QUANTITATIVE APPROACHES TO INFORMATION SECURITY ASSURANCE IN MILITARY COMPUTER NETWORKS

Fiodor TIMERCAN

"Alexandru cel Bun" Armed Forces Military Academy, Republic of Moldova (fiodor.timercan@army.md)

DOI: 10.19062/2247-3173.2026.27.19

Abstract: *Modern military computer networks operate in environments characterized by high operational tempo, adversarial interference, and dynamic threat evolution. Under these conditions, information security assurance cannot rely exclusively on qualitative assessments or compliance-based controls; it requires quantifiable, mathematically grounded evaluation frameworks capable of modeling uncertainty, adversarial behavior, and structural vulnerability.*

This paper proposes a quantitative analytical approach to information security assurance in military computer networks, integrating principles from network science, probability theory, and resilience engineering. The study conceptualizes military networks as dynamic graph structures in which nodes represent mission-critical assets and edges represent secured communication channels. Within this formal structure, security assurance is defined as a measurable function dependent on network connectivity, redundancy, probabilistic threat occurrence, and recovery capacity.

The proposed framework introduces three complementary analytical dimensions: (1) structural vulnerability assessment based on graph-theoretic metrics such as node centrality and connectivity thresholds; (2) probabilistic modeling of attack propagation using stochastic processes; and (3) resilience quantification through performance degradation and recovery rate functions. This approach aligns with contemporary cybersecurity risk quantification paradigms as outlined in the NIST Risk Management Framework (NIST SP 800-37) and incorporates resilience concepts consistent with NATO's cyber defence policy principles. Additionally, the formalization of security as a measurable system property reflects foundational concepts from Shannon's theory of information, where system robustness is inherently linked to signal integrity and controlled entropy (Shannon, 1948).

The objective is to bridge theoretical mathematical modeling with operational military network security requirements, providing a structured methodology for evaluating and improving security assurance in contested digital environments. By transforming abstract security concepts into quantifiable metrics, the study supports evidence-based decision-making in military cyber defence planning and network architecture design.

Keywords: *information security assurance; military computer networks; quantitative security metrics; cyber resilience; graph theory; stochastic modeling; network vulnerability analysis; risk quantification; adversarial threat modeling; secure network architecture; operational cyber defence; network robustness; mission-critical systems security.*

1. INTRODUCTION

Military computer networks represent the digital backbone of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architectures. Unlike civilian infrastructures, these networks operate in adversarial environments where intentional disruption, deception, and degradation are expected rather than exceptional.

Consequently, information security assurance within military systems must be approached not merely as regulatory compliance, but as a measurable property of operational survivability.

Traditional security frameworks emphasize policy enforcement, access control, and cryptographic mechanisms. While indispensable, such measures alone do not provide a quantitative understanding of how a network behaves under coordinated attack or systemic stress. In military contexts, the essential question is not only whether protective controls exist, but whether the network can maintain mission-essential information flows under hostile conditions.

The necessity of measurable security has been formally recognized in risk-based cybersecurity governance models such as the NIST Risk Management Framework, which promotes continuous risk assessment and quantitative evaluation of system security posture (NIST SP 800-37 Rev. 2, 2018). Similarly, NATO's Cyber Defence Policy underscores resilience and operational continuity as strategic requirements in contested digital environments (NATO, 2021). These doctrinal orientations implicitly demand analytical tools capable of translating security concepts into quantifiable indicators.

From a theoretical perspective, the foundation of secure communication can be traced to Shannon's formulation of information theory, where signal integrity and entropy determine the limits of reliable transmission (Shannon, 1948). Although originally developed for communication channels, these principles extend naturally to military computer networks, where information degradation, interception, or manipulation can be interpreted as disturbances affecting system entropy and reliability.

Recent research in network science further supports the need for structural analysis of interconnected systems. Studies on network robustness demonstrate that connectivity patterns and node centrality significantly influence the resilience of complex infrastructures under targeted disruption (Albert, Jeong & Barabási, 2000). In military networks, where certain nodes represent high-value command or sensor assets, structural vulnerability becomes a critical security determinant.

In light of these considerations, this study adopts a quantitative perspective on information security assurance. Military computer networks are modeled as dynamic graph-based systems subject to probabilistic threat events. Security assurance is treated as a measurable function dependent on structural integrity, threat likelihood, and recovery capability. By integrating graph-theoretic analysis, stochastic modeling, and resilience metrics, the research aims to provide a rigorous framework for evaluating and improving security posture in operational military environments.

The objective is not to replace existing doctrinal security standards, but to complement them with mathematically grounded evaluation methods that support evidence-based defensive planning and architectural optimization. In complex operational theaters, the capacity to measure security becomes inseparable from the capacity to defend it.

2. STRUCTURAL VULNERABILITY ANALYSIS OF MILITARY NETWORKS (GRAPH-THEORETIC PERSPECTIVE)

Military computer networks can be represented as a graph $G = (V,E)$, where V is the set of assets (C2 servers, cryptographic gateways, tactical routers, ISR sensors, mission terminals) and E is the set of communication links (logical or physical, wired/wireless, often layered through encryption and routing policies). This abstraction is not decorative, graph structure strongly constrains what an adversary can break and what a defender can preserve.

Network science shows that robustness is often a property of topology as much as it is a property of individual security controls. In particular, heterogeneous (hub-dominated) networks can tolerate many random failures but collapse rapidly under targeted removal of high-importance nodes. This "robust-yet-fragile" pattern is a standard result in complex networks literature and is directly relevant to military architectures where certain nodes concentrate authority, routing, or trust. [1].

a) Threat model mapped to graph operations

In a graph model, disruptive actions translate naturally into operations on *G*:

- **Random faults / incidental failure:** random removal of nodes or edges (e.g., equipment failure, weather-related link loss).
- **Targeted attack:** removal/compromise of specific nodes/edges selected by a criterion (e.g., highest betweenness, gateway nodes, core routers, C2 hubs).
- **Cascading effects:** failures that propagate (e.g., routing overload, key-management disruption, trust-chain invalidation), captured by iterative removal or degradation of edges/nodes.

The key analytic idea is to compare mission-level connectivity before and after perturbations. A common topological objective is maintaining a sufficiently large giant component (largest connected subgraph) so that required command-and-control information flows remain feasible. Classical results on random graphs and degree sequences formalize when a giant component exists and when fragmentation becomes inevitable. [2]

b) Identifying critical nodes and links

Structural vulnerability assessment begins by identifying which elements are "structurally critical", not because they are valuable in isolation, but because their position makes them indispensable for connectivity or flow. Core metrics (practical and interpretable):

- **Degree centrality *k (v)*:** number of links at node *v*. High-degree nodes can be high-impact points, but degree alone can be misleading in networks with layered routing or redundancy. [3]
- **Betweenness centrality *BC (v)*:** fraction of shortest paths passing through *v*. Nodes with high betweenness often act as chokepoints (e.g., cross-domain guards, aggregation routers, SATCOM gateways). Their loss can partition the network even if degree is moderate. [3]
- **Articulation points / bridges:** nodes/edges whose removal disconnects the graph. These map cleanly to "single points of failure" in topology. [3]
- **k-core / core-periphery structure:** the maximal subgraph where all nodes have degree $\geq k$. Military networks often mix a hardened core (fixed infrastructure, redundant backbones) with fragile periphery (mobile/tactical edges). k-core analysis helps separate where resilience truly lives. [3]

Operational interpretation (military-specific): A node's structural criticality can reflect trust concentration (key distribution, authentication services), routing concentration (where paths converge), or domain crossing (classification boundaries). Compromise of a domain-crossing gateway is not only a connectivity event; it can also be a policy breach. The graph model lets you quantify the connectivity impact, while security policy analysis handles classification/control impact, both are needed, but the graph step is the clean quantitative foundation.

c) Measuring robustness: what "damage" means in topology

Robustness can be quantified using multiple, complementary measures:

- **Largest component size *L***: increases indicate degraded latency/throughput and higher exposure to interception points. [3]

- **Algebraic connectivity** λ_2 (Fiedler value of Laplacian): a spectral measure capturing how "well-knit" the graph is; higher λ_2 generally implies more resilience to cuts and better diffusion properties. [3]
- **Targeted-attack sensitivity curve:** plot $S(\rho)$ as a function of fraction ρ of removed nodes, with removal ordered by a criterion (e.g., descending betweenness). A steep drop under targeted removal is a red flag. The hallmark result is that scale-free-like structures show high robustness to random removals but high vulnerability to targeted removals. [1][4]

Percolation-based results connect these observations to thresholds: for some degree distributions, extremely large fractions of random removals are required to shatter the giant component, while small targeted removals can be catastrophic, again echoing why "hub and gateway protection" is disproportionately valuable in real systems. [4]

d) Practical outcome: from topology to design decisions

The graph-theoretic analysis produces directly actionable design outputs::

- A ranked list of **critical nodes/edges** (by betweenness, articulation status, bridge edges, core membership).
- Quantified **fragmentation risk** under realistic disruption models (random vs targeted).
- Evidence for architectural interventions: adding alternate routes, reducing chokepoints, duplicating gateways, separating trust services, or building multiple smaller command graphs instead of one monolith.

Percolation-based results connect these observations to thresholds: for some degree distributions, extremely large fractions of random removals are required to shatter the giant component, while small targeted removals can be catastrophic, again echoing why "hub and gateway protection" is disproportionately valuable in real systems. [4]

In a military setting, the goal is not maximal connectivity at any cost, it is **mission connectivity under constraint**, meaning connectivity that remains feasible under loss, deception, and strict security policy.

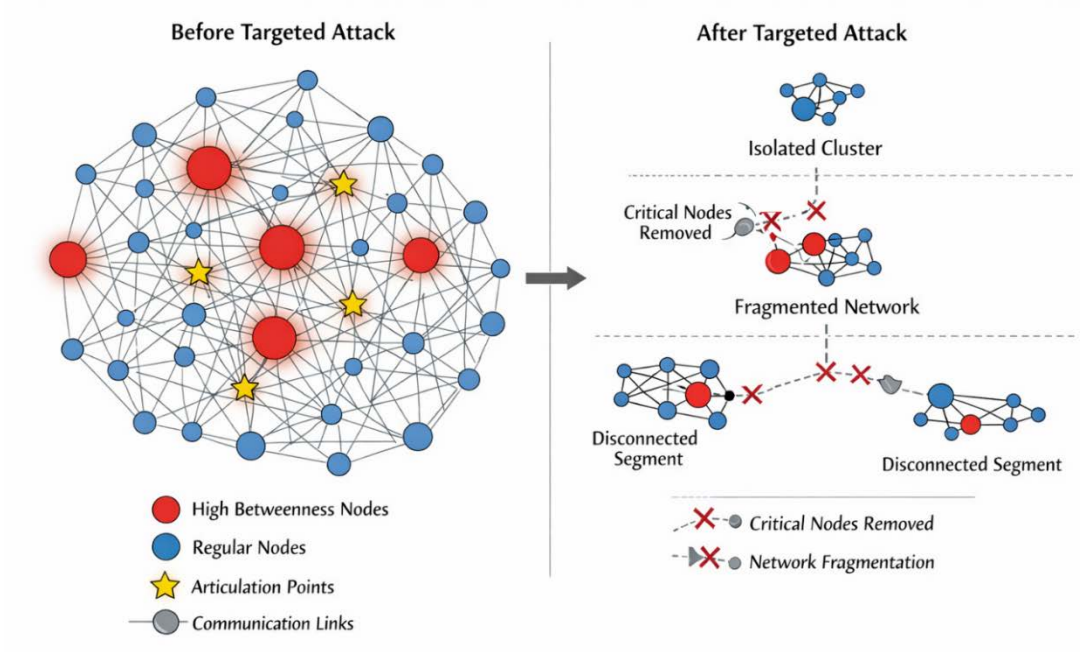

FIG. 1 Structural vulnerability in a military network graph: centrality + fragmentation under targeted node removal

3. PROBABILISTIC MODELING OF ATTACK PROPAGATION AND RISK QUANTIFICATION

Structural analysis explains where a military network is vulnerable. Probabilistic modeling explains how likely those vulnerabilities are to be exploited and how disruption propagates once initiated.

In adversarial environments, cyber incidents are not isolated deterministic events; they evolve dynamically depending on system state, defensive posture, and attacker strategy. For this reason, information security assurance in military networks must incorporate stochastic modeling techniques capable of capturing uncertainty and state transitions over time.

1) System State Representation

Let the operational state of a military computer network at time ***t*** be represented as a stochastic process ***X (t),*** defined over a discrete set of states:

- ***S_0:*** Fully Secure
- ***S_1:*** Partially Compromised
- ***S_2:*** Operationally Degraded
- ***S_3:*** Mission-Critical Failure
- ***S_4:*** Recovery / Restored

Transitions between states are governed by probabilities $P_{ij} = P(X_{t+1} = S_j \mid X_t = S_i)$, forming a Markov chain model [5]. This approach allows quantification of:

- Probability of escalation from local compromise to systemic degradation
- Mean Time to Compromise (MTTC)
- Mean Time to Recovery (MTTR)
- Steady-state probability of mission-critical failure

Markov models have been widely used in reliability engineering and cybersecurity risk analysis for dynamic system evaluation [6][7].

2) Attack Propagation Modeling

In networked environments, compromise rarely remains localized. Propagation can be modeled through:

- Epidemic-type diffusion models (analogous to SIR models in network epidemiology) [8]
- Continuous-time Markov chains for lateral movement analysis [9]
- Bayesian networks for conditional dependency modeling among vulnerabilities [10]

If β denotes compromise propagation rate and γ recovery rate, then network-wide compromise dynamics can be approximated by:

$$\frac{dI(t)}{dt} = \beta I(t)(N - I(t)) - \gamma I(t)$$

where *I(t)* is the number of compromised nodes at time *t*, and *N* is total nodes.

Such formulations provide measurable thresholds for outbreak-like compromise cascades, particularly relevant for tactical environments with shared credentials or centralized trust services.

Propagation modeling is consistent with systemic risk concepts in complex networks, where interdependence increases vulnerability to cascading failures [11].

3) Risk Quantification Framework

Risk in military cybersecurity can be defined as:

$$R = P(A)xI(A)$$

where *P(A)* = Probability of attack success, *I(A)* = Operational impact

This aligns with formal risk assessment frameworks such as NIST SP 800-30 and NIST SP 800-37 [12][13].

However, in military contexts, impact is not purely economic; it is mission-centric. Therefore, impact may be measured as:

- Loss of connectivity between C2 nodes
- Delay in ISR data transmission
- Reduction in secure communication capacity
- Probability of mission objective failure

Bayesian updating allows real-time recalibration of risk as new intelligence becomes available:

$$P(A|E) = \frac{P(E|A)P(A)}{P(E)}$$

where E represents observed events or anomaly indicators [10].

This enables dynamic risk posture evaluation instead of static compliance assessment.

4) Operational Interpretation

The integration of stochastic modeling with structural analysis produces a powerful capability:

- Structural metrics identify critical nodes.
- Probabilistic models estimate the likelihood of their compromise.
- Combined, they produce expected fragmentation risk curves.

Such modeling supports:

- Defensive resource prioritization
- Redundancy planning
- Mission-level contingency preparation
- Cyber defense readiness assessment

In contested operational theaters, security must be expressed as probability distributions rather than binary classifications.

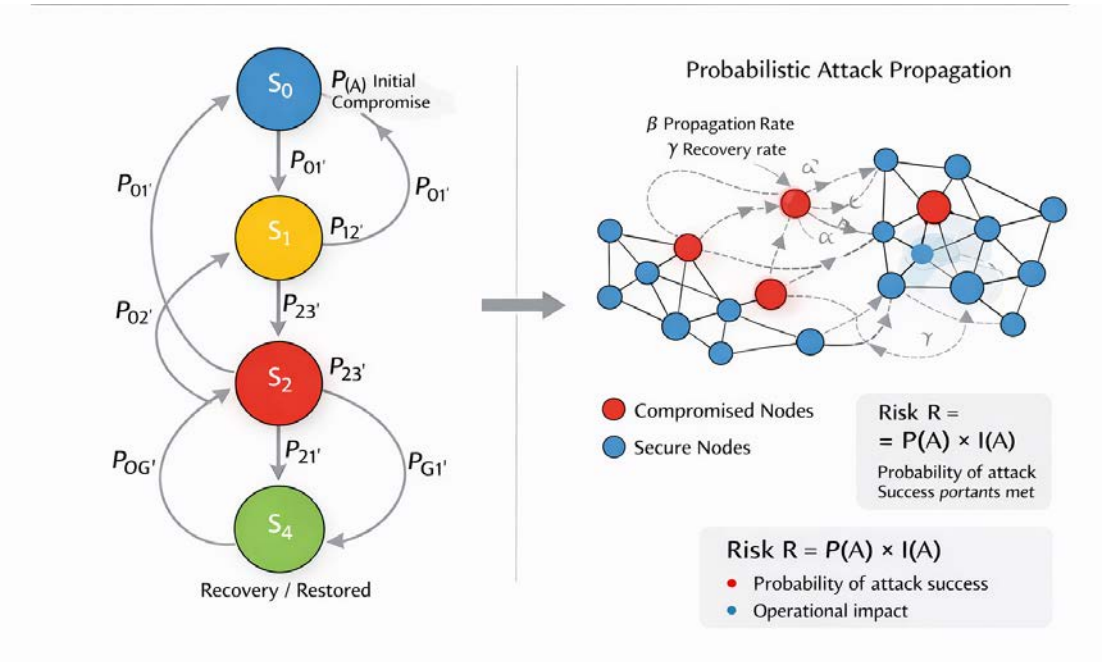

FIG. 2 Probabilistic Attack Propagation Model

3. QUANTITATIVE RESILIENCE AND RECOVERY METRICS IN MILITARY NETWORKS

In military operational environments, security cannot be defined solely by the absence of compromise. A network may be partially degraded yet still mission-capable. Therefore, resilience becomes a central quantitative parameter in evaluating information security assurance.

Resilience is defined here as the measurable capacity of a military computer network to maintain or rapidly restore mission-essential functionality under adverse cyber conditions [14][15].

a) Formal Definition of Network Resilience

- $\mathbf{P_{nominal}}$ = baseline operational performance (e.g., throughput, latency, secure session availability),
- $\mathbf{P_{attack}(t)}$ = performance under adversarial conditions,
- $\mathbf{T_r}$ = recovery time after disruption.

Resilience over time may be expressed as:

$$R(t) = \frac{P_{attack}\ (t)}{P_{nominal}}$$

where $0 \leq R(t) \leq 1$.

A fully operational network has $R(t)=1$; complete failure corresponds to $R(t) \approx 0$.

This formulation aligns with resilience engineering principles applied in critical infrastructure protection [16] and is consistent with NATO's resilience doctrine emphasizing continuity of essential functions [17].

b) Performance Degradation and Recovery Curve

Operational resilience is best visualized as a time-dependent degradation and recovery curve. Key measurable parameters:

- Time to Detect (TTD)
- Time to Contain (TTC)
- Mean Time to Recovery (MTTR)
- Maximum Performance Degradation (ΔPmax)
- Area Under the Performance Curve (AUPC) – representing cumulative operational loss

Mathematically, cumulative mission impact may be approximated as:

$$Impact = \int_{t_0}^{t_r} [1 - R(t)]dt$$

This integral provides a quantitative measure of total mission degradation, not just peak disruption.

Resilience literature emphasizes that systems with identical peak degradation may differ significantly in recovery velocity and therefore in total mission impact [18][19].

c) Redundancy and Connectivity Thresholds

From a network science perspective, resilience depends on:

- Redundant routing paths,
- Distributed control nodes,
- Absence of single points of failure,
- Maintenance of connectivity above percolation threshold [20].

If connectivity drops below a critical fraction $\boldsymbol{p_c}$, the giant component collapses and coordinated operations become infeasible [21].

Thus, resilience planning involves ensuring that:

$|C_{largest}| \geq \alpha N$

Where $\boldsymbol{\alpha}$ is a mission-defined minimum operational connectivity threshold.

In military architectures, this may correspond to:

- Minimum required connectivity between command echelon nodes,
- Sustained ISR data flow to decision centers,
- Secure cross-domain communication continuity.

d) Mission-Oriented Interpretation

Resilience must be mission-centric rather than infrastructure-centric. A network is resilient if:

- Command authority remains synchronized,
- Situational awareness is preserved,
- Secure communications are sustained,
- Recovery mechanisms prevent cascading systemic failure.

Modern cyber defense doctrine emphasizes that resilience is not static robustness but adaptive capacity [22].

- Quantitative resilience metrics therefore support:
- Defensive investment prioritization,
- Redundancy allocation strategies,
- Cyber exercise evaluation,
- Operational readiness certification.

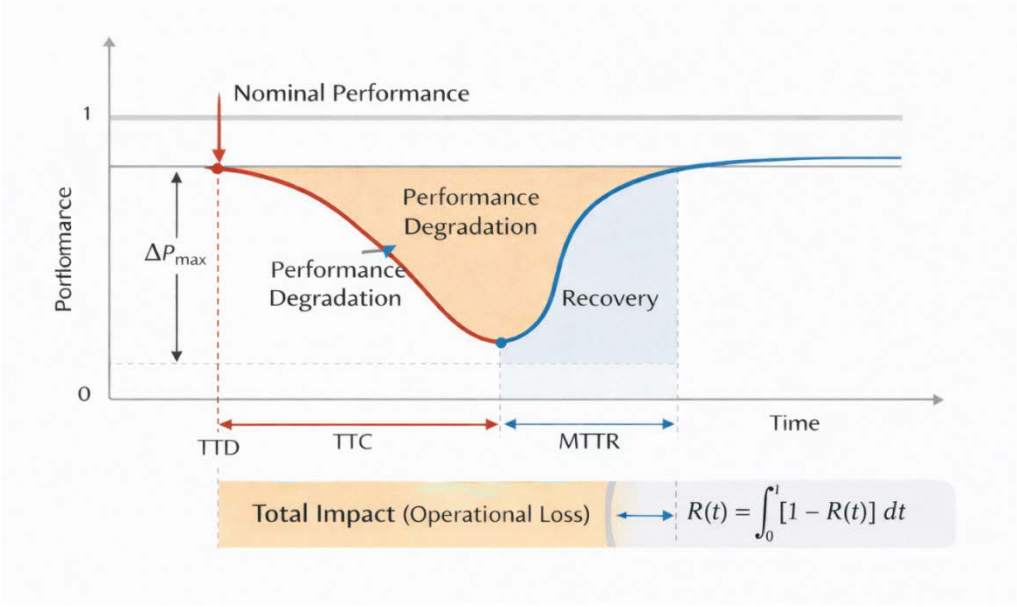

FIG. 3 Network Performance Degradation and Recovery Model

The diagram illustrates the temporal evolution of network performance during and after a cyber disruption in a military operational environment. At the moment of attack onset, performance begins to degrade until reaching a minimum operational level. The duration between attack detection and containment (TTD and TTC) directly influences the depth of degradation. The recovery phase (MTTR) reflects the system's resilience capacity and defensive preparedness. The shaded area represents cumulative operational loss, which quantifies total mission impact rather than peak disruption alone.

The resilience profile is reflected in both degradation slope and recovery speed, which indicate defensive effectiveness.

A rapid recovery phase suggests adequate redundancy and coordinated response mechanisms. Minimizing cumulative performance loss over time remains the primary objective of mission-oriented security assurance.

CONCLUSIONS

The quantitative analysis developed in this study demonstrates that information security assurance in military computer networks cannot be effectively evaluated through static compliance mechanisms alone. In operational military environments, where adversarial intent, technological asymmetry, and temporal pressure coexist, security must be defined as a measurable and dynamically evolving system property. By integrating structural graph analysis, stochastic modeling of adversarial propagation, and resilience-based performance metrics, the research establishes a coherent analytical framework capable of supporting mission-oriented cybersecurity assessment.

The structural vulnerability perspective confirms that network topology directly influences operational survivability. Centralized architectures, while efficient in peacetime configurations, may introduce disproportionate systemic risk when high-centrality nodes are targeted [1][4]. Graph-theoretic indicators such as betweenness, connectivity thresholds, and articulation points provide objective criteria for identifying critical structural dependencies [3]. These findings support architectural diversification and redundancy planning as fundamental elements of military network design.

The probabilistic dimension further reinforces the necessity of dynamic evaluation. By modeling cyber incidents as stochastic state transitions, the study aligns with established risk-based frameworks that emphasize continuous assessment and adaptive response [5][12][13]. The integration of Markov processes and Bayesian updating allows for real-time estimation of compromise likelihood and escalation probability. Such modeling transforms cybersecurity from reactive mitigation to predictive defense, enabling prioritization of resources based on quantified exposure rather than assumed threat posture.

Equally important is the resilience-oriented interpretation of security. In military operations, complete prevention of compromise cannot be guaranteed; however, mission continuity must be preserved. The resilience framework presented herein quantifies degradation, recovery velocity, and cumulative mission impact, emphasizing that total operational loss over time is a more meaningful metric than instantaneous failure magnitude [14][18][19]. This approach is consistent with contemporary resilience doctrine and critical infrastructure protection principles [16][17], where adaptability and recovery capacity are integral to strategic defense planning.

Taken together, the three analytical dimensions, structural robustness, probabilistic risk propagation, and quantitative resilience, form a unified scientific methodology for evaluating and strengthening information security in military computer networks. The framework supports evidence-based decision-making in architectural design, cyber defense investment, and operational readiness assessment. It bridges theoretical foundations in network science and probability theory with the practical realities of contested digital battlefields.

ACKNOWLEDGMENT

The author expresses appreciation to the academic and professional community whose scientific contributions in the fields of network science, cybersecurity and resilience engineering provided the theoretical foundation for this research.

The development of this work benefited from constructive professional discussions and the broader body of established research in quantitative risk assessment and military information systems security.

The responsibility for the content, interpretations, and conclusions presented in this paper rests entirely with the author.

REFERENCES

[1] R. Albert, H. Jeong, A.-L. Barabási, *Error and attack tolerance of complex networks,Nature*, vol. 406, pp. 378–382, 2000;
[2] M. Molloy, B. Reed, *A critical point for random graphs with a given degree sequence*, Random Structures & Algorithms, vol. 6, no. 2–3, pp. 161–180, 1995;
[3] M. E. J. Newman, *Networks: An Introduction*, Oxford, UK: Oxford University Press, 2010;
[4] R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, *Resilience of the Internet to random breakdowns*, Physical Review Letters, vol. 85, no. 21, pp. 4626–4628, 2000;
[5] J. R. Norris, Markov Chains. Cambridge, UK: Cambridge University Press, 1998;
[6] K. S. Trivedi, *Probability and Statistics with Reliability*, Queuing, and Computer Science Applications, 2nd ed. New York, NY, USA: Wiley, 2001;
[7] J. Wang, J. Liu, Y. Zhang, *Security risk assessment model based on Markov chains*, Computers & Security, vol. 28, no. 6, pp. 447–456, 2009;
[8] R. Pastor-Satorras, A. Vespignani, *Epidemic spreading in scale-free networks*, Physical Review Letters, vol. 86, no. 14, pp. 3200–3203, 2001;
[9] S. Jajodia, P. Liu, V. Swarup, C. Wang (Eds.), *Cyber Situational Awareness*, Boston, MA, USA: Springer, 2010;
[10] J. Pearl, Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. San Francisco, CA, USA: Morgan Kaufmann, 1988;
[11] S. V. Buldyrev et al., *Catastrophic cascade of failures in interdependent networks*, Nature, vol. 464, pp. 1025–1028, 2010;
[12] NIST, *Guide for Conducting Risk Assessments*, NIST SP 800-30 Rev. 1, 2012;
[13] NIST, *Risk Management Framework for Information Systems and Organizations*, NIST SP 800-37 Rev. 2, 2018;
[14] I. Linkov, A. Kott (Eds.), *Cyber Resilience of Systems and Networks*, Cham, Switzerland: Springer, 2019;
[15] D. D. Woods, *Four concepts for resilience and the implications for the future of resilience engineering*, Reliability Engineering & System Safety, vol. 141, pp. 5–9, 2015;
[16] National Research Council, Disaster Resilience: A National Imperative. Washington, DC, USA: National Academies Press, 2012;
[17] NATO, Commitment to Enhance Resilience, Brussels, Belgium, 2016;
[18] D. Henry, J. E. Ramirez-Marquez, *Generic metrics and quantitative approaches for system resilience*, Reliability Engineering & System Safety, vol. 99, pp. 114–122, 2012;
[19] S. Hosseini, K. Barker, J. E. Ramirez-Marquez, *A review of definitions and measures of system resilience*, Reliability Engineering & System Safety, vol. 145, pp. 47–61, 2016;
[20] D. S. Callaway et al., *Network robustness and fragility: Percolation on random graphs*, Physical Review Letters, vol. 85, no. 25, pp. 5468–5471, 2000;
[21] M. E. J. Newman, *Spread of epidemic disease on networks*, Physical Review E, vol. 66, 016128, 2002;
[22] National Academies of Sciences, Enhancing the Resilience of the Nation's Electricity System, Washington, DC, USA: National Academies Press, 2017;
[23] ISO/IEC, Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27001, 2013;
[24] ENISA, Cybersecurity Risk Management Framework, European Union Agency for Cybersecurity, 2016;
[25] C. Tankard, Advanced persistent threats and how to monitor and deter them, Network Security, vol. 2011, no. 8, pp. 16–19, 2011;
[26] A. Kott , C. Arnold, *The promise of autonomous intelligent cyber-defense agents*, Computer, vol. 46, no. 11, pp. 56–63, 2013.