Article

Complex Network-Based Resilience Capability Assessment for a Combat System of Systems

Wenyu Chen 1,2, Weimin Li 2 and Tao Zhang 2,*

1 Graduate Collage, Air Force Engineering University, Xi’an 710051, China; lorilouto_cwy@163.com
2 Air and Missile Defense College, Air Force Engineering University, Xi’an 710051, China
* Correspondence: zhangtao2016@163.com

Abstract: With the increasing complexity and frequency of interactions among a large number of heterogeneous nodes within a combat system of systems (SoS), evaluating the capability of the SoS to withstand external attacks and interferences has become an increasingly challenging and urgent issue. However, the complexity of a combat SoS often brings about difficulties in quantitative analysis. This paper proposes a method to assess the resilience of a combat SoS. Firstly, a network model of a combat SoS is constructed, taking into account multi-functional composite nodes. Secondly, the combat capability model of the combat SoS is built based on the capabilities of the kill chains and kill networks. Lastly, an approach is proposed to calculate the combat capability of the system based on the network’s two-terminal connectivity. Moreover, based on the SoS’s combat capability, the resilience is analyzed from the dimensions of anti-destruction, survival, and recovery. The simulation experiments show that, compared to other methods, the method in this paper for calculating the combat capability of the combat SoS does not depend on the number of kill chains and aligns with the combat processes and actual patterns. Additionally, the resilience measurement method can effectively analyze its capability to cope with external interferences.

Keywords: combat system of systems; resilience; complex network; kill chain

1. Introduction

In the context of the information and intelligence era, the concept of the “interconnection of everything” has emerged as the driving force behind development, promoting advancements in productive forces and significantly impacting the dynamics of modern combat success. The modern combat system of systems (SoS) comprises numerous combat elements, and the growingly interrelated “interconnection, intercommunication, and interoperability” among these elements considerably enhances the combat SoS’s capability. From a microscopic viewpoint, the material, information, and energy flow efficiently intermingle among diverse combat elements, engendering interactive influences among them. From a macroscopic viewpoint, the combat SoS manifests intricate cascading and emergent, nonlinear, and collapsing features, markedly complicating the assessment of the combat capabilities. Due to the inability to statically display the macroscopic characteristics of the combat SoS and their nonconformity with the general principle of linear superposition, static analytical evaluation methods become inadequate. Furthermore, the combat SoS’s complexity and the diversity of its elements present greater challenges in constructing evaluation models and examining the combat SoS’s dynamic features.

Commanders and decision-makers are increasingly concerned about whether a combat SoS, driven by complex interactive relationships, poses the essential capability to accomplish tasks, adapt to damage, and recover in the face of external impacts. These capabilities demonstrate the combat SoS’s resilience. Resilience refers to a system’s or entity’s ability to, despite facing external impacts, still provide the necessary functions for tasks and restore overall functionality through the reconstruction and recovery of internal elements.
A modern combat SoS is characterized by diverse and heterogeneous internal elements, complex interactive relationships between elements, and inherent passivity when involved in defensive combat tasks. Therefore, evaluating the resilience of a combat SoS to external interference and strikes has become a challenging and urgent issue.

With combat SoS increasingly displaying networked characteristics, abstracting them into a networked model and applying complex network theory to evaluating its combat capabilities is gaining acceptance among more scholars, gradually emerging as a novel method for assessing the system’s combat capabilities. Complex network theory can effectively analyze the dynamic and complex characteristics of a SoS and has become an important analytical method [1]. Studies on evaluating combat SoS based on complex networks primarily center on analyzing the system’s resilience to destruction [2,3], assessing the importance of system nodes [4–6], determining the system contribution rates [7,8], and evaluating the combat capabilities [9]. However, there is currently limited research on assessing the overall resilience of a combat SoS.

The evaluation of the resilience of a combat SoS needs to be based on the SoS’s operational capability. In practice, however, the SOS capability involves a complex open system that requires a systems approach and tools to recognize [10–12]. In the current research, the mainstream method for calculating the combat capability of a SoS is based on the number of kill chains. Reference [13] calculates the combat capability of the SoS based on the number of kill chains and subsequently analyzes the resilience through the changes in its combat capability. Other references that calculate the combat capability of a SoS based on the number of kill chains include references [14–16].

In fact, the number of kill chains that a SoS can form cannot fully describe the combat capability of the SoS, as the combat capability of the SoS often focuses more on the effective kill scale that one side of the SoS can achieve against the other. On the one hand, using only the number of kill chains cannot describe the extent of damage inflicted on the enemy SoS, as many kill chains may target the same target node, and there may be many common nodes between multiple kill chains. When the common nodes fail, this leads to the disruption of many kill chains, making the SoS inherently vulnerable, regardless of the high number of kill chains based on the common nodes. Therefore, a method based on the number of kill chains is not suitable for calculating the capability of the combat system.

The resilience capability differs from static combat capability, as it primarily captures the dynamic response of the system to external disturbances and impacts, which delineates the system’s adaptability and recovery capacity in the face of external interference. A deep understanding of the inherent nature can only be achieved through the analysis of the system’s dynamic behavior.

In response to the above problems, this study examines the effects of external factors on the capabilities of a combat SoS and proposes to characterize the resilience in terms of anti-destruction, survival, and recovery capability. The analysis involves the construction of a combat network model, which abstracts the interconnected interactions between combat elements as nodes and edges, with the performance indicators of combat elements being used to gauge their fulfillment of basic tasks within this model. The paper also presents a quantitative approach to assessing a SoS’s combat capability through the establishment of kill chain and kill network capabilities. In comparison with other research, the proposed system combat capability model aligns more closely with the processes and characteristics of system combat, making it highly relevant for enhancing system resilience and conducting resilience assessments for combat SoS. Moreover, based on the proposed system combat capability calculation model, resilience calculation models for anti-destruction, survival, and recovery capability are constructed, with simulation experiments examining the SoS’s resilience under varying attack strategies to validate the method’s effectiveness. This article primarily comprises an analysis of resilience elements and models, the development of a network model for a combat SoS, quantification of the kill chain and kill network capabilities, and analysis of simulation experiments.
2. Analysis of Elements of Combat SoS Resilience

The concept of resilience originally emerged in the field of materials, denoting a material’s capacity to revert to its original form after enduring external forces. As comprehension of the research subjects across disciplines deepened, the concept of “resilience” continuously evolved and expanded, becoming a prominent feature across various research domains. In 1973, Holling systematically elucidated the resilience of ecological systems in his paper [17], defining it as the ability of an ecological system to endure external disruptions without collapsing, gradually restoring itself. Subsequently, the integration of resilience into the realm of social ecology gained widespread acceptance. This concept was swiftly incorporated into the realms of engineering technology and military. The resilience of engineering and weapon systems has evolved into a pivotal measure of overall equipment performance. In 2011, the US Department of Defense launched a project to establish adaptable resilient engineering systems within the context of weapon equipment system construction. Likewise, the US military accentuated the resilience of space systems [18], officially defining resilience as “the capability of a type of structural system to provide the necessary functions even under adversarial actions or adverse conditions”. By 2013, the US Joint Military Operations Research Society delineated resilience as the capability of an entity to prevent, resist, absorb, respond to, and adapt to external disruptions while maintaining its fundamental structure and function.

In recent years, there has been a notable surge in interest among military researchers in the development of adaptable combat SoS, making research on resilience a prominent area within the field of military system engineering. In the context of evolving combat strategies, the pursuit of distributed and decentralized combat elements has become a key winning mechanism. This involves forming system synergy through functional decoupling and dynamic reorganization. In scenarios where combat elements are destroyed or fail, an elastic hinge bridging approach is employed to construct a highly elastic and self-healing wide area kill chain, thereby creating an elastic combat SoS. Notably, the US military has embraced concepts such as “mosaic warfare”, “kill chain”, and “joint all-domain operations”, serving as quintessential examples in this regard. Consequently, resilience has emerged as a dependable approach to a combat SoS to confront uncertain threats and generate system synergy.

The resilience of a combat SoS is primarily evidenced in the following ways:

1. Despite external strikes or disruptions, the combat SoS retains the ability to fulfill its mission and maintain its fundamental capabilities.
2. When certain combat elements are damaged or fail, resulting in a reduction in the SoS’s capability, the combat SoS can progressively restore and enhance its overall capability using strategies such as element repair, reconstruction, and dynamic adjustment.

It is evident that resilience serves as a comprehensive performance indicator. As the number of elements within the combat SoS increases and their interactions become more intricate, assessing the system’s capabilities becomes increasingly complex. Can the current combat SoS withstand enemy strikes? Will it succumb to these strikes? Can the system’s capabilities be reinstated through the repair of its combat elements, thereby achieving subsequent essential tasks? These are crucial questions that must be addressed through an assessment of the combat SoS’s resilience.

This article posits that the resilience of a combat SoS is crucial for maintaining and restoring the combat capability of the system after it is subjected to influence, suppression, or attack by hostile forces. As illustrated in Figure 1, all external interferences, suppressions, and attacks experienced by a combat SoS are classified as “influences” [19]. The impact on the combat SoS unfolds in three stages: the unimpacted stage, impacted stage, and impact elimination stage.
In Figure 1, $C(T)$ denotes the SoS’s capability at $T$, while $C_{kt}(T)$ represents the essential capability necessary for the mission fulfillment, referred to as the task baseline. $t_0$ marks the initial moment, while $t_r$ represents the onset of the system impact. $t_f$ signifies the point at which the SoS’s combat capability declines to the task baseline. If the SoS combat capability falls below the task baseline, it indicates the SoS’s inability to carry out its mission. $t_m$ is the moment when the combat SoS’s capability reaches its lowest level, $t_r$ represents the moment that the SoS’s combat capability gradually recovers to the task baseline, and $t_s$ denotes the time at which the SoS’s combat capability is restored to its original level. Of course, not all of the SoS’s recovery capabilities are sufficient to restore the SoS capability to its original level, in which case $t_s$ can make choices based on the actual situation.

The resilience of the combat SoS manifests itself in different forms at various time stages. In $[t_0, t_f)$, resilience primarily lies in the system’s capability to accomplish its mission despite attacks, thus averting the rapid deterioration of its overall capability. Despite the decline in combat capability in this phase, it still satisfies the fundamental mission requirements and remains above the task baseline. This phase is commonly denoted as the anti-destruction phase. During $[t_f, t_m)$, the combat capability declines further below the task baseline due to the cumulative impact of the enemy influence. Despite failing to meet the basic mission requirements, the system does not entirely collapse or become ineffective. Resilience is exemplified by hindering additional degradation of its overall capability by repairing specific combat elements; this phase is the survive phase. In $[t_m, t_s)$, resilience primarily encompasses the recovery and restoration of the SoS’s capability. The capability rebounds from its lowest point and gradually restores to the level of executing basic missions, or even surpasses its initial level due to internal repair and reconstruction of the system [19].

The expressions of the three capabilities are as follows:

**Definition 1.** Anti-destruction capability $C_K$.

From the moment the combat SoS encounters enemy attacks, the overall combat capability of the system will continue to decline. However, the system’s resilience will prevent a rapid decline in its capability, ensuring that the system can still meet the basic mission requirements and maintain the SoS’s combat capability above the task baseline. The task baseline capability represents the minimum capability required to fulfill the mission tasks. This paper posits that the anti-destruction capability stems from the components’ ability to resist destruction, maintaining a certain level of combat capability even after
sustaining damage. Additionally, it originates from the pre-deployed backup kill chains within the system. Even if some of these chains are disrupted due to damage and cannot fulfill the mission tasks, other pre-deployed kill chains can be swiftly adjusted to substitute for the damaged ones, compensating for the loss in functionality and ensuring the overall completion of the combat tasks. The accumulation of the SoS’s combat capability during the resistance phase is used to depict its resilience, and the mathematical model is given by

\[ C_K = \int_{t_e}^{t_f} C(T)dt \]  

Equation (1) physically represents the area enclosed by the SoS’s capability and the timeline in the anti-destruction phase. A larger area suggests a less severe degradation of the system’s overall capability during this phase, signifying the stronger anti-destruction capability of the combat SoS.

**Definition 2. Survival capability \( C_W \).**

The survival capability is primarily demonstrated when the capability of the SoS is lower than the task baseline requirements. After being attacked by the enemy, numerous nodes and edges within the combat SoS lose their functionality. The survive capability further resists subsequent external impacts and adapts to the damage caused by the attack, preventing a further decline in the capability and avoiding complete failure. The survival capability comes from two aspects: on the one hand, partially damaged nodes begin to restore their functionality through repairs, and on the other hand, there are still some redundant kill chains within the SoS capable of completing certain combat missions. Although they cannot meet the combat mission requirements, the SoS still possesses the ability to strike and deter the enemy. The accumulation of the SoS’s combat capability during the survival phase is used to describe the survival capability: the mathematical model is

\[ C_W = \int_{t_f}^{t_m} C(T)dt \]  

Similar to the physical meaning of the anti-destructive capability, Equation (2) represents the area enclosed by the SoS’s combat capability and the timeline in the survival phase. The larger the area, the milder the degradation of the system’s overall capability during this phase, indicating a stronger survival capability of the combat SoS.

**Definition 3. Recovery capability \( C_R \).**

Recovery capability refers to the SoS’s capability to recover to the task baseline level or even normal levels after it has decreased to the lowest point. This recovery is achieved using measures such as node repair and reconstruction. The primary source of the recovery capability lies in the repair of damaged nodes. As more nodes regain normal functionality, the SoS’s combat capability will rise again. Therefore, the recovery capability mainly depends on the speed of node repair. The accumulation of the SoS’s combat capability during the recovery phase is used to describe the recovery capability: the mathematical model is

\[ C_R = \int_{t_m}^{t_s} C(T)dt \]  

Similarly, Equation (3) represents the area enclosed by the SoS’s capability and the timeline in the recovery phase. The larger the area, the better the performance in the recovery of the SoS, indicating a stronger resilience of the combat SoS.

**Definition 4. Resilience \( R \).**
The overall resilience of the combat SoS is a comprehensive reflection of the anti-
destruction, survival, and recovery capability. Combined with Figure 1, this paper defines
the overall resilience of the system as

$$R = C_K + C_W + C_R = \int_{t_s}^{t_f} C(T)\,dt$$  \hspace{1cm} (4)$$

Equation (4) represents the area enclosed by the SoS’s combat capability and the
timeline from the initial moment of encountering the influence until the moment when the
SoS’s capability is restored. Generally speaking, setting \(t_s\) is not strictly required and can
be determined by the actual combat analysis. It can be seen that the key to quantitative
analysis of the resilience is to obtain the SoS’s combat capability \(C(T)\). The following section
will provide a detailed introduction.

3. Construction of a Networked Model for a Combat SoS

3.1. Combat Network Modeling

3.1.1. Node Modeling of a Combat Network

The networked characteristics presented by modern combat SoS provide the basis for
building a networked combat model. The nodes of these combat models are abstracted from
combat elements with independent functionalities, such as weaponry and equipment units
and task forces, and abstracted from the interrelationships between the combat elements.
Many researchers have abstracted combat elements into different types of network nodes
based on their functionalities: the most widely used is the Information Age Combat Model
proposed by American scholar Cares [20,21]. The OODA loop (Observation, Orientation,
Decision, Action) is a concept in military strategy, initially developed by US Air Force
officer John Boyd in the 1950s. The theory emphasizes rapid, agile, and flexible responses
to enemy actions in order to gain advantage in combat. According to the functionalities
of the combat elements in the OODA loop, the model of Cares abstracts the combat
elements into reconnaissance nodes, decision-making nodes, effect nodes, and target nodes,
and it has been widely applied [14]. This model effectively describes the heterogeneity
and complexity of combat networks, which distinguishes them from general networks.
However, it tightly couples the combat elements with specific functionalities, so it is not
suitable for modeling multi-functional composite nodes such as integrated reconnaissance
strike drones, which simultaneously have reconnaissance and strike capabilities. Cares’
model can only abstract these as reconnaissance nodes or effect nodes. Similarly, warning
aircraft with both reconnaissance and command control functions cannot be fully described
by Cares’ model.

To express the multi-functional combat elements more clearly, this paper improves
Cares’ model by considering composite functional nodes when constructing the node type
model. Simultaneously, the paper establishes the nodes’ functional models and maps the
node type model to the functional model, distinguishing different application scenarios
and facilitating subsequent analysis of the impact of the nodes on the combat capability of
the system.

In the combat SoS, the combat elements can be classified into the following three
categories based on their functionalities:

- **Observation function (O):** The function of implementing early warnings, detection,
  reconnaissance, and surveillance missions on enemy targets;

- **Decision function (D):** The function of analyzing and processing reconnaissance and
  early warning information, undertaking decision analysis, and issuing combat orders;

- **Action function (A):** The function of conducting firepower strikes and electronic
  jamming on enemy targets.

According to the types of functionalities that the nodes possess, the nodes can be
divided into the following seven categories:

- **Sensor nodes (S),** combat elements that only possess observation functions;
Command and control (C2) nodes (C), combat elements that only possess decision functions;
Influence nodes (I), combat elements that only possess action functions;
Sensor–command and control composite nodes (SC), combat elements that possess both observation and decision functions;
Sensor–influence composite nodes (SI), combat elements that possess both observation and action functions;
Sensor–C2–influence composite nodes (SCI), combat elements that possess observation, decision, and action functions;
Enemy target nodes (T), which mainly refer to all enemy nodes.

The mapping relationship between node types and functions is shown in Figure 2 below:

**Figure 2.** Node types and function mapping relationships.

\[ V_{\text{type}} = \left\{ v^1_{\text{type}}, v^2_{\text{type}}, \ldots, v^j_{\text{type}} \right\} \]

represents a set of nodes of the same type, \( \text{type} \in \{S, C, I, SC, SI, SCI, T\} \) represents the node type, and 1, 2, \( \ldots, j \) represent the order of the node in the set. For example, the element \( v^i_{\text{type}} \) represents the \( i \)th sensor type node, while \( N_{\text{type}} = \left\{ n^1_{\text{type}}, n^2_{\text{type}}, \ldots, n^j_{\text{type}} \right\} \) represents a set of nodes with the same function, with the subscript \( \text{type} \in \{O, D, A\} \) representing the function type and the superscript 1, 2, \( \ldots, j \) representing the order of the node in the set of nodes with the same function.

The opposing sides are divided into the red side and blue side. RS, RC, and RI can, respectively, represent the red side sensor-type nodes, red side command-and-control-type nodes, and red side effect-type nodes, with similar representation methods for other nodes, which will not be elaborated on further.

The node set can be represented either by node type or node function. It can be represented as a set of nodes with different node types as

\[ V = V_R \cup V_B \]  

(5)

In Equation (5), \( V_R = \{V_{RS} \cup V_{RC} \cup V_{RI} \cup V_{RSC} \cup V_{RSI} \cup V_{RSCI} \} \) represents the set of red nodes; \( V_B = \{V_{BS} \cup V_{BC} \cup V_{BI} \cup V_{BSC} \cup V_{BSI} \cup V_{BSCI} \} \) represents the set of blue nodes; \( |V| = |V_B| + |V_R| \) represents the total number of nodes for both the red and blue sides, where \( |V_{\text{type}}| \) represents the number of nodes of type; and when analyzing problems from the perspective of the red side, all the nodes on the blue side are uniformly considered as target-type nodes, that is, \( V_T = V_B \).

It should be noted that this paper assumes that different functions of composite nodes are mutually independent, and different functions do not affect each other. Only when a node is destroyed or fails due to unreliability will all its functions disappear simultaneously. The capability of a node to perform its functions under normal conditions can be described by its reliability, which represents the probability of a node to function normally, denoted as \( C_{\text{type}} \), and is typically obtained from the reliability data of the combat elements.
In other cases, unless otherwise specified, this paper considers a composite node that performs a certain function as a single-type node that performs the same function, and uses this function to represent the type of the composite node. For example, when an SC node provides early warning information to other nodes, it only performs its observation function, and it can be considered an O functional node.

3.1.2. Edge Modeling of the Combat Network

The edges of the network are abstracted from the interaction relationships of the combat elements. According to the analysis of the role of the node functions in the OODA loop, there are mainly the following six types of connection relationships, corresponding to six directed edges in the network; the detailed meanings are shown in Table 1.

<table>
<thead>
<tr>
<th>Number</th>
<th>Edge</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$E_1 : T \rightarrow O$</td>
<td>Target nodes are detected by observation functional nodes</td>
</tr>
<tr>
<td>2</td>
<td>$E_2 : O \rightarrow D$</td>
<td>Observation functional nodes upload intelligence information to decision functional nodes</td>
</tr>
<tr>
<td>3</td>
<td>$E_3 : O \rightarrow O$</td>
<td>Sharing of reconnaissance intelligence information between observation functional nodes</td>
</tr>
<tr>
<td>4</td>
<td>$E_4 : D \rightarrow D$</td>
<td>Sharing of decision informational between decision function nodes</td>
</tr>
<tr>
<td>5</td>
<td>$E_5 : D \rightarrow A$</td>
<td>Decision functional nodes issue commands to the action functional nodes</td>
</tr>
<tr>
<td>6</td>
<td>$E_6 : A \rightarrow T$</td>
<td>Action functional nodes strike the target enemy nodes</td>
</tr>
</tbody>
</table>

In Table 1, O, D, and A represent the functions provided by the nodes, and the actual node type can be determined by the mapping relationship between the function and the type. The set $E = \{E_1 \cup E_2 \cup \ldots \cup E_r \cup \ldots \cup E_6\}$ represents the edge set of the network, and $E_r$ represents the edge set formed by the $r$th type of interaction relationship, where $r = 1, 2, \ldots, 6$. The edges between nodes are directed edges, representing the direction of material, information, and energy flow. An edge from a source node to a target node is denoted by $e_{i \rightarrow j}^{type_1 \rightarrow type_2}$, indicating a directed edge from node $v_{type_1}^i$ to $v_{type_2}^j$.

In conclusion, the network model of the SoS can be represented by

$$G = (V, E)$$

3.2. Edge Capability Modeling

The capability of a combat SoS to accomplish top-level mission tasks depends on numerous combat elements being able to complete their basic combat missions. In the combat network, the interaction process between nodes is the process by which various elements of the combat SoS complete basic combat missions. The edge capacity of the network represents the ability of nodes to interact and thus complete basic missions. Edge capability refers to the possibility of the source node actively interacting with another node and establishing a directed edge, or the degree to which the source node satisfies the interaction requirements of the target node, represented as $C_{i \rightarrow j}^{type_1 \rightarrow type_2} \in [0, 1]$. $C_{i \rightarrow j}^{type_1 \rightarrow type_2}$ represents the ability or possibility of building a directed edge from $v_{type_1}^i$ to $v_{type_2}^j$. In the context of actual scenarios, $e_{i \rightarrow j}^{type_1 \rightarrow type_2}$ signifies the capability of $v_{type_1}^i$ to successfully match and execute the corresponding mission with $v_{type_2}^j$. The magnitude of the edge capacity depends on the extent to which the combat nodes satisfy the specific task requirements. Each combat node has multiple performance indicators related to basic combat tasks, which collectively determine the likelihood of the node’s completion of the basic tasks and consequently determine the edge capacity. This article measures the edge capacity using probabilities, assuming that the capacities of edges of the same type follow a normal distribution.
4. Combat SoS Capability Model Based on Kill Chain and Kill Network Capability

4.1. Mathematical Model of Kill Chain Capability

A kill chain refers to the closed-loop mode of task operation, in which various chain elements, based on a preplanned fixed architecture, are interdependent and operate sequentially to produce a lethal effect on a specific type of target. The fundamental characteristics of a kill chain include closure, orderliness, and dependency, with its core objective being to contribute to the effectiveness of achieving a lethal effect [22]. Reference [23] defines the continuous path of “observation–decision–strike” actions containing target nodes as the kill chain in the combat SoS network. In this paper, we continue to adopt this concept and define a kill chain as a combat loop that can effectively exert an impact on the target nodes and operate sequentially through the observation, decision-making, and effect functional nodes. Its composition structure is shown in Figure 3. The closed chain formed by the red arrows represents the kill chain of the red system against the blue target, and the closed chain formed by the blue arrows represents the kill chain of the blue system against the red target.

![Figure 3. Kill chain diagram.](image)

The premise for the formation of the combat capability of the kill chain is to form a complete OODA loop regarding the target. Based on the relationships between the node functions, typical kill chains mainly include in the Table 2.

<table>
<thead>
<tr>
<th>Killing Chain</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>T-O-D-A-T</td>
<td>Basic kill chain</td>
</tr>
<tr>
<td>T-O-O-D-A-T</td>
<td>Kill chain including collaborative reconnaissance</td>
</tr>
<tr>
<td>T-O-D-A-T</td>
<td>Kill chain including decision-making synergy</td>
</tr>
<tr>
<td>T-O-O-D-A-T</td>
<td>Kill chain including coordinated reconnaissance and decision-making</td>
</tr>
</tbody>
</table>

The necessary condition for the kill chain to have a killing effect is closed, and closure can be considered as the reliable operation of each node in the kill chain and normal connections between nodes. Therefore, the kill chain capability is determined by the reliability of the nodes on the kill chain and the edge capabilities; therefore, we provide the definition of kill chain capability as follows:

**Definition 5.** The kill chain capability is the probability that the nodes and edges maintain normal connectivity in the kill chain under the influence of uncertainty factors.

If there is a kill chain to target node $T$, consisting of functional node $n_{D}^{i}n_{D}^{j}n_{A}^{k}$ and target node $v_{T}^{m}$, then the capability of this kill chain is

$$ C_{chain} = C_{O-D}^{i}C_{D-A}^{j}C_{A-T}^{k} $$

(7)

$C_{O-D}^{i}$ and $C_{A}^{k}$ represent the reliability of the functional nodes $n_{D}^{i}$ and $n_{A}^{k}$, respectively. $C_{O-D}^{j}$, $C_{D-A}^{j}$, and $C_{A-T}^{k}$ are the edge capabilities of the directed edges $e_{O-D}^{i}$ between
node $n^i_O$ and $n^j_D$, $e^i_{D-A}$ between node $n^i_D$ and $n^j_A$, and $e^{k-m}_{A-T}$ between node $n^k_A$ and the target node $v^m_T$.

4.2. Mathematical Modeling of Kill Network Capability

4.2.1. Description of the Kill Network Capability

The kill network is a combinational integrated entity that achieves multiple functions and multiple path kill effects by associating specific elements and executing multiple independent kill chains. Built on the basis of kill chains, the kill network is formed by overlaying different types of kill chains to form a comprehensive kill network as a whole. In the interaction process of a combat SoS, the attack on the nodes of one party by the other party is often the result of the comprehensive effect of multiple kill chains. Multiple kill chains involve the organic integration of all the operational elements into the operational action to form the network capability against a specific node of the enemy. Therefore, the kill capability of a specific node of the enemy by the entire SoS needs to be viewed from the perspective of the system’s kill network. Figure 4 illustrates a combination of two kill chains acting on a target node.

![Illustration of two kill chains.](image)

In combination with the relationship between the kill network and kill chain, as well as the definition of the kill network in relevant discussions, this paper provides the definition of the kill network capability as follows:

**Definition 6.** The comprehensive kill capability of all kill chains within the SoS against a specific enemy target is the kill network capability. The mathematical meaning is: If there are $n$ kill chains for target $T$ in the red combat SoS, then the kill network capability of the red SoS against $T$ is the probability that at least one of the $n$ kill chains works normally.

The events required for the $n$ kill chains against $T$ to work normally are, respectively, denoted as $A_1, A_2, \ldots, A_n$. The kill network capability is the probability of at least one of these $n$ kill chains working normally, denoted as $p = \{A_1 \cup A_2 \cup \ldots \cup A_n\}$.

From this, we can obtain the expression for the kill network capability of the system:

$$p = \{A_1 \cup A_2 \cup \ldots \cup A_n\} = p(A_1) + p(A_2) + \ldots + p(A_n) - [p(A_1A_2) + p(A_1A_3) + \ldots + p(A_1A_n)] + \ldots + (-1)^{n-1}p(A_1A_2\ldots A_n)$$

(8)

Due to the existence of common nodes between kill chains, the events $A_1, A_2, \ldots, A_n$ are not independent events, and solving the above problem directly requires a large amount of computation. However, the kill network capability of the SoS is the probability of all nodes within the combat SoS forming a path around the target node. If the target node is split into source and terminal nodes, the above problem can be transformed into a two-terminal network connectivity problem. The two-terminal network connectivity problem aims to find the probability of a connection (i.e., the existence of a path) between the source...
node $s$ and the terminal node $t$. This problem has been widely studied in the contexts of infrastructure, communication, and wireless networks [24–26].

There are currently several exact solution methods for the two-terminal connectivity of networks [27–29], and reference [30] has proven that the exact solution to the problem in networks is an NP-hard problem. In addition, the existing analytical solution methods mainly focus on equiprobable networks. However, the network of this paper has non-equal connection probabilities, and the node types are heterogeneous, which makes it a non-equiprobable network. Analytical calculations require additional computational complexity. The advantage of the Monte Carlo simulation method lies in the speed of convergence of its error, which is independent of the scale and dimension of the problem and only depends on the number of simulations. Therefore, its time complexity is $O(N)$, where $N$ is the total number of simulations per run. To avoid the exponential explosion problem caused by an increase in the network size, this paper adopts the Monte Carlo simulation method to solve the kill chain capability of the system.

4.2.2. Solving the Kill Network Capability Based on Monte Carlo Simulation

The Monte Carlo simulation (MCS) method uses multiple experiments to determine the on–off frequency of the network’s two points. According to the Kolmogorov Strong Law of Large Numbers, when the number of simulations is large enough, the on–off frequency will approach the connectivity probability of the two points. It can be divided into the following parts:

1) Determine the adjacency matrix

The adjacency matrix reflects the matrix of interactive relationships between nodes, aiming to properly describe the various interaction relationships between nodes. First, based on the six types of relationships between nodes, including early warning reconnaissance, intelligence uploading, collaborative reconnaissance, collaborative decision-making, command execution, and effect application, subnetworks describing these six relationships are established:

$$G_1 = (V, E_1)$$

(9)

$$G_2 = (V, E_2)$$

(10)

$$G_3 = (V, E_3)$$

(11)

$$G_4 = (V, E_4)$$

(12)

$$G_5 = (V, E_5)$$

(13)

$$G_6 = (V, E_6)$$

(14)

In Equations (9)–(14), $G_1$ is the reconnaissance relationship network between observation functional nodes and target nodes; $G_2$ is the interaction relationship network between observation and decision functional nodes; $G_3$ is the interaction relationship network between observation functional nodes; $G_4$ is the interaction relationship network between decision functional nodes; $G_5$ is the interaction relationship network between decision and action functional nodes; and $G_6$ is the interaction relationship network between action and enemy target class nodes. The adjacency matrices of the six subnetworks are $M_1$, $M_2$, $M_3$, $M_4$, $M_5$, and $M_6$. When there is an interaction relationship between corresponding nodes, the elements of the adjacency matrix represent the probability of interaction between the nodes. The adjacency matrix of the overall network of the combat SoS is denoted as $M$.

$$M = M_1 + M_2 + M_3 + M_4 + M_5 + M_6$$

(15)
(2) Determining the kill chain on–off situation in the kth sampling

In the kth sampling, \( x_{\text{type}}^i \) represents the operational status of node \( v_{\text{type}}^i \), where \( x_{\text{type}}^i = 1 \) indicates that the \( v_{\text{type}}^i \) node is operating normally in this sampling, and \( x_{\text{type}}^i = 0 \) indicates otherwise.

\[
x_{\text{type}}^i = \begin{cases} 
1, & \theta_k \leq R_{\text{type}}^i \\
0, & \theta_k > R_{\text{type}}^i 
\end{cases}
\]  

(16)

According to the edge relationship constraint, \( y_{\text{type1}-\text{type2}}^{i-n} \) represents the edge status between nodes \( v_{\text{type1}}^i \) and \( v_{\text{type2}}^n \) in this sampling. \( y_{\text{type1}-\text{type2}}^{i-n} = 1 \) indicates the existence of active interaction, and \( y_{\text{type1}-\text{type2}}^{i-n} = 0 \) indicates the absence of active interaction.

\[
y_{\text{type1}-\text{type2}}^{i-n} = \begin{cases} 
1, & \epsilon_k \leq c_{\text{type1}-\text{type2}}^{i-n} \\
0, & \epsilon_k > c_{\text{type1}-\text{type2}}^{i-n}
\end{cases}
\]  

(17)

In Equations (16) and (17), \( \theta_k \) and \( \epsilon_k \) are random values generated in the kth sampling, \( \theta_k, \epsilon_k \in [0, 1] \). Based on \( \theta_k, \epsilon_k \), the node reliability and edge capacity, the status of the nodes and edge connections in the kth sampling can be determined, thus establishing the network structure and obtaining the adjacency matrix for each sampling state.

According to the high-order adjacency matrix method for solving the directed graph cycle theorem, the number of operational cycles for a specific node in a directed operational network corresponds to the diagonal elements of the matrix obtained after multiple adjacency matrix multiplications. Let \( W_m \) be the adjacency matrix of network \( G_m \), where \( m = 1, 2, 3, 4 \); then,

\[
W_{T-O-D-A-T} = W_1 W_2 W_3 W_6 
\]  

(18)

\[
W_{T-O-D-A-T} = W_1 W_2 W_3 W_6 
\]  

(19)

\[
W_{T-O-D-D-A-T} = W_1 W_2 W_4 W_5 W_6 
\]  

(20)

\[
W_{T-O-D-D-A-T} = W_1 W_3 W_2 W_5 W_6 
\]  

(21)

The subscripts of the matrices \( W_{T-O-D-A-T}, W_{T-O-D-A-T}, W_{T-O-D-D-A-T}, \) and \( W_{T-O-D-D-A-T} \) correspond to the types of kill chains, and their diagonal elements, respectively, represent the number of kill chains targeting enemy target nodes for each type of kill chain. Taking the matrix \( W_{T-O-D-A-T} \) as an example, the values of the diagonal elements corresponding to the target node numbers represent the number of T-O-D-A-T-type kill chains targeting the corresponding targets.

(3) Calculation of the SoS’s capability to attack nodes

In k samplings, the occurrence of kill chains targeting the node \( v_T^i \) appeared a total of \( \hat{k} \) times. The SoS’s capability to attack the node \( v_T^i \) is

\[
p_i = \frac{\hat{k}}{k}
\]  

(22)

Based on the description in items (1) to (3), a flow chart for solving the kill chain capability based on Monte Carlo simulation is constructed, as shown in Figure 5.
The subscripts of the matrices $T-O-D-A-T\_W$, $T-O-O-D-A-T\_W$, $T-O-D-D-A-T\_W$, and $T-O-O-D-D-A-T\_W$ correspond to the types of kill chains, and their diagonal elements, respectively, represent the number of kill chains targeting enemy target nodes for each type of kill chain. Taking the matrix $T-O-D-A-T\_W$ as an example, the values of the diagonal elements corresponding to the target node numbers represent the number of T-O-D-A-T-type kill chains targeting the corresponding targets.

(3) Calculation of the SoS’s capability to attack nodes

In $k$ samplings, the occurrence of kill chains targeting the node $i$ appeared a total of $\hat{k}$ times. The SoS’s capability to attack the node $i$ is $\hat{i} = 0\hat{k}$.

Based on the description in items (1) to (3), a flow chart for solving the kill chain capability based on Monte Carlo simulation is constructed, as shown in Figure 5.

4.3. Mathematical Model of Combat SoS’s Capability

The kill network capability can be expressed as the combat capability of the SoS against a specific enemy node. However, it is more important to analyze the overall impact on the enemy’s system. This paper considers establishing a model of the SoS’s combat capability, making it easier to analyze the SoS’s resilience based on changes in the system’s combat capability.

**Definition 7.** The SoS’s combat capability refers to the likelihood of one combat SoS causing a certain scale of node damage to the other SoS. The greater the likelihood, the stronger the SoS’s combat capability.

If the enemy has $t$ nodes, the kill network capabilities of our SoS against the enemy nodes are $p_1, p_2, \ldots, p_t$, respectively. Assuming that the effects on different nodes do not affect each other, the probability $p_m$ of destroying $m$ nodes among the enemy’s $t$ nodes can be represented as follows.

When $m = 0$,

$$P_0 = P\{m = 0\} = (1 - p_1)(1 - p_2)\ldots(1 - p_t) \quad (23)$$
When \( m = 1 \),
\[
P_1 = P\{m = 1\} = p_1(1 - p_2) \ldots (1 - p_t) \\
+ (1 - p_1)p_2(1 - p_3) \ldots (1 - p_t) \\
+ \ldots + p_t(1 - p_1)(1 - p_2) \ldots (1 - p_{t-1}) \\
= \sum_{k=1}^{t} p_k \left( \prod_{l=1}^{t} (1 - p_l) \right)_{l \neq k} 
\]
(24)

When \( m = 2 \),
\[
P_2 = P\{m = 2\} = p_1p_2(1 - p_3) \ldots (1 - p_t) + p_1p_3(1 - p_2) \ldots (1 - p_t) \\
+ \ldots + p_{t-1}p_t(1 - p_1)(1 - p_2) \ldots (1 - p_{t-1}) \\
= \sum_{i=1}^{t} \sum_{j=i+1}^{t} p_ip_j \left( \prod_{l=1}^{t} (1 - p_l) \right)_{l \neq i, j} 
\]
(25)

We can deduce that
\[
P_m = \sum_{i=1}^{t} \sum_{j=i+1}^{t} \sum_{k=i+m-1}^{t} p_ip_j \ldots p_k \left( \prod_{l=1}^{t} (1 - p_l) \right)_{l \neq i, j, k} 
\]
(26)

If the damage to nodes of “a certain scale” is considered to be at least causing \( m \) nodes to be damaged, then the combat capability of the system can be represented by
\[
C = \sum_{i=m}^{t} p_m 
\]
(27)

Once the combat capability of the SoS is obtained, the resilience of the system can be analyzed based on Equations (1)–(3). According to the above content, the logical framework for analyzing the resilience of the combat SoS in this paper is shown in Figure 6.

---

**Figure 6.** Logical framework diagram.
5. Analysis and Verification of Indicator Rationality

5.1. Design of Attack and Reconstruction Strategy

Nodes are the basic entities of the combat network, so all faults and attacks occur at the nodes. The state of the nodes will further affect the state of the edges, thereby further affecting the combat capability of the SoS. In the existing research, attack strategies can mainly be divided into two types: random attacks and deliberate attacks.

5.1.1. Analysis and Design of Attack Strategy

(1) Random attack strategy

Random attacks refer to the enemy not distinguishing between the types and importance of our nodes and conducting attacks on nodes in a completely random manner. This attack strategy is suitable for scenarios where the enemy is unclear about the internal nodes and structure of our SoS, highlighting the randomness and uncertainty of the threat. Under the random attack mode, \( Y_k \) represents the number of our nodes lost in the \( k \)th wave, and \( Y_k \sim b(|V_R|, p_a) \) follows a binomial distribution. \( p_a \) is the probability of each node being subjected to a random attack. After being attacked, the node is damaged, and all its edges become ineffective.

(2) Deliberate attack strategy

Deliberate attacks are based on the enemy’s thorough understanding of our SoS’s structure. The enemy can determine the importance of nodes based on the information it has and conduct attacks according to the importance of the nodes. In practice, high-military-value targets are often prioritized, and nodes with high importance are attacked first. There are different calculation methods for the node importance, including the node degree, node betweenness, network performance gradient [31], node cohesion, and density.

In this paper, the method of node degree is used to determine the deliberate attack strategy for nodes. In an undirected unweighted network, the degree \( k_{\text{type}} \) of node \( v_{\text{type}} \) represents the number of edges connected to that node. Since the combat network in this paper is a directed weighted network, the degree \( k_{\text{type}} \) of node \( v_{\text{type}} \) is defined as the sum of the weights of all edges connected to \( v_{\text{type}} \). Before initiating the attack, it is assumed that the blue side determines the attack order based on the size of the red side’s node degrees. For comparative analysis, the number of nodes lost under a deliberate attack strategy is the same as under a random attack strategy within the same time frame.

5.1.2. Reconstruction Strategy

A SoS typically has two strategies to deal with external disturbances: (1) task reorganization of the SoS structure; (2) maintenance and repair of the components. Among them, task reorganization of the system structure in the combat network is manifested as the activation of backup redundant kill chains, which is related to the structural properties of the system itself. Maintenance and repair of the components mainly involve repair of the damaged nodes. Node repair refers to the repair of nodes that have been damaged and are in a failed state, and this repair process takes time. If node \( v_{\text{type}} \) fails at time \( t_1 \), the repair begins from the moment of failure, and the reliability of the node is 0 when it is in a failed state. By time \( t_2 \), node \( v_{\text{type}} \) restores its original reliability level and reestablishes normal relationships with other nodes before the failure. This process is the node repair process, and the duration of node repair is related to the node type, depending on the actual difficulty of the repair of the combat forces.

5.2. Rationality Analysis of the SoS Combat Capability Calculation Model

To validate the rationality of the SoS capability calculation method proposed in this paper and its superiority compared to other methods, this section conducts an analysis and validation comparing it with the method proposed by Li Jichao in the references [15,16]. The main steps for calculating the combat capability using Li’s method are:
Step 1

For a certain kill chain $l_j$, the set of sensor nodes it contains is $S = \{s_j\}$, the set of decision-making nodes is $D = \{d_j\}$, and the set of influence nodes is $I = \{i_j\}$. The combat capability of this kill chain is represented by

$$U(l_j) = \frac{1}{|l_j|} \times \max_{s_j \in S} CA_S(s_j) \times \max_{d_j \in D} CA_D(d_j) \times \max_{i_j \in I} CA_I(i_j)$$  \hspace{1cm} (28)

where $CA_S(s_j)$, $CA_D(d_j)$, and $CA_I(i_j)$ are the capabilities of the sensor, decision-making, and influence nodes in the system, respectively, while $|l_j|$ is the length of the kill chain $l_j$.

Step 2

For a combat SoS, if it contains a set of $m$ kill chains, $L_G = \{l_k\} k = 1, 2, 3, \ldots, m$, then the combat capability of this SoS is represented by

$$J(G) = \sum_{l_k \in L_G} U(l_k)$$  \hspace{1cm} (29)

Table 3. Nodes of operation.

<table>
<thead>
<tr>
<th>Node Type</th>
<th>Proportion (%)</th>
<th>Functional Type</th>
<th>Edge Capability Expectation</th>
<th>Edge Capability Variance</th>
<th>Reliability Expectation</th>
<th>Reliability Variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>10</td>
<td>O</td>
<td>0.2</td>
<td>0.1</td>
<td>0.85</td>
<td>0.02</td>
</tr>
<tr>
<td>C</td>
<td>20</td>
<td>D</td>
<td>0.2</td>
<td>0.1</td>
<td>0.85</td>
<td>0.02</td>
</tr>
<tr>
<td>I</td>
<td>20</td>
<td>A</td>
<td>0.2</td>
<td>0.1</td>
<td>0.85</td>
<td>0.02</td>
</tr>
<tr>
<td>SC</td>
<td>20</td>
<td>O</td>
<td>0.2</td>
<td>0.1</td>
<td>0.85</td>
<td>0.02</td>
</tr>
<tr>
<td>SI</td>
<td>20</td>
<td>A</td>
<td>0.2</td>
<td>0.1</td>
<td>0.85</td>
<td>0.02</td>
</tr>
<tr>
<td>SCI</td>
<td>10</td>
<td>O</td>
<td>0.2</td>
<td>0.1</td>
<td>0.85</td>
<td>0.02</td>
</tr>
</tbody>
</table>

Based on the above data, the number of Monte Carlo simulations is set to 2000. To ensure the stability of the results using Li’s method, the mean of the kill chain capability is also calculated 2000 times. During the simulation verification process, the change trend in the SoS capability is analyzed using both random and deliberate attack strategies. Assuming that the number of nodes in our SoS is 40, and the number of target nodes is 15, 20, 25, 30, 35, and 40, the method in this paper sets the enemy’s damage scale at 70%, indicating that the SoS’s combat capability represents the probability of causing damage to over 70% of the enemy’s nodes in our combat SoS.

The performance of the two methods is shown in Figure 7. The simulation results are shown in Figure 7a–f. From Figure 7, it can be seen that as the number of target nodes increases, the initial value of the SoS’s combat capability by Li’s method will also increase. This is because the calculation of the SoS’s combat capability using Li’s method relies on the number of kill chains. When the node reliability and edge capability remain unchanged, the more target nodes there are, the more kill chains can be formed from the nodes to the enemy’s nodes, resulting in a larger initial value of the SoS’s combat capability. This does not align with the view that combat capability is an essential attribute of the combat SoS itself, and the combat capability of our system is inherent to the system and should not change due to variations in the number of enemy nodes. In contrast, the method proposed in this paper does not depend on the number of enemy nodes and the
number of kill chains but focuses more on the overall effectiveness of the system’s combat, thereby achieving a comprehensive measurement of the combat capability.

![Graphs showing performance under different attack strategies.](image)

**Figure 7.** Performance of the two methods under different attack strategies. (a) The number of target nodes is 15. (b) The number of target nodes is 20. (c) The number of target nodes is 25. (d) The number of target nodes is 30. (e) The number of target nodes is 35. (f) The number of target nodes is 40.

At the same time, when the number of deleted nodes is small, the SoS’s combat capability computed in this paper remains unchanged, indicating that the loss of a few nodes does not affect the SoS’s capability to complete basic tasks. Other pre-existing kill chains in the SoS can compensate for the broken kill chains caused by the failed nodes. In contrast, as the SoS’s combat capability depends on the number of kill chains, the SoS’s combat capability calculated using Li’s method begins to decrease when a small number of nodes are deleted. This method fails to describe the robustness of the SoS when some
nodes are lost, and the change in trends also fails to reflect the collapse effect of the SoS’s capability and is unable to reflect mutations in the combat SoS.

However, both methods indicate that a deliberate attack strategy results in a faster decrease in the SoS’s combat capability compared to a random attack strategy, indicating that the loss of more important nodes has a greater impact on the SoS’s combat capability.

5.3. Resilience Analysis under Different Attack Strategies

Let us assume that the combat SoS begins to suffer the first wave of attacks from the enemy at $t_1 = 4$ h and then encounters an attack every hour, experiencing a total of five waves of enemy attacks. Under the random attack strategy, the probability of all combat nodes being attacked within each wave is $P_a = 0.20$; under the deliberate attack strategy, the number of nodes lost in each wave is the same as the random attack strategy, but the nodes with high importance will be attacked first. Once attacked, the node immediately fails, and all connected edges also fail. After the failure, the node starts to recover, and the recovery time depends on the type of node. It is assumed that the recovery time for different types of nodes is as shown in Table 4.

<table>
<thead>
<tr>
<th>Node Type</th>
<th>S</th>
<th>C</th>
<th>I</th>
<th>SC</th>
<th>SI</th>
<th>SCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Duration (h)</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>8</td>
<td>8</td>
<td>10</td>
</tr>
</tbody>
</table>

This experiment only considers the situation where the nodes are affected by external interference and does not consider failures caused by the unreliability of the nodes themselves. Therefore, at the initial moment, the reliability of our combat nodes is set to 1. Unless otherwise specified, the node is the same as in Table 3. The task baseline is set to 0.7, which means that the probability of causing effective damage to more than 70% of the enemy’s targets needs to reach 0.7.

The importance of our combat nodes is measured according to the node degree, and the importance of our combat nodes is as seen in Table 5.

<table>
<thead>
<tr>
<th>Node</th>
<th>$v_1^3$</th>
<th>$v_2^3$</th>
<th>$v_3^3$</th>
<th>$v_4^3$</th>
<th>$v_5^1$</th>
<th>$v_6^1$</th>
<th>$v_7^1$</th>
<th>$v_8^1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree</td>
<td>21.16</td>
<td>21.71</td>
<td>22.55</td>
<td>21.77</td>
<td>16.06</td>
<td>16.08</td>
<td>15.24</td>
<td>15.71</td>
</tr>
<tr>
<td>Node</td>
<td>$v_1^4$</td>
<td>$v_2^4$</td>
<td>$v_3^4$</td>
<td>$v_4^4$</td>
<td>$v_5^4$</td>
<td>$v_6^4$</td>
<td>$v_7^4$</td>
<td>$v_8^4$</td>
</tr>
<tr>
<td>Degree</td>
<td>14.04</td>
<td>15.53</td>
<td>11.64</td>
<td>10.92</td>
<td>10.93</td>
<td>12.61</td>
<td>11.42</td>
<td>11.32</td>
</tr>
<tr>
<td>Node</td>
<td>$v_1^{1C}$</td>
<td>$v_2^{1C}$</td>
<td>$v_3^{1C}$</td>
<td>$v_4^{1C}$</td>
<td>$v_5^{1C}$</td>
<td>$v_6^{1C}$</td>
<td>$v_7^{1C}$</td>
<td>$v_8^{1C}$</td>
</tr>
<tr>
<td>Degree</td>
<td>37.45</td>
<td>36.93</td>
<td>36.67</td>
<td>37.11</td>
<td>38.09</td>
<td>38.45</td>
<td>36.24</td>
<td>36.12</td>
</tr>
<tr>
<td>Node</td>
<td>$v_1^{2A}$</td>
<td>$v_2^{3A}$</td>
<td>$v_3^{3A}$</td>
<td>$v_4^{3A}$</td>
<td>$v_5^{3A}$</td>
<td>$v_6^{3A}$</td>
<td>$v_7^{3A}$</td>
<td>$v_8^{3A}$</td>
</tr>
<tr>
<td>Degree</td>
<td>34.17</td>
<td>31.42</td>
<td>35.84</td>
<td>35.98</td>
<td>31.97</td>
<td>34.56</td>
<td>47.48</td>
<td>48.41</td>
</tr>
</tbody>
</table>

The nodes are ranked in order of importance as:

$v_1^{3C} > v_1^{3SI} > v_1^{3SCI} > v_2^{3SI} > v_2^{3SCI} > v_3^{3SI} > v_3^{3SCI} > v_4^{3SI} > v_4^{3SCI} > v_5^{3C} > v_5^{3SI} > v_5^{3SCI} > v_6^{3C} > v_6^{3SI} > v_6^{3SCI} > v_7^{3C} > v_7^{3SI} > v_7^{3SCI} > v_8^{3C} > v_8^{3SI} > v_8^{3SCI} > v_1^{4C} > v_1^{4SI} > v_1^{4SCI} > v_2^{4C} > v_2^{4SI} > v_2^{4SCI} > v_3^{4C} > v_3^{4SI} > v_3^{4SCI} > v_4^{4C} > v_4^{4SI} > v_4^{4SCI} > v_5^{4C} > v_5^{4SI} > v_5^{4SCI} > v_6^{4C} > v_6^{4SI} > v_6^{4SCI} > v_7^{4C} > v_7^{4SI} > v_7^{4SCI} > v_8^{4C} > v_8^{4SI} > v_8^{4SCI}$

From the ranking, it can be seen that the importance of the composite functional nodes is higher than that of single functional nodes, and they will be given priority in deliberate attacks. In a certain experiment, the situation of losing nodes within each wave under the two strategies is shown in Table 6. It can be seen that there is no obvious pattern of losing nodes under random attacks, while deliberate attacks give priority to losing composite functional nodes with higher importance.
The resilience performance of the combat SoS is shown in Figures 8 and 9. From Figure 8, it can be seen that the combat SoS exhibits better resilience in response to random attacks compared to deliberate attacks. At the beginning of the attack at time $t = 5$ h, the operational capability of the system under deliberate attacks starts to decline rapidly. This is because during the first wave of attacks, the combat SoS loses many nodes with high importance, which are highly involved in constructing the kill chain and kill network. However, the combat capability of the SoS under random attacks remains stable for a certain period of time because the loss of some nodes does not significantly affect the operational capability. However, with an increasing number of attack waves, the number of nodes lost under both strategies increases, leading to a further decrease in the operational capability of the combat SoS, falling below the task baseline and even reaching 0. As time progresses, the failed nodes of the SoS begin to recover gradually, and the operational capability of the SoS under the random attack strategy gradually increases. In contrast, the operational capability of the SoS under deliberate attacks remains at zero for a longer period, representing that during this period, the probability of causing damage to 70% of the enemy’s targets by the own combat SoS is 0. This is because the failures under deliberate attack strategies are mostly in composite functional nodes, which have a longer recovery time, leading to slower recovery of the operational capability.
The anti-destruction capability, survival capability, recovery capability, and overall resilience under different attack strategies are shown in Table 7:

Table 7. Combat SoS resilience under two attack strategies.

<table>
<thead>
<tr>
<th>Attack Strategy</th>
<th>Anti-Destruction Capability</th>
<th>Survival Capability</th>
<th>Recovery Capability</th>
<th>Resilience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random attack</td>
<td>6.6080</td>
<td>0.4121</td>
<td>20.1311</td>
<td>27.1512</td>
</tr>
<tr>
<td>Deliberate attack</td>
<td>4.5165</td>
<td>0.3965</td>
<td>17.4223</td>
<td>22.3353</td>
</tr>
</tbody>
</table>

Combining Figure 9 and Table 7, it can be seen that under both strategies, the combat SoS exhibits similar persistence. However, the SoS’s anti-destruction and recovery capability under deliberate attacks are significantly inferior to those under random attack strategies. The overall resilience of the system under random attacks also outperforms that under deliberate attack strategies.

6. Conclusions

This paper constructs a combat network model and proposes a method for quantifying the combat SoS’s combat capability and resilience, describing the resilience of the SoS from the dimensions of anti-destruction, survival, and recovery ability. Experimental verification shows that the capability indicators proposed in this paper have advantages in measuring the SoS’s resilience, reflecting the practical combat process performance, rather than relying on subjective human judgment.

Specifically, the problem of solving the combat SoS’s combat capability is transformed into a network two-terminal connectivity problem. Considering the infeasibility of obtaining an analytical solution, the Monte Carlo method is used to solve the two-terminal connectivity of the network.

Based on the method presented in this paper, it is possible to conduct an analysis and assessment of the resilience capability of an actual combat SoS, and follow-up analyses will be conducted based on the actual performance of a combat SoS.

Author Contributions: Conceptualization, W.L. and T.Z.; methodology and other work, W.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All the data generated or analyzed during this study are included in this published article.

Conflicts of Interest: The authors declare no conflict of interest.
References


27. Monfared, M.A.S.; Rezazadeh, M.; Alipour, Z. Road networks reliability estimations and optimizations: A bi-directional bottom-up, top-down approach. Reliab. Eng. Syst. Saf. 2022, 222, 108427. [CrossRef]


**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.