Advances in Military Technology
Vol. 21, No. 1, 2026, pp. 223-246
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.02065

Network-Centric Warfare in the Age of Chaos, Complexity, and Cyber Conflict

C. Şen*

NATO Communications and Information Systems Group (NCISG), Mons, Belgium

The manuscript was received on 7 December 2025 and was accepted after revision for publication as a case study on 17 May 2026.

Abstract:

Modern warfare is shaped by a convergence of digital connectivity, multi-domain operations, and persistent cyber threats, which undermine information reliability and command and control coherence. This article develops a theoretical framework that reconceptualizes Network-Centric Warfare as a socio-technical system composed of four interdependent layers: cognitive, organizational, technological, and cyber. Drawing on cyber warfare research, chaos theory, and knowledge management, it explains how forces can sustain decision advantage when contested networks degrade, misinform, and cascade failures across units. The framework challenges classical NCW assumptions of stable networks, trustworthy information, transparent operational pictures, and advances an integrated model with research propositions linking cyber resilience and network redundancy to organizational adaptability and cognitive performance. It informs future design of C4ISR and multinational cyber cooperation.

Keywords:

Network-Centric Warfare, Multi-Domain Operations, chaos and complexity, cyber warfare, situational awareness, military decision systems

1 Introduction

This study's primary novelty lies in developing an integrated multi-layered conceptual framework that explicitly connects cognitive, organizational, technological, and cyber layers within Network-Centric Warfare (NCW). Unlike prior studies that examine these elements separately, this framework reconceptualizes NCW as a cyber-resilient socio-technical system in which information integrity becomes the central determinant of decision superiority.

Twenty-first-century warfare is evolving rapidly as digitalization, AI, and cyber operations shift the focus from physical maneuver and firepower toward information

* *Corresponding author: NATO CIS Group, SHAPE, Rue Grande, 7010, Mons, Belgium. Phone: +32(0)6544 1575, E-mail: cem.sen@nato.int. ORCID 0000-0002-7300-0170.*

flows, network structures, and cognitive processes. This transformation fundamentally changes how military forces perceive and respond to modern threats [1–4].

Traditional warfare emphasized maneuver, firepower, and territorial control. Contemporary conflict increasingly turns on information flows, network structures, and the cognitive processes that shape how militaries perceive, interpret, and respond to threats. Modern armed forces therefore rely on highly interconnected socio-technical systems that integrate humans, machines, algorithms, and cyber infrastructures across multiple domains of conflict [5, 6].

These trends offer strategic advantages, including faster decision cycles, cross-domain synchronization, and greater operational reach, but they also introduce systemic fragilities. Modern forces depend on accurate, continuous data flows, resilient communications, and coherent shared situational awareness. Cyber disruption, misinformation campaigns, and autonomous adversarial agents can therefore rapidly degrade decision-making and operational performance [7].

Three structural shifts distinguish contemporary warfare from earlier eras. First, the modern battlespace is data-saturated. Prolific Intelligence, Surveillance and Reconnaissance (ISR) platforms, autonomous systems, cyber sensors, and open-source intelligence generate massive quantities of heterogeneous data [8, 9]. This abundance offers power but also causes cognitive strain, as leaders must distinguish signal from noise under pressure [10, 11]. Second, military operations increasingly resemble Complex Adaptive Systems (CAS) marked by nonlinearity, emergence, interdependence, and rapid shifts in adversary behavior [12–14]. Outcomes emerge from dynamic interactions between humans, machines, and algorithms rather than predictable patterns. Third, the cyber domain has fundamentally altered the ontology of conflict. Adversaries can now attack the informational foundations of decision-making by corrupting data, spoofing sensors, eroding trust in command systems, and manipulating shared mental models [15, 16]. Cyber operations therefore target not only physical capabilities but the cognitive and organizational processes that shape military action.

Introduced in the late 1990s, NCW sought to harness emerging information technologies by networking sensors, shooters, and decision-makers to improve shared situational awareness, accelerate decision cycles, and enhance mission effectiveness [1, 17, 18]. It strongly influenced U.S., NATO, and allied doctrine, particularly in Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) development and joint operations [9, 4]. However, its core assumptions predate state-sponsored cyber warfare, AI-enabled misinformation tools, and mature distributed Multi-Domain Operations (MDOs). NCW must therefore be reconceptualized to remain relevant in the cyber age.

Despite substantial research in the individual areas of NCW, cyber warfare, chaos theory, complexity science, and knowledge management, the literatures remain fragmented. NCW studies often focus on technological architecture and interoperability but under-theorize the impact of contested, deceptive, or corrupted data [3, 19]. Cyber warfare literature emphasizes offensive and defensive operations but rarely integrates the organizational and cognitive components essential to NCW decision superiority [15, 20]. Complexity theorists describe adaptation and emergence but seldom connect these concepts to network-centric command structures [12, 14, 18]. Finally, Knowledge Management (KM) and sense-making research highlights how individuals interpret ambiguous information but does not fully consider how cyberattacks manipulate cognitive processes at scale [6, 21–23].

This article argues that NCW remains a valuable doctrinal foundation but must evolve into a cyber-resilient, cognitively informed, complexity-aware socio-technical doctrine. Specifically, NCW must shift from connectivity to trustworthy connectivity and from information volume to information integrity, while strengthening organizational adaptability and cognitive resilience [2, 5, 7]. The article develops an integrated, multi-layered model comprising:

- cognitive layer (sense-making, attention, mental models, cognitive overload),
- organizational layer (mission command, decentralization, adaptive structures),
- technological layer (network topology, redundancy, cyber defense architecture),
- cyber layer (adversarial manipulation, misinformation, deception, cyber-physical disruption).

Following the development of this framework, the article proposes research propositions that connect cyber resilience, network structures, sense-making quality, and decision superiority. The remainder of the article proceeds as follows. Section 2 reviews key theoretical foundations across NCW, cyber warfare, complexity science, chaos theory, and knowledge management. Section 3 examines cyber warfare as a transformational domain. Section 4 reconceptualizes NCW considering cyber-contested environments. Section 5 integrates chaos and complexity insights into NCW dynamics. Section 6 presents the multi-layered conceptual model and associated research propositions. Section 7 discusses implications for C4ISR, MDO, NATO doctrine, and future warfare. Section 8 outlines limitations and future research directions, followed by the conclusion.

This article contributes to the literature by introducing a novel integrative model that explains NCW effectiveness under cyber-contested conditions. The framework advances existing theory by explicitly linking cyber resilience, cognitive sense-making, organizational adaptability, and technological robustness within a single coherent structure.

2 Literature Review and Theoretical Background

The inclusion of situational awareness theory, chaos theory, complexity science, and knowledge management serves a specific integrative purpose. These perspectives collectively explain how cyber disruption influences cognition, organizational adaptation, technological resilience, and operational effectiveness, forming the theoretical foundation of the proposed integrated model.

To clarify the manuscript's scope and goal, Situational Awareness (SA), chaos theory, complexity science, and knowledge management are used as complementary lenses rather than separate topical excursions. Together, they explain how cyber-contested information environments translate into NCW outcomes at different levels of analysis. SA captures the perception-comprehension-projection process through which degraded information integrity produces fragile or false awareness. KM and sense-making address how organizations validate, share, and update meaning under ambiguity and deception. Chaos theory highlights sensitivity to initial conditions and the nonlinear amplification of small digital perturbations, while complexity/CAS theory explains emergence, adaptation, and cascading failure in tightly coupled networked forces. These foundations motivate the four-layer model (cognitive, organizational, technological, cyber) and underpin the propositions linking cyber resilience, network design, organizational adaptability, and cognitive performance to decision superiority.

2.1 Network-Centric Warfare: Evolution, Assumptions, and Critiques

NCW emerged in the late 1990s as a transformative concept designed to leverage advances in information technology, digital communications, and C4ISR systems. Its core logic rests on a widely cited operational chain in which: Information Superiority → Shared Situational Awareness → Self-Synchronization → Increased Combat Power.

This logic is anchored in three foundational pillars articulated by Alberts [1]:

- high-quality shared information,
- robustly networked forces,
- decentralized decision-making.

Subsequent work has revisited and refined these pillars for the contemporary information age, emphasizing agility, focus, and convergence in complex environments [1, 3]. NCW reflected the technological optimism of its time: the Internet was expanding rapidly, cyber risks were less visible, and military networks were assumed to be relatively secure. Early NCW debates therefore prioritized connectivity, interoperability, and information flow, often implying that more data and more connectivity would automatically translate into better decisions and faster operational tempo [18, 19].

Foundational Assumptions of Classical NCW

NCW was built on several assumptions that, although reasonable at the time, no longer hold in cyber-contested environments. These include:

- data is reliable and largely trustworthy,
- networks operate with minimal hostile interference,
- information sharing reliably enhances operational clarity,
- decision-makers can interpret shared information effectively,
- connectivity correlates directly with military advantage.

These assumptions reflected a pre–cyber warfare environment in which adversaries had limited capacity to manipulate data or degrade networks at scale. But today, cyber adversaries can corrupt data, inject false information, spoof sensors, or degrade networks [15, 16]. Under cyberattack, more data does not necessarily mean more clarity; it can mean more confusion.

Critiques of Classical NCW

Recent scholarship has challenged the applicability of NCW's original assumptions in contemporary operations.

Technological Determinism: NCW has been criticized for overemphasizing technology while underemphasizing human cognition, organizational culture, and the socio-technical dynamics of command [24].

Cyber Vulnerability: NCW's reliance on uninterrupted networks is increasingly unrealistic. Cyberattacks can corrupt data, disrupt communications, spoof sensors, or inject false information [16].

Cognitive Overload: The exponential growth of data does not always improve decision-making. Endsley [11, 25] argues that information overload can degrade situational awareness, especially when data is ambiguous or compromised.

Given these challenges, scholars argue that NCW must shift from an architecture-centric approach to an integrity- and resilience-centric framework capable of operating effectively under contested conditions [1, 2, 19].

2.2 Knowledge Management, Information Processing, and Military Sense-making

KM plays a central role in contemporary military operations, shaping how organizations acquire, interpret, store, and disseminate knowledge. Nonaka's [21] distinction between tacit and explicit knowledge remains particularly relevant in operational settings where intuition, experience, and context-specific understanding are indispensable for interpreting ambiguous information. The broader knowledge-creating firm perspective further underscores how organizational structures and routines convert individual insights into collective capability [6, 22]. In defense organizations undergoing rapid digital transformation, KM systems and command structures increasingly co-evolve with network-centric architectures [2, 5].

Sense-Making Under Ambiguity

Weick's [23] sense-making framework provides valuable insight into how individuals construct meaning in fast-moving, uncertain environments. Military sense-making involves:

- extracting relevant cues from the environment,
- filtering noise from chaotic information flows,
- developing shared mental models,
- updating interpretations as the situation evolves.

Cyber warfare significantly complicates these processes. When adversaries deliberately manipulate data, decision-makers must not only interpret ambiguous inputs but also question the authenticity of the information itself [15].

Information Overload and Cognitive Saturation

Endsley [10, 11] highlights the growing risk of cognitive saturation in data-rich battlefields. When information exceeds human processing capacity, situational awareness deteriorates. This effect is intensified in cyber-contested environments where

- contradictory data sources,
- inconsistent system outputs, and
- spoofed or corrupted sensor feeds

force operators to continuously distinguish trustworthy information from adversarial manipulation. Thus, sense-making becomes the cognitive anchor of NCW, especially when cyber threats introduce ambiguity and distrust into the information ecosystem [2, 6].

2.3 Chaos Theory: Nonlinearity, Sensitivity, and Disorder in Warfare

NCW systems magnify this sensitivity because their interdependencies amplify local shocks [12]. Viewing militaries as Complex Adaptive Systems (CAS) shows that they function best at the "edge of chaos" – balancing structure with the fluidity needed for rapid adaptation [26].

Chaos theory offers a useful lens for understanding the unpredictability of modern military operations [27]. Lorenz's [28] principle of sensitivity to initial conditions, known as the "butterfly effect", illustrates how minor disruptions can produce disproportionate operational consequences.

Examples relevant to NCW include:

- a brief communications outage,

- a corrupted or spoofed sensor reading,
- a misinterpreted intelligence cue,
- a small cyber intrusion that escalates unexpectedly.

These disturbances can initiate nonlinear chain reactions, particularly in networked environments where interdependencies amplify the impact of local disruptions [29]. NCW systems magnify this sensitivity because networks connect distributed units, making them more effective but also more vulnerable to systemic shock [12].

2.4 Complexity Theory: Military Systems as Complex Adaptive Systems (CAS)

Complexity theory conceptualizes military organizations as CAS - structures composed of interacting agents that continually adapt to changing conditions. Modern militaries embody key CAS characteristics:

- continuous adaptation to adversarial strategies,
- dynamic interactions among human and technological actors,
- feedback loops that accelerate decision cycles,
- emergent behaviors that arise without central coordination.

Scholars such as Holland [13] and Mitchell [14] note that CAS often operate far from equilibrium, precisely the conditions that characterize modern MDO. Bar-Yam [12] similarly shows how complex military conflicts exhibit nonlinear, emergent dynamics.

NCW aligns naturally with CAS theory because it:

- encourages decentralized adaptation,
- enables self-synchronization,
- supports rapid feedback and reconfiguration,
- leverages distributed decision-making [18].

However, this interconnectedness also creates vulnerabilities. Under cyberattack, tightly coupled systems may fail catastrophically, demonstrating the need for resilient, adaptive structures [7, 30].

2.5 Cyber Warfare: Information Integrity as the New Battlespace

Cyber warfare represents a qualitative shift in how militaries contest and achieve advantage, in other words, it alters the ontology of warfare itself. Rather than targeting physical assets alone, cyber operations increasingly aim to compromise:

- the authenticity and reliability of information,
- the credibility of command structures,
- the functionality of sensors and data streams,
- the cognitive processes through which humans interpret information [15, 16].

As comes to the characteristics of cyber warfare, cyber conflict is characterized by:

- Stealth: intrusions may remain undetected for long periods,
- Speed: operations unfold at machine pace,
- Ambiguity: attribution is often uncertain,
- Pervasiveness: impacts span all operational domains,
- Manipulation: operations target perception, cognition, and trust [15, 16].

In NCW, where the quality of shared information is paramount, cyber threats undermine the core mechanism through which decision superiority is achieved.

Cyberattacks do not only disrupt operations, but they also reshape the informational and cognitive environment upon which NCW depends [2, 7].

In summary, foundational assumptions of military networking, such as the inherent reliability of data and the stability of networks are now compromised by cyber adversaries. Consequently, military "sense-making" must serve as the cognitive anchor to help commanders distinguish signal from noise and navigate the "butterfly effect" of small digital disruptions.

3 Cyber Warfare as a Transformative Operational Domain

Cyber warfare represents one of the most profound conceptual and operational transformations in the history of armed conflict. Unlike land, maritime, air, and space, the cyber domain has no physical terrain, material boundaries, or fixed battle lines. Instead, it is a battlespace constituted by information flows, computational architectures, machine logic, and the cognitive vulnerabilities of human operators [15, 16]. Its effects are tangible and often strategically decisive: attacks can disable critical infrastructure, hijack unmanned systems, corrupt targeting data, disrupt logistics networks, and degrade Command-and-Control (C2) functions [3, 7].

Within an NCW environment, operational effectiveness depends on trustworthy data, resilient networks, and uninterrupted connectivity. Cyber warfare has therefore emerged as a decisive arena in which information integrity and decision-making superiority are contested [1, 2, 4].

3.1 The Cyber Battlespace: Speed, Stealth, and Ambiguity

Cyber conflict unfolds at machine speed. Kinetic engagements involve detection, assessment, and action cycles measured in minutes or hours; cyber actions can propagate across networks in milliseconds, far faster than human cognition can perceive and react [2, 8]. This acceleration compresses the Observe-Orient-Decide-Act (OODA) loop and challenges commanders' ability to detect unfolding attacks, interpret their meaning, and respond before significant operational degradation occurs.

Stealth further distinguishes the cyber domain. Intrusions can remain latent for months, hidden within legitimate processes or encrypted traffic [15, 16]. Whereas traditional ISR capabilities detect physical signatures such as troop movements, missile launches, or maritime maneuvers where cyber penetrations often leave no observable trace until activated. This stealth, combined with the problem of attribution, means commanders may face paralyzing uncertainty: Who attacked? What is the intent? Is the intrusion ongoing? Can data still be trusted? Such uncertainty directly undermines NCW's foundational assumption of trustworthy shared information.

Ambiguity is perhaps the defining characteristic of cyber conflict. Data may appear valid but be manipulated; systems may operate normally while feeding corrupted outputs into C4ISR networks; and logs may be falsified to fabricate threats or conceal real ones. Cyber operations weaponize epistemic uncertainty, generating what scholars describe as a synthetic fog of war – not by an absence of information, but by an excess of unreliable or deceptive information [7, 15].

Speed, stealth, and ambiguity make cyber warfare a domain where adversaries aim not only to disrupt systems but also to shape perception, distort decision-making, and exploit vulnerabilities in networked military ecosystems [3, 16].

3.2 Cyber-Induced Chaos and Cascading Failures

NCW architectures integrate vast arrays of sensors, platforms, data repositories, and decision nodes, creating tightly coupled, interdependent systems. Cyberattacks exploit these couplings, initiating cascading failures that propagate rapidly across the entire network [12, 30].

In complex, interconnected military ecosystems, a single corrupted data point can ripple through an entire C4ISR structure:

- a spoofed GPS signal may divert unmanned aerial systems,
- a falsified radar return may trigger false air-defense engagements,
- a compromised sensor may distort the Common Operational Picture (COP),
- malware in logistics systems may halt mobilization or deployment.

This fragility is consistent with complexity science findings: the more interconnected the system, the more vulnerable it becomes to catastrophic cascades [7, 12].

Zero-day vulnerabilities allow adversaries to infiltrate networks without detection. Once inside, they may:

- alter system parameters,
- corrupt firmware,
- implant logic bombs,
- manipulate data flows.

These latent intrusions transform military networks into potential battlespaces preshaped for adversary advantage. Integrity can no longer be assumed; trust becomes a contested resource [7, 16].

The Network-Centric Warfare (NCW) doctrine traditionally assumes that connectivity functions as an operational force multiplier. Yet cyber warfare exposes the paradox of over-connectivity; the more connected the force, the greater its systemic exposure to disruption. Over-networked systems risk *operational rigor mortis*, wherein the compromise of one subsystem cascades, crippling the force's ability to sense, decide, and act [3, 30].

3.3 Algorithmic Conflict and Cognitive Manipulation

The fusion of AI, machine learning, and cyber tools has transformed cyber conflict into an algorithmic struggle. Cyberattacks no longer simply disable systems, they manipulate cognition, perception, and organizational behavior [2, 8].

AI-enabled tools can generate falsified:

- audio commands,
- video broadcasts,
- sensor outputs,
- operational orders.

These fabrications undermine trust in data, leadership, and the chain of command. Tailored misinformation leverages psychological, cultural, and organizational biases to degrade cohesion and morale. Examples include:

- fake battlefield reports that distort situational awareness,
- AI-generated imagery embedded in ISR streams,
- manipulated social media narratives targeting deployed forces,
- false commands intended to create hesitation or disorder.

The strategic aim is not merely to deceive systems but to undermine human sense-making. By delaying decisions and fracturing unity of effort, adversaries force commanders to operate in a cognitive environment dominated by uncertainty [15, 23].

Autonomous cyber tools introduce additional complexity. Machine-speed defensive and offensive algorithms can interact in ways that create feedback loops and escalation dynamics that outpace human control or comprehension. As these agents shape the tempo and structure of cyber engagements, operational authority may shift from human to machine, enabling algorithmic tempo dominance beyond conventional command hierarchies [2, 8].

In short, the cyber domain weaponizes speed and ambiguity to manipulate human perception and erode trust in the chain of command. Because military systems are so tightly coupled, a single corrupted data point can trigger "cascading failures" that cripple a force's ability to act.

4 Network-Centric Warfare in a Cyber-Contested Age

The limiting factor of modern NCW is no longer network capacity, but network trustworthiness.

4.1 Revisiting the Core Assumptions of NCW

NCW was built on several implicit assumptions about the information environment:

- data is trustworthy,
- sensors report accurate observations,
- networks remain reliable and available,
- adversaries and effects can be consistently attributed,
- cognitive environments remain stable and cooperative.

These assumptions aligned with the techno-optimism of the early digital age but no longer hold in contemporary cyber-contested battlespaces [1, 17, 19]. Cyber operations systematically target the very foundations on which NCW depends [15, 16].

In a cyber-threatened environment:

- more information may create less clarity, as volume amplifies noise and adversarial manipulation [10, 11],
- faster information flows may propagate corrupted data more rapidly, accelerating decision-making errors [2],
- shared information can synchronize forces around falsehoods, producing coherent but inaccurate cops.
- decentralization increases the speed at which compromised data spreads, magnifying system-wide damage [7, 30].

Thus, NCW must shift from an emphasis on information abundance to information integrity. The limiting factor of contemporary NCW is no longer network capacity but network trustworthiness. When the authenticity and integrity of data cannot be guaranteed, the network becomes a liability that amplifies confusion, distorts decision cycles, and produces false confidence [16, 20].

A reconceptualized NCW model must therefore recognize that connectivity without trust creates strategic vulnerability [19, 24].

4.2 Information Integrity: The New Foundation of Situational Awareness

Endsley's [25] three-stage model of SA, which are perception, comprehension, and projection, provides a theoretically rigorous framework for understanding the impacts of cyber operations on military decision-making [10, 11, 15].

Cyberattacks undermine each stage of SA:

- Perception: By corrupting sensor data, spoofing signatures, or manipulating telemetry streams, adversaries degrade the initial layer of environmental understanding,
- Comprehension: By altering meaning through data injection, algorithmic misinformation, or falsified ISR outputs, cyber operations distort commanders' mental models of the battlespace,
- Projection: By manipulating data trends or fabricating future threat indicators, cyber tools compromise commanders' expectations of enemy action, force posture, and operational tempo.

The result is false SA, a condition in which decision-makers hold high confidence in a COP that is fundamentally inaccurate. False SA is more dangerous than low SA because it encourages decisive action based on erroneous assumptions [2, 10, 11].

To counteract this risk, NCW architectures must incorporate mechanisms for continual trust recalibration, such as:

- automated integrity assessment,
- sensor and data provenance verification,
- anomaly detection supported by AI and machine learning,
- authentication protocols for high-consequence communications,
- hybrid human-machine sense-making systems [6, 7].

Information integrity, rather than information volume, must therefore become the central design principle of NCW-enabled operations. Without it, the cognitive and organizational advantages promised by NCW collapse [1, 5].

4.3 Distributed Autonomy and Mission Command in Cyber-Degraded Environments

As NCW architectures face increasing cyber degradation, the viability of traditional centralized C2 structures becomes impaired. In such contexts, militaries rely more on mission command, a philosophy rooted in Auftragstaktik (mission-type tactics), which empowers subordinates to act independently based on the commander's intent rather than on detailed instructions [4, 31].

Mission command becomes critical in cyber-contested environments because it enables:

- operational continuity when communications are disrupted,
- independent decision-making without full COP visibility,
- rapid adaptation to unexpected local conditions,
- resilience when central nodes or headquarters are compromised.

Distributed autonomy transforms the force into a CAS, a network capable of self-organization, redundancy, and emergent coordination even when parts of the system fail [13, 18]. Rather than collapsing under centralized system degradation, the organization retains the capacity to sense, decide, and act locally.

However, increased autonomy carries trade-offs. Greater decentralization may reduce synchronization, complicating efforts to maintain unity of effort and operational coherence. NCW in a cyber-contested context must therefore balance:

- flexibility, to allow initiative at the tactical edge,
- coherence, to preserve alignment with strategic objectives,
- robustness, to withstand cyber disruption,
- convergence, to ensure distributed actions reinforce each other [4, 12].

The cyber domain fundamentally shifts this balance toward enhanced decentralization. The organization that survives and succeeds is one that tolerates controlled divergence, leverages distributed cognition, and integrates mission command at scale [5, 24].

NCW must succeed transition from valuing information volume to prioritizing information integrity. To survive in cyber-degraded environments, militaries must rely on distributed autonomy and mission command, empowering subordinates to act on intent even when their digital systems fail.

5 Chaos, Complexity, and Nonlinear Dynamics in Multi-Domain Operations (MDOs)

Contemporary military operations increasingly resemble complex adaptive systems (CAS) characterized by nonlinearity, unpredictability, and rapidly emerging behaviors. As NCW architectures converge with cyber-physical systems, autonomous agents, AI-enabled decision tools, and human operators across all operational domains (land, air, maritime, space, and cyber), the resulting battlespace becomes too dynamic to be understood through linear, reductionist models. Chaos and complexity theories offer powerful lenses to explain these dynamics and to guide the redesign of NCW for cyber-contested environments [13, 14, 27]. They highlight how small perturbations can escalate into major operational shifts, how tightly coupled systems can cascade toward failure, and how adaptation and self-organization can emerge unexpectedly across distributed forces [12, 29].

5.1 The Edge-of-Chaos Spectrum in Military Operations

Complex systems, including modern militaries, operate within a dynamic interval between rigid order and uncontrolled disorder – what Kauffman [26] terms the "edge of chaos". Systems positioned in this band exhibit:

- high adaptability and agility,
- efficient information flows,
- rapid and coordinated response,
- capacity for reorganization under stress,
- tolerance for uncertainty and unpredictability.

Military organizations function most effectively within this zone. Excessive structure results in rigidity and slow adaptation; insufficient structure leads to fragmentation and loss of coherence. For NCW in the cyber age, the central challenge is sustaining this delicate equilibrium amid pervasive cyber disruption [12, 18].

Order → Rigidity → Collapse

Systems that over-emphasize hierarchical control, centralized decision-making, and rigid procedural adherence tend to demonstrate:

- paralysis when plans fail or communications degrade,
- sluggish decision cycles incompatible with cyber-induced tempo,

- dependency on centralized networks prone to disruption,
- inability to improvise under conditions of uncertainty.

Overly ordered NCW systems thus risk brittle failure during cyber shocks [4, 7].

Chaos → Fragmentation → Failure

Conversely, systems that lean too far toward decentralization and fluidity may exhibit:

- competing or misaligned objectives across units,
- misinterpretation of operational signals,
- inability to concentrate effects or mass combat power,
- erosion of unity of effort and operational coherence.

This extreme results in fragmentation, where distributed forces act in parallel but not in concert.

The NCW Challenge

NCW was originally designed to move forces closer to the edge of chaos by enabling:

- shared situational awareness,
- decentralized self-synchronization,
- operational agility,
- adaptive decision cycles [17, 18].

However, cyber warfare threatens to push the system past the edge into instability. To prevent this, NCW systems must incorporate:

- information integrity verification,
- organizational resilience mechanisms,
- adaptive autonomy governed by commander's intent,
- robust sense-making processes capable of filtering deception [11, 23, 25].

Maintaining balance along the order–chaos continuum is thus essential for future NCW effectiveness [12, 26].

5.2 Emergence and Self-Organization in Distributed Forces

Emergence refers to global patterns, behaviors, or capabilities that arise from local interactions between individual elements without centralized control. In distributed military operations, emergent phenomena may include:

- spontaneous coordination among dispersed units,
- rapid adaptation to local conditions without explicit orders,
- innovative tactics developed at the tactical edge,
- self-reconfiguration of force posture to exploit opportunity or mitigate threat.

In theory, NCW amplifies positive emergence by enhancing connectivity and shared understanding. Yet cyber warfare fundamentally threatens these processes. In theory, NCW amplifies positive emergence by enhancing connectivity and shared understanding [1, 3]. Yet cyber warfare fundamentally threatens these processes.

Cyber Effects on Emergence

Adversarial cyber operations can:

- inject false or contradictory information into network flows,
- corrupt shared mental models and operational expectations,

- create divergent or incompatible COPs,
- erode trust between units and between humans and machines [7, 15].

These effects directly undermine emergent coordination and generate maladaptive emergence, where dysfunctional or contradictory behaviors proliferate across the force.

Self-Synchronization in NCW

Self-synchronization, a cornerstone NCW concept, describes the ability of distributed units to coordinate actions based solely on shared intent and situational awareness [1, 17]. For self-synchronization to occur effectively, several conditions must be met:

- reliable, authentic data,
- trusted information systems,
- confidence in mutual understanding,
- stable, coherent communication pathways.

When these foundations hold, units can operate with initiative and unity of purpose even without central direction.

The Cyber Disruption Problem

Cyberattacks that compromise data integrity undermine the very conditions necessary for self-synchronization. When information is corrupted:

- shared situational awareness becomes fractured,
- interpretations diverge across units and echelons,
- synchronization becomes misalignment,
- emergent behavior shifts from functional to dysfunctional [11, 15, 25].

This mirrors a fundamental principle of chaos theory: small perturbations in initial conditions can generate disproportionately large system-wide consequences [27, 28]. A single corrupted sensor feed can ripple through NCW architectures, producing cascading tactical and strategic distortions [12, 29].

5.3 Complex Network Effects and Cyber Conflict

Complex network science offers essential insights into how cyber operations propagate within NCW systems. Barabási [30] demonstrates that most real-world networks, including military C4ISR structures, exhibit scale-free properties, meaning they are dominated by highly connected nodes or hubs. These hubs represent critical vulnerabilities.

High-value military hubs include:

- central C2 and battle management servers,
- joint ISR fusion centers,
- satellite communication uplinks,
- strategic logistics databases,
- public key infrastructure and encryption servers.

Targeting these hubs enables adversaries to generate disproportionately large effects with minimal effort [7, 16].

Cyberattacks as Epidemic Phenomena: Cyber intrusions propagate through NCW networks much like biological epidemics:

- one compromised node infects adjacent systems,

- lateral movement expands adversary access,
- malware spreads across domains and classification boundaries,
- autonomous cyber agents exploit predictable network paths [12, 30].

Examples of cascading failures include:

- GPS spoofing → sensor misalignment → flawed targeting → strategic misjudgment,
- compromised logistics database → supply delays → operational stagnation → force degradation,
- air defense malware → false confidence in sensor coverage → catastrophic vulnerability.

The Complexity Paradox

Complexity science demonstrates that predictability decreases as coupling increases. NCW intentionally increases coupling through:

- more connections among units, sensors, and domains,
- higher data flow volume,
- greater reliance on automation and algorithmic processing.

Yet these same characteristics expand the number of pathways through which cyberattacks can propagate and compound [7, 12]. The paradox is clear: The more networked and data-rich an NCW system becomes, the more vulnerable it is to nonlinear disruption. To resolve this paradox, NCW must incorporate new design principles that explicitly manage complexity, such as modularity, adaptive decoupling, cyber-resilient redundancy, and human-in-the-loop cognitive safeguards [2, 7, 9].

In summary, the "Complexity Paradox" reveals that the more networked and data-rich a system becomes, the more pathways it offers for cyber-disruption to propagate. Future NCW designs must therefore incorporate modularity and "adaptive decoupling" to prevent localized cyberattacks from becoming systemic catastrophes.

6 The Multi-Layered Integrated Model of NCW in Cyber-Contested Environments

The four layers proposed in this model are dynamically interdependent. The technological and cyber layers shape the quality and integrity of information available to the cognitive layer, while the organizational layer governs how decisions are coordinated and implemented. Cyber threats exert cross-layer influence, affecting technological functionality, organizational coherence, and cognitive reliability simultaneously.

Fig. 1 summarizes the four layers (cognitive, organizational, technological, and cyber), their hierarchical and horizontal relationships, directional dependencies between layers, the influence of cyber threats across all layers, and how these interactions collectively influence decision superiority.

This section presents the central theoretical contribution of the study: a four-layer integrated model that conceptualizes NCW as a cyber-resilient socio-technical ecosystem. Contemporary battle networks cannot achieve decision superiority through technology alone; they require cognitive adaptability, organizational resilience, technological robustness, and active cyber defense [1, 2, 5].

Because each layer is interdependent, none is individually sufficient. Their interaction forms a CAS capable of maintaining functionality under adversarial pressure.

The four layers (cognitive, organizational, technological, and cyber) are explained below together with their derived research propositions.

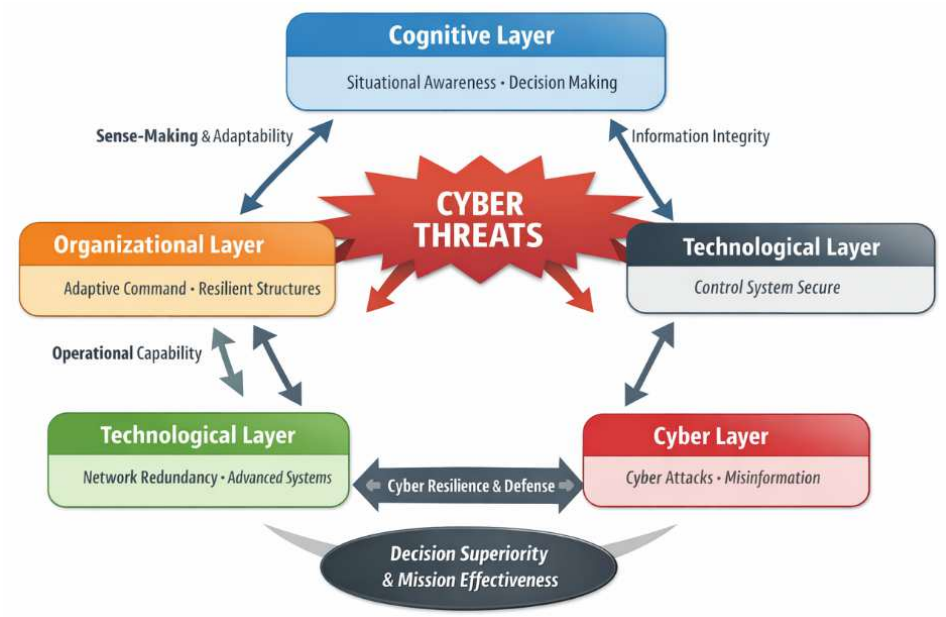

Fig. 1 The Multi-Layered Integrated Model of NCW in Cyber-Contested Environments

6.1 Cognitive Layer: The Foundation of Decision Superiority

Human cognition remains the decisive element in NCW, serving as the locus where information becomes knowledge and action. As Weick [23] emphasizes, sense-making involves continuously:

- noticing relevant cues,
- interpreting evolving patterns,
- constructing coherent meaning,
- projecting implications into the future.

Cyber warfare destabilizes each of these processes. Adversaries deliberately inject noise, fabricate false patterns, corrupt perceptions, and undermine trust in data sources [6, 15]. Under such pressure, operators face cognitive overload, making it increasingly difficult to discriminate:

- reliable from unreliable information,
- authentic from falsified signals, and
- operationally meaningful from irrelevant data [11, 25].

In cyber-contested environments, operators must therefore continuously calibrate trust, asking whether anomalies reflect technical malfunction, hostile manipulation, or natural system variation. Decision superiority thus hinges on the ability to maintain sense-making accuracy despite informational degradation [2, 23].

Because cyber manipulation increases uncertainty and contaminates information environments, the relationship between information volume and situational awareness

becomes fundamentally unstable; additional data may reduce clarity rather than enhance it. Hence, the following proposition is developed:

Proposition 1: *Cyber-induced uncertainty moderates the relationship between information volume and situational awareness.*

Given that high-integrity data cannot aid decision-making unless commanders can successfully interpret and integrate it, sense-making capability becomes the mediating cognitive mechanism linking data quality to decision performance. Thus, the following proposition is advanced:

Proposition 2: *Sense-making capability mediates the effect of information integrity on decision superiority.*

6.2 Organizational Layer: Resilience, Flexibility, and Mission Command

Where the cognitive layer concerns individual interpretation, the organizational layer reflects how militaries coordinate and adapt collectively. Modern operations require organizations that can maintain coherence when communications degrade, networks are attacked, or information becomes ambiguous [13, 18].

The NATO philosophy of Mission Command, centered on commander's intent, subordinate initiative, and decentralized execution, becomes indispensable in environments where centralized control is vulnerable to disruption [4]. Such structures form plastic organizations capable of:

- reconfiguring quickly,
- absorbing cyber-induced shocks,
- sustaining operational continuity despite degraded C2 [5, 7].

Cyber-contested NCW therefore shifts humans from system-dependent operators to supervisory decision-makers, whose judgement becomes even more vital when automation is compromised [2, 8].

Because decentralized organizations do not rely exclusively on central nodes, they are better able to sustain operations during communication loss or cyber disruption, thereby increasing resilience. Hence, the following proposition is created:

Proposition 3: *Decentralized structures enhance operational resilience under cyber degradation.*

Since adaptation must occur even when upper echelons lack complete situational awareness, mission command enables faster, localized adjustments that preserve momentum and coherence [4, 13]. Thus, the following proposition is developed:

Proposition 4: *Mission command positively influences the speed of adaptation in complex, cyber-contested environments.*

6.3 Technological Layer: Network Architecture, Redundancy, and Cyber Defense

The technological layer provides the infrastructure through which data is sensed, processed, and distributed. Resilient NCW architectures require:

- distributed nodes to avoid single points of failure,
- redundant pathways to preserve information flow, and
- failover mechanisms to ensure continuity under attack [7, 30].

Equally essential are cyber-defense functions such as integrity verification, anomaly detection, encryption, and AI-assisted threat monitoring [7, 16]. However,

while AI accelerates decision-making, it also introduces vulnerabilities including adversarial spoofing and reduced transparency [2, 8].

Because redundancy provides alternative routes for communication when primary systems are compromised, it mitigates the operational impact of cyber disruption by maintaining information flow. Therefore, the following proposition is developed:

Proposition 5: *Network redundancy moderates the effect of cyber disruption on information-flow continuity.*

As AI-enabled C2 systems depend on the integrity of the data they analyze, their ability to enhance decision superiority hinges on robust cyber defense mechanisms that maintain trustworthy data streams [6, 9]. Accordingly, the following proposition is proposed:

Proposition 6: *AI-assisted C2 systems amplify decision superiority when cyber defenses protect data integrity.*

6.4 Cyber Layer: The Adversarial Information Battlespace

The cyber layer represents the domain in which adversaries actively target the informational foundations of NCW. Here, information integrity becomes contested terrain, defined by:

- authenticity,
- accuracy,
- reliability, and
- coherence [15, 16].

Attacks on these dimensions can produce not only informational distortion but also physical consequences, such as drone hijacking, GPS spoofing, corrupted missile trajectories, and manipulated radar signatures. Simultaneously, disinformation campaigns erode:

- trust,
- coordination,
- morale, and
- shared cognitive cohesion [2, 23].

As sustained cyber resilience enables units to preserve valid situational awareness despite ongoing manipulation attempts, it becomes a direct predictor of the accuracy and consistency of the operational picture [7]. Accordingly, the following proposition is advanced:

Proposition 7: *Cyber resilience directly predicts the reliability of shared situational awareness.*

Because adversarial misinformation disrupts shared mental models and degrades synchronization, it diminishes the overall effectiveness of NCW systems regardless of technological sophistication [2, 15]. Thus, the following proposition is developed:

Proposition 8: *Adversarial misinformation negatively moderates the effectiveness of NCW systems.*

In short, decision superiority is achieved through the synergy of all four layers, where human cognition remains the decisive element for “rust calibration”. The model suggests that sense-making capability is the critical mechanism that turns high-integrity data into actual operational success.

7 Implications for C4ISR, MDOs, and Future Warfare

The integrated model developed in this study provides theoretical and practical implications for command-and-control design, organizational culture, coalition interoperability, and the emerging realities of cyber-enabled conflict. Future military effectiveness will depend not only on technological advances, but also on cognitive, organizational, and doctrinal transformations that allow forces to operate effectively within complex, adversarial information environments [1, 4].

7.1 Implications for C4ISR Development

Contemporary C4ISR architectures were originally conceived during a period when data authenticity was largely assumed, and adversary interference was limited in sophistication. The evolving cyber threat landscape has upended these assumptions [7, 16]. As a result, modern C4ISR must be redesigned around integrity-first rather than connectivity-first principles. This shift entails the systematic integration of:

- native cyber-integrity verification embedded in all data flows,
- dynamic trust scoring that assesses the reliability of sensors, platforms, and data sources in real time,
- AI-enabled anomaly detection capable of identifying adversarial manipulation across both classified and unclassified networks,
- redundant, self-healing communication pathways that preserve information continuity under cyber-attack [2, 6, 9].

This reorientation represents a fundamental paradigm change: the critical question for decision-makers is no longer "Is the network available?" but rather "Can I trust the information flowing through it?" [1, 19].

Such a shift transforms the philosophical foundations of command and control and elevates cyber integrity to the core determinant of operational coherence [3, 5].

7.2 Implications for MDOs

MDOs rely on rapid integration of effects across land, air, maritime, space, and cyber domains. This fusion depends heavily on the accuracy, timeliness, and trustworthiness of shared information [4, 9]. In this environment, even minor cyber disruptions can have disproportionate consequences [7, 12].

Cyber integrity becomes essential for enabling:

- cross-domain targeting, where corrupted data may result in misaligned kinetic or non-kinetic effects,
- converging operational effects, which require tight temporal synchronization across domains,
- electromagnetic spectrum operations, whose success depends on reliable situational awareness,
- joint ISR coherence, where misinformation or sensor spoofing can distort the shared operational picture [2, 3].

A compromised cyber environment can trigger nonlinear cascading effects: a single corrupted data point may propagate through the network, degrade cross-domain synchronization, and contribute to strategic failure [12, 30].

7.3 Implications for Organizational Culture and Doctrine

Technological adaptation alone cannot ensure operational resilience. The complexity and volatility of cyber-contested environments require profound cultural and doctrinal change [4, 5]. Military organizations will need to foster:

- a tolerance for ambiguity, recognizing that perfect information is unattainable,
- rapid adaptive learning cycles that allow units to update mental models quickly,
- decentralized initiative, empowering lower echelons to act autonomously when communications degrade,
- cognitive resilience, ensuring personnel can sustain performance under uncertainty, deception, and information overload [10, 23, 25].

Mission command, long valued for its ability to empower initiative, becomes not only desirable but structurally necessary in cyber-compromised contexts [4, 13]. A centralized command system that requires constant, reliable information is simply too brittle in an environment where disruption is expected rather than exceptional.

7.4 Implications for Human-Machine Teaming

As AI systems increasingly support military decision-making, human commanders must be prepared to operate in environments where:

- AI can be deceived through adversarial manipulation,
- automated decision-support tools may fail silently,
- humans must override machine recommendations when trust collapses, and
- trust between humans and machines must be recalibrated dynamically, based on operational context [2, 8]. The future of human-machine teaming in warfare is therefore neither replacement nor blind reliance, but adaptive partnership. Humans should retain interpretive authority while leveraging machine speed and analytical capacity [5, 6].

7.5 Implications for International Security

For alliances such as NATO, the integrated model underscores the necessity of rethinking how coalitions operate in a contested information environment. Cyber operations do not respect national boundaries or stove-piped command structures, making interoperability a strategic imperative [3, 4]. Future coalition forces will require:

- shared cyber-defense architectures and standards**,**
- common integrity verification protocols**,**
- joint frameworks for countering misinformation and cognitive manipulation,
- harmonized multinational sense-making and decision-making processes [7, 15].

In this sense, cyber-integrated NCW becomes as much a diplomatic and institutional challenge as a technological one [2, 5].

To sum up, future military architectures must be built on “trustworthy connectivity” where data integrity is constantly verified through automated systems and human judgment. Success in MDOs depends on balancing technological integration with the “distributed autonomy” of subordinates, ensuring the force can still function if central command nodes are compromised.

8 Limitations and Future Research

While this study offers a comprehensive theoretical synthesis, several limitations highlight important directions for future investigation.

8.1 Conceptual Nature of the Framework

The multi-layered model remains conceptual and requires empirical evaluation. To support empirical verification, the research methods below are explicitly linked to each research proposition and show how they could be operationalized in practice Tab. 1.

These designs allow triangulation across controlled settings and realistic operational contexts, strengthening inference about the proposed mechanisms and boundary conditions [4, 7].

8.2 Scope Boundaries

This article focuses primarily on military operational contexts. Several significant adjacent domains fall outside the current scope, including:

- the influence of political decision-making cycles on cyber-integrated operations,
- civil-military interdependencies, such as shared cyber infrastructure, and
- broader economic and industrial implications of cyber conflict [3].

These omissions highlight opportunities for interdisciplinary expansion.

8.3 Technological Uncertainty

The pace of technological change introduces unavoidable uncertainty. Breakthroughs in quantum computing**,** general AI, or autonomous cyber agents may fundamentally alter NCW dynamics in ways that current theory cannot yet predict [2, 8].

Future conceptual models must therefore remain flexible, acknowledging that emerging technologies may reshape the informational foundations on which NCW rests.

8.4 Directions for Future Research

Building on the theoretical propositions presented, future research should focus on:

- coalition cyber resilience and multinational interoperability,
- AI-human co-sense-making in complex decision environments,
- cognitive and psychological mechanisms behind cyber deception,
- quantifiable resilience metrics for NCW networks,
- comparative analyses of centralized vs. distributed C2 under cyber-attack,
- cultural determinants of organizational adaptability in cyber-degraded contexts,
- ethical and legal questions surrounding algorithmic warfare, autonomy, and human oversight [4, 15, 16].

Such research will play an essential role in operationalizing the conceptual model for real-world military practice. While technology accelerates warfare, human cognition remains the decisive factor in filtering adversarial misinformation and maintaining a decision edge. The article concludes that military superiority in the 21st century will belong to those who can master cyber complexity without losing the organizational adaptability required by chaos.

Tab. 1. Linking research propositions to empirical methods and operationalization.

Research proposition	Method(s) best suited	Example application for empirical verification
P1 – Cyber-induced uncertainty moderates the relationship between information volume and situational awareness.	Controlled experiments; simulation/ network emulation	Manipulate information volume and inject cyber uncertainty (latency, packet loss, partial data corruption). Measure SA (e.g., SA Global Assessment Technique-SAGAT style probes), decision accuracy, and time-to-decision; test moderation.
P2 – Sense-making capability mediates the effect of information integrity on decision superiority.	Controlled experiments; field trials during exercises	Vary data integrity (tampered/verified feeds) and capture sense-making (think-aloud, cognitive task analysis, after-action interviews). Model mediation between integrity → sense-making → decision quality/tempo.
P3 – Decentralized structures enhance operational resilience under cyber degradation.	War gaming; exercise-based quasi-experiments; comparative case studies	Compare centralized vs decentralized C2 cells under the same cyber injects. Measure mission continuity, recovery time (Mean Time to Recover-MTTR), comms workload, and degraded-mode performance.
P4 – Mission command positively influences the speed of adaptation in complex, cyber-contested environments.	Field experiments/ observations in joint exercises; surveys + behavioral metrics	Assess mission command climate (validated questionnaires) and track adaptation speed (time-to-replan, number of effective workarounds, OODA-cycle duration) during scripted disruptions; test association.
P5 – Network redundancy moderates the effect of cyber disruption on information-flow continuity.	Network simulation/ digital twin; controlled red-team tests	Vary redundancy/topology (path diversity, alternate C2 nodes) under identical attack scenarios. Measure continuity (availability, throughput, message delay, COP update rates) and test moderation.
P6 – AI-assisted C2 systems amplify decision superiority when cyber defenses protect data integrity.	Controlled tool-comparison experiments; simulation w/ human-in-the-loop	Compare AI-enabled vs baseline decision aids with/without integrity controls (signing, provenance checks). Measure decision quality, false-positive actions, trust calibration, and workload.
P7 – Cyber resilience directly predicts the reliability of shared situational awareness.	Exercise data analytics; incident datasets; longitudinal organizational studies	Operationalize resilience (Mean Time to Detect-MTTD/MTTR, patch latency, backup/restore success, training level) and shared SA reliability (agreement/consistency across units). Use regression/SEM to test prediction.
P8 – Adversarial misinformation negatively moderates the effectiveness of NCW systems.	Controlled misinformation-injection experiments; historical incident analysis	Inject misinformation into COP/social channels during scenarios and vary detection/provenance tooling. Measure mission outcomes, belief correction speed, and decision errors; test negative moderation.

9 Conclusion

This article has presented a novel, integrated theoretical framework for reconceptualizing NCW in cyber-contested environments. The primary contribution of this study lies in the development of a multi-layered socio-technical model that explicitly links cognitive, organizational, technological, and cyber dimensions within a single coherent structure. Unlike previous studies that examine these domains in isolation, this framework explains their interdependencies and demonstrates how cyber threats simultaneously influence human sense-making, organizational resilience, and technological reliability.

By shifting the focus from connectivity alone to cyber-resilient information integrity, the study provides a new conceptual foundation for understanding decision superiority in contemporary military operations. Hence, three central insights emerge:

- information abundance is not equivalent to clarity. Decision superiority now depends primarily on information integrity, not volume [2, 10, 11],
- organizational adaptability and mission command are foundational. In cyber-degraded and uncertain environments, decentralized initiative and rapid sense-making become decisive [4, 13],
- CAS theory offers a more accurate model of modern warfare. NCW-enabled forces behave as dynamic, interdependent networks rather than linear, controllable hierarchies [14, 18].

Cyber warfare fundamentally reshapes the assumptions on which early NCW doctrine was built. Connectivity alone no longer guarantees superiority; advantage arises instead from resilient sense-making**,** distributed autonomy, and the ability to maintain trusted information amid systemic disruption.

In addition to integrating multiple theoretical traditions, this study contributes to literature by proposing a structured set of research propositions and a unified conceptual model to guide future empirical investigation, simulation, and doctrine development. The framework explains how cyber disruption propagates across cognitive, organizational, technological, and cyber domains, and how these interactions influence decision superiority. By modelling cross-layer dependencies, the study offers a conceptual tool for analyzing and designing cyber-resilient NCW systems, with implications for future C4ISR architectures, mission command, and coalition operations in adversarial information environments.

References

[1] ALBERTS, D.S. and R.E. HAYES. *Power to the Edge: Command and Control in the Information Age (Information Age Transformation Series).* Washington: Cforty Onesr Cooperative Research, 2003. ISBN 1-893723-13-5.

[2] GALLITELLI, V. Artificial Intelligence-Enabled Military Decision-Making Process: The Forgotten Lessons on the Nature of War. *Journal of Advanced Military Studies*, 2025, **16**(2), pp. 99-132. DOI 10.21140/mcuj.20251602005.

[3] GOMES, J.E.C., et al. Surveying Emerging Network Approaches for Military Command and Control Systems. *ACM Computing Surveys*, 2024, **56**(6), 143. DOI 10.1145/3626090.

[4] ZHANG, H., H. DING and J. XIAO. How Organizational Agility Promotes Digital Transformation: An Empirical Study. *Sustainability*, 2023, **15**(14), 11304. DOI 10.3390/su151411304.

[5] ADLER, J.N. *Modernizing Military Decision-Making: Integrating AI into Army Planning* [online]. 2025 [viewed 2025-09-01]. Available from: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2025/Modernizing-Military-Decision-Making/Modernizing-mdmp-UA1.pdf

[6] CASSOTTANA, B., M.M. ROOMI, D. MASHIMA and G. SANSAVINI. Resilience Analysis of Cyber-Physical Systems: A Review of Models and Methods. *Risk Analysis*, 2023, **43**(11), pp. 2359-2379. DOI 10.1111/risa.14089.

[7] CUMMINGS, M.L. *Artificial Intelligence and the Future of Warfare*. London: Chatham House for the Royal Institute of International Affairs, 2017. ISBN 1-78413-198-9.

[8] DAVIS, G.B. *The Future of NATO C4ISR: Assessment and Recommendations after Madrid*. Washington: Atlantic Council, 2023. ISBN 1-61977-273-6.

[9] ENDSLEY, M.R. Situation Awareness Misconceptions and Misunderstandings. *Journal of Cognitive Engineering and Decision Making*, 2015, **9**(1), pp. 4-32. DOI 10.1177/1555343415572631.

[10] STRATER, L., L. FAULKNER, J. HYATT and ENDSLEY, M.R. *Supporting Situation Awareness Under Data Overload in Command and Control Visualizations* [online]. 2006 [viewed 2025-11-29]. Available from: https://www.researchgate.net/publication/252218394_Supporting_Situation_Awareness_Under_ Data_Overload_in_Command_and_Control_Visualizations

[11] BAR-YAM, Y. *Complexity of Military Conflict: Multiscale Complex Systems Analysis of Littoral Warfare* [online]. 2003 [viewed 2025-02-06]. Available from: https://necsi.edu/complexity-of-military-conflict

[12] HOLLAND, J.H. *Complexity: A Very Short Introduction*. Oxford: Oxford University Press, 2014. ISBN 978-0-19-966254-8.

[13] MITCHELL, M. *Complexity: A Guided Tour.* Oxford: Oxford University Press, 2009. ISBN 978-0-19-972457-4.

[14] PARISH, B.R. and B.K. MADAHAR. *Understanding Cyberspace Through Cyber Situational Awareness* [online]. 2016 [viewed 2025-11-30]. Available from: https://www.sto.nato.int/document/understanding-cyberspace-through-cyber-situational-awareness/

[15] PERRY, W.G. *Information Warfare: Assuring Digital Intelligence Collection*. Florida: Joint Special Operations University Publications, 2019. ISBN 1-933749-37-7.

[16] ALBERTS, D.S. Agility, Focus, and Convergence: The Future of Command and Control [online]. *The International C2 Journal*, **1**(1), 2007 [viewed 2025-11-30]. Available from: https://apps.dtic.mil/sti/pdfs/ADA503771.pdf

[17] AKIN, R.P. Complexity Theory and Network Centric Warfare. *Air & Space Power Journal*, 2009. ISSN 1555-385X

[18] SUPRIYADI, T. and A.A. SUPRIYADI. Analysing the Effectiveness of Network-Centric Warfare-Based Defence Strategies in Responding to Asymmetric Threats:

A Quantitative Approach. *Perspektif*, 2025, **14**(3), pp. 638-647. DOI 10.31289/perspektif.v14i3.15359

[19] LJUNGKVIST K. The Military-Strategic Rationality of Hybrid Warfare: Everyday Total Defence under Strategic Non-peace in the Case of Sweden. *European Journal of International Security*, 2024, **9**(4), pp. 533-552. DOI 10.1017/eis.2024.18.

[20] NONAKA, I. A Dynamic Theory of Organizational Knowledge Creation. *Organization Science*, 1994, **5**(1), pp. 14-37. ISSN 1047-7039.

[21] NONAKA, I. and H. TAKEUCHI. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. New York: Oxford University Press, 1995. ISBN 0-19-509269-4.

[22] WEICK, K.E. *Sensemaking in Organizations*. Thousand Oaks: Sage, 1995. ISBN 0-8039-7177-X.

[23] WARD, P. Choice, Uncertainty, and Decision Superiority: Is Less AI-Enabled Decision Support More? *IEEE Transactions on Human-Machine Systems*, 2023, **53**(4), pp. 779-789. DOI 10.1109/THMS.2023.3279036.

[24] ENDSLEY, M.R. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, 1995, **37**(1), pp. 32-64. DOI 10.1518/001872095779049543.

[25] KAUFFMAN, S. *At Home in the Universe: The Search for the Laws of Self-Organization and Complexity*. New York: Oxford University Press, 1995. ISBN 0-19-509599-5.

[26] GLEICK, J. *Chaos: Making a New Science*. New York: Penguin Books, 2008. ISBN 0-14-311345-3.

[27] LORENZ, E.N. *The Essence of Chaos*. Seattle: University of Washington Press, 1995. ISBN 0-295-97514-8.

[28] BOUSQUET, A. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. Oxford: Oxford University Press, 2022. ISBN 0-19-765593-9.

[29] BARABÁSI, A.-L. *Network Science*. Cambridge: Cambridge University Press, 2016. ISBN 1-107-07626-9.

[30] LENGYEL, A. Auftragstaktik in the United States' AirLand Battle Doctrine. *Belvedere Meridionale*, 2023, **35**(2), pp. 158-165. DOI 10.14232/belv.2023.2.12.