IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 April 2025, accepted 2 June 2025, date of publication 6 June 2025, date of current version 13 June 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3577347

RESEARCH ARTICLE

Resilience Analysis of Coupling Combat Network: Considering Multiple Destruction-Recovery Processes

YUHENG DANG[1], HUIXIONG WANG[2,3], ZIMENG YIN[2], AND XING PAN[1,4], (Member, IEEE)

[1]School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China
[2]China Academy of Launch Vehicle Technology, Beijing 100076, China
[3]School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China
[4]National Key Laboratory of Reliability and Environmental Engineering, Beijing 100191, China

Corresponding author: Xing Pan (panxing@buaa.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 72071011.

ABSTRACT Modern military force operates in the form of combat systems of systems (CSoS) involving multiple components assembled in terms of function and structure with abundant complex relationships, which can be abstracted as the coupling combat network (CCN). However, coupling failures render the CSoS more vulnerable and challenging to recover under external disturbances. As the battlefield environment grows increasingly variable and future operations confront high-intensity conflict, it is necessary for the CSoS to consider resilience against continuous strikes as well. As such, this paper proposes an analysis framework of resilience based on the CCN modeling. Then, considering multiple and continuous strikes from enemies, a resilience modeling and assessment method is developed based on trend analysis for multiple destruction-recovery processes (DRPs). Additionally, the notion of importance is introduced into the resilience analysis of the CCN, wherein the correlation of layers' resilience is investigated, encompassing both direct and coupling resilience importance. Finally, the CCN model for a typical CSoS is established to illustrate the proposed method and framework, which can serve as a reference for research on CSoSs' resilience.

INDEX TERMS Combat system of systems, coupling combat network, resilience, multiple DRPs.

I. INTRODUCTION

With the rapid advancement of information technology and in-depth research in the field of systems engineering, the concept of the complex system has become increasingly prevalent across various disciplines, including military, aerospace, and social science, to address challenges associated with multi-system integration, complex emergence, and coupling [1]. The system of systems (SoS) is characterized as a collection of multiple systems that are guided by a common mission [2]. Coupling refers to the functional interaction of system components to achieve specific objectives [3], which can be observed in a wide range of SoSs, such as urban SoSs [4], production SoSs [5], and equipment SoSs [6].

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

The patterns of modern warfare have evolved, shifting from platform-centric combat to countermeasures against multiple systems, namely combat SoS (CSoS) [7], [8]. Complex network modeling is a powerful complex system modeling method, with broad applications in fields such as urban transportation [9], railway transportation [10], communication [11], medicine [12], and industrial production [13], [14]. The general complex network is also utilized to represent the CSoS, where the nodes and links represent the entities and communications between entities, respectively [15], [16], [17]. While the CSoS is heterogeneous composed of various types of equipment operating independently, which are linked through more than one relationship [18], [19]. The CSoS encompasses a hierarchical relationship of command and control (C2) among its equipment entities, as well as a supportive relationship to ensure operational effectiveness.

Therefore, the CSoS with multi-platform coupling can be well modeled as multiplex networks with multiple layers, namely coupling combat network (CCN), rather than a single network.

Recent studies have demonstrated that coupling networks are very vulnerable on account of node cascading failures (NCFs) caused by node coupling relationships [1], [2], [3], [4]. With the development of weapons and warfare methods, it's noteworthy that the CSoS confronts the multi-dimensional and high-intensity enemy attack from land, sea, air, space, network, electromagnetic, and cognitive [5]. In the context of this uncertain environments and intensive threats, the coupling relationships that commonly exist within the CCN can lead to the propagation of failures, resulting not only in the failure of individual components but also in the failure of multiple interconnected equipment units, leading to vulnerability of the CSoS. To be more precise, the destruction of equipment systems may induce node cascading failures, including intra-layer node failures (i.e., failures of nodes in the same layer) and inter-layer node failures (i.e., failures of nodes in the other layers) [6], [7]. For instance, attacks against the command links might trigger the failures of nodes both in the command layer and operation layer simultaneously that are highly coupled in the CSoS. Consequently, to eliminate the threats of failures and enhance the survivability of equipment in such conditions, the resilience of CSoS has become an increasingly critical issue in the field of military [8], [9], [10], [11], [12], [13].

The concept of resilience was initially introduced in the field of ecology by Holling, who defined it as a measure of a system's ability to absorb disturbances. Holling integrated the theory of stability of nonlinear systems with resilience to establish a metric for resilience, which quantifies the maximum amount of disturbance that can be absorbed while maintaining a certain steady state [14]. Following its introduction, the concept of resilience was swiftly applied to various other domains such as engineering, society, and economy, which marked a gradual transition to a higher system dimension in terms of the problems of survivability and reliability [15]. Generally, resilience denotes the capability to withstand a loss in performance and recover to a normal level when a system is subjected to adverse events such as environmental disturbances and failures [16]. The definition of resilience encompasses two aspects: the loss of system performance, that is, the degree to which the system deviates from its normal performance level under disturbances [17], and the recovery of system performance, namely, the ability of the system to gradually regain its performance from the lowest point with the assistance of its inherent characteristics or external intervention [18]. Furthermore, resilience has developed into a comprehensive concept of reliability, preparedness, survivability, robustness (i.e. vulnerability), adaptability, recoverability, resourcefulness, etc [19], [20]. Notably, while resilience benefits systems over a long period of time, these attributes only apply to certain time periods.

Scholars have conducted preliminary research work on resilience of CSoS, mainly including two aspects: resilience evaluation [8], [9], [10] and resilience optimal design [11], [12], [13]. The resilience of CSoSs is defined as the capability of CSoSs to avoid failures, to maintain and recover system performance or desired functions under the external variable environments and enemy attack [21]. To quantify this capacity of CSoSs, performance-based methods are utilized as the foundation for resilience optimization or reconfiguration of CSoSs, such as the integral model [22], multi-parameter model [23] and baseline model [24]. These resilience modeling and assessment relied on changed performance in one single resilience process, which can be separated into destruction and recovery periods in above studies [25]. However, the destruction-recovery process (DRP) of performance is not independent but consecutive and correlative due to multiple and continuous attacks against CSoSs. Meanwhile, the resilience modeling method based on the general complex network may not be adequate in addressing the coupling problems in resilience of CSoSs, particularly about the interplay between the resilience of subsystems, which has not been extensively explored in existing research.

Therefore, the model of CCN is proposed in the paper, which includes the representation of the network topology and coupling relationship. Furthermore, this paper extends the existing research on resilience, which has been limited to the assessment of resilience in a single DRP, to assess the network resilience for multiple DRPs. The correlation of layers' resilience is also analyzed based on the importance measure. Finally, a case analysis of a typical CSoS is conducted based on the CCN model and resilience modeling considering multiple DRPs.

The rest of this paper is organized as follows: Section II provides a framework for modeling the structure of the CSoS based on the CCN. Section III presents a resilience modeling method considering multiple DRPs. In Section IV, the model and the method proposed in the paper are verified via illustrative experiments. Section V concludes the paper with a summary and suggests future directions of research.

II. COUPLING COMBAT NETWORK MODEL

In this section, we present the method for establishing the coupling combat network model. Additionally, the performance metrics of coupling combat network are provided, which are essential for resilience analysis.

A. COUPLING NETWORK MODEL OF COMBAT SYSTEM-OF-SYSTEM

As with many complex systems, the CSoS is characterized by intricate and complex network relationships between entities, which exhibit significant coupling. The complex network modeling method is a general method for complex system modeling, especially appropriate for the resilience analysis of the CSoS, where the nodes and edges indicate the entities and connection, respectively [26].

The OODA loop is an operation cycle first proposed by U. S. Air Force Maj. John Boyd [27]. In the OODA theory, military operations are conceptualized as a closed-loop process comprising four fundamental activities: observation, orientation, decision-making, and action. During this process, sensors detect the target and transmit relevant information to the decision point. The decision point then analyzes both the target information and operational context to make informed decisions and issue appropriate orders. Subsequently, influencers take necessary actions while sensors re-detect the target to confirm successful engagement. Finally, based on this confirmation, the decision point determines whether a subsequent action is required. In this way to connect, a CSoS can be refined as a heterogeneous and ring network, comprising multiple OODA loops [28], [29].

The increasing comprehension of complex systems, especially CSoS, necessitates the combat network model to evolve beyond a single layer and instead form a multi-layer coupling network due to diverse connection relationships. The combat network model of the CSoS is formed based on the operational processes of OODA, which are influenced by C2 (command and control) and supportive relationships within the equipment. The combat network model thus embodies the characteristics of multi-layer network coupling, with the operation network serving as the upper layer and the command and logistics network as the lower layer, as depicted in Fig. 1.

In the paper, a CSoS is intended to be represented as a coupling combat network (CCN) composed by the command layer, logistics layer, and operation layer:

$$\mathrm{CCN} = (\mathrm{SNet}, \mathrm{SCouple}) \tag{1}$$

where $\mathrm{SNet} = \{\mathrm{Net}_o, \mathrm{Net}_c, \mathrm{Net}_l\}$ denotes the set of three network layers consisting of operation layer, command layer, and logistics layer, and $\mathrm{SCouple} = \{\mathrm{Couple}_{o,c}, \mathrm{Couple}_{o,l}, \mathrm{Couple}_{l,c}\}$ denotes the set of coupling relationships between layers.

Each network layer can be represented as

$$\mathrm{Net}_i = (\mathrm{SN}_i, \mathbf{A}_i) \tag{2}$$

where $\mathrm{Net}_i (i \in \{o, c, l\})$ indicates a network layer, $\mathrm{SN}_i = \{N_1^i, N_2^i, N_3^i, \ldots, N_{n_i}^i\}$ indicates the set of nodes in the layer i, $n_i = |\mathrm{SN}_i|$ represent the number of nodes in layer i, and $\boldsymbol{A}_i = \left[a_{\mathrm{pq}}\right]_{n_i \times n_i}$ is a $n_i \times n_i$ adjacency matrix representing the edges, where

$$a_{\mathrm{pq}} = \begin{cases} 1, \text{node } p \text{ is conected to node } q \\ 0, \text{node } p \text{ is not conected to node } q \end{cases} \tag{3}$$

Furthermore, the composition of nodes and edges in each layer varies to some extent due to distinct generation logic. For instance, Net_o generates based on OODA loops, which encompass target nodes and edges connecting fire strike equipment to the targets, whereas Net_c and Net_l do not include these specific nodes and edges.

$\mathrm{Couple}_{i,j} \in \mathrm{SCouple}\ (i, j \in \{o, c, l\}\ i \neq j)$ denotes the set of undirected coupling edges between layer i and layer j. In addition, $m_{\mathrm{ij}} = \left|\mathrm{Coupling}_{i,j}\right|$ indicates the number of coupling edges to describe the tightness of coupling relationship between two layers. Normalized degree of coupling is expressed as

$$Q_i = \frac{m_{\mathrm{ij}}}{n_i}, Q_j = \frac{m_{\mathrm{ij}}}{n_j} \tag{4}$$

where Q_i and Q_j represent the degree of coupling of two coupled layers respectively, and $m_{\mathrm{ij}} \leq n_i, n_j$ [30].

The coupling relationship in CCN is established by linking identical nodes across different networks. Note that the coupling edges specifically connect corresponding identical nodes within these distinct networks.

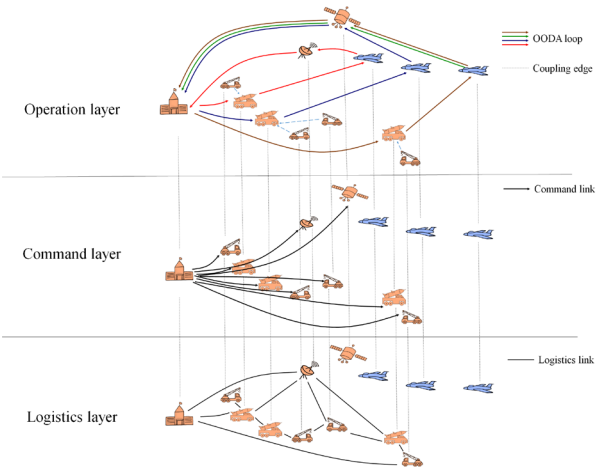

FIGURE 1. Coupling combat network model of CSoS.

B. PERFORMANCE METRICS OF COUPLING COMBAT NETWORK

The resilience evaluation of networks relies on the analysis of performance fluctuations over a specific time period [22]. Therefore, it is essential to consider performance metrics of network layers in the CCN for conducting resilience analysis in Section III.

1) PERFORMANCE OF NET_O, $\varphi_O(T)$

Net_o pertains to the assigned the missions and tasks of the CSoS, which are executed in operation loops. Note that, the greater the number of OODA loops, the wider the range of links and paths available to the CSoS for executing strike missions, thereby enhancing its capability to such missions. Therefore, the number of OODA loops serves as the performance metric [10].

The adjacency matrix, $\mathbf{A}_o$, can depict the connectivity of edges in Net_o. The diagonal element, a_{ii}^k, of $\mathbf{A}_o^k$ count loops with a length of k passing through node i, thus the total number of OODA loops with a length of k in Net_o is

$$S_k = \sum_{i=1}^{N} a_{\mathrm{ii}}^k = \mathrm{trace}(\mathbf{A}_o^k) \tag{5}$$

where trace($\mathbf{A}_o^k$) is the sum of matrix eigenvalues according to the matrix theory, rewritten as

$$S_k = \text{trace}(\mathbf{A}_o^k) = \sum_{i=1}^{N} \lambda_i^k \tag{6}$$

where $\lambda_1^k, \lambda_2^k, \ldots, \lambda_N^k$ are matrix eigenvalues of $\mathbf{A}_o^k$.

As such, the number of OODA loops of all lengths in Net_o is

$$S = \sum_{k=1}^{\infty} S_k = \sum_{k=1}^{\infty} \sum_{i=1}^{N} \lambda_i^k \tag{7}$$

However, it is worth noting that the longer the OODA loop, the greater the reaction and action time, resulting in lower operation effectiveness. The number of OODA loops after weighted simplification and measure to performance of Net_o is thus determined as

$$\varphi_o(t) = S'(t) = \sum_{k=1}^{\infty} c_k S_k(t) = \sum_{k=1}^{\infty} \sum_{i=1}^{N} \frac{\lambda_i^k(t)}{k!} = \sum_{i=1}^{N} e^{\lambda_i(t)} \tag{8}$$

2) PERFORMANCE OF NET_C, $\varphi_C(T)$

Net_c is established based on the hierarchical network topology, which aligns with a three-tier command structure consisting of the joint command center, base-level command center, and brigade-level command center. The command links are designed to effectively transmit instructions to all equipment units. Therefore, the accessibility of the instruction is the desired function, which can be measured as the number of nodes in the maximal connected subgraph of Net_c [31]:

$$\varphi_c(t) = \frac{n_{\text{LCC}}(t)}{n_c} \tag{9}$$

where n_c is the number of nodes and n_{LCC} is the number of nodes in the maximal connected subgraph in Net_c.

3) PERFORMANCE OF NET_L, $\varphi_L(T)$

Net_lexhibits the spatial embedding characteristics of actual roads, which are generated based on the rule that nodes with nearby locations are connected first. Net_l aims to ensure efficient and fast transportation of military support materials, network efficiency is employed as a metric to evaluate the performance of Net_l. Network efficiency is calculated by averaging the reciprocal of the shortest distances between all connected nodes [32]:

$$\varphi_l(t) = \frac{1}{n_l(n_l-1)} \sum_{i \neq j, i,j \in SN_l} \frac{1}{d_{i,j}(t)} \tag{10}$$

where n_l is the number of nodes, SN_l is the collection of nodes, and $d_{i,j}$ is the shortest topological distance from node i to j in Net_l.

III. RESILIENCE ANALYSIS OF COUPLING COMBAT NETWORK

In this section, a resilience metric for multiple DRPs is first extended. Subsequently, an importance-based resilience model is proposed to analyze the coupling relationship among resilience factors of CCN.

A. RESILIENCE ANALYSIS FOR MULTIPLE DRPs

The network model serves as a pivotal component in the modeling and analysis of resilience for the CSoS. Network performance, encompassing both topological and functional characteristics, is quantified to facilitate resilience analysis. By capturing the dynamics of network performance in a single destruction-recovery process (DRP), recent work leverages proportional, triangular, or integral models to derive resilience metrics.

The paper provides the resilience multi-parameter model, which utilizes a combination of multiple indicators instead of relying on a single indicator [23]. The model consists of four resilience factors, which are the integral performance factor, degradation velocity factor, recovery degree factor, and recovery time factor. The network performance, $\varphi(t)$ (i.e. $\varphi_o(t)$, $\varphi_c(t)$, $\varphi_l(t)$), and multiple resilience factors are shown in Fig. 2.

1) INTEGRAL PERFORMANCE FACTOR

The integral performance factor, α, accounts for the ratio of the integral of the performance over time for the whole resilience process to the integral of the performance index over time in the condition of no disturbance. The factor is calculated as

$$\alpha_i = \frac{\int_{t_{e_i}}^{t_{c_i}} \varphi(t)dt}{(t_{c_i} - t_{e_i})\varphi(t_{e_1})} \tag{11}$$

where α_i denotes the integral performance factor of the i-th DRP, t_{e_i} denotes the start time of destruction of the i-th DRP, and t_{c_i} represents end time of recovery of the i-th DRP.

2) DEGRADATION VELOCITY FACTOR

The degradation velocity factor, β, represents the rate at which the performance decreases during the performance degradation phase. To simplify the representation, the slope of the line connecting the starting point of the performance degradation (the point where the damage event occurs) and the ending point (the lowest point of performance) is used to express the rate of performance degradation. The factor can be expressed mathematically as

$$\beta_i = \frac{\varphi(t_{e_i}) - \varphi(t_{r_i})}{t_{r_i} - t_{e_i}} \tag{12}$$

where β_i is the degradation velocity factor of the i-th DRP and t_{r_i} is the end time of destruction of the i-th DRP.

3) RECOVERY DEGREE FACTOR

The recovery degree factor, γ, is used to measure the degree of performance improvement during the recovery phase

which is equal to the ratio of the performance at the end of recovery to the minimum performance, expressed as

$$\gamma_i = \frac{\varphi(t_{c_i})}{\varphi(t_{r_i})} \tag{13}$$

where γ_i denotes the recovery degree factor of the i-th DRP.

4) RECOVERY TIME FACTOR

Different from the recovery degree factor, the recovery time factor is the measure of the duration from the beginning to the end of system recovery. This factor is expressed as

$$\delta_i = \frac{t_{r_i} - t_{e_i}}{t_{f_i} - t_{r_i}} \tag{14}$$

where δ_i represents the recovery time factor and t_{f_i} denotes the time for performance to recover to the initial level. If the performance fails to recover to its initial level, it is specified that t_{f_i} becomes infinite, resulting in δ_i equal to 0, indicating the poorest recovery capability.

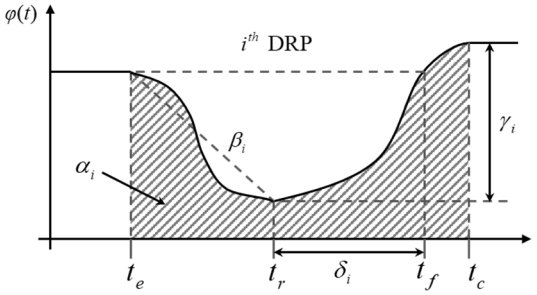

FIGURE 2. Destruction-recovery process (DRP).

Exposed to the complex and volatile battlefield environment, the CSoS suffers damage not in a single instance but recurrently. The structure of CCN iterates in the continuous DRPs, rendering resilience metrics in a single DRP inappropriate. Therefore, it is necessary to provide a resilience measure for multiple DRPs.

As depicted in Fig. 3, within each DRP, the initial occurrence of damage or perturbation to CCN leads to a subsequent decline in performance. Once performance reaches a certain threshold, the CCN initiates its recovery strategy to restore functioning. Following a period of recuperation, another disruption or perturbation arises, marking the commencement of a new iteration of the DRP. The aforementioned cyclic pattern leads to the emergence of multiple consecutive DRPs.

Therefore, by conducting performance simulations or collecting actual operational data for CCN, the time-sequenced vectors of the aforementioned parameters can be obtained and a resilience measurement for multiple DRPs can be provided:

$$\mathcal{R}_{\mathrm{DRP_s}} = M(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\delta}) \tag{15}$$

where $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_n)$, $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_n)$, $\boldsymbol{\delta} = (\delta_1, \delta_2, \ldots, \delta_n)$, and M indicates the method of resilience analysis.

Furthermore, the framework for resilience analysis of the CCN is proposed oriented to multiple DRPs. This framework,

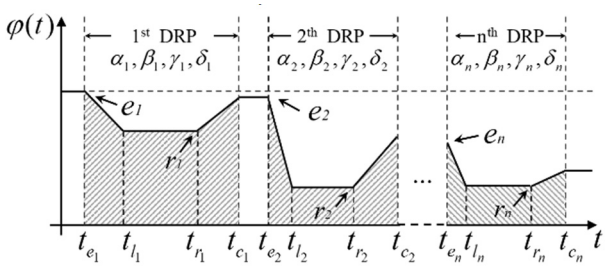

FIGURE 3. Multiple DRPs.

as shown in Fig. 4, delineates the correlation between the multiple DRPs and resilience analysis, providing procedural guidance for resilience simulation analysis of CSoS. The Simulation for DRP of CNN begins with node failures in one layer and ends with the recovery of the nodes after intra-layer node failures and inter-layer node failures. In each iteration of multiple DRPs, the performance metrics proposed are employed to evaluate the performance of CNN. The performance data of CNN for multiple DRPs inputs into the resilience analysis and supports the case study presented in this paper.

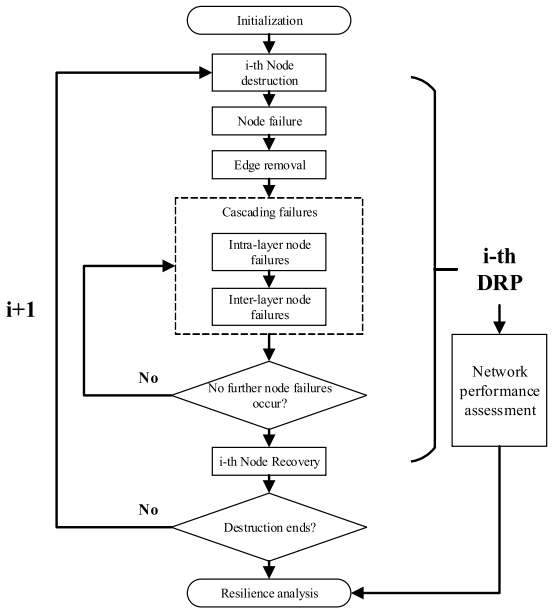

FIGURE 4. Framework of network DRP simulation for resilience analysis.

B. IMPORTANCE-BASED RESILIENCE MODEL

The CSoS is a coupling system with complex compositions and multiple complexities of the environment and external factors. Resilience is a comprehensive representation of system configuration, environmental perturbations, and adaptability, which is influenced by various aspects. The recent research on resilience modeling methods for the CSoS is still scarce. Based on the CCN model of CSoS, the resilience modeling method based on the importance measure

and the correlation between the resilience of layers will be discussed in this section.

The contribution of the equipment is a crucial factor in the design and optimization of the CSoS. Importance measure is a widely used approach for quantifying the contribution of a component to the overall system [33], [34]. The CSoS mainly conducts the operation process of observation, orientation, decision, and action, thus operation layer. The operation layer serves as the core of the CCN model, as it facilitates the operation process encompassing observation, orientation, decision, and action within CSoS. Consequently, the resilience of the operation layer can be considered as the overall resilience of CSoS, which will be influenced by the command layer and logistics layer, as illustrated in Fig. 5.

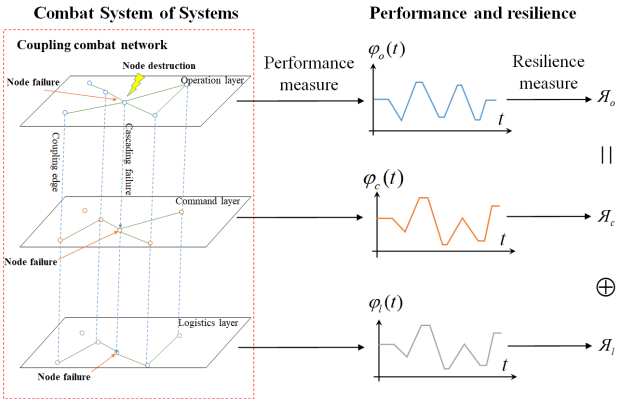

FIGURE 5. Resilience modeling of the CSoS.

The importance measure of network layers' resilience in this study is quantified as the overall improvement in resilience of the operation layer resulting from a specific layer [10], which is composed of direct resilience importance and coupling resilience importance. The direct resilience importance, DIP, is determined by calculating the partial derivative of the operation layer's resilience with respect to the resilience of this layer, as represented in (16) and (17):

$$\mathrm{DIP}_c = \frac{\Delta \mathcal{R}_o}{\Delta \mathcal{R}_c} = \frac{\partial \mathcal{R}_o}{\partial \mathcal{R}_c} \tag{16}$$

$$\mathrm{DIP}_l = \frac{\Delta \mathcal{R}_o}{\Delta \mathcal{R}_l} = \frac{\partial \mathcal{R}_o}{\partial \mathcal{R}_l} \tag{17}$$

where DIP_c and DIP_l represent the importance measure linearly attributed by the command layer and logistics layer, respectively; $\partial \mathcal{R}_o$, $\partial \mathcal{R}_c$ and $\partial \mathcal{R}_l$ are the differential of the operation layer's, command layer's and logistics layer's resilience respectively.

Since there are also interactions between the layers resulting in the resilience contribution of each layer often not being independent, it is necessary to consider the nonlinear part of resilience contribution coupling between the command layer and logistics layer. The coupling resilience importance, CIP, is expressed as

$$\mathrm{CIP} = \frac{\partial \mathcal{R}_o}{\partial (\mathcal{R}_c \mathcal{R}_l)} \tag{18}$$

Therefore, the importance-based resilience model of CCN considering multi-DRP can be represented as

$$\mathcal{R}_o = \mathrm{DIP}_c \times \mathcal{R}_c + \mathrm{DIP}_l \times \mathcal{R}_l + \mathrm{CIP} \times \mathcal{R}_c \mathcal{R}_l + C \tag{19}$$

where $\mathcal{R}_i$ $(i = o, c, l)$ indicates resilience measured by resilience factors (i.e. α, β, γ and δ), with each specific factor of one layer being solely associated with the corresponding factor in another layer and no significant correlation with other resilience factors; C is a constant term representing the inherent resilience of CCN.

The resolution of the resilience model in CCN entails the computation of direct and coupling importance, as well as inherent resilience, by polynomial regression analysis. The importance measures can assume positive values, with higher resilience of the layers resulting in greater resilience of the CCN. Conversely, negative values can also be observed, indicating that higher resilience of layers leads to lower resilience of the CCN. When the importance approaches zero, it suggests that there is no significant relationship between them.

IV. ILLUSTRATIVE EXPERIMENTS

According to the method of coupling combat network modeling, a three-layer CCN for a typical CSoS can be established, as shown in Fig. 6. The command layer exhibits a hierarchical network structure comprising 566 edges, while the logistics layer demonstrates a lattice structure with 139 edges. Additionally, the operation layer manifests as a directed ring network in accordance with the OODA loop.

We will conduct the DRP simulation and analyze the resilience of the above CCN model. The simulation modeled a total of 13 DRPs, with 10 nodes in each DRP being damaged and triggering a series of cascading failures. Note that cascading failure occurs when the failure of a node in one layer results in the subsequent failure of the corresponding node in another interconnected layer. After the destruction, the recovery strategy is conducted to recover nodes that have failed in each time interval and restore the connection relationship between that node and its original neighbors.

With the performance data obtained in the simulation as shown in Fig. 7, we calculate the resilience factors for the operation layer, command layer, and logistics layer separately to support the resilience analysis. Furthermore, the effects of the degree of coupling and recovery strength (i.e., the ratio of the number of nodes recovered to the average number of nodes damaged in each DRP) on the resilience of CCN are also explored.

A. RESILIENCE ANALYSIS OF CCN

Time series of resilience factors in the multiple DRPs are obtained through network simulation, enabling the determination of importance measures for each layer. The trend of the resilience factors for each network layer is shown in Fig. 8.

Obviously, different resilience factors have different trends in the multi-DRP, while the trends of the same resilience factor of different layers demonstrate relatively close alignment. The present finding partially supports the assumption that the

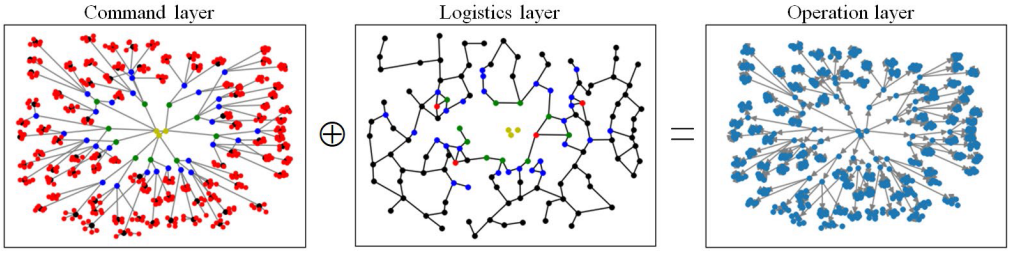

FIGURE 6. The CCN model for a typical CSoS.

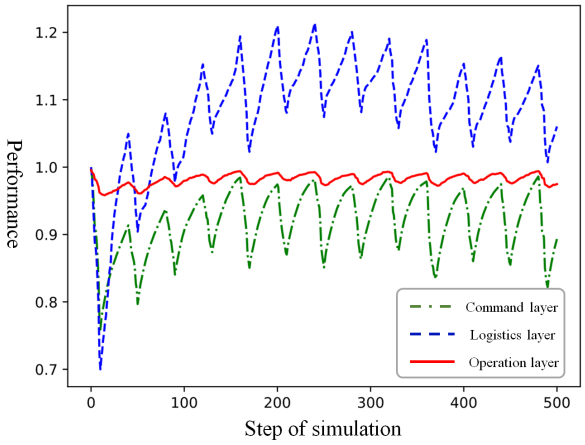

FIGURE 7. The performance of CCN in the simulation.

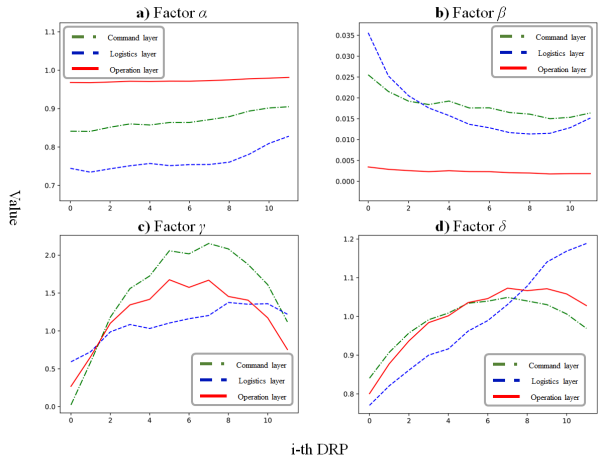

FIGURE 8. The trend of resilience factors for each layer.

resilience factor is associated with its presence in every layer, rather than being influenced by unrelated factors.

The Pearson correlation test is conducted on the resilience factors of the operation layer (i.e. Net_o), command layer (i.e. Net_c) and logistics layer (i.e. Net_l) as shown in Table 1. And it revealed that the correlation coefficients of α, β are higher, while the correlation coefficients of γ, δ are lower. According to the nature of the Pearson correlation coefficient, it is determined that the correlation of γ, δ of Net_l to Net_o is not significant and can be eliminated. Moreover, the multiple linear regression is conducted to obtain the importance of each resilience factor considering the resilience of Net_c, $\mathcal{R}_c$, the resilience of Net_l, $\mathcal{R}_l$, and the product of $\mathcal{R}_c$ and $\mathcal{R}_l$ as independent variables and the resilience of Net_o as dependent variables, results of which are shown in Table 2.

TABLE 1. Correlation table of the resilience factors of each layer.

Resilience factor	Layer	Correlation coefficient	p-value
α	Net_c & Net_l	0.920	2.31×10^{-5}
	Net_c & Net_o	0.994	4.13×10^{-11}
	Net_l & Net_o	0.948	2.80×10^{-6}
β	Net_c & Net_l	0.958	1.01×10^{-6}
	Net_c & Net_o	0.986	4.01×10^{-9}
	Net_l & Net_o	0.911	3.72×10^{-5}
γ	Net_c & Net_l	0.820	1.10×10^{-3}
	Net_c & Net_o	0.973	1.06×10^{-7}
	Net_l & Net_o	0.683	1.44×10^{-2}
δ	Net_c & Net_l	0.627	2.90×10^{-2}
	Net_c & Net_o	0.956	1.24×10^{-2}
	Net_l & Net_o	0.827	8.98×10^{-4}

TABLE 2. Importance of each resilience factor.

Resilience factor	Type of importance	Resilience of network layers	Value of importance
α	DIP	$\mathcal{R}_c$	-0.056
		$\mathcal{R}_l$	-0.244
	CIP	$\mathcal{R}_c\mathcal{R}_l$	0.302
	C	--	1.008
β	DIP	$\mathcal{R}_c$	0.231
		$\mathcal{R}_l$	-0.014
	CIP	$\mathcal{R}_c\mathcal{R}_l$	-0.527
	C	--	-0.001
γ	DIP	$\mathcal{R}_c$	0.647
		$\mathcal{R}_l$	--
	CIP	$\mathcal{R}_c\mathcal{R}_l$	--
	C	--	0.237
δ	DIP	$\mathcal{R}_c$	1.104
		$\mathcal{R}_l$	--
	CIP	$\mathcal{R}_c\mathcal{R}_l$	--
	C	--	-0.089

As a result, the importance-based resilience model of the CCN can be given as

$$\begin{aligned}\alpha_o &= -0.056\alpha_c - 0.244\alpha_l + 0.302\alpha_c\alpha_l + 1.008\\ \beta_o &= 0.231\beta_c - 0.014\beta_l - 0.527\beta_c\beta_l - 0.001\\ \gamma_o &= 0.647\gamma_c + 0.237\\ \delta_o &= 1.104\delta_c - 0.089\end{aligned} \tag{20}$$

The above expression can reveal that the command network offers larger contribution for the resilience factors of β_o, γ_o and δ_o, while the coupling importance and the inherent resilience are larger for α_o.

In addition, there is the condition that the importance of some of the layer resilience terms is negative, which is mainly because the coupling resilience importance is mainly attributed to the resilience of the coupling network in the model fitting. Hence, it is demonstrated that improving the resilience of only one of the network layers is not sufficient to improve the overall resilience, while a higher resilience of the coupling network can be obtained when the resilience of all layers is improved simultaneously.

In addition, the above results indicate that

- Improvements to α should be made for both the command system and the logistics system, such as increasing system membership and improving quality of service;
- Improvements to β should emphasize optimizing the robustness and resistance of the command system, such as adding redundant units and adopting the derating design;
- Improvements to γ require additional recovery resources for the command system, increasing the amount of its performance recovery;
- Improvement of δrequires the optimization of the recovery rate of both the command system and the logistics system.

B. ANALYSIS OF COUPLING DEGREE

This section investigates the influence of the coupling degree, Q_o, on the resilience of the coupling network (i.e. resilience of Net$_o$) by simulation. Fig. 9 represents the variation of each resilience factor in multi-DRP for different degrees of coupling in the form of a heat map.

The impact of coupling degree on various resilience factors varies to different extents, leading to the conclusion that their interrelationships are not uniformly influenced. Among the four resilience factors, the results of α_o, γ_o and δ_o reveal a more obvious negative correlation between resilience and degree of coupling, which indicates that the increase of coupling edges will make the resilience decrease significantly. In contrast, for β_o, no significant effect of coupling degree on the resilience is shown. This indicates that the rate of performance degradation is not sensitive to the degree of coupling when the system is subjected to damage. Among the four resilience factors, α_o exhibits a more significant negative correlation with degree of coupling as seen in Fig. 9. Therefore, in the design of CSoS, it is recommended to minimize coupling among equipment platforms and enable them to operate independently.

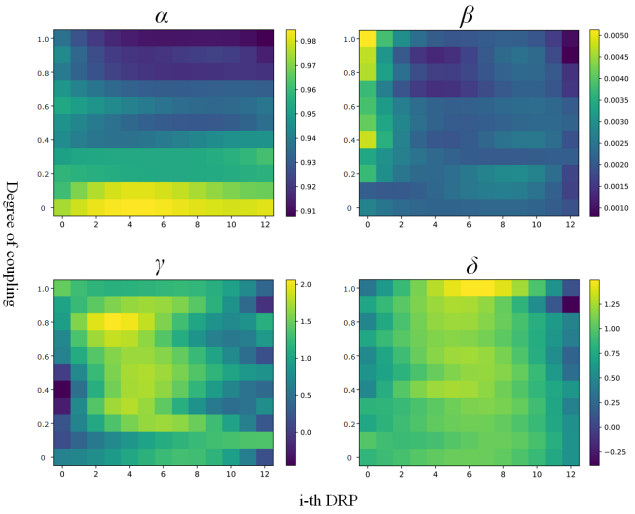

FIGURE 9. Correlation between resilience and degree of coupling.

C. ANALYSIS OF RECOVERY STRENGTH

Recovery, as a pivotal driver of the destruction-recovery process, exerts significant influence on resilience. This section specifically studies the resilience under different recovery strengths (i.e. the ratio of the average number of the restored nodes to the average number of the destroyed nodes in each DRP) as shown in Fig. 10. The result reveals that different resilience factors respond differently to the recovery strength, yet with the increase of recovery strength, each resilience factor appears to increase in different magnitudes. With the increase of recovery strength, resilience factors all showed different degrees of increase, among which the α_o and β_o are significantly enhanced with the increase of recovery strength. This indicates that the system has a significant improvement in its average performance and the rate of performance declining in the DRP when the recovery strength increases. There was no significant trend in γ_o for the recovery strength, but it is observed that a higher level of γ_o occurs in some cases at recovery strengths of 4 and 5. α_o reveals a more obvious trend as the multi-DRP advances, and the recovery strength varies, and the positive correlation between the recovery strength and α is relatively strong.

The recovery strength of the network stands out as the primary determinant of resilience in the CSoS, exerting the most significant influence among various contributing factors. When CSoS does not have any ability to recover, it quickly tends to collapse in the multi-DRP. Whereas, when the recovery strength surpasses the destruction strength, the CSoS can achieve a remarkable level of performance, exhibiting excellent vitality and survivability.

V. DISCUSSION

The analysis results of the above resilience simulation for the CCN model can be summarized as the following four points.

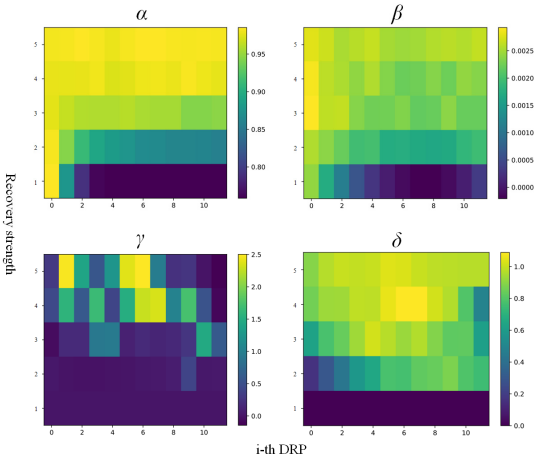

FIGURE 10. Influence of recovery strength on resilience.

(1) The resilience factors have different representations in the multi-DRP. In this paper, the integral performance factor, degradation velocity factor, recovery degree factor, and recovery time factor are examined as the four aspects of resilience. Among them, the integral performance factor and degradation velocity factor usually show monotonic trends with the progression of multi-DRP, while the recovery time factor and recovery degree factor show an increasing and then decreasing trend.

(2) The degree of coupling affects different resilience factors to varying extents. Among the four resilience factors, α , γ and δ gradually decrease with the increase of coupling degree, which indicates that the increase of coupling will significantly reduce the average performance, recovery efficiency, and recovery effect of the system, thus leading to the CSoS with lower resilience. When establishing a CSoS, it is imperative to minimize coupling between network layers and ensure the autonomy of system members.

(3) Among the various factors influencing resilience investigated, the recovery strength of the network exerts the most significant influence on the CSoS. In the absence of any recovery capability, the CSoS tends to rapidly collapse under continuous attacks; however, when the recovery strength surpasses its destruction strength, the CSoS is capable of maintaining a high level of operational performance.

VI. CONCLUSION

Aiming at the coupling and multi-DRP issues of the research on resilience of the CSoS, this paper proposes the CCN model that captures the interdependencies and interactions among the elements of the CSoS. Moreover, the multiple destruction-recovery processes and the coupling correlation of resilience in the CSoS are also investigated based on the CCN model, which provide a valuable reference for resilience studies in the context of CSoS.

Firstly, this paper introduces a modeling method for the CSoS based on the coupling network, which encompasses the model of network topology and measure of network performance, thereby providing an abstracted model for investigating the resilience issues associated with coupling in the CSoS. Additionally, we propose a resilience evaluation method for multiple DRPs that incorporates continuous measurement of individual resilience over time. This approach enables the application of the resilience metric to continuous damage scenarios and expands the temporal dimension of existing CSoS resilience research. Furthermore, the paper introduces the concept of network component importance into resilience research of coupling resilience and investigates the relationship among the resilience of each layer. Ultimately, a case study of a typical CSoS is presented to illustrate the impact of the command layer, logistics layer, and their coupling relationship on the overall resilience of CSoS.

As a result, the findings in this paper provide useful insights for designing a more resilient CSoS. However, this paper has identified several limitations that could be addressed in future research. Firstly, the development of a comprehensive resilience characteristic of a given CSoS could be achieved through a multi-factor resilience model, with varying levels assigned to each resilience factor in different contextual scenarios. This would facilitate the structure design of CSoS and optimization of resilience strategies. Furthermore, the structure of CSoS that was studied consists solely of command layer, logistics layer, and operation layer, without delving into the ramifications of coupling more layers. Therefore, the resilience of CSoS with more complex coupling is also a promising research topic.

REFERENCES

[1] M. Gong, L. Ma, Q. Cai, and L. Jiao, "Enhancing robustness of coupled networks under targeted recoveries," *Sci. Rep.*, vol. 5, no. 1, Feb. 2015, Art. no. 08439, doi: 10.1038/srep08439.

[2] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 69, no. 4, Art. no. 045104, doi: 10.1103/physreve.69.045104.

[3] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010, doi: 10.1038/nature08932.

[4] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of a network of networks," *Phys. Rev. Lett.*, vol. 107, no. 19, 2011, Art. no. 195701, doi: 10.1103/physrevlett.107.195701.

[5] Q. Han, B. Pang, S. Li, N. Li, P.-S. Guo, C.-L. Fan, and W.-M. Li, "Evaluation method and optimization strategies of resilience for air & space defense system of systems based on kill network theory and improved self-information quantity," *Defence Technol.*, vol. 21, pp. 219–239, Mar. 2023, doi: 10.1016/j.dt.2023.01.005.

[6] L. Ma, X. Zhang, J. Li, Q. Lin, M. Gong, C. A. C. Coello, and A. K. Nandi, "Enhancing robustness and resilience of multiplex networks against node-community cascading failures," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 6, pp. 3808–3821, Jun. 2022, doi: 10.1109/TSMC.2021.3073212.

[7] D. Duan, C. Lv, S. Si, Z. Wang, D. Li, J. Gao, S. Havlin, H. E. Stanley, and S. Boccaletti, "Universal behavior of cascading failures in interdependent networks," *Proc. Nat. Acad. Sci. USA*, vol. 116, no. 45, pp. 22452–22457, Nov. 2019, doi: 10.1073/pnas.1904421116.

[8] G. Bai, Y. Li, Y. Fang, Y.-A. Zhang, and J. Tao, "Network approach for resilience evaluation of a UAV swarm by considering communication limits," *Rel. Eng. Syst. Saf.*, vol. 193, Jan. 2020, Art. no. 106602, doi: 10.1016/j.ress.2019.106602.

[9] Z. Chen, T. Zhao, J. Jiao, and J. Chu, "Performance-threshold-based resilience analysis of system of systems by considering dynamic reconfiguration," *Proc. Inst. Mech. Eng., B, J. Eng. Manuf.*, vol. 236, no. 14, pp. 1828–1838, Dec. 2022, doi: 10.1177/0954405420937528.

[10] P. Xing, W. Huixiong, Y. Yanjing, and Z. Guozhong, "Resilience based importance measure analysis for SoS," *J. Syst. Eng. Electron.*, vol. 30, no. 5, pp. 920–930, Oct. 2019, doi: 10.21629/JSEE.2019.05.10.
[11] Q. Feng, X. Hai, B. Sun, Y. Ren, Z. Wang, D. Yang, Y. Hu, and R. Feng, "Resilience optimization for multi-UAV formation reconfiguration via enhanced pigeon-inspired optimization," *Chin. J. Aeronaut.*, vol. 35, no. 1, pp. 110–123, Jan. 2022, doi: 10.1016/j.cja.2020.10.029.
[12] Q. Sun, H. Li, Y. Wang, and Y. Zhang, "Multi-swarm-based cooperative reconfiguration model for resilient unmanned weapon system-of-systems," *Rel. Eng. Syst. Saf.*, vol. 222, Jun. 2022, Art. no. 108426, doi: 10.1016/j.ress.2022.108426.
[13] H. Li, Q. Sun, Y. Zhong, Z. Huang, and Y. Zhang, "A soft resource optimization method for improving the resilience of UAV swarms under continuous attack," *Rel. Eng. Syst. Saf.*, vol. 237, Sep. 2023, Art. no. 109368, doi: 10.1016/j.ress.2023.109368.
[14] C. S. Holling, "Resilience and stability of ecological systems," in *The Future of Nature: Documents of Global Change*. New Haven, CT, USA: Yale University Press, 2013, doi: 10.12987/9780300188479-023.
[15] J. Gao, B. Barzel, and A.-L. Barabási, "Universal resilience patterns in complex networks," *Nature*, vol. 530, no. 7590, pp. 307–312, Feb. 2016, doi: 10.1038/nature16948.
[16] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Rel. Eng. Syst. Saf.*, vol. 145, pp. 47–61, Jan. 2016, doi: 10.1016/j.ress.2015.08.006.
[17] B. Allenby and J. Fink, "Toward inherently secure and resilient societies," *Science*, vol. 309, no. 5737, pp. 1034–1036, Aug. 2005, doi: 10.1126/science.1111534.
[18] D. Henry and J. Emmanuel Ramirez-Marquez, "Generic metrics and quantitative approaches for system resilience as a function of time," *Rel. Eng. Syst. Saf.*, vol. 99, pp. 114–122, Mar. 2012, doi: 10.1016/j.ress.2011.09.002.
[19] H. Baroud, K. Barker, J. E. Ramirez-Marquez, and C. M. Rocco, "Inherent costs and interdependent impacts of infrastructure network resilience," *Risk Anal.*, vol. 35, no. 4, pp. 642–662, Apr. 2015, doi: 10.1111/risa.12223.
[20] A. Shafieezadeh and L. Ivey Burden, "Scenario-based resilience assessment framework for critical infrastructure systems: Case study for seismic resilience of seaports," *Rel. Eng. Syst. Saf.*, vol. 132, pp. 207–219, Dec. 2014, doi: 10.1016/j.ress.2014.07.021.
[21] B. Yang, L. Zhang, B. Zhang, Y. Xiang, L. An, and W. Wang, "Complex equipment system resilience: Composition, measurement and element analysis," *Rel. Eng. Syst. Saf.*, vol. 228, Dec. 2022, Art. no. 108783, doi: 10.1016/j.ress.2022.108783.
[22] M. Bruneau, S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. von Winterfeldt, "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthq. Spectra*, vol. 19, no. 4, pp. 733–752, Nov. 2003.
[23] H. T. Tran, M. Balchanos, J. C. Domerçant, and D. N. Mavris, "A framework for the quantitative assessment of performance-based system resilience," *Rel. Eng. Syst. Saf.*, vol. 158, pp. 73–84, Feb. 2017, doi: 10.1016/j.ress.2016.10.014.
[24] Q. Sun, H. Li, Y. Zhang, Y. Xie, and C. Liu, "A baseline assessment method of UAV swarm resilience based on complex networks," in *Proc. IEEE 19th World Symp. Appl. Mach. Intell. Informat. (SAMI)*, Jan. 2021, pp. 000083–000086, doi: 10.1109/SAMI50585.2021.9378640.
[25] Y. Cheng, E. A. Elsayed, and Z. Huang, "Systems resilience assessments: A review, framework and metrics," *Int. J. Prod. Res.*, vol. 60, no. 2, pp. 595–622, Jan. 2022, doi: 10.1080/00207543.2021.1971789.
[26] W. Yunming, C. Si, P. Chengsheng, and C. Bo, "Measure of invulnerability for command and control network based on mission link," *Inf. Sci.*, vol. 426, pp. 148–159, Feb. 2018, doi: 10.1016/j.ins.2017.10.035.
[27] M. F. Ling, T. Moon, and E. Kruzins, "Proposed network centric warfare metrics: From connectivity to the OODA cycle," *Mil. Oper. Res.*, vol. 10, no. 1, pp. 5–13, Dec. 2005, doi: 10.5711/morj.10.1.5.
[28] J. Li, B. Ge, K. Yang, Y. Chen, and Y. Tan, "Meta-path based heterogeneous combat network link prediction," *Phys. A, Stat. Mech. Appl.*, vol. 482, pp. 507–523, Sep. 2017, doi: 10.1016/j.physa.2017.04.126.
[29] J. Li, D. Zhao, J. Jiang, K. Yang, and Y. Chen, "Capability oriented equipment contribution analysis in temporal combat networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 2, pp. 696–704, Feb. 2021, doi: 10.1109/TSMC.2018.2882782.
[30] C. M. Schneider, N. Yazdani, N. A. M. Araújo, S. Havlin, and H. J. Herrmann, "Towards designing robust coupled networks," *Sci. Rep.*, vol. 3, no. 1, Jun. 2013, Art. no. 01969, doi: 10.1038/srep01969.
[31] L. M. Shekhtman, M. M. Danziger, and S. Havlin, "Recent advances on failure and recovery in networks of networks," *Chaos, Solitons Fractals*, vol. 90, pp. 28–36, Sep. 2016, doi: 10.1016/j.chaos.2016.02.002.
[32] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Phys. Rev. Lett.*, vol. 87, no. 19, Oct. 2001, Art. no. 198701, doi: 10.1103/physrevlett.87.198701.
[33] K. Barker, J. E. Ramirez-Marquez, and C. M. Rocco, "Resilience-based network component importance measures," *Rel. Eng. Syst. Saf.*, vol. 117, pp. 89–97, Sep. 2013, doi: 10.1016/j.ress.2013.03.012.
[34] C. D. Nicholson, K. Barker, and J. E. Ramirez-Marquez, "Flow-based vulnerability measures for network component importance: Experimentation with preparedness planning," *Rel. Eng. Syst. Saf.*, vol. 145, pp. 62–73, Jan. 2016, doi: 10.1016/j.ress.2015.08.014.

YUHENG DANG received the B.S. degree in aircraft quality and reliability and the M.S. degree in safety science and engineering from Beihang University (BUAA), Beijing, China, in 2020 and 2023, respectively, where he is currently pursuing the Ph.D. degree in safety science and engineering with the School of Reliability and Systems Engineering. His research interests include resilience modeling and assessment and optimization for complex networks.

HUIXIONG WANG received the B.S. degree in aircraft quality and reliability and the M.S. degree in control science and engineering from Beihang University (BUAA), Beijing, China, in 2018 and 2021, respectively. He is currently pursuing the Ph.D. degree with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. His research interests include system engineering and complex networks.

ZIMENG YIN received the B.S. degree in aircraft quality and reliability and the M.S. degree in control science and engineering from Beihang University (BUAA), Beijing, China, in 2010 and 2013, respectively. He is currently with China Academy of Launch Vehicle Technology, Beijing, China. His research interests include system engineering and equipment reliability.

XING PAN (Member, IEEE) was born in 1979. He received the B.S. degree in mechanical engineering and the Ph.D. degree in systems engineering from Beihang University (BUAA), Beijing, China, in 2000 and 2005, respectively. From 2005 to 2009, he was an Assistant Professor with the School of Reliability and Systems Engineering, BUAA, where he has been an Associate Professor, since 2009, and has been a Professor, since 2020. From 2012 to 2013, he was a Visiting Scholar with the Department of Systems and Industrial Engineering, University of Arizona, Tucson, AZ, USA. He is currently the Head of the Department of Safety Science and Engineering, School of Reliability and Systems Engineering. His research interests include reliability engineering, systems engineering, and system risk analysis.