14th International Defense and Homeland Security Simulation Workshop, 003
21th International Multidisciplinary Modeling & Simulation Multiconference

2724-0363 © 2024 The Authors.
doi: 10.46354/i3m.2024.dhss.003

Modelling the Promotion of Warriors' Resistance to Information Warfare Threats through Fuzzy DEMATEL with Trapezoidal Structure

Svajone Bekesiene*

General Jonas Žemaitis Military Academy of Lithuania, Silo 5a, Vilnius, 10322, Lithuania

*Corresponding author. Email address: svajone.bekesiene@lka.lt

Abstract

In today's geopolitical landscape, Russia's mastery of hybrid warfare poses a significant challenge to international stability, particularly in neighbouring states. This paper examines the theory and practice of hybrid conflicts, focusing on their impact on international security dynamics. We analyse Russia's aggressive tactics, which have been exemplified in events such as the 2014-2015 Ukraine crisis, and explore the implications for global security. Through a comprehensive literature review, we identify key dimensions of information warfare threats and assess their impact on military resilience. Drawing on the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method, we conduct a structured analysis to elucidate the causal relationships between various factors affecting military preparedness. Our findings highlight the multifaceted nature of information warfare and underscore the importance of adaptive strategies in countering emerging threats. By employing the DEMATEL method, this study provides valuable insights into the complex dynamics of information warfare and offers actionable recommendations for enhancing military resilience. With this innovative approach, testing cause and effect relationships provides an innovative approach to soldier resilience: (i) it systematically identifies the links between information warfare threats, which are usually assessed in isolation, and thus provides a comprehensive set of potential interventions to enhance overall soldier resilience; (ii) it clarifies the relationships between different manifestations of information warfare threats, which may reveal unintended consequences for soldier resilience; and (iii) it identifies a comprehensive set of potential interventions to enhance overall soldier resilience in a military context. It is concluded that the proposed approach is promising to enhance the effectiveness of information warfare training.

Keywords: Information warfare threats; fuzzy DEMATEL; trapezoidal fuzzy number; warriors' resistance; influence–relation map

1. Introduction

In today's environment of military and political strategies, the theory and practice of hybrid conflicts is Russia's greatest achievement. Hybrid warfare, widely regarded as the most effective method of forcing neighbouring states to submit to the Kremlin's dictates, is a major challenge to international stability. Therefore, in all cases of Russian aggression, it becomes crucial to anticipate the use of hybrid warfare capabilities and tactics, which have been thoroughly tested in the events of 2014-2015 in Ukraine.

The logic of global events, including the partial success of the West's sanctions policy against Russia and its economic isolation, together with the volatility of oil prices, is encouraging the Kremlin regime to rapidly implement its aggressive plans towards its neighbouring countries. This urgency stems from the fact that Russia's chances of success in conflicts are decreasing in proportion to its economic decline. In addition, internal political conflicts, exacerbated by the

economic downturn, force the Russian public to immediately turn its attention to external adversaries, thus continuously legitimising the Kremlin regime through the display of foreign policy and military victories.

Over the past decade, not only NATO and the EU but also the Lithuanian Armed Forces have increasingly encountered manifestations of information warfare. However, there is a lack of comprehensive studies by Lithuanian authors on how information threats affect Lithuanian military units and whether sufficient efforts are being made to build resilience to these threats.

The concept of resilience to information threats is primarily found in the works of foreign scholars. Gibson (2010) presented a model of resilience principles, while Theohary (2018) examined the balance of informational power, and Fridman (2019) and Libicki (1995) introduced information warfare tools. Kitsa et al. (2019), Pocheptsov (2018), and Cyrulik (1999) studied Russia's information confrontations, hybrid warfare tools, and information threats as a form of warfare, while Firinci (2020) focused on information threats. Zachary et al. (2021) described the impact operations, and for the Lithuanian Armed Forces, studies by Zachary et al. (2021), Thomas (2014), Franke (2015), Racz (2015), and Ajir et al. (2018) provided insights into various aspects of information threats.

Analyzing methods to enhance resilience to information threats in the Lithuanian Armed Forces, researchers such as Zanfir (2012), Tashev et al. (2019), Thiele (2016), Blay et al. (2020), and Valli et al. (2006) have contributed valuable knowledge on information operations tools, Russian information warfare methods, areas of focus for enhancing resilience, cognitive abilities, and information assessment structures.

Lithuanian scholars have also delved into this topic. Žilinskas (2017) examined the resilience of the military to information warfare, with a focus on the mind and soft power as the primary targets. Bajarūnas et al. (2018) identified elements of hybrid threats, Miliušas (2020) researched information threats to Lithuania, while Cesiulis (2014), Vaišnys et al. (2017), and Kasčiūnas et al. (2017) discussed education as a weapon, countermeasures, and audience manipulation. Grincevičius (2019) explored factors influencing the development and management of resilience.

Given that Information Warfare encompasses various dimensions of threats, it requires evaluation and modelling using the multiple-criteria decision-making (MCDM) method (Yazdi et al., 2020). This approach recognizes that Information Warfare is not a monolithic phenomenon but rather a complex interplay of diverse elements such as cyberattacks, disinformation campaigns, psychological operations, and physical sabotage. Each of these dimensions presents unique challenges and requires distinct strategies for mitigation and defence. By employing the MCDM method, decision-makers can systematically assess the relative importance of different threat factors, prioritize response measures, and allocate resources effectively to address the multifaceted nature of Information Warfare. This allows for a more nuanced understanding of the threat landscape and enables organizations to develop comprehensive and adaptive strategies to counter emerging threats in the information domain.

The Decision-Making Trial and Evaluation Laboratory (DEMATEL) method, pioneered by the Battelle Memorial Institute, has emerged as a cornerstone tool for resolving complex issues arising from the intricate and multi-layered relationships inherent in multicriteria decision-making within social science problems (Fontela et al., 1976). By revealing the significance and interconnectedness among various criteria or dimensions, DEMATEL provides invaluable insights into decision-making processes.

One of the primary advantages of the DEMATEL method lies in its ability to address the limitations of traditional statistical analysis methods. Unlike conventional approaches, DEMATEL analysis goes beyond mere correlation assessment by offering insights into the directionality of relationships and the degree of impact between investigated criteria. This nuanced understanding enables decision-makers to navigate complex decision landscapes with greater precision and confidence. Moreover, the DEMATEL method facilitates the visualization of intricate causal relationships through models or diagrams, thereby enhancing comprehension and decision-making efficacy. Its versatility has been demonstrated across diverse domains, where it has been successfully employed to analyze factor correlation and unravel complex relationships (Jiao et al., 2020; Liu et al., 2020).

In this paper, we investigate the utility and applications of the DEMATEL method, exploring its role in addressing contemporary challenges and providing actionable insights for decision-makers across Information Warfare Threats fields. Through a synthesis of recent research and case studies, we aim to showcase the flexibility and effectiveness of DEMATEL as a powerful tool for understanding and navigating complex decision environments.

Despite extensive research in the field of Information Warfare Threats (IWT), scholars have yet to pinpoint the primary factor or dimension playing a pivotal role in shaping these threats. This ambiguity underscores the need for a comprehensive analysis to elucidate the evolving trends of IWT and their implications for active-duty soldiers. In particular, understanding how information threats impact the resilience of the Lithuanian Armed Forces is imperative for devising effective mitigation strategies.

To address this gap, the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method has been chosen as a robust analytical framework. Known for its ability to tackle group decision-making problems, DEMATEL offers a structured approach to dissecting complex relationships and identifying key drivers within a multifaceted issue (Bekesiene et al., 2021). By leveraging the DEMATEL method, this study aims to provide clarity on the dynamics of IWT and assess their impact on the resilience of the Lithuanian Armed Forces. In addition to its analytical prowess, the DEMATEL method offers a unique advantage in handling uncertainty and ambiguity inherent in the assessment of resilience criteria. Unlike traditional approaches that rely on crisp values, the DEMATEL method allows for the expression of criteria assessment and directed influential degrees using trapezoidal fuzzy numbers. This fuzzy approach enhances the granularity and accuracy of the analysis, enabling a more nuanced understanding of the resilience landscape in the face of IWT.

The following sections of this study are organised as follows. First, we define the identified research gap related to Information Warfare Threats (IWT) in the military context and present our methodology, which uses fuzzy-DEMATEL modelling to address this gap. The second section provides a comprehensive literature review on the criteria relevant to Information Warfare Threats (IWTs), providing a contextual framework for our analysis. The third section analyses the fuzzy numbers, arithmetic operations and methodologies applied to the fuzzy-DEMATEL approach, clarifying the technical foundations of our approach. In the fourth section, we present the main findings of the proposed method and show that it is effective in explaining the complex dynamics of inland waterway transport and its impact on military resilience. Section five discusses in detail the main findings of the study and explains their theoretical and practical implications. Finally, the sixth chapter presents the overall conclusions drawn from the analysis, together with recommendations for future research aimed at better understanding IWT and enhancing military preparedness in the face of evolving information threats.

2. Literature Review Focused on Information Warfare Threats in the Military Context

With the advancement of technology, as highlighted by Firinci (2020), comes an increased impact on the military. The widespread availability of global information on the internet presents both opportunities and risks in the information landscape. Within the context of informational and psychological attacks, where techniques commonly employed in marketing prevail, the pursuit of rapid, effective, and practical action relies heavily on manipulation.

By utilizing information threats as tools, the Russian Federation (RF) employs Information Technology (IT), Information Operations (IO), and Psychological Operations (PO) to target human cognitive domains. These operations are part of Russia's broader strategy to influence perceptions, behaviour, and decision-making processes both domestically and internationally.

1. Information Technology (IT):
   - The Russian government and affiliated actors leverage IT capabilities to conduct cyber operations aimed at infiltrating, disrupting, or manipulating digital systems and networks. These operations can range from cyber espionage and data theft to sabotage and disruption of critical infrastructure.
   - Advanced hacking techniques, such as phishing, malware deployment, and distributed denial-of-service (DDoS) attacks, are commonly used to gain unauthorized access to sensitive information and compromise the integrity of digital platforms.
   - IT-based operations also include the spread of disinformation and propaganda through social media platforms, websites, and online forums. By exploiting vulnerabilities in online communication channels, Russia seeks to disseminate false narratives, sow discord, and undermine trust in democratic institutions.
2. Information Operations (IO):
   - Information operations encompass a wide range of activities aimed at shaping perceptions, influencing opinions, and shaping the narrative in support of Russian interests. These operations often involve the strategic dissemination of propaganda, misinformation, and fake news through various media channels.
   - Russia employs IO tactics to create confusion, manipulate public opinion, and exploit societal divisions within target countries. These operations may include the use of state-controlled media outlets, covert influence campaigns, and the manipulation of online discourse.
   - IO also involves the use of psychological warfare techniques to undermine confidence in democratic institutions, destabilize governments, and foster internal divisions. By targeting key influencers, opinion leaders, and vulnerable populations, Russia seeks to amplify its messaging and exert influence over public discourse.
3. Psychological Operations (PO):
   - Psychological operations are designed to influence the emotions, beliefs, and behaviours of individuals or groups through

targeted messaging and persuasion techniques. These operations may involve the use of propaganda, disinformation, psychological warfare, and social engineering tactics.
- Russia employs PO to exploit psychological vulnerabilities, manipulate perceptions, and induce fear, uncertainty, and doubt among its adversaries. These operations often target specific demographics, such as military personnel, political leaders, or ethnic minorities, with tailored messaging designed to elicit specific responses.
- By leveraging psychological operations, Russia seeks to undermine the morale, cohesion, and resilience of its adversaries while projecting strength and legitimacy. These operations may be conducted overtly through state-controlled media outlets or covertly through proxy groups and disinformation networks.

Overall, the Russian Federation's use of Information Technology, Information Operations, and Psychological Operations reflects a comprehensive strategy aimed at exerting influence, shaping perceptions, and advancing its geopolitical objectives on the global stage.

Leveraging linguistic and artificial intelligence capabilities, informational activities are directed towards shaping audience perception. Thus, based on the tools and methods proposed by scholars in the field of information warfare, it can be inferred that one of the most effective methods in information warfare is influencing warriors' psychological and cognitive behaviour through informational and psychological operations.

In accordance with the conceptual framework of information warfare, a comprehensive review of prior scholarly literature was undertaken to discern the primary threats identified by researchers in this domain. Through this review, a systematic classification of key information warfare threats was established, delineating their respective scopes and areas of influence. The categorization of these threats was predicated on their impact across distinct dimensions, namely, Awareness of Resistance to Informational Threats (A), Information Dissemination Sources (B), Impact of Information Threats (C), Decision-Making in the Environment of Information Attacks (D), and Strengthening Resistance to Informational Threats in LAM (E).

This approach facilitated a nuanced understanding of the multifaceted nature of information warfare and its attendant challenges. By categorizing threats based on their operational domains and strategic implications, researchers were able to delineate the intricate interplay between various elements within the information environment. Moreover, this classification framework served as a basis for developing targeted strategies and countermeasures to mitigate the risks posed by information warfare activities.

Within the scope of Awareness of Resistance to Informational Threats (A), scholars examined the extent to which individuals and organizations were cognizant of the diverse array of threats posed by information warfare. This encompassed an assessment of awareness-raising initiatives, educational programs, and training efforts aimed at enhancing resilience to malicious information activities.

Information Dissemination Sources (B) pertained to the channels and platforms utilized by adversaries to disseminate propaganda, disinformation, and other forms of hostile content. Researchers analyzed the role of traditional media, social networking sites, and online forums in facilitating the spread of misinformation and shaping public perceptions.

The Impact of Information Threats (C) focused on the tangible and intangible consequences of information warfare operations on individuals, communities, and societies. This included an examination of the psychological, social, and political ramifications of information manipulation and propaganda campaigns.

Decision-Making in the Environment of Information Attacks (D) explored the complexities of decision-making processes in the context of information warfare. Scholars investigated how cognitive biases, perceptual distortions, and information overload could affect decision-makers' judgment and strategic responses to emerging threats.

Lastly, Strengthening Resistance to Informational Threats in LAM (E) involved efforts to fortify defences and resilience against information warfare within military and defence organizations. These encompassed initiatives aimed at enhancing technological capabilities, training protocols, and doctrinal frameworks to withstand and counteract adversarial information operations.

Additional details regarding the dimensions of Information Warfare Threats and their associated aspects are substantiated by a wide range of previous studies. Some of these studies are included as supporting literature for the conducted investigations, as shown in Table 1.

Table 1. Literature supporting the categorisation of the main information warfare threats.

Information warfare threats dimension and associate	Categorization of key information warfare threats	Previous research authors

aspects			
Awareness of Resistance to Informational Threats (A)	A1	Level of awareness among warriors regarding informational threats posed by Russian psychological operations.	Hill'as, 2006; Bajarūnas & Keršanskas, 2018; Kitsa et al., 2019; Pocheptsov, 2018; Firinci, 2020; Zachary et al., 2021.
	A2	The extent to which soldiers understand the tactics, techniques, and objectives of Russian information warfare efforts..	
	A3	the effectiveness of training programs and educational initiatives aimed at increasing soldiers' awareness of informational threats.	
Information Dissemination Sources (B)	B1	The sources and channels used by Russian psychological operations to disseminate information and influence warriors.	Bokša, 2022; Prier, 2020; Polyakova & Boyer, 2018; Whyte, 2020; McGeehan, 2018.
	B2	State-controlled media outlets, social media platforms, and other communication channels utilized by adversaries to spread propaganda and disinformation.	
	B3	The credibility and reliability of information sources used in Russian information warfare campaigns targeting military personnel.	
Impact of Information Threats (C)	C1	The impact of Russian psychological operations on the cognitive and emotional well-being of warriors.	Zachary et al. 2021; Thomas, 2014; Franke, 2015; Racz, 2015; Ajir et al., 2018.
	C2	The degree to which soldiers' beliefs, attitudes, and behaviours are influenced by exposure to propaganda, disinformation, and psychological manipulation.	
	C3	The psychological effects of information threats on military personnel, including stress, anxiety, and morale.	
Decision-Making in the Environment of Information Attacks (D)	D1	The decision-making processes of warriors in the face of information attacks orchestrated by the Russian Federation.	Russell & Abdelzaher, 2018; Gill et al.,2020; Van Den Bosch & Bronkhorst, 2018; Hansel, 2018; Egloff, & Smeets, 2023.
	D2	How soldiers assess and respond to information warfare tactics employed by adversaries.	
	D3	The effectiveness of decision-making strategies and countermeasures implemented to mitigate the impact of information threats on military operations.	
Strengthening Resistance to Informational Threats in LAM (E)	E1	The resilience-building efforts and initiatives undertaken by the Lithuanian Armed Forces (LAM) to counter Russian psychological operations.	Zachary et al. 2021; Thomas, 2014; Franke, 2015; Racz, 2015; Ajir et al., 2018; Žilinskas, 2017; Bajarūnas et al. 2018; Miliušas, 2020; Cesiulis 2014), Vaišnys et al., 2017; Kasčiūnas et al., 2017; Grincevičius, 2019.
	E2	The effectiveness of training programs, awareness campaigns, and psychological resilience training aimed at enhancing soldiers' resistance to informational threats.	
	E3	Gaps and areas for improvement in LAM's strategies for strengthening resilience to Russian information warfare tactics.	

The systematic categorization of the primary threats within information warfare has established a structured framework conducive to the analysis and evaluation of the multifaceted challenges presented by adversaries operating within the information domain. By delineating these threats from various perspectives, it became feasible to develop a more comprehensive questionnaire tailored for expert assessment.

3. Materials and Methods

The primary objective of this research is to explain the causal relationship between the dimensions of information warfare and their impact on soldiers psychological and cognitive behaviour, particularly through the implementation of informational and psychological operations. This investigation adheres to a rigorous and structured methodology to systematically explore these phenomena. To achieve this goal, a comprehensive research framework was developed, delineating the sequential steps involved in the analytical process. This framework serves as a guiding structure for the systematic investigation of the issues at hand, facilitating the identification of causal relationships among various factors that underlie the influence of informational and psychological operations on soldiers psychological and cognitive behaviour.

By precisely following this structured methodology, the study aims to uncover the intricate cause-and-effect dynamics inherent in the relationship between information warfare dimensions and their effects on soldiers' cognition and psychology. Through rigorous analysis and systematic investigation, the research goings-on to provide valuable insights into the mechanisms through which informational and psychological operations employ influence on soldiers' behaviour in the context of contemporary information warfare scenarios.

3.1. Steps of the Conducted Research

The Decision-Making Trial and Evaluation Laboratory (DEMATEL) technique, a sophisticated analytical methodology, stands out for its efficacy in discerning causal relationships among designated dimensions or factors. The delineated steps of the analytical framework employed in this study are illustrated in Figure 1. The primary objective of this investigation entailed the meticulous selection of key factors pertaining to psychological resilience, as

previously delineated in pertinent literature, and their relevance to active-duty soldiers. To achieve this, an extensive survey was conducted across multiple databases, employing a variety of keywords to identify studies elucidating the nuances influencing soldiers' psychological and cognitive behaviour. Subsequently, twenty-seven original articles meeting stringent criteria were meticulously curated for their insights into information warfare and its implications on the psychological and cognitive dynamics of soldiers.

The concept of information warfare encompasses a wide range of activities aimed at influencing, disrupting, or controlling the flow of information in various contexts, including military operations, political campaigns, and cybersecurity. Scholars have extensively studied IW threats to understand their nature, scope, and impact on society and national security. Through a systematic review of the literature, we categorize these threats into five key scopes, namely: Awareness of Resistance to Informational Threats (A), Information Dissemination Sources (B), Impact of Information Threats (C), Decision-Making in the Environment of Information Attacks (D), and Strengthening Resistance to Informational Threats in LAM (E). The subsequent step involved the formulation of a questionnaire for conducting pair-wise assessments of criteria. Subsequently, active-duty officers from the Lithuanian Armed Forces were invited to provide their evaluations concerning resilience factors.

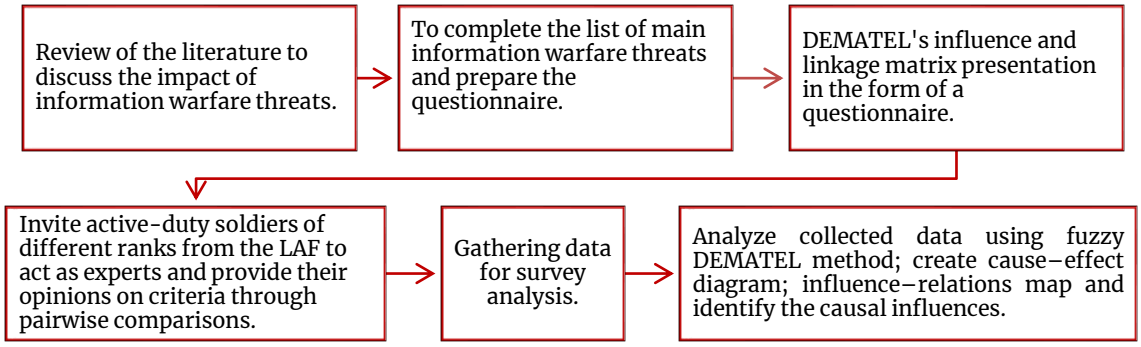


Figure 1. The key steps of the conducted research are presented in the scheme.

Examine the collected data using the fuzzy DEMATEL method to produce cause-and-effect illustrations, effect and relationship maps, and categorise the causal influences. Commencing from the third step, we employed the fuzzy DEMATEL technique to scrutinize and evaluate the indefinite and ambiguous landscape of information warfare threats (IWT). The multidimensional and interactive nature of IWT was explored through a comprehensive methodology. The fuzzy theory was employed to transform expert valuations of semantic IWT into the evaluator's valuation degree value using the membership function with trapezoidal fuzzy numbers. Lastly, the modelling results were represented in two diagrams: a cause-and-effect diagram and an influence–relations map.

3.2. Fuzzy Trapezoidal DEMATEL Analysis: A Methodological Approach

A linguistic variable, also known as a linguistic term, refers to a variable in which the value is not expressed as a precise numerical quantity but rather as a word or a sentence in a natural language. This allows for the representation of concepts that are inherently fuzzy or uncertain in nature, such as temperature, brightness, or satisfaction level. By using linguistic terms, the variability and nuances of human perception and interpretation can be captured more effectively than with traditional crisp numerical values. Linguistic variables are commonly employed in fuzzy logic systems to model and analyse complex systems where uncertainty and imprecision are prevalent.

The solution derived from fuzzy numbers provides a valuable outcome because it allows for the representation of uncertainty and variability inherent in linguistic decisions required to express important relationships. Fuzzy numbers enable the modelling of imprecise or vague information, which is often encountered in real-world scenarios where decisions need to be made based on incomplete or subjective data. By incorporating fuzzy numbers into the analysis, the nuances and subtleties of human perception and interpretation can be effectively captured, leading to more robust and meaningful results in decision-making processes.

In line with previous research (Chen-Yi et al., 2007), the evaluation scores of linguistic variables were described using five specific linguistic terms, the chosen experts may use linguistic term set L={L0: Very Low; L1: Low; L2: Medium; L3: High; L4: Extremely High} to express his/her opinion. These terms were

associated with positive trapezoidal-fuzzy numbers and influence score of trapezoidal fuzzy numbers as outlined in Table 2. To handle uncertain linguistic terms when employing trapezoidal fuzzy numbers and

to represent the gathered data effectively, we adhered to the methodologies outlined in prior studies (Felix and Devadoss, 2014).

Table 2. Term set for linguistic values of trapezoidal fuzzy numbers.

Term set	Linguistic relationships	Influence score	Linguistic values of fuzzy trapezoidal measurements			
			v_1	v_2	v_3	v_4
0=L0	Very low/**VL**	0.125	(0.00,	0.00,	0.00,	0.25)
1=L1	Low influence /**LI**	0.1875	(0.00,	0.00,	0.25,	0.50)
2=L2	Medium influence/**MI**	0.375	(0.00,	0.25,	0.50,	0.75)
3=L3	High influence/**HI**	0.625	(0.25,	0.50,	0.75,	1.00)
4=L4	Extremely high influence/**EH**	0.8125	(0.50,	0.75,	1.00,	1.00)

Note: Five linguistic terms describe the linguistic variables assessment scores (Chen-Yi et al., 2007).

These scholars provided investigation on the grouping technique of trapezoidal fuzzy numbers and offered how linguistic terms $[L_l, L_u]$ and $[L_\alpha, L_\beta]$ can be transformed to a equivalent trapezoidal fuzzy value by employing arithmetic procedures and the membership function characterized by equation (1):

$$\mu_{\tilde{v}}(X) = \begin{cases} \dfrac{X - v_1}{v_2 - v_1}, v_1 \le x \le v_2, \\ 1, v_2 \le x \le v_3, \\ \dfrac{v_4 - X}{v_4 - v_3}, v_3 \le x \le v_4, \\ 0, \quad otherwise. \end{cases} \tag{1}$$

where $\tilde{v}$ is a fuzzy set of actual numbers R and membership can be obtainable as $\tilde{v}: R \to [0,1]$, $x \in R$, $\tilde{v}(x) = 1$. So, the aggregation processes (addition ($\oplus$), substraction ($\ominus$), multiplication ($\otimes$) and division ($\oslash$)) among two linguistic terms $[L_l, L_u]$ *and* $[L_\alpha, L_\beta]$ can be calculated by the equations presented below:

$$[L_l, L_u] \oplus [L_\alpha, L_\beta] = \left(v_{lu}^1 + v_{\alpha\beta}^1, \cdots, v_{\alpha\beta}^4 + v_{lu}^4\right); \tag{2}$$

$$[L_l, L_u] \ominus [S_\alpha, S_\beta] = \left(v_{lu}^1 - v_{\alpha\beta}^1, \cdots, v_{\alpha\beta}^4 - v_{lu}^4\right); \tag{3}$$

$$\mathrm{k} \otimes [L_l, L_u] = \left(k \times v_{lu}^1,\ k \times v_{lu}^2, k \times v_{lu}^3,\ k \times v_{lu}^4\right); \tag{4}$$

$$[L_l, L_u]^{-1} \cong \left(\frac{1}{v_{lu}^4}, \frac{1}{v_{lu}^3}, \frac{1}{v_{lu}^2}, \frac{1}{v_{lu}^1}\right). \tag{5}$$

Subsequently, the entire process of fuzzy DEMATEL approach involves a comprehensive analysis encompassing eight distinct steps.

Step 1. First, the assessment data matrix must be generated. This matrix serves as the basis for further analysis using the fuzzy DEMATEL method. This matrix captures the collective judgment of the experts regarding the relationships and influences among the resilience dimensions. It provides valuable insights into the interconnectedness and importance of each dimension in the information warfare threats as a context of the study. So, mathematically it can be presented as the creation of the direct – relation matrix $\widehat{M}_k = \left[\hat{m}_{ij}\right]_{nxn}$. Initially, a finite set of information warfare threats $T = \{T_1, T_2, \cdots, T_n\}$ have to be selected, where T_1 represents the i^{th} dimension with $i \in \{1,2,\cdots,n\}$. Additionally, a set of professional soldiers (experts) $E = \{E_1, E_2, \cdots, E_l\}$ who were selected for this study is utilized, where E_k represents the k^{th} expert $k \in \{1,2,\cdots,l\}$. Subsequently, individually completed matrices of experts' decisions are collected, forming a set of linguistic terms $T = \{t_0, t_1, \cdots, t_g\}$, where t_s represents the L^{th} linguistic term, $L \in \{1,2,\cdots,g\}$. Consequently, the direct-relation matrix provided by each expert E_k is established and represented by the following equation (2):

$$\widehat{M} = \left[\hat{m}_{kij}\right]_{n\times n} = \begin{matrix} T_1 \\ T_2 \\ \vdots \\ T_n \end{matrix} \begin{bmatrix} 0 & \hat{m}_{k12} & \cdots & \hat{m}_{k1n} \\ \hat{m}_{k21} & 0 & \cdots & \hat{m}_{k2n} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{m}_{kn1} & \hat{m}_{kn2} & \cdots & 0 \end{bmatrix}, \quad k \in 1,2,\cdots,l\,. \tag{6}$$

where $k \in \{1,2,\cdots,l\}$.

Step 2. Following Equation (1), the values in the direct-relation matrices need to be converted into trapezoidal fuzzy numbers. In this study, all experts are considered to be of equal importance, and their judgments are aggregated to create the main criteria assessment matrix. To accomplish this, arithmetic mean operations are applied to the trapezoidal fuzzy numbers, transforming the matrix $\widehat{M} = \left[\hat{m}_{kij}\right]_{n\times n}$ into $\widetilde{M} = \left[\tilde{m}_{kij}\right]_{n\times n}$. The process involves aggregating all direct-relation matrices $\widehat{M}_1, \widehat{M}_2, \cdots, \widehat{M}_k$ into the main matrix using the arithmetic procedures outlined in Equations 2 and 4. Each element of the main matrix represents the aggregated assessment of the information warfare threats based on the collective judgments of the experts. By applying arithmetic operations to the trapezoidal fuzzy numbers, the main criteria assessment matrix $\widehat{M}$ is derived, providing a comprehensive evaluation of the relationships and influences among information warfare threats. This matrix serves as the foundation for further analysis using the fuzzy DEMATEL method, enabling to uncover valuable insights into the causal relationships within the system.

Step 3. Have to be constructed the group uncertain direct relation matrix $\widetilde{M} = \left[\tilde{m}_{kij}\right]_{n\times n}$, where each $\tilde{m}_{kij} = \left(m_{kij}^1, m_{kij}^2, m_{kij}^3, m_{kij}^4\right)$ component for this matrix can be calculated by the equations from 7 to 10:

$$m_{kij}^1 = \frac{1}{n}\sum_{k=1}^{n} m_{kij}^1, \qquad i,j = 1,2,\cdots,n; \tag{7}$$

$$m_{kij}^2 = \frac{1}{n}\sum_{k=1}^{n} m_{kij}^2, \qquad i,j = 1,2,\cdots,n; \tag{8}$$

$$m_{kij}^3 = \frac{1}{n}\sum_{k=1}^{n} m_{kij}^3, \qquad i,j = 1,2,\cdots,n; \tag{9}$$

$$m_{kij}^4 = \frac{1}{n}\sum_{k=1}^{n} m_{kij}^4, \qquad i,j = 1,2,\cdots,n. \tag{10}$$

Step 4. Now the group uncertain direct relation matrix $\tilde{M} = [\tilde{m}_{kij}]_{n\times n}$ have to be converted into the normalized indefinite direct-relation matrix $\tilde{Z} = [\tilde{z}_{ij}]_{n\times n}$, where each $\tilde{z}_{ij} = (z_{ij}^1, z_{ij}^2, z_{ij}^3, z_{ij}^4)$ component for this matrix can be designed by these equations from 11 to 14:

$$z_{ij}^1 = {m_{ij}^1}\Big/{\max_{1\le i\le n}\left\{\sum_{j=1}^{n} m_{ij}^1\right\}}, i,j = 1,2,\dots,n; \tag{11}$$

$$z_{ij}^2 = {m_{ij}^2}\Big/{\max_{1\le i\le n}\left\{\sum_{j=1}^{n} m_{ij}^2\right\}}, i,j = 1,2,\dots,n; \tag{12}$$

$$z_{ij}^3 = {m_{ij}^3}\Big/{\max_{1\le i\le n}\left\{\sum_{j=1}^{n} m_{ij}^3\right\}}, i,j = 1,2,\dots,n; \tag{13}$$

$$z_{ij}^4 = {m_{ij}^4}\Big/{\max_{1\le i\le n}\left\{\sum_{j=1}^{n} m_{ij}^4\right\}}, i,j = 1,2,\dots,n. \tag{14}$$

where the key rule must be unbroken, which is

$$\max_{1\le i\le n}\left\{\sum_{j=1}^{n} m_{ij}^4\right\} \neq 0, and\ 0 \le z_{ij}^1 \le z_{ij}^2 \le z_{ij}^3 \le z_{ij}^4 < 1. \tag{15}$$

Following, the matrix $\tilde{Z}$ have to be changed into four crisp-value matrices Z^1, Z^2, Z^3, Z^4:

$$Z^1 = \begin{bmatrix} 0 & z_{12}^1 & \cdots & z_{1n}^1 \\ z_{21}^1 & 0 & \cdots & z_{2n}^1 \\ \vdots & \vdots & \ddots & \vdots \\ z_{n1}^1 & z_{n2}^1 & \cdots & 0 \end{bmatrix}, Z^2 = \begin{bmatrix} 0 & z_{12}^2 & \cdots & z_{1n}^2 \\ z_{21}^2 & 0 & \cdots & z_{2n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ z_{n1}^2 & z_{n2}^2 & \cdots & 0 \end{bmatrix},$$

$$Z^3 = \begin{bmatrix} 0 & z_{12}^3 & \cdots & z_{1n}^3 \\ z_{21}^3 & 0 & \cdots & z_{2n}^3 \\ \vdots & \vdots & \ddots & \vdots \\ z_{n1}^3 & z_{n2}^3 & \cdots & 0 \end{bmatrix}, Z^4 = \begin{bmatrix} 0 & z_{12}^4 & \cdots & z_{1n}^4 \\ z_{21}^4 & 0 & \cdots & z_{2n}^4 \\ \vdots & \vdots & \ddots & \vdots \\ z_{n1}^4 & z_{n2}^4 & \cdots & 0 \end{bmatrix}.$$

and computed the $\tilde{Z}^k$ by employing the multiplication method of crisp value matrices.

Step 5. This step belongs to the procedure where the total-relation matrix $\tilde{G}$ have to be defined by steps obtainable below:

$$\tilde{G} = \lim_{k\to+\infty}(\tilde{Z}^1 \oplus \tilde{Z}^2 \oplus \dots \oplus \tilde{Z}^k);\ \tilde{G} = [\tilde{g}_{ij}]_{n\times n} \tag{16}$$

If we let matrix $\tilde{G}$ be characterised as follows:

$$\tilde{G} = \begin{bmatrix} \tilde{g}_{11} & \tilde{g}_{12} & \cdots & \tilde{g}_{1n} \\ \tilde{g}_{21} & \tilde{g}_{22} & \cdots & \tilde{g}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{g}_{n1} & \tilde{g}_{n2} & \cdots & \tilde{g}_{nn} \end{bmatrix}, \quad where\ \tilde{g}_{ij} = (g_{ij}^1, g_{ij}^2, g_{ij}^3, g_{ij}^4). \tag{17}$$

Accordingly, the total-relation matrix can be calculated by subsequent the equations 18-21:

$$[g_{ij}^1]_{n\times n} = G^1(I - G^1)^{-1}, \ i,j = 1,2,\cdots,n; \tag{18}$$

$$[g_{ij}^2]_{n\times n} = G^2(I - G^2)^{-1}, \ i,j = 1,2,\cdots,n; \tag{19}$$

$$[g_{ij}^3]_{n\times n} = G^3(I - G^3)^{-1}, \ i,j = 1,2,\cdots,n; \tag{20}$$

$$[g_{ij}^4]_{n\times n} = G^4(I - G^4)^{-1}, \ i,j = 1,2,\cdots,n. \tag{21}$$

Step 6. To identify the total strengths of influencing and influenced association of information warfare threats $T_1, T_2, \cdots, T_n$ involved into examination, the sum of each row $(\tilde{r}_i = (r_i^1, r_i^2, r_i^3, r_i^4)$ of matrix $\tilde{G}$ must be computed. Additionally, we can compute the sum of each column $\tilde{c}_i = (c_i^1, c_i^2, c_i^3, c_i^4)$ of matrix $\tilde{G}$ and recognise the general strength in which the IW threat T_n is caused by others.

Step7. This step involves determining the uncertain distinction and relation of each dimension by calculating the sum of their respective values $\tilde{r}_i$ and $\tilde{c}_i$, the equations 22-25:

$$s_i^1 = r_i^1 + c_i^1, i = 1,2,\dots,n; \tag{22}$$

$$s_i^2 = r_i^2 + c_i^2, i = 1,2,\dots,n; \tag{23}$$

$$s_i^3 = r_i^3 + c_i^3, i = 1,2,\dots,n; \tag{24}$$

$$s_i^4 = r_i^4 + c_i^4, i = 1,2,\dots,n. \tag{25}$$

Correspondingly, the associations of examined IW threats can be computed as the variance among $\tilde{r}_i$ and $\tilde{c}_i$, as shown in the equations 26-29:

$$d_i^1 = r_i^1 - c_i^1, i = 1,2,\dots,n; \tag{26}$$

$$d_i^2 = r_i^2 - c_i^2, i = 1,2,\dots,n; \tag{27}$$

$$d_i^3 = r_i^3 - c_i^3, i = 1,2,\dots,n; \tag{28}$$

$$d_i^4 = r_i^4 - c_i^4, i = 1,2,\dots,n. \tag{29}$$

Step 8. The crisp importance and relation of each IW threat is identified by using the centroid (centre of gravity) measures (Yager et al., 1994) that can be calculated by using equations 30 and 31:

$$s_i = \tfrac{1}{4}\left(s_i^1 + s_i^2 + s_i^3 + s_i^4\right); \tag{30}$$

$$d_i = \tfrac{1}{4}\left(d_i^1 + d_i^2 + d_i^3 + d_i^4\right). \tag{31}$$

To illustrate the study results graphically, a causal diagram can be constructed based on the calculated values of s_i and d_i calculated. This visualization method effectively portrays the significance and categorization of the examined dimensions. By plotting these values on a graph, researchers can visually represent the causal relationships and distinctions between different dimensions within the studied system. This graphical representation enhances the understanding of how various factors influence each other and provides

valuable insights into the overall structure and dynamics of the system under investigation.

4. Research Findings and Analysis

The fuzzy – trapezoidal DEMATEL method was implemented through a series of eight main steps. Initially, a panel of sixteen experts was carefully selected to provide their assessments on four psychological resilience dimensions and seventeen sub-factors. These assessments were gathered using a pair-wise comparisons questionnaire, where experts expressed their opinions using linguistic terms specified in a pre-defined linguistic term set (refer to Table 2). The questionnaire facilitated the evaluation of the strength of correlation between any two given factors. In this assessment, five linguistic terms were employed to describe the assessment scores of the linguistic variables: "NI" (No Influence), "VL" (Very Low), "LI" (Low), "HI" (High), and "EH" (Extremely High). These linguistic terms were mapped to positive trapezoidal–fuzzy numbers, enabling the aggregation of experts' judgments into a cohesive analysis framework (see Table 2). The gathered data provided the foundation for an all-inclusive analysis, enabling the implementation of all eight steps of the fuzzy – trapezoidal DEMATEL method.

4.1. Assessment Cause-and-Effect Relations Between the Information Warfare Threats

Step 1. We start from aggregation of initial direct-relation matrix constructed from experts' opinions in linguistic terms on five information warfare threats dimensions: *Awareness of Resistance to Informational Threats* (A); *Information Dissemination Sources* (B); *Impact of Information Threats* (C); *Decision-Making in the Environment of Information Attacks* (D); *Strengthening Resistance to Informational Threats in LAM* (E) (see Table 3).

Table 3. Experts' opinions presented in initial direct-relation matrix

	A	B	C	D	E
A	–	HI	EH	EH	LI
B	LI	–	LI	HI	VL
C	MI	HI	–	EH	LI
D	LI	LI	LI	–	VL
E	LI	MI	LI	EH	–

Note: aggregated experts' assessments on five information warfare threats.

Step 3. Fuzzy initial direct-relationship matrix denoted as $\tilde{M}$, was constructed by computing the arithmetic average of assessments provided by the experts. This process involved collecting the individual assessments from each expert for every pair-wise comparison of factors or dimensions relevant to the analysis. Once all assessments were gathered, the arithmetic mean was calculated for each pair-wise comparison, resulting in the values of the fuzzy initial direct-relationship matrix.

Table 4. Fuzzy initial direct-relation matrix denoted as $\tilde{M}$ in this study.

	A	B	C	D	E
A	(0, 0, 0, 0)	(0.25, 0.5, 0.75, 1)	(0.5, 0.75, 1, 1)	(0.5, 0.75, 1, 1)	(0, 0, 0.25, 0.5)
B	(0, 0, 0.25, 0.5)	(0, 0, 0, 0)	(0, 0, 0.25, 0.5)	(0.25, 0.5, 0.75, 1)	(0, 0, 0, 0.25)
C	(0, 0.25, 0.5, 0.75)	(0.25, 0.5, 0.75, 1)	(0, 0, 0, 0)	(0.5, 0.75, 1, 1)	(0, 0, 0.25, 0.5)
D	(0, 0, 0.25, 0.5)	(0, 0, 0.25, 0.5)	(0, 0, 0.25, 0.5)	(0, 0, 0, 0)	(0, 0, 0, 0.25)
E	(0, 0, 0.25, 0.5)	(0, 0.25, 0.5, 0.75)	(0, 0, 0.25, 0.5)	(0.5, 0.75, 1, 1)	(0, 0, 0, 0)

This approach allowed us to aggregate the diverse judgments of the experts into a single matrix, providing a comprehensive representation of the relationships between the various factors or dimensions under consideration. The resulting fuzzy initial direct-relationship matrix served as the foundation for further analysis using the DEMATEL method, enabling us to identify and evaluate the causal relationships and influences among the factors or dimensions involved in the prepared by computing the arithmetic average of assessments (see Table 4).

Table 5. The generalized fuzzy direct-relation matrix.

	A	B	C	D	E
A	0.000	0.256	0.333	0.333	0.077
B	0.077	0.000	0.077	0.256	0.051
C	0.154	0.256	0.000	0.333	0.077
D	0.077	0.077	0.077	0.000	0.051
E	0.077	0.154	0.077	0.333	0.000

Step 4. To further this analysis, calculations were continued by generalizing the fuzzy direct-relation matrix using influence scores represented by trapezoidal fuzzy numbers: 0.125, 0.1875, 0.375, 0.625, and 0.8125. This step allowed to incorporate the fluctuating degrees of influence assigned to different factors or dimensions within the matrix. Also, must be mention that was applied equation 15 to calculate the maximum rate, which facilitated the transformation of the fuzzy initial direct-relation matrix into a normalized fuzzy directed-relation matrix (see Table 5). This normalization process ensured that the values within the matrix were scaled appropriately, allowing for a more accurate representation of the relationships between the various factors or dimensions under consideration.

Table 6. The values of total-relation matrix.

	A	B	C	D	E
A	0.194	**0.527**	**0.513**	**0.770**	0.198
B	0.158	0.138	0.182	**0.441**	0.107
C	**0.283**	**0.456**	0.194	**0.666**	0.171
D	0.135	0.179	0.156	0.174	0.092
E	0.183	**0.310**	0.211	**0.570**	0.075

Note: According the mean average the threshold number α= 0,283.

Continuing with the current research, Step 5 entailed conducting procedures to concept the generalized (overall) relation matrix, a pivotal component in the DEMATEL method. This matrix serves as a comprehensive framework for capturing and quantifying the interrelationships among the various determinants under investigation. The values resulting from these procedures were precisely documented in Table 6, providing a detailed information of the interconnectedness between the different factors.

Aligned with the primary objective of the DEMATEL method,

Step 7 delved into the fundamental task of delineating cause-and-effect relationships among the determinants. This involved the application of equation 30 to compute the sum of each row and equation 31 to calculate the sum of each column of the generalized relation matrix. By systematically analysing these computations, we were able to discern the intricate patterns of influence and dependency among the factors, shedding light on the underlying dynamics of the system. The resulting computation results were meticulously documented in Table 7, offering valuable insights into the relative importance and impact of each determinant within the overarching network.

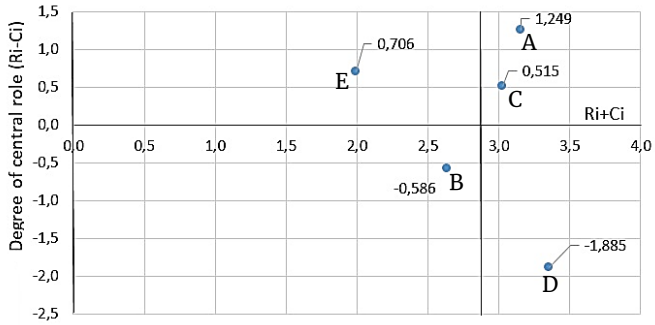
Table 7. Final psychological resilience dimensions' assessment output.

Dimension	Ri	Ci	Ri+Ci	Ri-Ci	Identity	Rank
A	2,202	0,953	3,155	1,249	Cause	1
B	1,025	1,611	2,636	-0,586	**Effect**	4
C	1,771	1,257	3,028	0,515	Cause	3
D	0,736	2,620	3,356	-1,885	**Effect**	5
E	1,350	0,643	1,993	0,706	Cause	2

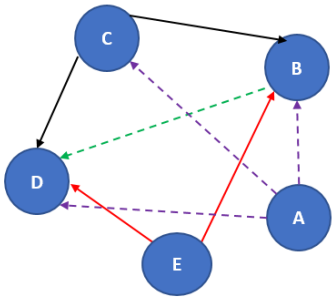
Note: Ci= sum of column values; Ri= sum of row values; (Ri+Ci) is the degree of centrality; (Ri-Ci) is the representation of causality.

Furthermore, in Step 8, our objective was to develop a comprehensive structural model that encapsulates the complex web of causal influences and relationships among the determinants. This was achieved through the creation of a cause-and-effect diagram and an influence–relation map, as illustrated in Figure 2. These visual representations serve as powerful tools for elucidating the underlying dynamics of the studied phenomena, offering a nuanced understanding of the factors at play and their respective roles within the broader context of the research domain. By visually depicting the intricate interconnections among the determinants, these models facilitate a deeper comprehension of the complex relationships that govern the system, thereby enhancing the overall effectiveness of the research analysis and interpretation.

As showed in the causal diagram in Figure 2 (a), the evaluation of Information Warfare Threats (IWT) dimensions is divided into causal criteria, including *Awareness of Resistance to Informational Threats* (A), *Strengthening Resistance to Informational Threats in LAM* (E), and *Impact of Information Threats* (C). On the other hand, the effect criteria encompass *Information Dissemination Sources* (B) and *Decision-Making in the Environment of Information Attacks* (D).



(a)



(b)

Figure 2. Graphical illustration of the structural model with five informative warfare threats (Awareness of Resistance to Informational Threats (A); Information Dissemination Sources (B); Impact of Information Threats (C); Decision-Making in the Environment of Information Attacks (D); Strengthening Resistance to Informational Threats in LAM (E)): a) a cause-and-effect diagram; A, C and E are measured to be as causal dimensions, and B and D are observed as an effect dimensions; b) influence–relation map representing connections among five informative warfare threats dimensions.

Following the afore-presented causal-and-effect diagram, one can have valuable insight into which criteria are the most significant with respect to promotion of active-duty soldiers' resistance to IWT. The (R+C) axis in Figure 2 (a) can be used to characterize the importance between this study dimensions, and (R+C) values can characterize the degree of importance in the over-all system

structure. Thus, the following five dimensions of IWT can be listed in rank order by their importance: A > E > C > B > D.

Additionally, the vertical axis (as shown in Figure 2(a)), representing the degree of centrality of each Information Warfare Threats (IWT) dimension included in this study, provides a nuanced depiction of the impact of each dimension on the overall model structure. If the (C-R) value is positive, it falls within the causal criteria group, which comprises three dimensions: *Awareness of Resistance to Informational Threats* (A), *Strengthening Resistance to Informational*

Threats in LAM (E), and *Impact of Information Threats* (C). Conversely, if the calculated causality (C-R) value is negative, it signifies an effect, and in this case, we have two dimensions: *Information Dissemination Sources* (B) and *Decision-Making in the Environment of Information Attacks* (D).

Moreover, the causal relationship analysis of centrality and causality enabled us to identify that the strongest effect of Information Warfare Threats (IWT) dimensions was manifested as a positive outcome in *Awareness of Resistance to Informational Threats* (A). Additionally, the most affected IWT dimension was *Decision-Making in the Environment of Information Attacks* (D) (see Table 7). Furthermore, in Figure 2(b), the influence–relationship map between the five informational warfare threats dimensions is illustrated. However, to accurately identify the existing relationships between study variables and avoid an overly complex map of influence-relationships, we applied a threshold value calculated as an average following previous research (Hsu et al., 2007). Thus, values greater than the threshold (α= 0.283) in the presented total-relation matrix (see Table 6) were utilized as indicators of dimensions' relationships, thereby distinguishing the influence by the identity of dimensions (see Table 7). The different-coloured lines denote the IWT dimension that affects another, and the arrows indicate which of the two constructs affects the other.

5. Discussion

The conducted study aimed to elucidate the developmental trends of soldiers' resistance to Information Warfare Threats (IWT) with the goal of enhancing the preparedness of military personnel for their active-duty service. This endeavour began with a thorough literature review to identify the primary dimensions of IWT, which are crucial for expanding psychological resilience among soldiers. Five main dimensions were selected based on their relevance to psychological resistance and their potential involvement in military training programs aimed at bolstering combat readiness.

The identified dimensions, namely Awareness of Resistance to Informational Threats (A), Information Dissemination Sources (B), Impact of Information Threats (C), Decision-Making in the Environment of Information Attacks (D), and Strengthening Resistance to Informational Threats in LAM (E), formed the foundation for the subsequent phases of the study. These dimensions were chosen to encompass the multifaceted nature of IWT, considering its implications at individual, interpersonal, and intrapersonal levels. To gather expert insights and opinions on the selected IWT criteria, ten experts were invited to participate in the study. They were provided with a pair-wise comparison questionnaire to express their judgments and assessments regarding the chosen dimensions. Given the complexity and subjective nature of IWT, linguistic terms were employed to capture the nuances of expert opinions, facilitating a more comprehensive assessment of the phenomena under study. Following the collection of expert assessments, a trapezoidal fuzzy DEMATEL analysis was conducted to predict causal relationships between the selected IWT dimensions. This analytical approach allowed for the exploration of causal dynamics and interactions among different dimensions, providing valuable insights into the underlying mechanisms driving soldiers' resistance to IWT. The modelling results were presented in two distinct formats to facilitate a comprehensive understanding of the study findings. Firstly, a cause-effect diagram was developed to clarify the significant relationships between different IWT dimensions, illustrating the causal links and dependencies among them. Secondly, an influence–relations map model of the five IWT dimensions was constructed to visualize the influence dynamics and interrelationships among these dimensions, offering further insights into the complex nature of IWT. Overall, this study contributes to the advancement of knowledge in the field of military psychology and information warfare by shedding light on the developmental trends of soldiers' resistance to IWT. The findings have implications for the design of effective training programs and strategies aimed at enhancing the psychological resilience and combat readiness of military personnel in an era of evolving information threats.

The outcomes of our study corroborate the findings of prior research, particularly in relation to the dimension of Decision-Making in the Environment of Information Attacks (D) (Russell & Abdelzaher, 2018; Gill et al.,2020; Van Den Bosch & Bronkhorst, 2018; Hansel, 2018; Egloff & Smeets, 2023). According to the literature review conducted as part of our study, Decision-Making in the Environment of Information Attacks emerged as a pivotal dimension within the realm of Information Warfare Threats (IWT). This dimension encompasses the cognitive processes and decision-making mechanisms employed by military personnel when confronted with information attacks and propaganda tactics. Our analysis reaffirmed that Decision-Making in the Environment of Information Attacks is not only a critical aspect of IWT but also exerts a significant influence on soldiers' resistance to these threats. Specifically, our findings indicate that this dimension plays a central role in shaping soldiers' individual resilience and ability to withstand the psychological impacts of information warfare tactics.

6. Conclusions

This study employed the fuzzy DEMATEL method with trapezoidal numbers to ascertain the key realization factors and assess the relationships among the chosen five Information Warfare Threats (IWT) dimensions and military resilience dimensions. Drawing from a comprehensive review of twenty-three original articles representing five IWT dimensions, was

adopted a holistic approach to investigate possible trends for military psychological resistance. This analysis revealed three dimensions – Awareness of Resistance to Informational Threats (A), Strengthening Resistance to Informational Threats in LAM (E), and Impact of Information Threats (C) – as essential causal factors influencing warriors' resistance to IWT strategies. These dimensions emerged as significant determinants shaping the ability of military personnel to withstand and counter the psychological effects of information warfare tactics. The findings of this study hold practical implications for military organizations, offering insights into key determinants that should be prioritized in the development of military preparedness programs. By focusing on these critical factors, military leaders can tailor strategies and interventions to enhance soldiers' resilience against information warfare threats effectively. Moreover, the application of the fuzzy DEMATEL method demonstrates its potential as a valuable modelling approach for assessing and promoting warriors' resistance to IWT. This methodological approach provides a systematic framework for evaluating the effectiveness of training programs and identifying areas for improvement in military resilience-building initiatives.

However, it is essential to acknowledge certain limitations of this research. Firstly, the use of pair-wise questionnaires to gather expert opinions may introduce personal bias and individual variability in the assessment process. Secondly, the study focused on only five IWT dimensions, suggesting the need for future research to explore additional factors and dimensions that may influence military resilience to information warfare threats.

Funding

This research was funded by the Ministry of National Defence of Lithuania as part of the study project Study Support Projects No VI-18, dated 2 December 2021 (2021–2024), General Jonas Žemaitis Military Academy of Lithuania, Vilnius, Lithuania. The funders contributed neither to the design of the study, nor to the compilation, analysis or clarification of data, nor to writing a manuscript or making a decision to publish the results.

References

Ajir, M., & Vailliant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory Media Ajir and Bethany Vailliant. Strategic Studies Quarterly, p.– 70. Available from: https://www.jstor.org/stable/26481910?seq=1

Bajarūnas, E., & Keršanskas, V. (2018). Hybrid threats: analysis of content, challenges posed and measures to overcome. Lithuanian Annual Strategic Review., 16(2017-2018), 123-170.

Bekesiene, S., et al. (2021). Military Leader Behavior Formation for Sustainable Country Security. Sustainability., 13, 4521. https://doi.org/10.3390/su13084521

Blay, K. B., Yeomans, S., Demian, P., & Murguia, D. (2020). The Information Resilience Framework. Journal of Data and Information Quality, 12(3). https://doi.org/10.1145/3388786

Bokša, M. (2022). Russian Information Warfare in Central and Eastern Europe: Strategies, impact, countermeasures. German Marshall Fund of the United States.

Chen-Yi, H., Ke-Ting, C., & Gwo-Hshiung, T. (2007). FMCDM with Fuzzy DEMATEL Approach for Customers' Choice Behavior Model. International Journal of Fuzzy Systems, 9(4).

Egloff, F. J., & Smeets, M. (2023). Publicly attributing cyber attacks: a framework. Journal of Strategic Studies, 46(3), 502-533.

Fridman, O. (2018). Russian "Hybrid Warfare." Russian "Hybrid Warfare," September. p. – 16. https://doi.org/10.1093/oso/9780190877378.001.0001

Firinci, Y.(2020). "Countering Psychological Operations and Deceptions That Indoctrinate AntiIslam Hate and Violence". International Journal of Politics and Security, p.94-126.

Gill, P., Marchment, Z., Corner, E., & Bouhana, N. (2020). Terrorist decision making in the context of risk, attack planning, and attack commission. Studies in Conflict & Terrorism, 43(2), 145-160.

Hansel, M. (2018). Cyber-attacks and psychological IR perspectives: explaining misperceptions and escalation risks. Journal of International Relations and Development, 21, 523-551.

Yazdi, M., Khan, F., Abbassi, R., & Rusli, R. (2020). Improved DEMATEL methodology for effective safety management decision-making. *Safety science*, 127, 104705. https://doi.org/10.1016/j.ssci.2020.104705

Joyner, C. C., & Lotrionte, C. (2017). Information warfare as international coercion: Elements of a legal framework. In The Use of Force in International Law (pp. 433-473). Routledge.

Johnson, R. (2017). Evolution of Hybrid Threats through History. In Shifting Paradigm of War: Hybrid Warfare. Istanbul: Turkish National Defence Academy, p. 3. Available from: https://msu.edu.tr/eng/Documents/Hybrid%20Warfare.pdf

McGeehan, T. P. (2018). Countering Russian Disinformation. The US Army War College Quarterly: Parameters, 48(1), 7.

Prier, J. (2020). Commanding the trend: Social media as

information warfare. In Information warfare in the age of cyber conflict (pp. 88-113). Routledge.;

Polyakova, A., & Boyer, S. P. (2018). The future of political warfare: Russia, the West, and the coming age of global digital competition. Europe.; Whyte, C. (2020). Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare. Journal of Cybersecurity, 6(1), tyaa013.

Russell, S., & Abdelzaher, T. (2018, October). The internet of battlefield things: the next generation of command, control, communications and intelligence (C3I) decision-making. In MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM) (pp. 737-742). IEEE

Śliwa, Z., & Antczak, A. (2018). Military Domain as a Component of Information Warfare. Kaitseväe Akadeemia, 16-17. Available from https://www.baltdefcol.org/files/files/publications/zapad.pdf

.Theohary, C. A. (2018). Information Warfare: Issues for Congress. Information Warfare, p. 2–19. Available from: http://files/218/Theohary

Thomas, T. (2014). Russia's information warfare strategy: Can the nation cope in future conflicts? The Journal of Slavic Military Studies, 27(1):101–130. Available from: https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/281830

Vaišnys, A. (2016). Rusijos propagandos praktika daro įtaką teoriniam komunikacijos modeliui. Žiniasklaida ir komunikacija. Informacijos mokslai, p. 14. Available from: https://epublications.vu.lt/object/elaba:20308260/

Vaišnys, A., Kasčiūnas, L., Jastramskis, M. ir kt. (2017). Rusijos propaganda: analizė, įvertinimas, rekomendacijos. Monografija. Vilnius. p. 5 -45. Available from: https://www.eesc.lt/uploads/news/id987/RESC%20monografija_propaganda.pdf

Van Den Bosch, K., & Bronkhorst, A. (2018, June). Human-AI cooperation to benefit military decision making. NATO. Available from: https://www.karelvandenbosch.nl/documents/2018_Bosch_etal_NATO-IST160_Human-AI_Cooperation_in_Military_Decision_Making.pdf

Zachary, D., Gac, F., Rager, C., Reiner, P., & Snow, J. (2021). Strategic Latency Unleashed - The role of technology in a revisionist global order and the implications for special operations forces. Center for Global Security Research Lawrence Livermore National Laboratory, p. 101. Available from: https://www.osti.gov/servlets/purl/1782516

Žilinskas, R. (2017).Valstybės atsparumas išorinėms hibridinio pobūdžio grėsmėms: hipotetinis modelis. Politologija, Nr. 3 (87), Vilnius. p. 45.