (Management of critical infrastructure security and continuity of essential services of the state).* Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej.

[22] Krupa, T. and Ostrowska, T., 2012. Decision making in the flat and hierarchical decision problem. *Foundations of Management*, 4(2), pp. 23-36. https://doi.org/10.2478/fman-2013-0008.

[23] Krupa, T. and Wisniewski, M., 2015. Wykorzystanie wiedzy w zarządzaniu sytuacyjnym bezpieczeństwem infrastruktury krytycznej Polski (Use of knowledge in situational management of critical infrastructure security in poland). *Logistyka*, 5, pp. 1027-1033.

[24] Landucci, G., Argenti, F., Cozzani, V. and Reniers, G., 2017. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. *Process Safety and Environmental Protection*, 110, pp. 102-114. https://doi.org/10.1016/j.psep.2017.06.019.

[25] Landucci, G., Khakzad, N. and Reniers, G.L.L., 2020. *Physical security in the process industry: theory with applications.* Cambridge, MA: Elsevier.

[26] Leonhard, R. and Philips, S., 2015. *Little Green Men: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*. Fort

Bragg, NC: US Army Special Operations Command.

[27] Linebarger, C., 2021. Preventive medicine: domestic repression and foreign revolutionary states. *Dynamics of Asymmetric Conflict*, 14(1), pp. 3-24.

[28] Moosavi, N. and Taherdoost, H., 2023. Blockchain technology application in security: A systematic review. *Blockchains*, 1(2), pp. 58-72. https://doi.org/10.3390/blockchains1020005.

[29] Moteff, J., Copeland, C. and Fischer, J., 2003. Critical Infrastructures: *What Makes an Infrastructure Critical?* [online] Available at: <https://irp.fas.org/crs/RL31556.pdf>

[30] North Atlantic Council, 2016. *Deklaracja końcowa szczytu NATO w Warszawie (The Warsaw declaration on Transatlantic Security)*. [online] Available at: <https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf>

[31] OHCHR, 2024. *Office of the United Nations High Commissioner for Human Rights (OHCHR), Gaza Report on the Ground, OHCHR Press Briefing notes*. [online] Available at: <https://www.ohchr.org/en/press-briefing-notes/2024/01/gaza-report-ground>

[32] PAP, 2024. *Mieszkańcy Mariupola z głodu jedzą gołębie, brakuje wody pitnej (Mariupol residents eat pigeons out of hunger, drinking water is in short supply)*. Polish Press Agency (PAP). [online] Available at: <https://www.pap.pl/aktualnosci/news%2C1269876%2Cmieszkancy-mariupola-z-glodu-jedza-golebie-brakuje-wody-pitnej.html>

[33] Peterson, N., 2023. *The Chinese Communist Party's Theory of Hybrid Warfare*. [online] Available at: <https://www.understandingwar.org/sites/default/files/The%20Chinese%20 Communist%20Party%27s%20Theory%20of%20Hybrid%20Warfare_0.pdf>

[34] Singh, S.K. and Kumar, S., 2021. Blockchain technology: introduction. *Integration and Security Issues with IoT*. https://arxiv.org/abs/2101.10921.

[35] Statista Research Department, 2024. *Number of civilian casualties during the war in Ukraine 2022-2024*, Statista. [online] Available at: <https://www.statista.com/statistics/1293492/ukraine-war-casualties/>

[36] Tamplin, T., 2023. *Blockchain transaction verification, Meaning and how it works. Finance Strategists*. [online] Available at: <https://www.financestrategists.com>

[37] The Wall Street Magazine, 2023. *How are transactions verified in Blockchain: The ultimate guide to trust*. [online] Available at: <https://thewallstreetmagazine.com/how-are-transactions-verified-in-blockchain/>

[38] UN News, 2024. *Ukraine: Report reveals war's long-term impact which will be felt for generations, UN News, 22 February*. [online] Available at: <https://news.un.org/en/story/2024/ 02/1146842>

[39] Visser, M., van Eck, N. and Waltman, L., 2021. Large-scale comparison of bibliographic data sources: Scopus, Web of Science, Dimensions, Crossref and Microsoft Academic. *Quantitative Science Studies*, 2(1). https://doi.org/10.1162/qss_a_00112.

[40] VOA, 2024. *As Israel-Hamas War Reaches 100-Day Mark, Here's the Conflict by Numbers*. [online] Available at: <https://www.voanews.com/a/as-israel-hamas-war-reaches-100-day-mark-here-s-the-conflict-by-numbers-/7439224.html> [Accessed 18 July 2024].

[41] Walecki, O.B. and Niejełow, B.M., 2015. *Особенности партизанских и противопартизанских действий в ходе Иракской войны 2003-2011 (Features of guerrilla and anti-guerrilla actions during the Iraq War 2003-2011)*. Moscow.

[42] WHO, 2024. *Emergency Situation Update, Issue 28, 7 October 2023 - 20 April 2024*. [online] Available at: <https://www.emro.who.int/images/stories/Sitrep_-_issue_28b.pdf?ua=1>

[43] Wiśniewski, M., 2020. Methodology of Situational Management of Critical Infrastructure Security. *Foundations of Management*, 12(1), pp. 43-60. https://doi.org/ 10.2478/fman-2020-0004.

[44] Wiśniewski, M., Marczewski, M. and Kisilowski, M., 2016, Zasady budowy scenariuszy zdarzeń niekorzystnych w publicznym zarządzaniu kryzysowym (Rules ror Construction Scenarios Adverse of Events in the Public Crisis Management). [in] M. Ćwiklicki, M. Jabłoński I S. Mazur, red., *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego (Contemporary concepts of public management. Challenges of public sector modernization)*. Fundacja Gospodarki i Administracji Publicznej. pp. 97-110.

[45] World Health Organization Eastern Mediterranean Regional Office, 2024. *Emergency Situation Reports*. [online] Available at: <https://www.emro.who.int/opt/information-resources/emergency-situation-reports.html>

[46] Xu, J.J., 2016. Are blockchains immune to all malicious attacks? *Financial Innovation*, 2(25). https://doi.org/10.1186/s40854-016-0046-5.

[47] Zio, E., 2018. The future of risk assessment. *Reliability Engineering & System Safety,* 177, pp. 176-190. https://doi.org/10.1016/j.ress. 2018.04.020

[48] Zubaydi, H.D., Varga, P. and Molnár, S., 2023. Leveraging Blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review. *Sensors*, 23(2). https://doi.org/10.3390/ s23020788.

[49] Zwęgliński, T., Smolarkiewicz, M. and Gromek, P., 2020. *Efekt kaskadowy współczesnym wyzwaniem zarządzania kryzysowego (The cascading effect a modern challenge of crisis management)*. Szkoła Główna Służby Pożarniczej, ISBN 978-83-957235-9-9.