Systemic Warfare in the Networked Age:

Operational Systems, Information Competition, and Cumulative Pressure

Author: Shaoyuan Wu

ORCID: https://orcid.org/0009-0008-0660-8232

Affiliation: Global AI Governance and Policy Research Center, EPINOVA LLC

Date: March 17, 2026

Abstract

Contemporary warfare is undergoing a structural transformation driven by the growing centrality of interconnected operational systems and networked information environments. Existing frameworks, from industrial warfare to network-centric warfare, emphasize either territorial control or information superiority, but provide limited tools for explaining how cumulative disruption across infrastructures generates strategic effects.

This article introduces systemic warfare as a form of conflict in which actors seek to impose cumulative pressure across interconnected operational systems and information domains, rather than achieve decisive battlefield outcomes. Within this framework, Operational System Warfare (OSW) constitutes the material dimension of conflict, while information competition shapes its political and interpretive dynamics.

To formalize this framework, the article develops two analytical constructs: the Operational Node Criticality Score (ONCS), capturing the structural importance of infrastructure nodes, and the Systemic Pressure Index (SPI), representing the nonlinear accumulation of system-level stress across interdependent infrastructures. These constructs are intended as analytical tools for modeling interaction mechanisms rather than as directly observed empirical measures.

Drawing on observations from the initial phase of the 2026 U.S.–Israel–Iran conflict, the analysis suggests that systemic pressure may accumulate nonlinearly as disruptions target increasingly critical nodes and propagate across interconnected systems. Sustained multi-domain actions can generate effects that appear to exceed the additive impact of individual strikes, reconfiguring the logic of warfare from discrete engagements toward system-level competition.

The article contributes to the study of contemporary conflict in three ways: it reconceptualizes military effectiveness as system resilience under persistent disruption, introduces a formalized framework for analyzing cumulative pressure in networked conflict, and integrates operational and informational dynamics into a unified model of multi-domain warfare. More broadly, it argues that systemic warfare reflects a shift toward cumulative, system-level competition in which the interaction of material disruption and interpretive processes reshapes how strategic effects are generated.

Keywords: systemic warfare; operational system warfare; information competition; network-centric warfare; military infrastructure; narrative competition; multi-domain conflict; strategic resilience

Working Paper

F-Series Information:
The WP-F series explores AI governance and strategic risk through comparative and historical diagnostics, examining how inherited strategic and regulatory logics break down when transferred into AI-mediated contexts.

Recommended Citation:
Wu, Shaoyuan. (2026). *Systemic Warfare in the Networked Age: Operational Systems, Information Competition, and Cumulative Pressure* (EPINOVA Working Paper No. EPINOVA–WP–F–2026–07). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.5281/zenodo.19078936.

Disclaimer:
This working paper presents diagnostic and exploratory analysis intended to examine inherited strategic and governance logics under AI-mediated conditions. It does not constitute policy recommendations, predictive assessments, or official positions of any institution.

GLOBAL AI
GOVERNANCE
RESEARCH CENTER

EPINOVA

1. Introduction

The character of warfare evolves in response to changes in technology, organizational structures, and the infrastructures that sustain military power. Throughout the industrial era, warfare was largely defined by territorial campaigns, mass mobilization, and the destruction of enemy forces (Clausewitz, 1976; Keegan, 1993). Strategic success depended primarily on the ability to seize and hold territory while degrading the opponent's military capacity.

Beginning in the late twentieth century, advances in digital communications, precision-guided weapons, and surveillance technologies led to the development of network-centric warfare (Cebrowski & Garstka, 1998; Alberts et al., 2000). In this paradigm, military advantage derives from the integration of sensors, command systems, and weapons platforms across a shared information network. Operational effectiveness increasingly depends on information superiority, situational awareness, and rapid decision-making within a digitally connected battlespace. While this model significantly improved coordination and precision, it primarily focuses on information integration within the battlespace and pays limited attention to the vulnerability of the broader infrastructures that sustain military operations across regions.

Recent conflicts, however, suggest that an additional transformation may be underway. Modern military power now depends on large-scale operational systems composed of interconnected infrastructures. These include overseas bases, global logistics networks, satellite systems, energy supply chains, digital communications architectures, industrial production networks, and alliance partnerships.

Such infrastructures collectively sustain the ability of states to deploy and maintain military power across multiple regions. As a result, the resilience and stability of these systems have become central determinants of military effectiveness, while simultaneously introducing new forms of systemic vulnerability.

This article conceptualizes systemic warfare as an overarching framework of contemporary conflict characterized by cumulative pressure across interconnected operational and informational systems.

Within this framework, Operational System Warfare (OSW) constitutes the material dimension of conflict, focusing on the disruption, defense, and resilience of critical infrastructures.

Information competition, in turn, represents the interpretive dimension through which operational events are framed, amplified, and translated into political and strategic effects.

Together, these dimensions form a coupled system in which material disruption and narrative dynamics interact to produce systemic outcomes.

2. From Industrial Warfare to Systemic Warfare

Modern warfare has evolved through several distinct operational logics, each defined by the primary object of strategic competition and the dominant sources of military effectiveness.

2.1 Industrial Warfare

Industrial warfare, dominant during the nineteenth and twentieth centuries, centered on the mobilization of mass armies and industrial production. Victory was often achieved through territorial conquest and the destruction of enemy military forces.

The key characteristics included large-scale mobilization, industrial production capacity, front-line battlefield engagements, and territorial campaigns.

In this model, military power was primarily tied to the capacity to generate and concentrate force in physical space. Strategic competition therefore focused on territorial control and attritional destruction.

2.2 Network-Centric Warfare

Beginning in the late twentieth century, military thinking increasingly emphasized information dominance. Network-centric warfare sought to improve operational effectiveness through real-time information sharing across sensors, command systems, and weapons platforms (Alberts et al., 2000).

This approach aimed to accelerate decision cycles, enhance situational awareness, and increase precision in military operations. As a result, the focus of strategic competition shifted from the massing of forces to the integration of information within the battlespace.

However, while network-centric warfare significantly improved coordination and targeting capabilities, it largely assumes the stability of the broader infrastructures that enable military operations. It does not fully account for the growing dependence of modern militaries on globally distributed systems such as logistics networks, energy supply chains, and digital infrastructures.

2.3 Systemic Warfare

Contemporary conflicts suggest that warfare is increasingly shifting toward a systemic model (Wu, 2026a) in which strategic competition focuses on the disruption, protection, and resilience of interconnected operational systems.

In this model, military power is no longer defined solely by force concentration or information superiority, but by the integrity and functionality of distributed infrastructures that sustain operations across multiple regions. These infrastructures form complex operational systems whose components are highly interdependent.

As a result, strategic competition increasingly targets critical nodes within these systems in order to generate cascading effects that degrade overall operational capacity (Warden, 1995; Rinaldi et al., 2001). Rather than seeking decisive battlefield victories alone, actors attempt to impose cumulative systemic pressure across interconnected infrastructures.

Importantly, this systemic model also extends beyond the physical domain. As operational disruptions generate events that circulate through global information networks, warfare simultaneously unfolds within an informational dimension characterized by narrative competition and perception management.

This conceptual framework illustrates a structural shift from platform-centric and information-centric models of warfare toward a systemic model that integrates both operational infrastructures and information competition. While industrial warfare focused on territorial control and massed force, and network-centric warfare emphasized information integration and precision strike, contemporary warfare increasingly involves competition across distributed operational systems alongside parallel contestation within the information environment.

This evolution reflects a broader transition in operational logics from industrial warfare to network-centric warfare and, increasingly, to systemic warfare (Wu, 2026a).

Table 1. Evolution of Warfare Logics

Industrial Warfare	Network-Centric Warfare	Operational System Warfare	Information Competition
Territorial control	Sensors and data networks	Distributed military infrastructures	Narrative framing
Mass armies	Precision strike	Bases and logistics networks	Platform amplification
Industrial production	Information superiority	Satellites and digital systems	Strategic signaling
Frontline attrition	Platform connectivity	Alliance architectures	Perception management

3. Operational Systems in Contemporary Conflict

Operational systems consist of the infrastructures and organizational networks that enable military forces to operate across multiple geographic regions. Rather than functioning as isolated components, these elements form interconnected systems that collectively sustain the projection and maintenance of military power.

Core components of operational systems include overseas bases and forward operating locations, logistics and transportation networks, satellite constellations and space infrastructure, sensor and surveillance systems, energy supply networks, digital communications infrastructure, and industrial supply chains.

These components are not independent. They are functionally interdependent and operate as an integrated system in which the performance of each element depends on the stability of others. For example, logistics networks rely on digital communications and energy systems; military bases depend on supply chains and transportation networks; and satellite systems support command, control, and coordination across the entire operational architecture.

As a result of this interdependence, operational systems exhibit network-like properties (Rinaldi et al., 2001). Disruptions to one component can propagate through the system, producing indirect effects across multiple domains (Helbing, 2013). The operational effectiveness of military forces is therefore not determined solely by the performance of individual platforms, but by the integrity of the system as a whole.

This systemic structure creates both capability and vulnerability. On the one hand, interconnected infrastructures enable the rapid deployment and coordination of forces across regions. On the other hand, they introduce points of fragility in which localized disruptions can generate disproportionate system-wide consequences.

Strategic targeting within this framework therefore prioritizes critical nodes—the points within the system whose disruption can significantly degrade overall functionality. Attacks on such nodes may not produce immediate large-scale destruction, but can initiate cascading effects that reduce operational capacity over time.

In this sense, operational systems constitute the material backbone of systemic warfare. Localized disruptions, when applied to structurally significant nodes, can propagate through interconnected infrastructures, generating cumulative degradation of military effectiveness across the broader system.

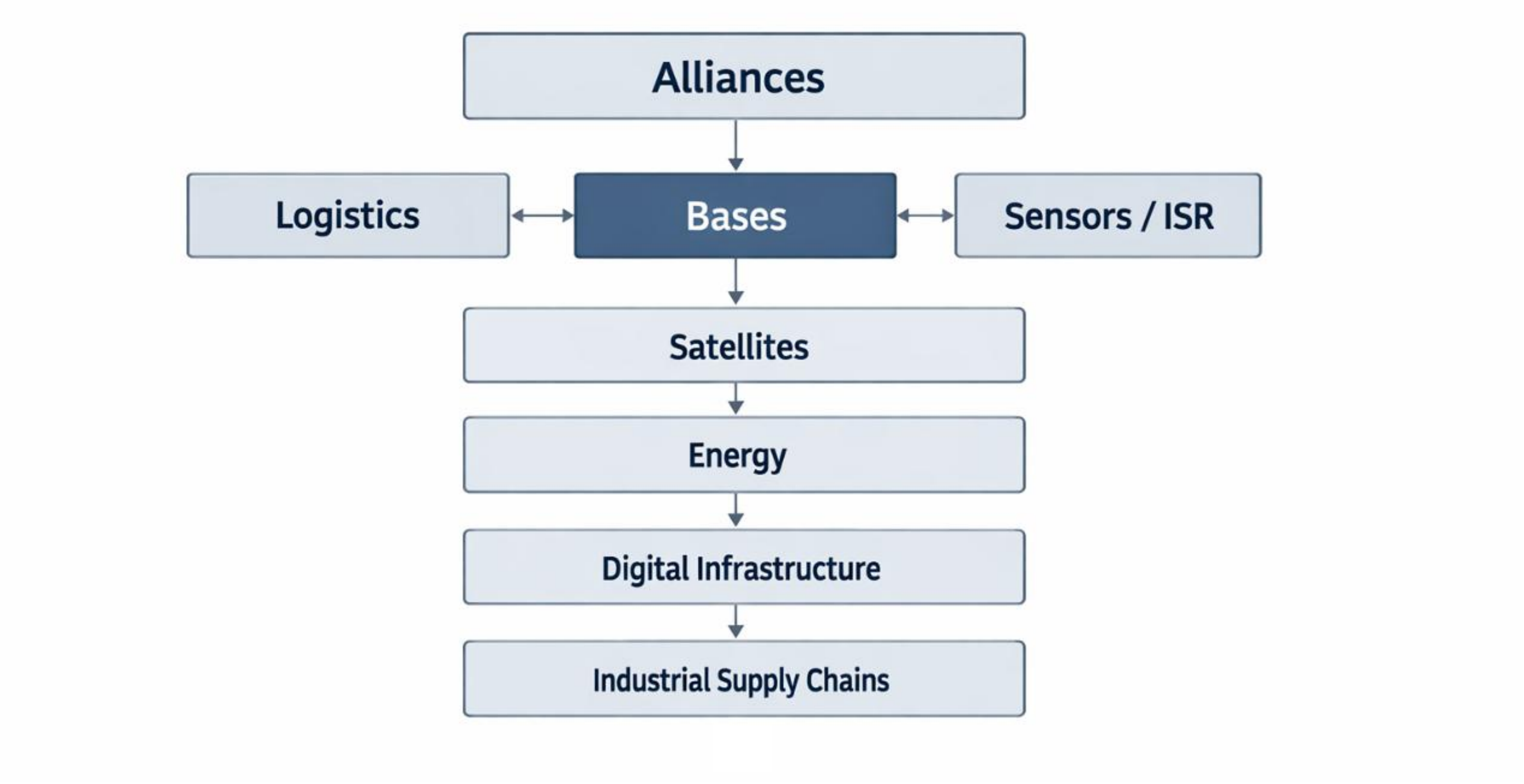

Figure 1. Operational System Architecture

This figure illustrates the layered and interconnected structure of operational systems in contemporary conflict. Military effectiveness increasingly depends on the interaction of multiple infrastructure layers, including bases, logistics networks, energy systems, satellite constellations, digital communications, industrial supply chains, and alliance structures. These layers form a distributed system in which disruptions can propagate across components rather than remaining localized.

4. Interaction Between Operational Systems and Information Competition

Building on the concept of systemic warfare, the analytical focus must shift from structural components to their interactional dynamics. Operational systems and information competition do not function as separate domains; rather, they form an integrated system in which material events and interpretive processes are continuously coupled. Understanding this interaction is essential for explaining how localized disruptions generate broader systemic effects.

4.1 Information Competition in the Networked Environment

Within the broader framework of systemic warfare, information competition constitutes a core dimension that operates in parallel with, and in constant interaction with operational systems (Nye, 2010).

Digital platforms, including X, Facebook, TikTok, and Instagram, have emerged as primary arenas for strategic communication. They enable both state and non-state actors to rapidly disseminate narratives, visual content, and interpretations of military events to global audiences in near real time.

Information competition in these environments is structured around competing legitimacy frames, through which actors seek to define the meaning and justification of military actions. Common frames include *self-defense*, *illegal aggression*, *humanitarian crisis*, and *resistance or liberation* (Wu, 2026b). These frames are not merely descriptive; they function as strategic instruments that shape audience perception, influence international responses, and affect alliance cohesion.

A defining feature of the networked information environment is its algorithmic amplification logic. Platform distribution systems prioritize content that is emotionally engaging, visually salient, or politically polarizing. As a result, localized or tactically limited military actions can be rapidly transformed into globally salient political events.

Crucially, information competition is not autonomous. Its effectiveness depends on its interaction with observable developments in operational systems. Military actions provide the empirical basis for narrative construction, while narratives structure how those actions are interpreted, evaluated, and politically mobilized.

4.2 Operational–Information Interaction Mechanism

Contemporary conflicts are not defined solely by the disruption of operational systems or by competition within the information domain. Rather, these two dimensions form an interdependent and mutually reinforcing system.

Operational actions generate informational effects, while information dynamics shape the interpretation, legitimacy, and strategic consequences of those actions. This interaction produces a recursive feedback loop that amplifies the overall impact of conflict (Boyd, 1996).

Military strikes targeting operational systems, such as logistics hubs, energy infrastructure, or forward bases, do not operate in isolation. Their strategic significance depends on how they are framed, interpreted, and disseminated across information networks. Even limited tactical actions can produce disproportionate strategic effects when embedded within broader narratives of escalation, deterrence, or legitimacy.

Conversely, information competition remains grounded in material events. Narratives derive credibility from observable developments, particularly those affecting operational systems. Claims such as *self-defense*, *escalation*, or *restraint* are reinforced—or undermined—by visible disruptions to infrastructure and force posture.

This interaction can be conceptualized as a dual-layer system:

- **Operational layer**: disruption, degradation, and defense of interconnected systems;
- **Information layer**: narrative construction, legitimacy contestation, and perception management.

The key mechanism linking these layers is **interpretive amplification**: operational events are translated into political meaning through information networks, while narratives generate political pressure that feeds back into operational decision-making.

Figure 2 conceptualizes this process as both sequential and recursive. Military operations generate observable events, which circulate through media and digital platforms. These events trigger narrative competition structured around legitimacy frames. Narrative dynamics produce political pressure via public opinion, diplomatic signaling, and alliance responses, which in turn imposes strategic constraints on decision-makers. These constraints shape subsequent operational choices, feeding back into the next cycle of interaction.

As a result, conflict outcomes are increasingly determined not only by physical damage to operational systems, but by the perceived trajectory of systemic stability or instability within the information environment.

Together, operational systems and information competition form a coupled system in which material disruption and narrative dynamics co-evolve, reinforcing each other over time.

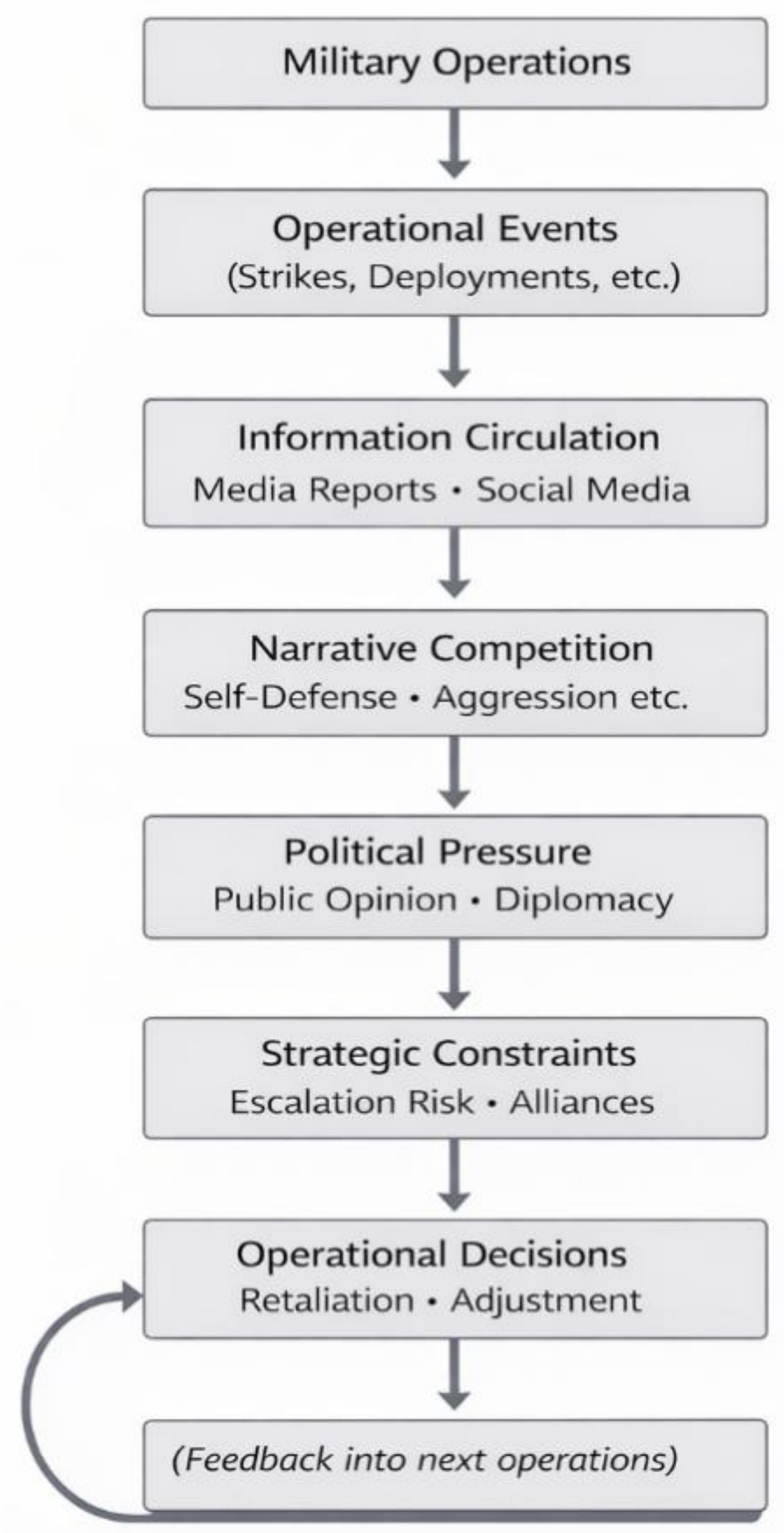
Military Operations
Operational Events
(Strikes, Deployments, etc.)
Information Circulation
Media Reports • Social Media
Narrative Competition
Self-Defense • Aggression etc.
Political Pressure
Public Opinion • Diplomacy
Strategic Constraints
Escalation Risk • Alliances
Operational Decisions
Retaliation • Adjustment
(Feedback into next operations)

Figure 2. Operational–Information Interaction

5. Quantifying Systemic Pressure and Operational Node Criticality

While the preceding sections conceptualize operational systems as interconnected infrastructures and identify critical nodes as primary targets within systemic warfare, a systematic analytical framework also requires a structured way to represent both node-level importance and system-level effects.

To address this need, this section introduces two complementary constructs: the Operational Node Criticality Score (ONCS) and the Systemic Pressure Index (SPI). These constructs are developed as analytical and illustrative tools designed to formalize how localized disruptions may translate into system-wide operational degradation. They are not intended as directly observed measures, but as a framework for structuring analysis and enabling comparative evaluation.

5.1 Operational Node Criticality Score (ONCS)

The Operational Node Criticality Score (ONCS) evaluates the strategic importance of individual nodes within an operational system. Rather than measuring target value in isolation, ONCS captures the structural position of a node within a network of interdependent infrastructures.

Formally, the ONCS of node i is defined as:

$$\boldsymbol{ONCS_i} = (\boldsymbol{F_i} \times \boldsymbol{C_i} \times \boldsymbol{D_i} \times \boldsymbol{S_i})^{\gamma} \tag{5.1}$$

where:

- F_i denotes functional importance, reflecting the role of the node in sustaining operational capability, such as command centers, logistics hubs, or satellite systems;
- C_i represents connectivity, capturing the degree to which the node links multiple subsystems within the broader network;
- D_i indicates dependency load, defined as the number and significance of subsystems reliant on the node;
- S_i denotes substitutability, expressed as the inverse of replacement availability, such that nodes with limited redundancy exhibit higher values;
- γ is a scaling parameter used to adjust sensitivity across different operational contexts.

This formulation emphasizes that node criticality is determined not solely by intrinsic value, but by network position. Nodes characterized by high connectivity, high dependency load, and low substitutability function as systemic bottlenecks.

For analytical purposes, normalized ONCS scores may be interpreted as:

- Critical nodes ($ONCS > 0.8$);
- High-value nodes ($0.5 \leq ONCS \leq 0.8$);
- Supporting nodes ($0.2 \leq ONCS < 0.5$);
- Peripheral nodes ($ONCS$ <0.2).

This classification provides a basis for prioritizing targets within Operational System Warfare.

5.2 Systemic Pressure Index (SPI)

Whereas ONCS captures node-level importance, the Systemic Pressure Index (SPI) represents the aggregate level of stress imposed on an operational system through multi-domain disruption.

SPI is defined as an analytical construct that integrates five dimensions: disruption intensity, network propagation, temporal persistence, node importance, and informational amplification.

The SPI at time t is defined as:

$$\boldsymbol{SPI_t} = \sum_{\boldsymbol{i}} (\boldsymbol{W_i} \times \boldsymbol{D_i} \times \boldsymbol{C_i} \times \boldsymbol{T_i} \times \boldsymbol{I_i}) \tag{5.2}$$

where:

- W_i represents node weight, typically derived from ONCS;
- D_i denotes disruption intensity, reflecting the severity of damage or functional degradation;
- C_i is the cascading multiplier, capturing the extent to which disruption propagates across interconnected systems;

- T_i denotes temporal persistence, reflecting the duration and recovery delay associated with disruption;
- I_i represents information amplification, capturing the extent to which operational events are amplified within the information environment.

Note: For consistency, W_i is operationalized as a normalized transformation of ONCS.

The cascading multiplier is defined as:

$$\boldsymbol{C_i = 1 + \alpha \times Interdependency_i} \tag{5.3}$$

where $Interdependency_i$ measures the degree of coupling between the affected node and other subsystems.

The information amplification factor is defined as:

$$\boldsymbol{I_i = 1 + \beta \times NarrativeIntensity_i} \tag{5.4}$$

where $NarrativeIntensity_i$captures the prominence and emotional salience of narratives associated with the disruption across digital platforms.

The temporal persistence factor incorporates both duration and recovery constraints:

$$\boldsymbol{T_i = Duration_i \times RecoveryDelay_i} \tag{5.5}$$

Importantly, ONCS captures structural importance, whereas I_i captures political and perceptual amplification, ensuring that network structure and narrative dynamics are analytically distinguished rather than double-counted.

SPI values are best interpreted as relative indicators of systemic stress, rather than absolute measurements.

5.3 Linking Node Criticality and Systemic Pressure

The relationship between ONCS and SPI reflects the interaction between node-level targeting and system-level outcomes.

SPI can be reformulated as:

$$\boldsymbol{SPI_t = \sum_i (ONCS_i \times D_i \times C_i \times T_i \times I_i)} \tag{5.6}$$

This formulation highlights that targeting high-criticality nodes produces disproportionately higher systemic pressure than attacks on peripheral nodes.

Three stylized patterns emerge:

- High-criticality targeting with low frequency: efficient systemic pressure generation.
- Low-criticality targeting with high frequency: resource-intensive attrition.
- High-criticality targeting combined with strong information amplification: strategic-level effects extending beyond the operational domain.

Together, ONCS and SPI provide a unified framework linking micro-level targeting decisions with macro-level system outcomes.

5.4 Analytical Specification and Dynamic Simulation of SPI

5.4.1 Analytical Specification

To explore the analytical implications of the framework, this study specifies a reduced-form regression model linking observable proxies of the model's core dimensions to indicators of systemic stress.

Rather than estimating SPI directly, the model examines how its underlying components relate to measurable outcomes:

$$\boldsymbol{ln}(\boldsymbol{SPI_t}) = \boldsymbol{\alpha} + \sum_{\boldsymbol{k=1}}^{\boldsymbol{5}} \left(\boldsymbol{\beta_k} \times \ln\left(\boldsymbol{X_{k,t}}\right)\right) + \boldsymbol{\epsilon_t}$$

(5.7)

where $X_{k,t}$ represents proxies for node criticality, disruption intensity, cascading effects, persistence, and informational amplification.

Interaction terms may be introduced to capture coupling effects:

$$\mathbf{ln}(\boldsymbol{SPI_t}) = \boldsymbol{\alpha} + \sum_{\boldsymbol{k=1}}^{\boldsymbol{5}} \boldsymbol{\beta_k} \times \mathbf{ln}(\boldsymbol{X_{k,t}}) + \boldsymbol{\gamma_1}(\boldsymbol{ONCS_t} \times \boldsymbol{I_t}) + \boldsymbol{\gamma_2}(\boldsymbol{D_t} \times \boldsymbol{C_t}) + \boldsymbol{\mu_t}$$

(5.8)

This specification is intended to approximate relationships implied by the theoretical framework, rather than to provide definitive causal estimates.

5.4.2 Dynamic Simulation Framework

To capture temporal dynamics, SPI is modeled as a recursive process:

$$\boldsymbol{SPI_{t+1}} = (\mathbf{1} - \boldsymbol{\delta}) \times \boldsymbol{SPI_t} + \sum_{\boldsymbol{i}} (\boldsymbol{ONCS_i} \times \boldsymbol{D_{i,t}} \times \boldsymbol{C_{i,t}} \times \boldsymbol{T_{i,t}} \times \boldsymbol{I_{i,t}}) - \boldsymbol{\rho_t}$$

(5.9)

where:

- δ represents the natural dissipation rate of systemic pressure;
- ρ_t captures system recovery capacity, including repair, adaptation, and resource reallocation;
- the summation term represents the cumulative contribution of disruptions across targeted nodes i.

This formulation captures three core dynamics of systemic warfare:

- **Accumulation**: systemic pressure increases through repeated disruptions across multiple nodes;
- **Propagation**: effects are amplified through cascading interdependencies within operational systems;
- **Recovery**: systems exhibit partial resilience through repair and adaptive responses.

5.4.3 Threshold and Nonlinear Effects

To capture nonlinear escalation dynamics, the cascading multiplier $C_{i,t}$can be modeled as a function of systemic pressure thresholds:

$$\boldsymbol{C_{i,t} = \begin{cases} c_1, & SPI_t < \tau_1 \\ c_2, & \tau_1 \leq SPI_t < \tau_2 \\ c_3, & SPI_t \geq \tau_2 \end{cases}}$$

(5.10)

This threshold structure reflects the transition from localized disruption to system-level stress. At low levels of systemic pressure, disruptions remain relatively contained. As pressure accumulates, interdependencies intensify, increasing the likelihood of cascading failures across the system.

5.4.4 Network Extension

To capture interdependencies among operational nodes, the model can be extended into a network-based formulation:

$$\boldsymbol{P_{i,t+1} = P_{i,t} + \sum_j \left(w_{ji} \times P_{j,t}\right) + S_{i,t} - R_{i,t}}$$

(5.11)

where:

- $P_{i,t}$ represents the pressure level at node i;
- w_{ji} captures interdependence between nodes;
- $S_{i,t}$ denotes exogenous disruption input;
- $R_{i,t}$ represents recovery at node i.

Aggregate systemic pressure is then defined as:

$$SPI_t = \sum_i \left(ONCS_i \times P_{i,t}\right) \tag{5.12}$$

This extension enables the simulation of disruption propagation across interconnected infrastructures and allows comparison of alternative targeting strategies under different network configurations.

Figure 3 illustrates how observed strike activity and information competition can be integrated into a hybrid representation of systemic pressure accumulation. Values are scaled for analytical illustration and do not represent calibrated real-world magnitudes.

This figure employs a hybrid methodological approach that integrates empirically anchored inputs with analytically derived system dynamics. Strike counts are approximated from publicly reported operational activity, while ONCS values are derived from structured analysis of 5,000 conflict-related social media posts across major platforms, as detailed in Wu (2026b) and the EPINOVA conflict information dataset (AIPAMS Analytical Platform, 2026). SPI is not directly observed; rather, it is modeled as a nonlinear interaction function between kinetic activity and information competition. The figure is intended to illustrate interaction mechanisms and nonlinear accumulation dynamics rather than to provide precise measurement.

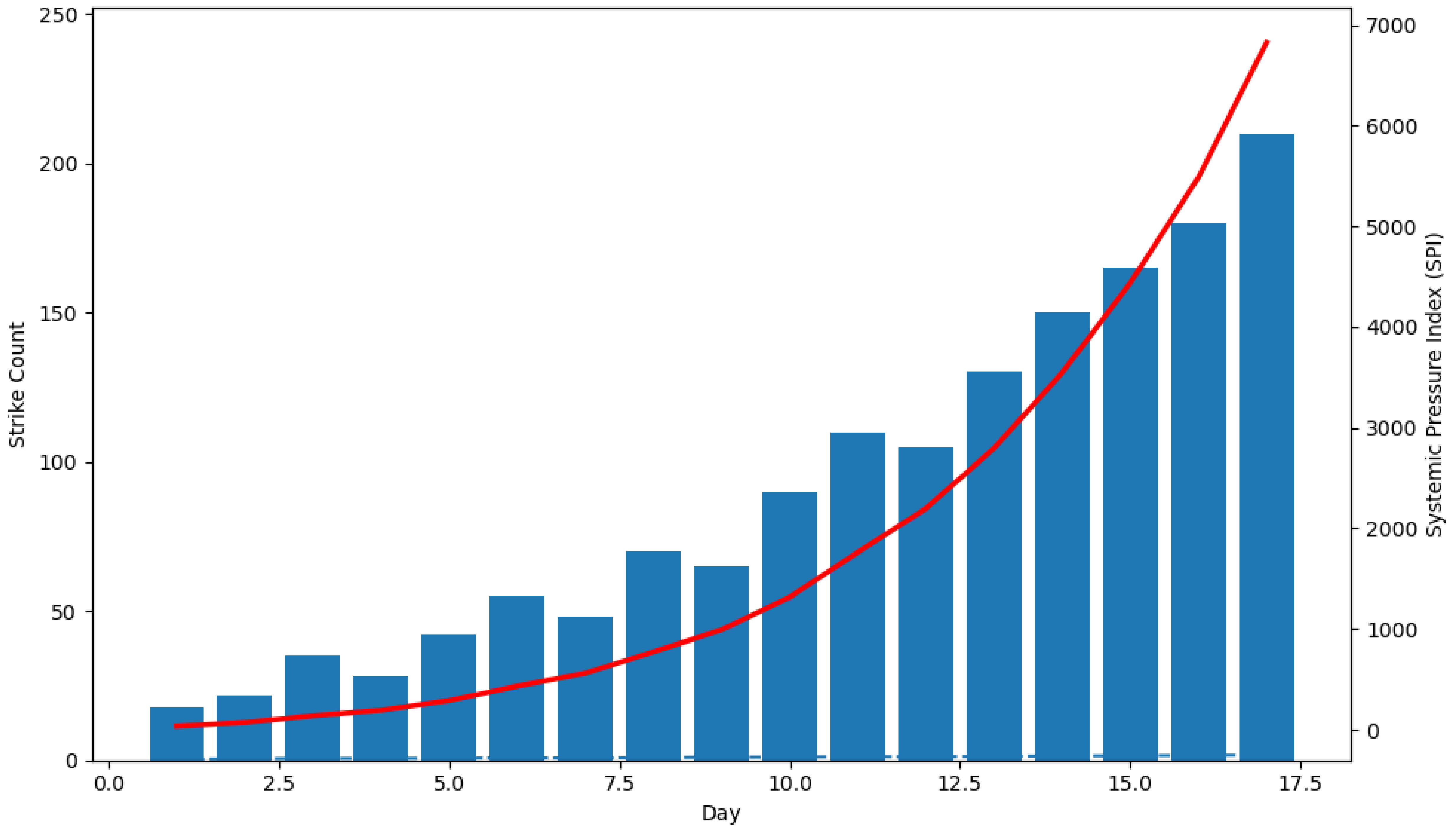

Figure 3. Simulated Trajectories of Systemic Pressure Under Escalation Scenarios

Note: Values are scaled for analytical illustration and do not represent calibrated real-world magnitudes. The figure is intended to illustrate theoretical dynamics rather than to provide empirical estimation.

5.4.5 Analytical Contribution

Taken together, these formulations provide a structured analytical framework for examining systemic warfare. The regression specification offers a reduced-form mapping between observable variables and systemic stress, while the simulation framework captures the temporal and nonlinear dynamics of pressure accumulation.

This dual approach links conceptual modeling with empirical approximation, providing a tractable basis for analyzing system-level stress in contemporary multi-domain conflict environments. The framework is therefore best understood as a theoretically grounded modeling approach that generates testable implications for future empirical research, rather than as a fully specified predictive model.

More broadly, this analytical structure clarifies how localized disruptions, when applied to structurally significant nodes and amplified through interconnected systems, can translate into cumulative systemic effects over time.

6. Case Illustration: The U.S.–Israel–Iran Conflict

This case is not intended to provide definitive empirical validation, but to illustrate how the interaction mechanisms proposed in the theoretical framework may operate under contemporary conflict conditions. It is used for analytical illustration rather than as a comprehensive empirical assessment.

The case highlights the interaction between the two core dimensions of systemic warfare—operational systems and information competition—while also demonstrating how conflict dynamics extend across additional domains. The confrontation involving the United States, Israel, and Iran reflects several key mechanisms associated with systemic warfare in the networked age, including the coupling of material disruption and interpretive processes across interconnected systems.

6.1 Operational Systems Dimension

At the operational level, the conflict involves a complex regional architecture of interconnected military infrastructures, including U.S. bases across the Gulf region, Israeli air-defense systems, Iranian missile and drone networks, and maritime logistics routes.

Military operations targeting these infrastructures are not primarily oriented toward territorial conquest, but toward imposing cumulative operational pressure across the regional system. Strikes against radar sites, military bases, logistics facilities, and air-defense installations seek to generate localized disruptions that can propagate through the broader operational network.

These actions correspond to the core mechanism of Operational System Warfare: targeting critical nodes to induce cascading effects. Even limited damage to key components may degrade command coordination, air-defense coverage, and logistical flows across the regional security architecture.

6.2 Information Competition Dimension

Simultaneously, the conflict has generated intense narrative competition across global digital platforms. Available observations of conflict-related social media content suggest that different platforms perform distinct functional roles within the information environment.

X serves as a primary arena for real-time narrative contestation, where political framing and strategic messaging emerge rapidly. By contrast, platforms such as TikTok and Instagram function primarily as channels of visual amplification and viral dissemination, extending the reach and emotional resonance of conflict-related content.

Across platforms, narratives emphasizing self-defense and illegal aggression dominate the information space, reflecting a broader legitimacy contest typical of contemporary conflicts (Hoskins & O'Loughlin, 2015). These narratives are not merely interpretive; they shape international perception, alliance cohesion, and domestic political support.

These patterns are illustrated by a dataset of 5,000 social media posts collected between February 28 and March 14, 2026 across four platforms: X, Facebook, TikTok, and Instagram.

Figure 4 illustrates the structural distribution of platform roles within the information domain, highlighting how real-time narrative formation, advocacy networks, and visual amplification operate as differentiated but interconnected components of the broader information system.

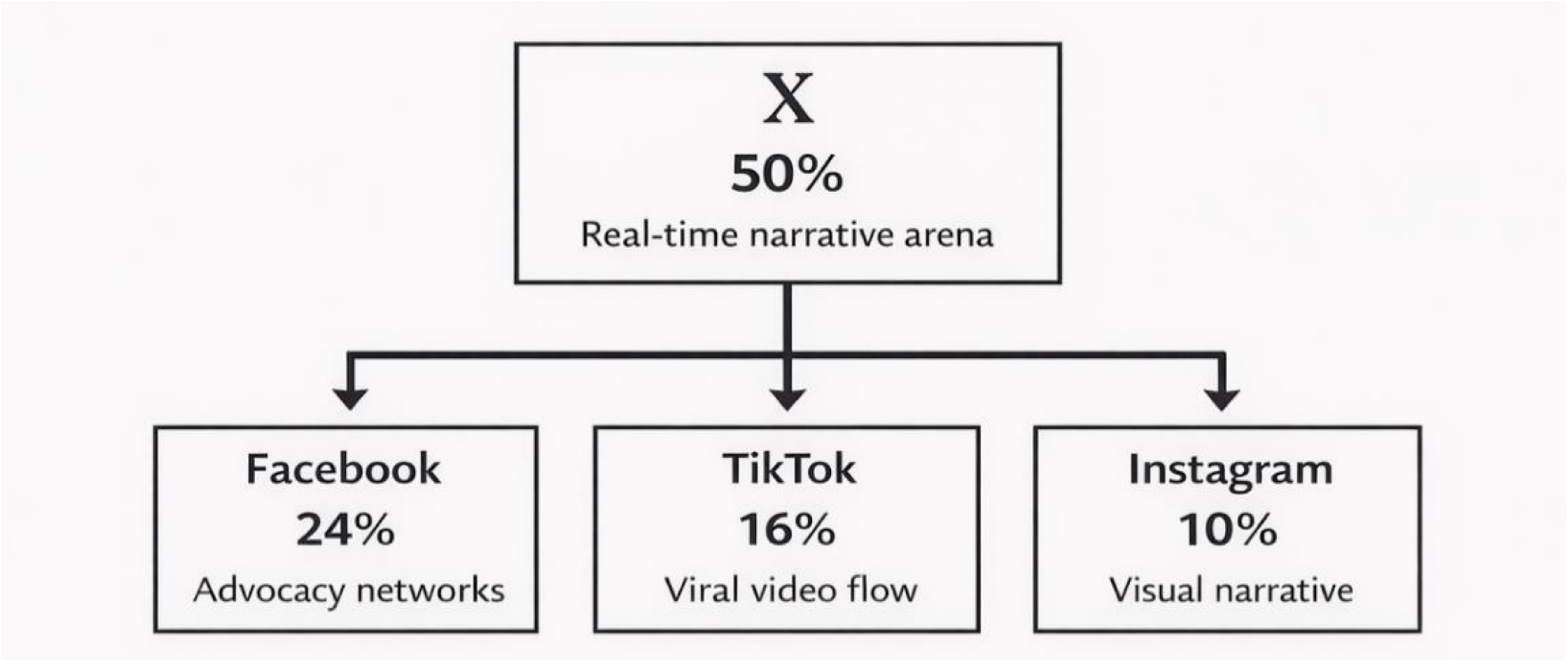

Figure 4. Platform Distribution of Conflict-Related Social Media Posts

(February 28 – March 14, 2026, N = 5,000)

6.3 Operational–Information Interaction

The interaction between operational systems and information competition reflects the feedback mechanism outlined in **Figure 2**. Disruptions to operational infrastructures generate observable events, which are rapidly translated into narratives within the information environment. These narratives amplify the perceived significance of operational actions, extending their strategic impact beyond the immediate battlefield.

This dynamic illustrates the process of interpretive amplification, through which localized military actions acquire broader political and strategic consequences via their circulation within networked information systems.

6.4 Cyber and Cross-Domain Expansion

Beyond the physical and informational domains, the conflict has also extended into cyberspace. One notable development has been a cyber incident affecting a major U.S.-based medical technology company. According to multiple reports by major international media outlets, including the *Associated Press* and *The Wall Street Journal*, a cyberattack disrupted the global network operations of the medical device manufacturer Stryker (Associated Press, 2026; The Wall Street Journal, 2026).

Although the company reported no evidence of ransomware or destructive malware, the incident caused substantial operational disruption across its global network infrastructure. This episode illustrates the growing role of cyber operations as instruments of strategic pressure in contemporary conflict (Rid, 2013; Valeriano & Maness, 2015).More broadly, this episode suggests how systemic warfare can extend beyond the immediate theater of operations into distributed digital infrastructures. Rather than directly targeting critical national infrastructure, the disruption affected a civilian industrial network whose operational consequences propagated globally.

This development highlights a defining feature of systemic warfare: the expansion of conflict across domains and geographic space (Rid, 2013; Valeriano & Maness, 2015). Military pressure can propagate through digital networks, economic systems, and civilian infrastructures, generating indirect but cumulative effects.

Cyber operations therefore function as an additional mechanism of systemic pressure. Even limited disruptions to corporate systems, logistics platforms, or industrial networks may impose operational, reputational, and financial costs, while signaling the capacity to extend conflict beyond the battlefield without triggering full-scale escalation.

6.5 Multi-Domain Systemic Effects

Taken together, missile exchanges in the Middle East, narrative competition across digital platforms, and cyber disruptions affecting U.S.-based networks illustrate how contemporary conflict unfolds across interconnected domains.

Figure 5 conceptualizes this structure as a multi-domain system. Operational infrastructures form the physical backbone of military power, while the information domain shapes legitimacy and perception. Cyber operations target digital and industrial systems that underpin both military and civilian activity, and economic networks transmit pressure across global supply chains.

These domains are not independent. They form an interconnected system in which disruptions in one domain can propagate across others, generating cumulative systemic effects.

This case is consistent with the central argument of this article: contemporary warfare is best understood as a form of systemic competition across coupled operational and informational systems, embedded within a broader multi-domain structure.

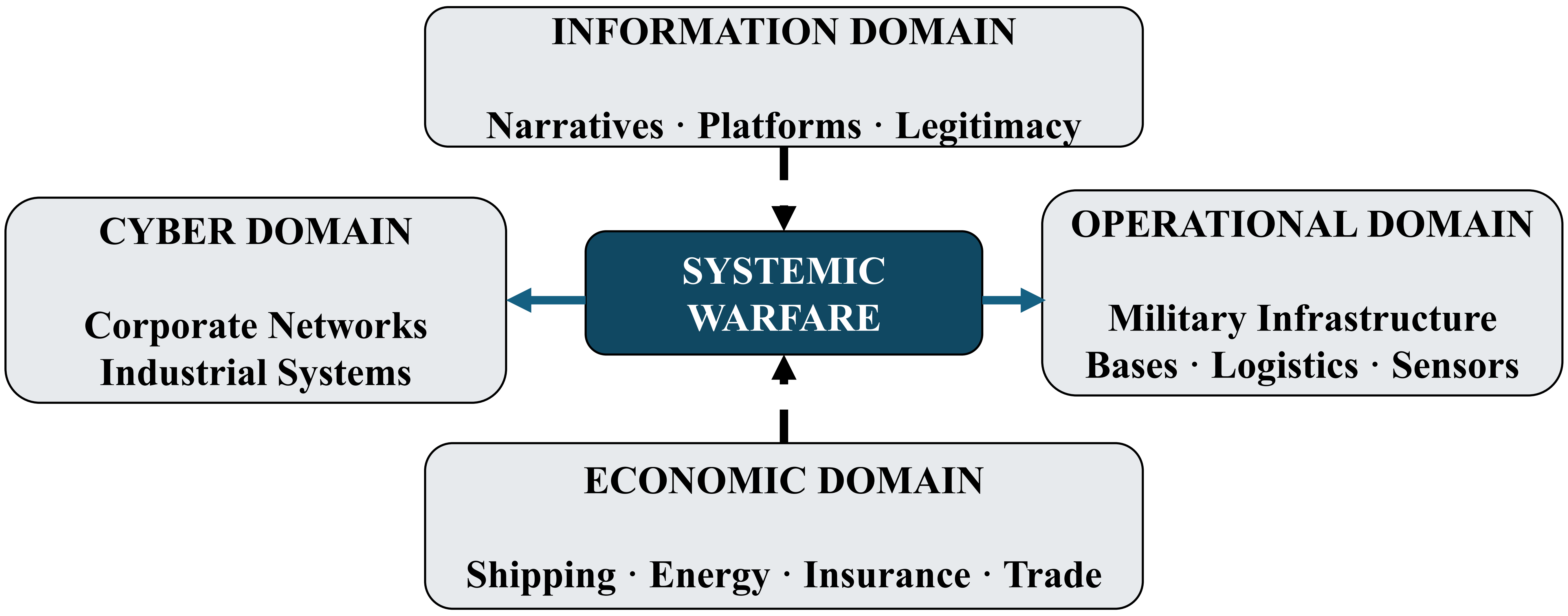

Figure 5. Multi-Domain Systemic Warfare

7. Strategic Implications

The emergence of systemic warfare, structured around the interaction between operational systems and information competition, carries significant implications for military strategy and national security policy. These implications reflect a shift from platform-centric and battlefield-oriented thinking toward system-level resilience, perception management, and cross-domain integration.

7.1 Systemic Vulnerability of Global Operational Networks

As military power becomes increasingly dependent on globally distributed operational systems, states face growing exposure to cross-regional disruption. The interdependence of infrastructures, such as bases, logistics networks, energy systems, and digital communications, creates conditions in which localized disruptions can propagate across the broader system.

Actors with extensive global footprints may therefore possess greater power projection capabilities, but also face heightened systemic vulnerability. Strategic competition increasingly targets these vulnerabilities rather than attempting direct force-on-force confrontation.

7.2 Centrality of System Resilience

In this context, military effectiveness depends not only on offensive capability, but on the resilience and adaptability of operational systems. Protecting critical nodes, ensuring redundancy, and maintaining the capacity to absorb and recover from disruption become central strategic priorities.

Resilience shifts from a supporting function to a core determinant of operational effectiveness within systemic warfare.

7.3 Information Competition as Strategic Leverage

Information competition emerges as a co-equal dimension of warfare. Control over narrative framing influences political legitimacy, alliance cohesion, and international responses to military operations.

Because operational events are translated into political meaning through information networks, strategic success increasingly depends on the ability to manage perception alongside physical operations. Narrative dominance can amplify or constrain the effects of material actions.

7.4 Integration of Operational and Informational Strategy

The interaction between operational systems and information competition requires a more integrated approach to strategy. Military planning can no longer treat physical operations and information activities as separate domains.

Instead, effective strategy must account for the feedback loop between action and interpretation: operational decisions generate informational effects, while information dynamics shape subsequent operational constraints. Strategic planning must therefore be designed with both dimensions in mind from the outset.

7.5 Persistent and Multi-Domain Competition

Systemic warfare blurs the distinction between war and peace by extending competition across multiple domains and over prolonged time horizons. Rather than unfolding through discrete episodes of decisive battlefield engagement, conflict increasingly takes the form of continuous, distributed pressure on interconnected operational systems, coupled with ongoing narrative contestation in the information environment.

This dynamic produces a mode of persistent competition in which escalation is managed, indirect, and often strategically calibrated below the threshold of large-scale conventional confrontation (Mazarr, 2019).

More fundamentally, systemic warfare favors actors capable of imposing sustained, multi-domain pressure across interconnected systems without triggering decisive escalation. Strategic advantage derives not from singular battlefield victories, but from the ability to shape the trajectory of systemic stability over time through the combined effects of material disruption and interpretive amplification.

This represents a shift from traditional deterrence and coercion models toward a form of competition centered on managing systemic trajectories rather than achieving discrete strategic outcomes.

In this sense, systemic warfare is not defined by escalation to decisive conflict, but by the sustained management of pressure across interconnected domains.

Conclusion

Contemporary warfare is increasingly structured by the interaction between operational systems and information competition. Rather than focusing solely on battlefield engagements, modern conflicts involve coordinated efforts to disrupt interconnected infrastructures while simultaneously shaping political perceptions through global information networks.

This article has conceptualized systemic warfare as a form of conflict in which actors seek to impose cumulative pressure across interconnected operational systems and information environments, rather than relying on decisive battlefield outcomes. Within this framework, operational systems constitute the material foundation of military power, while information competition shapes how disruption is interpreted, amplified, and translated into strategic effects.

The analysis highlights a fundamental transformation in the logic of warfare. Military effectiveness is no longer determined solely by force concentration or information superiority in isolation, but by the ability to sustain operational systems under conditions of persistent disruption while managing perception within networked information environments.

The SPI–ONCS framework contributes to this understanding by providing a structured approach to analyzing how systemic pressure accumulates through the interaction of node criticality, disruption intensity, cascading effects, temporal persistence, and information amplification. The framework helps bridge the gap between conceptual analysis and empirical observation, offering a basis for analyzing system-level stress in contemporary conflict.

Understanding systemic warfare is therefore essential for analyzing conflict in an era defined by global connectivity, infrastructure interdependence, and persistent multi-domain competition. Strategic outcomes are shaped less by isolated strikes than by the cumulative accumulation of pressure across interconnected systems over time.

Systemic warfare can therefore be understood as a mode of conflict in which strategic outcomes emerge from the dynamic interaction between material disruption and interpretive amplification, rather than from discrete battlefield victories.

References

AIPAMS Analytical Platform. (2026). *2026 U.S. & allies–Iran conflict cost monitor (MCCM): An event-driven, daily expenditure and loss scenarios assessment series*. https://epinova.org/articles/f/2026-middle-east-conflict-cost-monitor-mccm

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). *Network-centric warfare: Developing and leveraging information superiority*. CCRP.

Associated Press. (2026, March 11). U.S. medical equipment company Stryker says cyberattack disrupted its global networks. https://apnews.com/article/stryker-cyberattack-iran-medical-equipment-products-8dd418618a3bd4fa4c97caf7978c11ee

Boyd, J. (1996). The essence of winning and losing. Unpublished briefing.

Cebrowski, A. K., & Garstka, J. J. (1998). Network-centric warfare: Its origin and future. Proceedings, 124(1), 28-35.

Clausewitz, C. von. (1976). On war (M. Howard & P. Paret, Eds. & Trans.). Princeton University Press.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42-79.

Helbing, D. (2013). Globally networked risks and how to respond. Nature, 497(7447), 51-59.

Hoskins, A., & O'Loughlin, B. (2015). Arrested war: The third phase of mediatization. Information, Communication & Society, 18(11), 1320-1338.

Keegan, J. (1993). A history of warfare. Vintage.

Mazarr, M. J. (2019). Understanding deterrence. RAND Corporation.

Nye, J. S. (2010). The future of power. PublicAffairs.

Rid, T. (2013). Cyber war will not take place. Oxford University Press.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), 11-25.

The Wall Street Journal. (2026, March 16). Hack on U.S. medical company shows reach of Iran's cyber capabilities. https://www.wsj.com/politics/national-security/hack-on-u-s-medical-company-shows-reach-of-irans-cyber-capabilities-85999878

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities. Oxford University Press.

Warden, J. A. (1995). The air campaign: Planning for combat. National Defense University Press.

Wu, S. (2026a). Industrial War and Network War: Operational Logics in the Russia–Ukraine War and the U.S.–Israel–Iran Conflict (v1.0). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.5281/zenodo.18972327

Wu, S. (2026b). *Terminal platform nodes and narrative competition in the U.S.–Israel–Iran conflict* (Policy Brief No. EPINOVA–2026–PB–13). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.5281/zenodo.19027188