Received 20 February 2024, accepted 1 March 2024, date of publication 4 March 2024, date of current version 8 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3373710

RESEARCH ARTICLE

Interoperable Defensive Strategies of Network Security Evaluation

ALA ABDULSALAM ALAROOD[1] **AND AHMED OMAR ALZAHRANI**[2]

[1]College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia
[2]Faculty of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia

Corresponding author: Ala Abdulsalam Alarood (aasoleman@uj.edu.sa)

This work was supported by the Deputyship for Research & Innovation, Ministry of Education, Saudi Arabia, under Project MoE-IF-UJ-22-4220746-2.

ABSTRACT To advance defense interoperability, foster productive collaboration, and enhance the capabilities of defense systems to respond to evolving threats, it is imperative to tackle the challenges of defensive strategic issues in Network security. That is why an experimental study was done to assess the application of the interoperability defense theory to an operational target network system. The study used five strategies, including ''Risk,'' ''Complexity,''Dependency,'' ''Personnel,'' and ''Environment,'' and employed DEMATEL and performance analysis evaluation. These five defense techniques to interoperability are conceptualized. The experimental results revealed that network defense, instead of being consistently passive, is the recipient of influence in an interoperable defensive system. Interoperability protective strategies have varying degrees of influence on network security evaluations. A significant relationship was observed between the level of technological complexity and the ability to tolerate its significant effects. Within the complexity group, further analysis showed a noteworthy reduction in ''Risk''. However, there were no significant variations in '' Environment'' before and after the interoperable implementation. Finally, the DEMATEL analysis indicates that the entire variables are effect criteria no cause criteria. Given that all criteria are categorized as ''effect'' and none as ''cause,'' it suggests a scenario in which each criterion is interconnected and influenced by other criteria within the system, but none of them serve as direct influencers or causes. Therefore, this study contributes to the evaluation of interoperability in strategic network security defense.

INDEX TERMS Network security, interoperable defense, interoperable complexity, defensive strategies.

I. INTRODUCTION

The current estimate for the worldwide defense communication system market in the year 2023 is approximately US$ 46.7 billion. The Department of Defense (DoD) is currently engaged in developing advanced communication capabilities for warfare, such as the Transformational Satellite Communications System (TSAT), the Joint Tactical Radio System (JTRS), and the Defense Information Systems Network-Next Generation (DISN-NG) [1]. These programs have the objective of bolstering the Department of Defense's capacity to exchange information, strengthen command and control, and revolutionize DoD operations. Furthermore, the compact dimensions, uncomplicated structure, and reduced expenses of digital switching systems are crucial attributes for military requirements [2]. There is a current transformation happening in the global telecommunications system, where Europe, India, and China are projected to achieve technological parity with the United States in the next decade [3]. The Department of Defense (DoD) is a major global consumer of communications, and the Defense Communications Agency (DCA) is actively striving to provide swift, dependable, and secure information transmission at a reasonable cost [4].

Studying defense interoperability has profound consequences for national security, global cooperation, and the efficiency of defense systems. Interoperability is essential

The associate editor coordinating the review of this manuscript and approving it for publication was Claudio Zunino.

in net-centric warfare for accomplishing mission objectives and for determining cost estimates and risk management assessments of intricate Department of Defense (DoD) programs [5], [6]. Furthermore, it is crucial for achieving multilateral command and control interoperability, as it facilitates cooperation among defense businesses from different nations and entry into global defense industry markets [7]. Utilizing interoperability as a criterion for assessing system-of-systems designs can furnish decision-makers with insights into the interoperability of a prospective architecture when choosing a new military system-of-systems [8]. In addition, enhancing the compatibility of interconnected systems is essential for network-centric operations, and the utilization of approaches to assess interoperability can enhance the overall compatibility of networks [9].

Research in defense interoperability is crucial for bolstering national security. Seamless communication and collaboration among defense systems enable faster and more effective responses to emerging threats, contributing to overall national defense capabilities [10]. The use of context-aware environmental monitoring systems in tactical edge networks can help guarantee system performance and interoperability in dynamic battlefield conditions [11]. Additionally, the optimization of large-scale heterogeneous combat networks can improve the ability of combat system-of-systems to work in complex battlefield environments [12]. Furthermore, the development of a dynamic context-aware security model in tactical networks can ensure data security and reduce communication overhead in varying network conditions [13]. Lastly, the integration of disparate security data sources into a unified cyber threat defense exchange platform can enhance the coordination and performance of security actions across networked computing devices [14].

This research has established that the integration of diverse defense systems for interoperability may introduce new security concerns and vulnerabilities. Cybersecurity risks, including the potential for unauthorized access and data breaches, could escalate during the implementation of interoperable solutions. The complexity of integrating various technologies within defense systems may lead to interoperability challenges. Incompatibility issues between different systems and difficulties in achieving seamless communication could arise, hindering the effectiveness of the interoperable network

Similarly, Inconsistent communication protocols and standards can hinder the exchange of information between different defense components. A lack of standardized communication may lead to misinterpretation and delays. Ensuring secure communication while maintaining interoperability is a challenge. Balancing the need for robust security measures with the imperative of information sharing is critical. The effectiveness of defense interoperability is influenced by the ability of personnel to understand and use the interoperable systems. Therefore, the main objective of this study is to establish a strategic network security defense interoperability technique. Since interoperability often requires alignment with policies and governance structures across different defense entities, inconsistent policies and governance models can impede collaboration. That is the justification of this research

The main outcomes of research dwells on defense interoperability development standards, this outcome collectively contribute to strengthening the overall capabilities and effectiveness of defense systems in a collaborative and interconnected world. As a result, this study contributes in the following ways:

- The research provides a comprehensive analysis of Interoperable Defensive Strategies and reveals a network of interrelated criteria (“Risk,” “Complexity,” “Dependency,” “Personnel,” and “Environment,”,) each impacting and reacting to modifications in the system. This complex interdependency suggests that no single criterion operates as a direct cause, but rather all are classified as “effects” influenced by other factors. This intricate web of relationships underscores the need for a comprehensive approach that acknowledges and values the interconnectedness of these criteria. This means that the key contribution here lies with recognizing all the criteria as the components to effectively address the specific defensive strategies of Network security requirements.
- The research contributes in highlighting that all interrelated criteria (“Risk,” “Complexity,” “Dependency,” “Personnel,” and “Environment,”,) are defensive component of Network security requirements
- The research outcomes contribute to the development of policy frameworks and governance structures that support defense interoperability. This could involve recommendations for aligning national and international policies, addressing legal considerations, and fostering collaboration between defense entities.
- The research also contributes in understanding that defense interoperability is expected to lead to the establishment of standardized protocols and interoperability frameworks. These standards would facilitate seamless communication and collaboration among diverse defense systems, both nationally and internationally.
- This research outcome may contribute to the development of improved decision-support systems that leverage interoperable data for enhanced situational awareness. This could result in tools and technologies that aid decision-makers in making informed and timely choices during defense operations.

The remaining sections of the paper are organized as follows: Section II discusses related work, providing context and background information. Sections III, IV, and V detail the methodology employed in the study, outlining the approach taken to address the research objectives. Finally, Sections VI and VII present the conclusions drawn from the study’s findings, summarizing key insights and implications for future research or practice.

II. RELATED WORK

Researchers engaging in the study of strategic network security defense interoperability evaluation can draw insights and build upon these related works to contribute to the advancement of knowledge in this critical field.

The Decision Making Trial and Evaluation Laboratory (DEMATEL) method is used to analyze the causal relationship between attack and defense strategies in a network system [15]. It constructs a matrix of ''expertise'' to calculate the effect of these strategies and assess their overall impact on the target network system. The method considers various attack strategies such as malicious code attack and denial of service attack, as well as defensive strategies like Web services security strategy defense and code reconstruction defense [16]. Another method for evaluating defense effectiveness in a network target range involves quantifying defense effects and objectively evaluating defense effectiveness based on the severity of potential attack risks and the response of defense equipment [17]. A dynamic Bayesian attack graph is proposed to quantify the effectiveness of cyber deception in a complex network environment, allowing for the formulation of optimal deception strategies [18]. A simulation platform-based method evaluates the performance of network attack and defense tools by considering efficiency indexes such as information acquisition capability and confrontation capability [19]. An attack and defense evaluation method automatically generates dynamic flags to judge the success of attack and defense actions in a network security context.

Deception based information security is a promising solution to enhance established defense mechanisms in network security [20]. A new model of computer network security, combining active and passive defense systems, has been proposed to improve security defense efficiency [21]. The key issues of campus network security prevention have been analyzed, and a campus network security system has been designed [22]. A security defense evaluation method based on the traffic of devices has been proposed to quantitatively evaluate the effectiveness of the defense system [23]. A dynamic classification network security defense strategy model has been proposed to address the limitations of static defense and adapt to dynamic changes in the security situation of complex computer networks [24].

Zhaofang [21] proposes a network security model based on an active and passive defense hybrid strategy. The study uses an advanced technical support platform and network security model to combine the active and passive defense systems. The effectiveness of the proposed defense model is evaluated through experiments, which show improved security defense efficiency and effective defense rate compared to the traditional PDRR security model. The experimental results support the claims of enhanced security defense efficiency and effective defense rate compared to the traditional security model.

Yunmin et al. [25] proposes a Double Defense strategy with Endogenous Safety and Security (DDESS) based on multi-identifier network (MIN) architecture, inspired by the establishment of multiple lines of defense in immunology. DDESS adopts a zero-trust network approach with identity authentication as the core for access control, solving security problems of traditional IP networks. It achieves individual static security defense through encryption and decryption, consortium blockchain, trusted computing whitelist, and remote attestation strategies.

Daniel et al. [20] proposes transferring strategic security and defense concepts from operations research, reliability engineering, and game theory to deception-based information security mechanisms. The research reveals that network security implications are analyzed in defender and attacker perspectives.

Ningbin et al. [26] proposed a defense graph model to assess the network information system and show attack and defense strategies and their cost. The defense graph was mapped to the attack and defense game model to provide a basis for active defense policy decision. Thereafter, a generation algorithm of defense graph was proposed to efficiently create the defense graph model.

Strategic network security defense involves the implementation of measures to protect network systems from cyber threats and attacks. It is important to have a comprehensive understanding of the security threat situation and utilize both active and passive defense systems [27]. Active defense systems can automatically generate defense strategies based on threat information, while passive defense systems provide a deep network defense system [28]. Additionally, a double defense strategy with endogenous safety and security (DDESS) can be employed, which combines identity authentication, encryption and decryption, consortium blockchain, trusted computing whitelist, and remote attestation strategies [21]. This strategy aims to achieve individual static security defense and active herd defense of network security [25]. Furthermore, network security protection strategies should be developed to standardize network security protection and ensure the normal use of the network [29]. These strategies should include preparation in advance, defense in the event, and response after the event.

The aims of this review is to explore how collaboration and communication capabilities of defense systems are discussed in the research domain. While this area of study is crucial for national security, several research gaps exist, representing opportunities for further exploration and development. One prominent research gap lies in understanding the nuanced interplay between security concerns and cybersecurity risks within interoperable defense systems. Current literature provides insights into general challenges, but there is a need for in-depth analyses of specific vulnerabilities introduced during the integration process. Unraveling the complexities of potential cyber threats and devising robust strategies to mitigate these risks remain unexplored areas. The gap in research on technological complexity and interoperability issues centers on the need for comprehensive frameworks that address the integration challenges posed by diverse defense technologies. Existing studies touch upon the general complexities but fall short in offering specific methodologies for overcoming technological hurdles. A deeper exploration is required to devise standardized protocols and solutions adaptable to the evolving defense landscape.

Addressing these gaps will contribute to a more robust and comprehensive understanding of defense interoperability, ultimately enhancing the effectiveness and resilience of defense systems in the face of evolving threats.

III. INTEROPERABLE DEFENSIVE STRATEGIES

The attainment of interoperable defensive strategies among different security components in a network can be accomplished by employing many aspect of defense approaches. Interoperable defensive techniques signify a fundamental change in how enterprises approach network security. The interaction among many security factors forms a unified and flexible defense system that can effectively handle the challenges of the current threat environment. By adopting interoperability, enterprises are creating a foundation for a stronger, more cooperative, and environmentally aware approach to network security. This ensures the protection of important digital assets in a world where everything is connected [30]. These approaches entail the amalgamation and synchronization of several security systems and domains to bolster network security as a whole and attain a collaborative defense outcome [31]. To enhance defense against unauthorized intrusions, security systems can implement a service-oriented cooperative defense model by deploying security nodes, security domain agents, and a service center. This approach enables the adoption of a unified transmission method, resulting in more efficient protection [32]. In a trusted domain environment, the incorporation of defensive mechanisms inside and between domains enables the exchange of defensive information and the effective identification and elimination of recurring incursions [33]. These compatible defensive methods serve as a foundation for making decisions on active defense policies and can be correlated with models of attack and defense in games [34].

A. THE DATA POINTS FROM THE VARIABLE

Every aspect within the global defense communication system market poses distinct issues that necessitate sophisticated and all-encompassing solutions. To effectively deal with security concerns, technological difficulties, budget limits, ethical considerations, and environmental implications, it is necessary for stakeholders in the military sector to work together strategically and collaboratively. The proposed solutions for each variable are designed to promote a robust and enduring defense. Figure 1 illustrates the five dimensions linked to 'Interoperable defensive techniques' as conceptualized in this study. The explanation of each dimension is included in subsections I to V below:

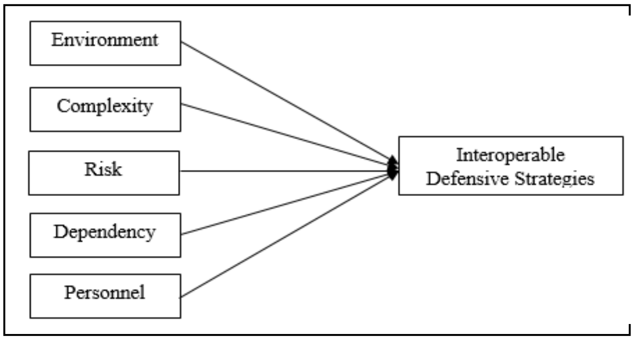

FIGURE 1. The interoperable defensive strategies.

1) SECURITY CONCERNS AND CYBERSECURITY RISKS (S1)

Security problems and cybersecurity risks are the most significant challenges in the field of defense communication systems [35]. The consequences are significant, encompassing unlawful entry into vital data and the potential for advanced cyber-attacks impeding military activities. Addressing S1 necessitates a multi-faceted approach. This research conceptualized that Interoperable defensive techniques in cybersecurity are essential to Network system because of the escalating security concerns and risks linked to cyber threats. Conventional defense strategies frequently prove inadequate when faced with novel forms of coordinated and sophisticated network attack [35].

Dynamic defense mechanisms, such as moving target defense and mimic defense, offer innovative approaches to counteracting the imbalanced nature of defense and attack in the realm of cyberspace [36], [37]. To evaluate security threats in cyber-physical systems, as part of the interoperable defensive system, it is necessary to explicitly analyze the network system and the impact of both technology-based defenses and the institutions that support them [38]. This study was able to extract 10 items under "Security Concerns and Cybersecurity Risks (S1)" that could lead to interoperable defensive strategies as presented in Table 1.

TABLE 1. IITEMS of security concerns and cybersecurity risks.

#	Categories of Security Concerns and Cybersecurity Risks (S1)
1	Total Number of Identified Cybersecurity Threats
2	Percentage of Threats with Potential for Data Breach
3	Average Time to Detect a Cybersecurity Incident
4	Percentage of Detected Incidents Resulting in Data Loss
5	Number of Cybersecurity Experts in the Defense System
6	Percentage of Budget Allocated to Cybersecurity Measures
7	Level of Cybersecurity Awareness Among Personnel
8	Number of Simulated Cybersecurity Drills Conducted Annually
9	Average Time to Patch Vulnerabilities After Identification
10	Level of Collaboration with External Cybersecurity Agencies

2) TECHNOLOGICAL COMPLEXITY AND INTEROPERABILITY ISSUES (S2)

As technological advancements surge, the integration of sophisticated features brings both advantages and intricacies. The challenge lies in ensuring that diverse technological components work seamlessly together, allowing for effective communication and collaboration across the defense landscape.

This research conceptualized "Technological complexity" associated to interoperability pose challenges for the implementation of interoperable defensive methods [39], [40]. The justification of this lies with the growing intricacy of systems and the diverse array of systems involved in information exchange provide substantial challenges [41]. Assessing the level of interoperability that may be attained is essential, and it involves analyzing, expressing, and quantifying interoperability [42]. The capacity for systems to work together and exchange information effectively relies on both the technical framework and the alignment of the meaning and structure of the underlying systems [43]. Nevertheless, the Non Polynomial complete character of interoperability poses a challenge as there are now no formal theories or computer programs capable of solving it [44].

According to the conceptual design propose for this study, interoperability solutions items associated to Technological Complexity and Interoperability Issues (S2) are proposed and presented in Table 2, which are extremely important when it comes to tackling compatibility issues that arise in complicated systems and training systems. The importance of carefully examining this component is brought to light by this. For the purpose of ensuring the safety and dependability of data sharing within an appropriate electronic system, the implementation of efficient identity management systems is very necessary. Consequently, the findings of this study offer evidence that evaluating this element may lead to the development of defense systems that are compatible with one another.

TABLE 2. ITEMS of technological complexity and interoperability issues.

#	Categories of Technological Complexity and Interoperability Issues (S2)
1	Number of Different Technologies Used in the Defense System
2	Percentage of Technologies That Require Proprietary Protocols
3	Average Time to Achieve Interoperability Between Different Systems
4	Number of Interoperability Standards Currently Implemented
5	Percentage of Defense Systems Using Legacy Technologies
6	Average Cost Overruns Due to Technological Integration Challenges
7	Number of Successful Interoperability Implementations in the Past Year
8	Level of Satisfaction Among Defense Personnel Regarding Interoperability
9	Percentage of Technologies Ready for Seamless Cloud Integration
10	Number of Cross-Domain Interoperability Challenges Encountered

3) DEPENDENCY ON COMMERCIAL TECHNOLOGIES AND COST CHALLENGES (S3)

When it comes to the development of technology for the future battlefield, the defense industry is becoming increasingly reliant on business partnerships with private sector [45]. The difficulties associated with independently safeguarding essential technologies can be somewhat alleviated through the implementation of international technology cooperation in the defense sector [46]. Nevertheless, there are limitations in terms of both time and money that need to be taken into consideration [47]. There is a need to find a way to overcome the transaction costs that are associated with Joint Service System-of-Systems (SoS) programs [48]. These programs offer prospects for better warfighting capabilities and efficiencies. It is possible for economic reasoning to be overshadowed by security concerns and politics in the defense industry when it comes to procurement decisions, which can limit the utilization of supply chains and manufacturing centers that are more cost-effective [49]. Although the Strategic Defense Initiative (SDA) is confronted with obstacles, it also presents opportunities for cost reductions and technology spinoffs.

This research established that assessing reliance on commercial technologies and the financial difficulties related to implementing compatible defensive solutions requires a comprehensive approach. This process combines qualitative assessments and quantitative measurements to measure dependence, and determine the effectiveness of these techniques in strengthening cybersecurity defenses. An extensive examination empowers firms to make well-informed choices, achieve a harmonious equilibrium between security and cost-effectiveness, and strengthen their ability to withstand cyber threats in a constantly changing environment. That is why, items associated to dependency on commercial technologies and cost challenges (S3) are conceptualized to measure the interoperability solutions of defensive strategies, and presented them in Table 3.

4) ETHICAL, LEGAL, AND HUMAN FACTOR CHALLENGES (S4)

This research has established that Interoperable defensive techniques encounter ethical, legal, and human aspect obstacles. Organizations face challenges in incorporating human factors into their multi-layered defense systems, which hinders the establishment of strong human defenses [50]. Deep neural networks (DNNs) are susceptible to adversarial examples, and current defenses are limited to addressing particular attacks, which presents a significant challenge [51], [52]. Assessing the effectiveness of security measures that are easy

TABLE 3. ITEMS OF dependency on commercial technologies and cost challenges.

#	Categories of Dependency on Commercial Technologies and Cost Challenges (S3)
1	Percentage of Defense Systems Using Commercial Off-the-Shelf (COTS) Products
2	Average Annual Expenditure on Commercial Technologies
3	Number of Commercial Technology Vendors with Significant Market Share
4	Percentage Increase in Annual Expenditure on Commercial Technologies
5	Average Cost Overruns in Defense Projects Due to Commercial Dependencies
6	Number of Collaborative Agreements with Commercial Technology Providers
7	Percentage of Defense Budget Allocated to Technology Acquisition
8	Level of Vendor Lock-in Concerns Among Defense Personnel
9	Average Time Required to Adapt Defense Systems to New Commercial Technologies
10	Number of Cost-Efficiency Initiatives Implemented in the Past Year

to use, such as anti-phishing defenses, necessitates users to behave in a normal manner without being overly cautious, which poses ethical and operational difficulties [53].

This research has established that it is necessary to have a thorough approach in order to evaluate the ethical, legal, and human challenges that are involved in the deployment of interoperable defensive techniques. It was conceptualized that during the process, ethical frameworks, legal evaluations, behavioral analysis, and effect measurement approaches are utilized in order to acquire a comprehensive understanding of the complex challenges that are associated with cybersecurity, as well as to address and manage these challenges. In a digital environment that is becoming increasingly interconnected, an exhaustive review makes it easier to devise strategies that not only increase safeguards but also assure ethical conformity, legal compliance, and security measures that are centered on the requirements of users [54]. For this reason, items associated to ethical, legal, and human factors, as shown in Table 4, are conceptualized in order to measure the interoperability solutions of defensive strategies.

TABLE 4. Items of ethical, legal, and human factor challenges.

#	Categories of Ethical, Legal, and Human Factor Challenges (S4)
1	Number of Reported Ethical Dilemmas in Defense Interoperability
2	Percentage of Personnel Requiring Additional Ethical Training
3	Average Time Spent Resolving Ethical Concerns
4	Number of Legal Compliance Issues Identified
5	Percentage Increase in Legal Compliance Training
6	Level of Employee Satisfaction with Ethical Practices
7	Number of Human-Related Errors Causing Interoperability Issues
8	Percentage of Personnel Open to Adopting New Technologies
9	Number of Lawsuits Related to Human Factors in the Past Year
10	Average Time Devoted to Human Factors Training Annually

5) STRATEGIC IMPLICATIONS AND ENVIRONMENTAL IMPACT (S5)

Interoperable defensive measures possess strategic ramifications and environmental consequences. Employing defensive behavior facilitates cooperation and can result in the enduring coexistence of cooperation and defection [55]. Gaining a comprehensive understanding of the strategic environment is of utmost importance for the establishment and operation of the defense system [56]. The environmental impacts of battle, whether deliberate or accidental, are enduring and encompass the devastation of infrastructure, oil fields, and the release of garbage [57]. The interconnections between infrastructures have an impact on the level of defense required to counter external attacks. diverse structural arrangements have diverse effects on defense methods [58]. Choosing to remain in an abusive relationship as a defensive strategy demonstrates an underlying belief that one has control over their own circumstances and serves to maintain the existing state of affairs [59]. It is crucial to take into account the strategic implications and environmental consequences of implementing interoperable defensive methods in order to effectively prepare for defense and allocate resources.

This research has conceptualized that Interoperable defensive methods have strategic ramifications that go beyond immediate security issues. Establishing collaborative alliances across various defense systems enables the exchange of intelligence and synchronized actions in

TABLE 5. Items of strategic implications and environmental impact.

#	Categories of Strategic Implications and Environmental Impact (S5)
1	Number of Strategic Collaborations Facilitated by Interoperability
2	Percentage Increase in Defense Capabilities Due to Collaboration
3	Average Time to Form New Strategic Alliances
4	Number of Environmental Impact Assessments Conducted
5	Percentage Reduction in Carbon Footprint Through Technology Adoption
6	Level of International Cooperation in Defense Strategies
7	Number of Strategic Disputes Resolved Through Collaborative Efforts
8	Percentage Increase in Defense Budget Allocated to Environmental Measures
9	Average Time Required for Environmental Compliance in Defense Projects
10	Number of Environmental Awards Received for Sustainable Practices

response to cyber-attacks. That organizations can strategically position themselves for collective defense by adopting interoperability, which allows them to utilize capabilities and skills from different sources. By adopting this collaborative strategy, not only is the entire defense posture improved, but strategic ties within the cybersecurity community are also fortified. That is why the research conceptualized items associated to strategic implications and environmental impact (see Table 5) in order to measure the interoperability solutions of defensive strategies.

IV. METHODOLOGY

In this essay, we will utilize the Decision Making Trial and Evaluation Laboratory (DEMATEL) technique with data to analyze the interdependencies among key challenges: ''Security Concerns and Cybersecurity Risks (S1)'', ''Technological Complexity and Interoperability Issues (S2)'', ''Dependency on Commercial Technologies and Cost Challenges (S3)'', ''Ethical, Legal, and Human Factor Challenges (S4)'', ''Strategic Implications and Environmental Impact (S5)''. The DEMATEL technique allows the research to understand the direct and indirect relationships among these challenges and evaluate their overall impact. The relationships were assumed to be reciprocal, indicating that each factor impacts and is impacted by the others.

Another justification for determine a key criterion among variety of interoperable defensive strategies of network security evaluation lies with the fact that, cybersecurity is undergoing a revolution as a result of the integration of many technical breakthroughs, with the primary focus being on the enhancement of defense mechanisms against evolving threats [60]. At the forefront of the field is radio frequency fingerprinting, a unique authentication system that does away with the requirement of passwords [61]. The introduction of RF fingerprinting that is based on deep learning promises to provide superior security measures, in contrast to the existing approaches that stand in comparison. Similarly, security vulnerabilities can result from altering Differentiated Services Code Point (DSCP) settings, thereby compromising data integrity and causing network performance degradation, this rest on some many dimension [62]. At the same time, the fight against eavesdropping is becoming more intense, which has led to the creation of realistic threat models and complex defense measures [63]. One such innovation is the invention of a construction known as physical intra-class universal adversarial perturbation (IC-UAP), which is specifically designed for wireless signal classifiers that are based on deep learning capabilities. This method develops powerful attacks against certain class samples by optimizing perturbations under random shifting. This strengthens the system's resilience against threats that use eavesdropping from other sources [64]. These improvements are examples of the proactive strategy that organizations take to strengthen their cybersecurity, as they attempt to maintain a competitive advantage in a threat landscape that is constantly shifting [65].

A. DEMATEL EVALUATION

Examining the complex interrelationships that exist between the various components that make up a system is the purpose of the DEMATEL approach [15]. When trying to understand the causal connections that exist between the various components that make up a system, it is commonly applied in fields including as management, engineering, and the social sciences. At the same time that it is used to analyze interoperable defensive strategies, DEMATEL can be utilized to evaluate the interconnections that exist between various methods, elements, or components in network security.

DEMETEL is adopted in this study because, Interoperable defensive strategies are characterized by a synergistic relationship between the variables that are central to the concept. These variables include security concerns and cybersecurity risks (S1), technological complexity and interoperability issues (S2), dependency on commercial technologies and cost challenges (S3), ethical, legal, and human factor challenges (S4), and strategic implications and environmental impact (S5). On account of the interaction between these elements, it is necessary to take a holistic and interconnected approach to the protection of networks.

1) SAMPLE EXPERTS PROFILE

When analyzing interoperable defensive measures for network security using DEMATEL, the anticipated experts may include the distribution of specialists in different categories and their length of service in order to offers valuable insights into the wide range of knowledge, experience, and views that may be utilized for evaluating and implementing effective defensive techniques in network security. According to Tarei et al. [66], the number of sample experts should be between five and ten. This is because responses from more than ten experts could potentially lead to a high degree of inconsistency, which would render the results unreliable. For DEMATEL, there is no such thing as a sample quantity. According to Tarei et al. [60], the experts are considered to be individuals who have approximately 80% of their experience in the industry and 20% of their experience in academia if there are from Industry and vice versa. For this reason, ten experts who are associated with Network Security and Cybersecurity have been chosen for the DEMATEL evaluation (see table 5).

The cumulative count of experts in the sample for this study is 10 (see Table 5), with Cybersecurity Analysts constituting

TABLE 6. The profile of the expert.

No of Expert	Title / Organization	Duration of Service
5	Network Security Engineer / Provide and Public sector	7 - 26
3	Cybersecurity Analysts / Provide and Public sector	11 - 21
2	Network Security Professors / Universities	17 - 32

the largest cohort (5), trailed by Network Security Engineers (3) and Network Security Professors (2). The specialists are separated into two groups: professionals in the business and public sectors, such as engineers and analysts, and those in academic institutions, such as professors. This distribution entails a combination of professionals from the industry and scholars with expertise in network security making contributions to the topic. The length of service varies among different groups, reflecting a range of expertise levels and backgrounds of these specialists contribute to a more comprehensive assessment of network security solutions utilizing DEMATEL, as they offer diverse viewpoints

2) DEMATEL PROCEDURE STEPS

The initiation of DEMATEL entails several crucial stages for the analysis of interrelationships among variables inside a system or problem. The approach is employed through the following sequential steps:

First Step. Developing approaches for acquiring expert insight: This study employs a table of collection of security incidence (Table 1 to Table 5) on each of the five dimensions conceptualized. Each dimension was accompanied by multiple choice options that are scored using a Likert scale.: 0 = "No Influence", 1 = "Low Influence", 2 = "Medium Influence", 3 = "Extreme Influence", and 4 = "High Influence". A total of ten expert selected were asked to score the criteria based on the items that made up each criterion, with the goal of assessing Interoperable Defensive Strategies. The expert's perceptions on the influence of each criterion are thus symbolized by their relevance. $x_{i,j}$ where i and j result into the cause and effect criteria respectively. Thus for each expert's response is obtained as $n = 1,2, 3\ldots, n$ and an $n\times n$ non-negative direct relation matrix is form by equation 1:

$$x^y = [x_{ij}^y]_{n\times n} \tag{1}$$

where $y$is the number of responses of each participant with1 $\leq y\leq q$ this generate matrix q for $x^1,\ x^2,\ldots x^q$ where q is the number of participants. The average aggregated decision matrix for all the participants Z =[z_{ij}]is presented by equation 2:

$$z_{ij=1/q\sum x_{ij}^y} \tag{2}$$

Second Step: This stage involves normalizing the direct relation matrix, which includes the use of Equation 3 to determine the normalized direct relations matrix D [67], which is as follows:

$$\mathrm{D} = \max[1/\max_{1\leq y\leq n}\textstyle\sum m_{ij} 1/\max_{1\leq y\leq n}\textstyle\sum m_{ij}] \\ \textit{from n to } j = 1_{,} \textit{ and from n to } i = 1] \tag{3}$$

The outcome will be that each element in matrix Z will possess a value within the range of [0, 1].

Third Step: The total relation matrix, denoted as T, is generated by raising the normalized initial direct-relation matrix, D, to the power of m. Here, m represents the indirect influence, D^{m}, which accounts for the length and extent of the influence in the relation matrix. The total relation matrix, T, is obtained by summing up D, D2, and so on, until D^{∞}, which converges to a zero matrix. Therefore, the equation for T is given by T = lim $(D{+}D^1{+}D^2{+}D^3{+}\ldots{+}D^m)$ as *m approach infinity* = $(1\text{-}D)^{-1}$ thus

$$\mathrm{T} = \mathrm{D}(1 - D)^{-1} \tag{4}$$

where I is an $n\times n$ identity matrix [68].

Fourth Step 4: Creating the rows and columns of a matrix: The matrix vectors of the complete relation matrix are organized in rows and columns. If the total of the rows and the total of the columns of matrix T are denoted by vectors r and c, respectively [69], then

$$\mathrm{r} = [r_i]_{n\times 1} = \left[\sum t_{ij}\right]_{n\times 1} \quad \textit{from n to } j = 1 \tag{5}$$

$$\mathrm{c} = [c_j]_{1\times n} {=} \left[\sum t_{ij}\right]_{1\times n} \quad \textit{from n to } j = 1 \tag{6}$$

The sum of ri and cj represents the impact of criteria i on j. If j = i, the sum indicates the overall effects received and given by criteria i, while the difference reflects the net contribution of criteria i to the system. When criteria i is positive, it acts as a net cause. Conversely, when criteria i is negative, it functions as a net effect. Therefore, the sum of r and c is referred to as the "Prominence," while the difference between r and c is known as the "Relation." If the result of rj - cj is positive, it indicates that the criteria has a significant influence on the other criteria and can be classified as a cause. On the other hand, if rj - cj is negative, it suggests that the criteria in question are being influenced by the other criteria as a whole and should be categorized as an effect.

The term "Prominence" is used to refer to the first part, whereas "Relation" is the term used for the second part.

Fifth Step: Specify a threshold value (α) in order to create an interaction diagram. The cutoff point is determined using equation 7.

$$\alpha = \sum\nolimits_{\mathrm{i}=1} \sum\nolimits_{\mathrm{j}=1} \mathrm{t}_{\mathrm{ij}}/\mathrm{N} \\ \textit{from n to } i = 1 \textit{ and from n to } j = 1 \tag{7}$$

Let N be the total number of matrix elements that will be generated by taking the average of the members of matrix T to exclude any insignificant impacts. This implies that the effect connections will exclude any impacts below the threshold amount [70].

Last Step: Create a causal relationship diagram: The results obtained from the calculations conducted in the preceding steps create the foundation for creating the relationship diagram. Thus, the cause and effect are systematically represented across all coordinate sets of the total of the rows and columns. The rows and columns in this representation depict the interactions between the criteria and offer valuable information for determining the most crucial criterion and their impact on others.

V. ANALYSIS AND PRESENTATION OF THE RESULT

A method known as DEMATEL has been applied in order to conduct an investigation on the major elements that have an effect on interoperable defensive strategies. Encoding the criteria and entering the data into a spreadsheet created in Microsoft Excel is the first step in the process of receiving the outcome of the analysis, which comes after the data collections have been completed. "S1," "S2," "S3," "S4", and "S5" were the categories that were used to classify the criteria. Therefore, the ten experts who gave their views for this study have been collected and displayed in the original individual matrix. The integer scores that were used for this study ranged from 0 to 4, providing a range of possible values. The expert responses are represented by this matrix, which is then translated into a non-negative direct relation matrix with dimensions of n×n after being transformed by equation 1:

The mean aggregate of expert's decision matrices, also referred to as the direct influence matrix, is calculated using Equation 2. Subsequently, the direct influence matrix is normalized using Equation 3, and the resulting values are displayed below:

$$D = \begin{matrix} 0.0000 & 0.2306 & 0.2141 & 0.2306 & 0.2221 \\ 0.2306 & 0.0000 & 0.2151 & 0.2411 & 0.2231 \\ 0.2310 & 0.2141 & 0.0000 & 0.2141 & 0.2172 \\ 0.2326 & 0.2411 & 0.2256 & 0.0000 & 0.2212 \\ 0.2306 & 0.2306 & 0.2056 & 0.2306 & 0.0000 \end{matrix}$$

The total relation matrix is calculated by applying equation 4 to the normalized initial direct-relation matrix, resulting in the quantification of the overall influence generated by the expert's response.

$$T = \begin{matrix} 2.5321 & 2.7621 & 2.4203 & 2.6426 & 2.6440 \\ 2.6404 & 2.6113 & 2.6172 & 2.7120 & 2.6434 \\ 2.5131 & 2.5344 & 2.2231 & 2.2109 & 2.4149 \\ 2.3458 & 2.7684 & 2.4159 & 2.3791 & 2.5346 \\ 2.6193 & 2.5243 & 2.4001 & 2.4246 & 2.4129 \end{matrix}$$

To determine the causes and effects, the research calculate the sums of the rows and columns of the total relation matrix, which consists of matrix vectors representing the rows and columns of the matrix. These values are calculated using equations 5 and 6, respectively. Put simply, if the research represents the sum of the rows and columns of the complete relation matrix as vectors r and c correspondingly, then the research identifies the "cause" and "effect". Therefore, the outcome of the computation of sums of the rows and columns is displayed in the Table 7.

TABLE 7. The sum of the rows and columns.

Factor	S1	S2	S3	S4	S5	r_i
S1	2.5321	2.7621	2.4203	2.6426	2.644	13.001
S2	2.6404	2.6113	2.6172	2.712	2.6434	13.224
S3	2.5131	2.5344	2.2231	2.2109	2.4149	11.896
S4	2.3458	2.7684	2.4159	2.3791	2.5346	12.443
S5	2.6193	2.5243	2.4001	2.4246	2.4129	12.381
c_i	12.650	13.200	12.076	12.369	12.649	

The final evaluation has the goal of determining the connection between the cause and the effect, is presented in Table 8.

TABLE 8. Direct influenced of the criteria among them.

Factor	r_i	c_i	r_i+c_i	r_i-c_i
S1	13.0011	23.4701	36.4712	-10.469
S2	13.2243	23.8082	37.0325	-10.5839
S3	11.8964	21.2797	33.1761	-9.3833
S4	12.4438	22.5418	34.9856	-10.098
S5	12.3812	22.1431	34.5243	-9.7619

Every single criterion is classified as belonging to the effect group, which indicates that they were influenced overall. There is a known impact of them on any other or cause them to act with other criteria. According to this, it appears that every criterion came to take part in the Interoperable Defensive Strategies analysis. It is implied that there is a situation in which each criterion is interrelated and impacted by other criteria within the system, but none of them operate as direct influences or causes. This is because all of the criteria within the system are classified as "effects," while none of them are labeled as "causes." This finding points to a complex network of interdependencies among the recognized components, showing that all criteria in the system are affected by and react to modifications to other criteria. It means that various factors are interdependent on one another and that no one criterion is functioning as the main driver of change.

These results may point to the necessity of taking a comprehensive strategy to meeting the specified requirements, one that recognizes and values their interdependence and connectivity. In order to develop strategies or interventions that take into account the systemic character of the components included in the analysis, it can be necessary to understand these complicated relationships. Considering the name of the variable, this research provides their short form and present in Table 9.

TABLE 9. Short form of the variables name.

Factors	Short form
Security Concerns and Cybersecurity Risks	Risk
Technological Complexity and Interoperability	Complexity
Dependency on Commercial Technologies and	Dependency
Ethical, Legal, and Human Factor Challenges	Personal
Strategic Implications and Environmental	Environmental

Figure 2 displays many things categorized as Risk, Complexity, Dependency, Personnel, and Environment. These items are used to assess the responses of experts, who provide estimates for the duration of their task. The total estimated number of identified cybersecurity threats is 150, posing a risk. The percentage of threats that have the potential to result in a data breach is 30%.

Item 9 - Mean Duration for Resolving Vulnerabilities Post-Identification (Complexity: 7 days). Item 3 - Mean Duration for Achieving Interoperability Among Diverse

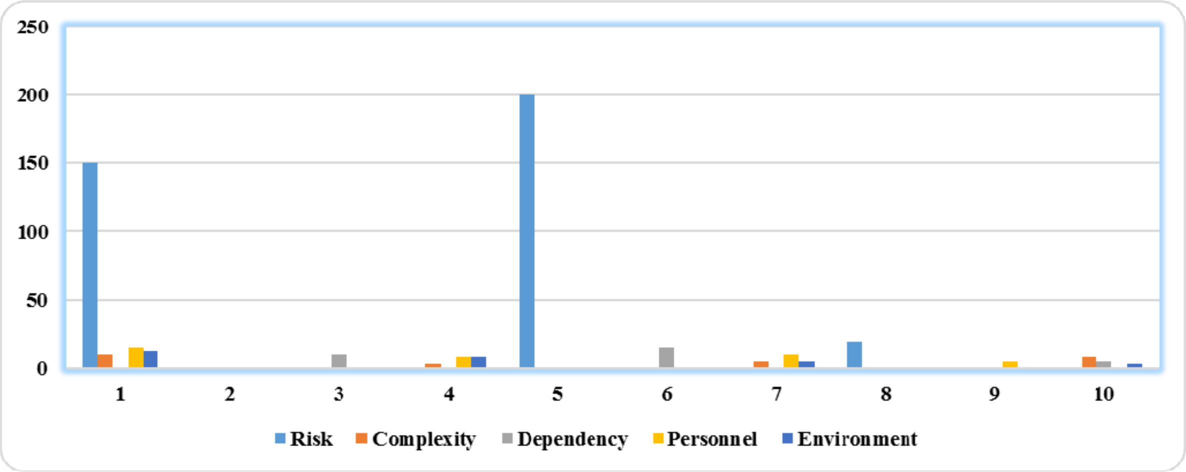

FIGURE 2. The distribution of response to each variable across the ten question for each of the viable.

Systems (Complexity: 6 months). The mean yearly spending on commercial technologies amounts to $1.5 billion. The defense system utilizes a total of 10 distinct technologies. Annual allocation of time for Human Factors training (40 hours). Cybersecurity personnel in the defense system: 200. The defense budget has allocated 8% of its funds towards environmental measures, representing the percentage increase. Number of accolades received for sustainable practices in the field of environment: 3.

This finding indicates that the range of risk indicators varies greatly, with a significant number of identified cybersecurity threats (150) and a percentage of threats that have the potential for data breaches (30%). This range signifies a thorough evaluation, encompassing different degrees of seriousness in identified risks. Complexity metrics vary in terms of timescales, ranging from prompt vulnerability patching (7 days) to more extended periods required for establishing system interoperability (6 months). This spectrum encompasses the diverse complexities and time commitments involved in overseeing technology issues. The reliance metrics reveal notable disparities, ranging from a considerable yearly outlay on commercial technology ($1.5 billion) to a restricted number of diverse technologies employed in the military system (10).

This discrepancy underscores the considerable variation in dependence on external technical solutions. Personnel-related data show different distributions of resources, with a significant amount of time being allocated each year to human factors training (40 hours) compared to the number of cybersecurity professionals in the defense system (200). This distribution indicates varying degrees of investment in human resources and training. Environmental indicators reveal a range of initiatives, including a significant 8% rise in the defense budget allotted to environmental measures and a very low tally of 3 environmental awards earned for sustainable activities. This distribution emphasizes the diverse degrees of dedication and acknowledgment in environmental sustainability activities.

TABLE 10. The inference of distribution of responses.

Items	Risk	Complexity	Dependency	Personnel	Environment
1	150	10	70%	15	12
2	30%	40%	$1.5 billion	25%	15%
3	72 hours	6 months	10	2 weeks	4 months
4	15%	3	8%	8	8
5	200	25%	12%	12%	20%
6	10%	15%	15	Moderate	High
7	High	5	20%	10	5
8	20	Moderate	High	60%	8%
9	7 days	60%	9 months	5	3 months
10	Moderate	8	5	40 hours	3

This distribution's impact stems from providing a systematic overview of diverse elements linked to distinct tasks (see Table 10). Stakeholders can efficiently evaluate and analyze the risk, complexity, reliance, people needs, and environmental factors of various project components or scenarios. This information is crucial for decision-making, resource allocation, and risk management techniques. Moreover, it helps enhance communication and teamwork among team members by offering a distinct reference point for conversations and planning. The distributions are a great tool for comprehending and handling the complexities of a project or scenario.

VI. DISCUSSION

The finding that all cybersecurity risk criteria and security issues are categorized as the "effect group," demonstrating their influence and interdependence, has significant implications for Interoperable Defensive Strategies (IDS). Interoperable. In the defense industry, stability, longevity, strategic significance, and synergy are the most important factors [71]. Defensive Strategies strengthen cybersecurity by integrating varied security components, facilitating smooth collaboration, and strengthening system resilience against evolving threats. A thorough and effective defensive strategy must include the multidimensional influence of the identified criteria on IDS. Risk assessments are crucial due to factors like the amount of cybersecurity threats, the percentage of threats with data breach potential, and data loss instances. An IDS must thoroughly assess these threats to design appropriate countermeasures and response techniques. An IDS's preparedness and capability depend on cybersecurity specialists and funds. These criteria emphasize the importance of qualified staff and sufficient resources to build and manage interoperable defense strategies.

Cybersecurity is time-critical, as measured by the average time to discover an event and patch vulnerabilities after detection. To quickly reduce cyber incidents, a good IDS should minimize detection and response times. Staff cybersecurity awareness and coordination with external cybersecurity organizations emphasize human aspects and external relationships. An IDS must include training to raise staff awareness and strengthen external collaborations for threat intelligence and response. The number of annual simulated cybersecurity drills emphasizes the need for practice and progress. Regular simulations and exercises should be prioritized by an IDS to improve response techniques and cyber threat readiness. Finally, the criteria' effects on Interoperable Defensive Strategies demonstrate the need for a comprehensive and adaptive cybersecurity strategy. An effective IDS should emphasize risk assessment, resource allocation, fast incident response, human-centric approaches, collaborative efforts, and continuous improvement through drills. By examining five key criteria, firms may strengthen their cybersecurity posture and defend against evolving cyber threats.

The classification of all criteria related to technological complexity and interoperability challenges as part of the "effect group" has important implications for Interoperable Defensive Strategies (IDS). These specified criteria are crucial in determining the framework for successful IDS implementation. Metrics such as the quantity of diverse technologies employed, the proportion necessitating exclusive protocols, and the existence of outdated technologies highlight the intricacy of technological integration. In order to achieve effective interoperability, IDS must successfully navigate through a variety of systems and protocols. The quantity of interoperability standards executed and the triumphant interoperability implementations in the previous year demonstrate the significance of standardization and effective integration. IDS should conform to recognized standards and utilize successful implementations as benchmarks. The necessity to adapt IDS to meet cloud environments and efficiently overcome cross-domain hurdles is shown by the readiness for cloud integration and the challenges experienced in cross-domain interoperability. Defense strategies should prioritize addressing technical difficulties, adhering to interoperability standards, streamlining integration procedures, managing time and budgets effectively, embracing cloud readiness, and adeptly handling cross-domain challenges. This will assure the development of robust and effective defense strategies that are interoperable.

The categorization of each criterion related to reliance on commercial technology and cost problems as part of the "effect group" has important consequences for the development and implementation of Interoperable Defensive Strategies (IDS). Metrics such as the proportion of defense systems utilizing Commercial Off-the-Shelf (COTS) goods, the yearly spending on commercial technology, and the quantity of notable market vendors highlight the dependence on commercial solutions. In order to achieve smooth integration and compatibility between different commercial technologies, IDS must take into consideration this interdependence. The quantity of collaborative agreements established with commercial technology providers, as well as the execution of cost-efficiency measures, serve as indicators for potential collaborations and the enhancement of cost optimization. IDS can derive advantages from strategic cooperation and activities aimed at augmenting military capabilities in a cost-efficient manner. Intrusion Detection Systems (IDS) may guarantee a strong defense infrastructure that effectively incorporates many commercial technologies without any disruptions, while also minimizing expenses and preserving flexibility in an ever-changing cybersecurity environment.

The ethical, legal, and human aspect difficulties within the "effect group" have significant consequences for the development and implementation of Interoperable Defensive Strategies (IDS). Indicators such as documented ethical challenges, the requirement for further ethical education, and the duration dedicated to addressing ethical issues highlight the importance of ethical considerations in defense interoperability. It is important for IDS to give priority to promoting ethical awareness and providing training in order to address difficulties and assure the implementation of ethical practices in defense efforts.

The significance of the criterion on Interoperable Defensive Strategies highlights the necessity for a comprehensive and people-oriented strategy. IDS should give highest importance to promoting ethical consciousness, guaranteeing adherence to the law, reducing mistakes caused by humans, cultivating a favorable work environment, and utilizing staff preparedness for technological progress. Through successful management of these difficulties, IDS may strengthen defense strategies, improve interoperability, and establish a robust defense infrastructure that seamlessly incorporates ethical, legal, and human factors.

VII. CONCLUSION

Interoperable defensive methods, which prioritize strategic implications and environmental impact, provide a new era of network security. This allows enterprises to improve their defense capabilities while also contributing to broader strategic and environmental goals. Through the utilization of the interplay between strategic partnerships, flexibility, and durability, companies can establish a trajectory towards a more robust, cooperative, and ecologically aware approach to network security in an interconnected world. The study's finding focuses on the integration of several factors, highlighting the complex nature of IDS. Security Concerns and Cybersecurity Risks (S1): Emphasized the necessity of adopting a comprehensive approach to evaluating and addressing risks, with a focus on having competent individuals, swift incident response, and cooperation with external organizations. Technological complexity and interoperability issues (S2) refer to the difficulties faced in combining different technologies, following standards, managing costs, and adapting to new technological developments. Reliance on commercial technologies and financial problems were demonstrated, highlighting the importance of cost reductions, vendor management, and strategic collaborations. Ethical, legal, and human factor challenges (S4) encompass a range of topics including ethical dilemmas, legal compliance, human-centric concerns, and the need for ethical awareness, legal adherence, and human-centric defense methods. The importance of strategic partnerships, sustainability, international cooperation, and budget allocation in promoting collaborations, embracing sustainability, and ensuring compliance is emphasized. The combination of these observations emphasizes the need for Intrusion Detection Systems (IDS) to be thorough, flexible, and encompassing. An efficient Intrusion Detection System (IDS) should integrate technological innovations, ethical considerations, legal compliance, financial prudence, collaborative initiatives, and environmental sustainability. This comprehensive strategy guarantees strong defense tactics, the ability to withstand changing dangers, and the creation of a secure, morally upright, and long-lasting defense infrastructure that is in line with worldwide necessities and growing difficulties.

REFERENCES

[1] D. D.-I. Giggenbach, "Global communication system using geostationary satellites and high altitude communication platforms," Tech. Rep., 2003.

[2] T. Meink, "Transformational communications systems for DoD net-centric operations," *CrossTalk, J. Defense Softw. Eng.*, vol. 19, Jul. 2006.

[3] E. F. Gallagher, "Communications: The military Goes digital: Digital switching and signaling, along with digital transmission, offer reliability in a hostile environment," *IEEE Spectr.*, vol. S-14, no. 2, pp. 42–48, Feb. 1977, doi: 10.1109/MSPEC.1977.6369327.

[4] B. Fonow, "Global networks: Emerging constraints on strategy," Tech. Rep., Jul. 2004, doi: 10.21236/ADA428304.

[5] M. Boniface, N. Fair, S. Modafferi, and J. Papay, "Security implications of interoperability," Tech. Rep., 2020.

[6] E. J. Wyatt, K. Griendling, and D. N. Mavris, "Addressing interoperability in military systems-of-systems architectures," in *Proc. IEEE Int. Syst. Conf.*, Mar. 2012, pp. 1–8, doi: 10.1109/SYSCON.2012.6189515.

[7] B. Healy, T. A. Mazzuchi, and S. Sarkani, "A framework for considering cost uncertainty for complex interdependent systems based on weighted nodal analysis," in *Proc. INCOSE Int. Symp.*, Jun. 2011, pp. 683–697, doi: 10.1002/J.2334-5837.2011.TB01236.x.

[8] S. P. Switzer and M. A. Stropki, "Effects of defense globalization: An examination of current and future command and control collaborations," *Defense Acquisition Rev. J.*, vol. 12, no. 3, pp. 155–175, 2005.

[9] T. Ford, J. Colombi, S. Graham, and D. Jacques, "The interoperability score," in *Proc. 5th Annu. Conf. Syst. Eng. Res.*, 2007, pp. 1–10.

[10] S. J. Kim, "Non-traditional security threats and methods to increase the effectiveness of the Korean national crisis management system—Focused on integrated defense system," *Korean J. Mil. Affairs*, vol. 12, pp. 37–71, Dec. 2022, doi: 10.33528/kjma.2022.12.12.37.

[11] C. Xie, H. Li, K. Chen, and Y. Li, "Research on large-scale heterogeneous combat network optimization based on SP-RV-moeanet algorithm," in *Proc. 2nd Int. Conf. Innov. Develop. Inf. Technol. Robot.*, 2023, pp. 54–58, doi: 10.1109/iditr57726.2023.10145995.

[12] H. Kwon, Y. Shin, J. Jeong, K. Kim, and D. Shin, "Measures to ensure the sustainability of information systems in the COVID-19 environment," *Sustainability*, vol. 15, no. 1, p. 35, 2022, doi: 10.3390/su15010035.

[13] S. Inshi, R. Chowdhury, H. Ould-Slimane, and C. Talhi, "Dynamic context-aware security in a tactical network using attribute-based encryption," in *Proc. IEEE Military Commun. Conf.*, Nov. 2022, pp. 49–54, doi: 10.1109/MILCOM55135.2022.10017647.

[14] P. Agbabian, R. Roupski, and L. Mulcahy, "Systems and methods for providing an integrated cyber threat defense exchange platform," Tech. Rep., 2021.

[15] L. Liu, C. Huang, Y. Fang, and Z. Wang, "Network attack and defense effectiveness evaluation based on dematel method," in *Proc. Int. Conf. Artif. Intell. Secur.*, 2019, pp. 564–575, doi: 10.1007/978-3-030-24271-8_50.

[16] S. Wang, T. Tu, and C. Li, "Defense effectiveness evaluation method applied to network target range," Tech. Rep., 2020.

[17] H. Wu, Y. Gu, G. Cheng, and Y. Zhou, "Effectiveness evaluation method for cyber deception based on dynamic Bayesian attack graph," in *Proc. 3rd Int. Conf. Comput. Sci. Softw. Eng.*, 2020, pp. 1–9, doi: 10.1145/3403746.3403897.

[18] R. Xi, Z. Hao, Z. Ding, and Y. Liu, "Network attack and defense tool performance evaluation method and system based on a simulation platform," Tech. Rep., 2019.

[19] L. Zhu, W. Sun, and P. Zhao, "Attack and defense evaluation method and device," Tech. Rep., 2019.

[20] D. Fraunholz and H. D. Schotten, "Strategic defense and attack in deception based network security," in *Proc. Int. Conf. Inf. Netw.*, 2018, pp. 156–161, doi: 10.1109/ICOIN.2018.8343103.

[21] Z. Du, "Network security model based on active and passive defense hybrid strategy," *Converter*, pp. 45–51, Jan. 2021., doi: 10.17762/CONVERTER.13.

[22] S. Zheng, Z. Li, and B. Li, "Campus network security defense strategy," in *Proc. Int. Conf. Mech., Electron., Control Automat. Eng.*, 2017, pp. 356–359, doi: 10.2991/MECAE-17.2017.67.

[23] X. Li, W. Zhang, T. Zhao, Z. Gan, and L. Zhao, "An evaluation method of internal network security defense ability based on device traffic," in *Proc. IEEE Int. Conf. Power Electron., Comput. Appl.*, 2021, pp. 238–244, doi: 10.1109/ICPECA51329.2021.9362650.

[24] J. Wei, R. Zhang, J. Liu, X. Niu, and Y. Yang, "Defense strategy of network security based on dynamic classification," *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 12, 2015, doi: 10.3837/TIIS.2015.12.021.

[25] Y. Wang, A. Smahi, H. Zhang, and H. Li, "Towards double defense network security based on multi-identifier network architecture," *Sensors*, vol. 22, no. 3, p. 747, 2022, doi: 10.3390/s22030747.

[26] N. Zhang, "Defensive strategy selection based on attack-defense game model in network security," *Int. J. Performability Eng.*, vol. 14, no. 11, p. 2633, 2018, doi: 10.23940/ijpe.18.11.p9.26332642.

[27] S. Zhang, S. Li, P. Chen, S. Wang, and C. Zhao, "Generating network security defense strategy based on cyber threat intelligence knowledge graph," in *Emerging Networking Architecture and Technologies*. Berlin, Germany: Springer, 2022, pp. 507–519.

[28] P. Wang, "Analysis of computer virus defense strategy based on network security," *Academic J. Comput. Inf. Sci.*, vol. 4, no. 14, pp. 33–39, 2022.

[29] Y. Ye, L. Yan, S. Ren, and Q. Zhang, "Research on network security protection strategy," in *Proc. Int. Conf. Robots Intell. Syst. (ICRIS)*, Jun. 2019, pp. 152–154.

[30] G. Shang, L. Yanqian, C. Shouming, L. Yunde, L. Fengzheng, H. Jutao, W. Baijian, Z. Kaidong, and M. Xiaohui, "Collaborative defense method for network protection and system," Tech. Rep., 2019.

[31] W. Ke, Q. Li, L. Jianmei, Y. Pengcheng, and H. Jun, "Network security cooperative defense method," Tech. Rep., 2018.

[32] S. Kao and L. Shiue, "Security management of mutually trusted domains through cooperation of defensive technologies," *Int. J. Netw. Manag.*, vol. 19, no. 3, pp. 183–201, May 2009, doi: 10.1002/nem.697.

[33] M. J. J. LaMantia, B. J. Buck, S. J. Edwards, and W. Robinson, "Coordinating multiple security components," Tech. Rep., 2017.

[34] H. Li, "Research on defensive strategy selection in network security," *Int. J. Secur. Appl.*, vol. 11, no. 1, pp. 23–34, Jan. 2017, doi: 10.14257/ijsia.2017.11.1.03.

[35] Y. Zheng, Z. Li, X. Xu, and Q. Zhao, ''Dynamic defenses in cyber security: Techniques, methods and challenges,'' *Digit. Commun. Netw.*, vol. 8, pp. 422–435, Aug. 2022, doi: 10.1016/j.dcan.2021.07.006.

[36] S. Amin, G. A. Schwartz, and A. Hussain, ''In quest of benchmarking security risks to cyber-physical systems,'' *IEEE Netw.*, vol. 27, no. 1, pp. 19–24, Jan. 2013, doi: 10.1109/MNET.2013.6423187.

[37] N. M. Scala, A. C. Reilly, P. L. Goethals, and M. Cukier, ''Risk and the five hard problems of cybersecurity,'' *Risk Anal.*, vol. 39, no. 10, pp. 2119–2126, 2019, doi: 10.1111/RISA.13309.

[38] J. H. Kim, J. I. Lim, and H. K. Kim, ''Collaborative security response by interworking between multiple security solutions,'' *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 23, no. 1, pp. 69–79, 2013, doi: 10.13089/JKIISC.2013.23.1.069.

[39] I. A. Stanescu, A. Stefan, M. Kravcik, T. Lim, and R. Bidarra, ''Interoperability strategies for serious games development,'' *Internet Learn.*, vol. 2, no. 1, p. 6, 2013.

[40] J. Pridmore and D. J. Rumens, ''Interoperability-how do we know when we have achieved it?'' in *Proc. 3rd Int. Conf. Command, Control, Commun. Manag. Inf. Syst.*, 1989, pp. 192–205.

[41] S. Y. Diallo, ''On the complexity of interoperability,'' in *Proc. Modeling Simul. Complexity Intell., Adapt. Auton. Syst.* , 2016, pp. 1–6.

[42] J. Searle and J. Brennan, ''General interoperability concepts,'' Tech. Rep., 2006.

[43] R. Wilson, ''Information management and interoperability strategies: The case for digital identifiers,'' in *Proc. IADIS Int. Conf.*, 2003, pp. 100–109.

[44] A. Z. Spyropoulos, C. Bratsas, G. C. Makris, E. Garoufallou, and V. Tsiantos, ''Interoperability-enhanced knowledge management in law enforcement: An integrated data-driven forensic ontological approach to crime scene analysis,'' *Information*, vol. 14, no. 11, p. 607, Nov. 2023.

[45] J. D. Aronowitz, *Controlling Militarily Significant Emerging Technologies*, 1999, doi: 10.21236/ADA363480.

[46] J. Lee and S. Shim, ''Critical success factors of government-led international technological cooperation for national defense core-technology R&D projects,'' *J. Adv. Mil. Stud.*, vol. 6, no. 1, pp. 77–97, Apr. 2023, doi: 10.37944/jams.v6i1.173.

[47] D. Angelis, J. Dillard, F. Melese, M. M. Brown, and R. M. Flowe, ''Application of transaction cost economics to capabilities-based acquisition: Exploring single service vs. joint service programs and single systems vs. system-of-systems,'' Tech. Rep., 2008.

[48] D. Maye, ''Autarky or interdependence: US vs. European security and defense industries in a globalized market,'' *J. Strategic Secur.*, vol. 10, no. 2, pp. 33–47, Jun. 2017, doi: 10.5038/1944-0472.10.2.1597.

[49] G. L. Monahan, ''Strategic defense initiative briefing for members of congress,'' Tech. Rep., 1990, doi: 10.21236/ADA338902.

[50] R. McLeod ''Issues in assuring human controls in layers-of-defences strategies,'' *Chem. Eng. Trans.*, vol. 48, pp. 925–930, Apr. 2016, doi: 10.3303/CET1648155.

[51] D. Wang, C. Li, S. Wen, S. Nepal, and Y. Xiang, ''Defending against adversarial attack towards deep neural networks via collaborative multitask training,'' *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 2, pp. 953–965, Mar. 2022, doi: 10.1109/TDSC.2020.3014390.

[52] D. Wang, C. Li, S. Wen, S. Nepal, and Y. Xiang, ''Defending against adversarial attack towards deep neural networks via collaborative multitask training,'' 2018, *arXiv:1803.05123*.

[53] R. Brzyski, ''Reply: Ethical and legal challenges,'' *Fertility Sterility*, vol. 89, no. 4, pp. 1032–1033, 2008, doi: 10.1016/J.FERTNSTERT.2008.02.113.

[54] A. Herzberg and R. Margulies, ''Conducting ethical yet realistic usable security studies,'' in *Proc. IEEE Security Privacy Workshops*, May 2013, pp. 1–4, doi: 10.1109/SPW.2013.6915056.

[55] L. Gao, Q. Pan, and M. He, ''Environmental-based defensive promotes cooperation in the prisoner's dilemma game,'' *Appl. Math. Comput.*, vol. 401, Jul. 2021, Art. no. 126074, doi: 10.1016/j.amc.2021.126074.

[56] D. Stojkovic and B. M. Radovic, ''Strategic environment influence on development of defense of the Republic of Serbia,'' *Vojno Delo*, vol. 69, no. 4, pp. 5–16, 2017, doi: 10.5937/VOJDELO1704005S.

[57] A. Mossalanejad, ''International security through environmental challenges,'' Tech. Rep., 2009.

[58] F. He, S. Chandrasekar, N. S. V. Rao, and C. Y. T. Ma, ''Effects of interdependencies on game-theoretic defense of cyber-physical infrastructures,'' in *Proc. 22th Int. Conf. Inf. Fusion*, 2019, pp. 1–8.

[59] E. Summers-Effler, ''Defensive strategies: The formation and social implications of patterned self-destructive behavior,'' in *Proc. Theory Res. Human Emotions*, 2004, pp. 309–325, doi: 10.1016/S0882-6145(04)21012-8.

[60] A. Abubakar and Z. M. Yusof, ''Streams of data flow in transmission control protocol (TCP) request-response cycle efficiency,'' *Int. J. Perceptive Cogn. Comput.*, vol. 10, no. 1, pp. 79–89, 2024.

[61] W. Wang, C. Luo, J. An, L. Gan, H. Liao, and C. Yuen, ''Semisupervised RF fingerprinting with consistency-based regularization,'' *IEEE Internet Things J.*, vol. 11, no. 5, pp. 8624–8636, Mar. 2024.

[62] A. A. Alarood, A. A. Ibrahim, and F. S. Alsubaei, ''Attacks notification of differentiated services code point (DSCP) values modifications,'' *IEEE Access*, vol. 13, pp. 126950–126966, 2023.

[63] A. Abubakar N. M. Najmuddin, R. A. Alwi, and N. A. Faizal, ''Examining potential threats of eavesdropping in TCP stream of personal interactive transmission session,'' *Int. J. Perceptive Cogn. Comput.*, vol. 10, no. 1, pp. 98–104, 2024.

[64] R. Li, H. Liao, J. An, C. Yuen, and L. Gan, ''Intra-class universal adversarial attacks on deep learning-based modulation classifiers,'' *IEEE Commun. Lett.*, vol. 27, no. 5, pp. 1297–1301, May 2023.

[65] M. M. H. Rahman, M. A. A. Naeem, and A. Abubakar, ''Threats from unintentional insiders: An assessment of an organization's readiness using machine learning,'' *IEEE Access*, vol. 10, pp. 110294–110308, 2022.

[66] P. K. Tarei, J. J. Thakkar, and B. Nag, ''A hybrid approach for quantifying supply chain risk and prioritizing the risk drivers: A case of Indian petroleum supply chain,'' *J. Manuf. Technol. Manage.*, vol. 29, no. 3, pp. 533–569, Mar. 2018.

[67] T. Smidovnik and P. Grošelj, ''Solution for convergence problem in DEMATEL method: DEMATEL of finite sum of influences,'' *Symmetry*, vol. 15, no. 7, p. 1357, Jul. 2023.

[68] H. T. Nguyen and T.-C. Chu, ''Ranking startups using DEMATEL-ANP-based fuzzy PROMETHEE II,'' *Axioms*, vol. 12, no. 6, p. 528, May 2023.

[69] K. K. Tp, M. Ramachandran, K. Ramu, and A. Murugan, ''Using this DEMATEL corporate social responsibility CSR,'' *REST J. Banking, Accounting Bus.*, vol. 2, no. 1, pp. 51–59, Apr. 2023.

[70] L. Abdullah, H. Mohd Pouzi, and N. A. Awang, ''Intuitionistic fuzzy DEMATEL for developing causal relationship of water security,'' *Int. J. Intell. Comput. Cybern.*, vol. 16, no. 3, pp. 520–544, Jul. 2023.

[71] A. Rahimi, M. Abbasi, and M. Berarnia, ''Proposing a model for the valuation of technology-based firms for acquisition by the department of defense (DOD),'' *Res. Production Oper. Manag.*, vol. 14, no. 4, pp. 1–30, 2024.

ALA ABDULSALAM ALAROOD received the Bachelor of Computer Science and Master of Computer Science degrees and the Ph.D. degree in computer science from the University of Technology Malaysia (UTM), in 2017. He is currently an Associate Professor with the Faculty of Computer Science and Engineering, University of Jeddah. His research interests include machine learning, the Internet of Things (IoT), multimedia security, and cybersecurity.

AHMED OMAR ALZAHRANI received the Master of Computer Science degree from California Lutheran University and the master's and Ph.D. degrees in information systems and technology from Claremont Graduate University. He is currently an Assistant Professor with the Faculty of Computer Science and Engineering, University of Jeddah. His research interests include geographic information systems (GIS), energy informatics, remote sensing, and machine learning.