Working Paper

F-Series Information:
The WP-F series examines systemic conflict, strategic risk, governance breakdown, and institutional adaptation under networked or high-complexity conditions. It includes studies of AI governance, geopolitical conflict systems, and complex strategic transitions.

Recommended Citation:
Wu, S. (2026). *The Decoupling of Geographic and Strategic Distance: Homeland Vulnerability, Effect Projection, and System Defense in Networked Warfare* (EPINOVA Working Paper No. EPINOVA–WP–F–2026–12). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.67037/epinova.wp.f.2026.012

GLOBAL AI GOVERNANCE RESEARCH CENTER

EPINOVA

The Decoupling of Geographic and Strategic Distance:

Homeland Vulnerability, Effect Projection, and System Defense in Networked Warfare

Author: Shaoyuan Wu

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

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

Date: September 3, 2026

Abstract

Strategic thought has traditionally treated geographic distance as a principal constraint on military reach. Threatening a distant homeland required the movement of destructive force across physical space through armies, naval forces, strategic aviation, missiles, or infiltrating personnel. That relationship remains important, but it is increasingly mediated by the distributed systems through which contemporary states generate and sustain power.

This article argues that networked warfare is producing a partial decoupling of geographic distance from strategic distance. An actor may lack the capacity to deliver sustained conventional firepower against a distant state while retaining the ability to generate strategically consequential effects through interconnected military, logistical, industrial, digital, financial, energy, maritime, and informational systems. The article develops five related concepts: strategic distance, systemic connectivity, effect projection, the system homeland, and system defense. Strategic distance refers to the difficulty of generating consequential effects against another actor; effect projection refers to the transmission of such consequences through connected systems without requiring direct territorial penetration. The system homeland comprises the distributed infrastructures, institutions, and relationships on which essential national functions depend, while system defense emphasizes continuity, redundancy, recovery, substitution, rerouting, and regeneration rather than asset protection alone.

Iran’s confrontation with the United States provides an illustrative case. Iran lacks a demonstrated conventional capability to conduct a sustained strike campaign against the continental United States, yet it can generate homeland-relevant effects through maritime disruption, cyber and informational pressure, threats to external operational nodes, and cumulative demands on U.S. logistics, inventories, alliances, markets, and political attention. The case is used to identify mechanisms rather than to validate the theory by itself.

The central transformation is therefore not the disappearance of geography, but the erosion of its exclusive role in determining strategic reach. Homeland defense must consequently address not only territory and individual assets, but also the continuity and regeneration of the systems that sustain national power.

Keywords: strategic distance; networked warfare; homeland vulnerability; effect projection; system homeland; system defense; deterrence; resilience; Iran; systemic warfare

1. Introduction

For much of modern history, consequential attacks on a homeland required the movement of destructive force into sovereign territory. Armies crossed borders, fleets approached coastlines, aircraft penetrated national airspace, missiles traversed continents, and terrorist organizations infiltrated personnel or matériel. Strategic reach and physical reach were therefore closely associated: geography protected states by increasing the costs, time, and logistical requirements of threatening their political, military, and economic centers (Douhet, 1921/2019; Mackinder, 1904; Mahan, 1890).

Long-range aviation and intercontinental missiles compressed this distance without eliminating its geographic foundations. Their strategic significance derived from their ability to overcome physical separation, and assessments of capability continued to depend on range, basing, flight time, warning systems, logistics, and survivability (Douhet, 1921/2019; Schelling, 1966).

Debate over whether Iran could retaliate against targets inside the United States illustrates the persistence of this framework. The conventional question is whether Tehran possesses an intercontinental missile, a strategic bomber force, a submarine-launched strike capability, or comparable means of reaching North America. On conventional terms, the answer remains restrictive. Iran has not tested or deployed a missile capable of striking the United States and lacks the global basing, long-range aviation, and logistical architecture required for a sustained conventional campaign against the continental United States (Missile Defense Project, 2026). The United States, by contrast, retains substantial advantages in long-range strike, naval power, intelligence, surveillance, reconnaissance, and globally integrated military operations (U.S. Department of Defense, 2022).

That assessment is correct but incomplete because it captures only one form of strategic reach. Modern states depend on systems extending beyond their territorial boundaries. Military operations rely on commercial shipping, overseas bases, satellite constellations, cloud services, software providers, industrial subcontractors, financial networks, energy markets, multinational supply chains, insurance systems, and allied infrastructure. These systems are geographically dispersed but functionally integrated. Disruption far from national territory can therefore affect military readiness, industrial production, economic continuity, political decision-making, and public confidence.

The argument advanced here is not that geography has become irrelevant. Physical distance continues to shape logistics, warning time, operational tempo, force survivability, and the feasibility of direct attack. Rather, geographic distance no longer exclusively determines strategic distance. States may remain geographically remote while becoming functionally adjacent through shared infrastructure, digital access, maritime exposure, commercial dependence, alliance commitments, or technological concentration. Conversely, geographic proximity may have limited strategic significance where relevant systems are weakly connected, redundant, or readily substitutable.

This article develops a framework for analyzing that divergence. It distinguishes geographic distance, the physical separation between actors, from strategic distance, the difficulty of generating consequential effects against them. It introduces effect projection as a mechanism distinct from, but often coupled with, conventional force projection; defines the system homeland as the distributed infrastructures, institutions, and relationships through which essential national functions are sustained; and conceptualizes system defense as the preservation and regeneration of those functions under disruption.

The framework advances four propositions:

Proposition 1: The Connectivity Effect. Strategic distance declines when an actor has exploitable access to critical, high-dependency connections for which timely substitution is limited.

Proposition 2: The Effect-Projection Effect. Actors unable to project conventional firepower across great distances may nevertheless project political, economic, informational, and operational effects through interconnected systems.

Proposition 3: The System-Homeland Effect. The functional homeland may extend beyond sovereign territory when essential national capabilities depend on distributed external systems.

Proposition 4: The Resilience-Deterrence Effect. The coercive value of systemic disruption declines as essential functions can be maintained, restored, rerouted, substituted, or regenerated.

Iran serves as an illustrative, theory-building case because the gap between its limited intercontinental firepower and its access to regional military, maritime, cyber, informational, and operational pathways makes the separation between physical reach and effect projection particularly visible. The case does not independently validate a general theory; it identifies mechanisms that can be examined comparatively across other regional powers, great powers, and nonstate actors.

The central analytical question is therefore not simply whether an adversary can reach the homeland territorially, but whether the systems sustaining the homeland extend beyond the territory of the state.

2. Geography, Reach, and the Industrial Model of Warfare

Modern strategic theory developed under conditions in which geography imposed substantial constraints on the movement and employment of military power. Armies depended on roads, railways, ports, fuel, ammunition, and continuous logistical support; oceans and terrain created defensive depth; and distance increased the costs of concentration and sustainment (Douhet, 1921/2019; Mackinder, 1904; Mahan, 1890).

Classical theories differed over the medium through which power operated, but all treated the physical organization of space as strategically consequential. Maritime power depended on sea lines of communication and access; land power on the organization of continental space; and airpower on range, basing, fuel, and access to targets. The nuclear revolution altered the scale and speed of strategic reach, yet continued to depend on launch geography, trajectories, warning systems, patrol areas, and survivable command structures (Douhet, 1921/2019; Mackinder, 1904; Mahan, 1890).

The underlying logic can be summarized as a sequence in which geographic distance conditions physical reach, and physical reach conditions strategic effect. The farther the target, the greater the difficulty of projecting force against it. Under the dominant material conditions of industrial warfare, this relationship was reinforced by the relative concentration of production, command, logistics, and infrastructure within national territory. Territorial defense therefore protected a large share of the systems through which national power was generated.

Globalization weakened this correspondence. Manufacturing became internationally distributed; commercial shipping assumed a larger role in military logistics; civilian communications and satellite services supported military operations; financial networks became instruments of coercion; and digital systems linked public institutions, private firms, defense contractors, and multinational service providers. The infrastructure of globalization increasingly became part of the infrastructure through which conflict effects are transmitted (Farrell & Newman, 2019; Rinaldi et al., 2001).

Traditional indicators such as missile range, fleet size, aircraft inventories, force structure, and territorial control remain indispensable, but they capture only part of this environment. Regional disruptions can now generate effects elsewhere without the physical movement of military force between the two locations. Maritime insecurity can alter shipping patterns across continents; component shortages can delay distant production; cyber incidents affecting commercial providers can interrupt public and defense functions across jurisdictions; and competition for interceptors, aircraft, surveillance platforms, or political attention in one theater can reduce availability in another (Rinaldi et al., 2001; Wu, 2026b, 2026c, 2026e).

These effects do not invalidate geographic analysis. They reveal an additional strategic space created by interdependence. Geography determines where actors and assets are located; networks condition how disruptions propagate among them. Strategic distance must therefore be treated as multidimensional: physical distance is measured in space, time, and logistical requirements, while strategic distance depends increasingly on the accessibility, criticality, and substitutability of the connections through which effects can be transmitted.

Proposition 1. The Connectivity Effect. Strategic distance declines when an actor has exploitable access to critical, high-dependency connections for which timely substitution is limited.

Connectivity does not create vulnerability alone. It can also generate access, redundancy, information, scale, and economic strength. The same network may therefore produce influence and exposure simultaneously. The analytical task is not to equate connectivity with weakness, but to identify when concentrated dependence creates pathways through which disruption can acquire strategic significance.

3. Strategic Distance in Networked Warfare

Networked warfare, as used here, is broader than network-centric warfare. The latter primarily concerns the integration of information, sensors, command systems, and weapons within military operations; the former refers to conflict in which strategic effects propagate through interconnected military and nonmilitary systems.

Strategic distance is defined here as the difficulty of generating consequential political, military, economic, or informational effects against another actor. Geography remains one determinant of strategic distance, but not the only one. A geographically distant actor can become strategically proximate when it possesses access to highly consequential networks on which the target depends.

This framework builds on, but is distinct from, existing work on network-centric warfare, critical-infrastructure interdependence, weaponized interdependence, and systemic warfare. Network-centric warfare primarily concerns the integration of information, command, sensors, and weapons within military operations, whereas the present framework examines how strategic effects propagate across interconnected military and nonmilitary systems (Alberts et al., 1999; Cebrowski & Garstka, 1998). Effect projection also differs from cascading failure: the latter describes the propagation of disruption across interdependent infrastructures, while effect projection concerns strategically consequential transmission within coercive interaction (Rinaldi et al., 2001). It further extends beyond weaponized interdependence by incorporating military, maritime, cyber, logistical, industrial, and informational pathways alongside economic-network coercion (Farrell & Newman, 2019). In this respect, it builds on the broader systemic-warfare argument that operational effectiveness and strategic pressure increasingly emerge from interactions among military, logistical, informational, industrial, and institutional systems rather than from kinetic force alone (Wu, 2026h).

Cyber-physical systems make this compression particularly visible. Where essential functions are reachable through shared digital or operational-technology layers, strategic distance may depend less on kilometers than on the number, resilience, and substitutability of the barriers separating an actor from the relevant function. Physical dispersion does not necessarily produce strategic separation when distributed assets remain coupled through common control, management, or dependency layers (National Institute of Standards and Technology [NIST], 2021; Rinaldi et al., 2001).

The same logic extends beyond cyber systems. Modern armed forces rely on commercial transport, civilian satellite services, private cloud infrastructure, software ecosystems, international ports, specialized industrial suppliers, financial services, and allied bases. The boundary between military capability and the commercial systems that sustain it is therefore increasingly porous (Alberts et al., 1999; Cebrowski & Garstka, 1998; U.S. Department of Defense, 2022).

Analytical restraint remains essential. Not every economic disruption constitutes warfare, and not every commercial dependency is strategically exploitable. A strategic effect should be linked to coercive interaction, hostile exploitation, or material consequences for essential national functions. Ordinary market volatility, technical failure, and incidental externalities should not be reclassified as hostile action merely because they impose costs.

3.1 From Force Projection to Effect Projection

Traditional force projection concerns the movement and employment of military power beyond its normal area of operation. Effect projection is distinct: whereas force projection moves capabilities toward a target, effect projection transmits strategic consequences through connected systems, regardless of where the initiating action occurs (Hurley, 2017).

The two mechanisms may operate together. A strike can produce immediate physical damage while also generating wider effects by altering shipping behavior, market expectations, alliance policy, or resource allocation. Effect projection may also occur without direct physical attack on the ultimate target. Maritime insecurity can redirect traffic before a chokepoint is physically closed; cyber operations can impose defensive and organizational costs despite limited immediate damage; information campaigns can increase political friction without persuading a majority of the population; and sanctions or export controls can constrain production without destroying productive capacity (Farrell & Newman, 2019; U.S. Energy Information Administration [EIA], 2026a).

For analytical purposes, effect projection requires three conditions. First, the initiating actor must possess access to a relevant system, whether geographic, digital, financial, political, maritime, or organizational. Second, the system must contain sufficiently concentrated or high-dependency relationships that disruption cannot be absorbed or substituted without meaningful cost. Third, the resulting consequences must materially influence the target's capabilities, choices, or political calculations.

Proposition 2. An actor unable to project conventional firepower over long distances may still project strategic effects when it possesses access to systems on which the distant target depends.

This mechanism can partially offset limitations in range or force structure, but it is not a substitute for conventional military power. Actors lacking credible force may be unable to protect their access, prevent retaliation, or convert disruption into durable political outcomes. Effect projection is therefore best understood as a mechanism of leverage and cost imposition rather than as an alternative form of strategic parity.

3.2 Strategic Adjacency

Systemic connectivity can create strategic adjacency: a condition in which disruptions affecting one actor propagate rapidly into the military, economic, or political systems of another despite substantial geographic separation. The United States and Iran are geographically distant, yet they are connected through U.S. regional deployments, Gulf energy markets, maritime commerce, alliance relationships, sanctions, digital networks, and political commitments. Iran cannot readily project sustained conventional force onto the continental United States, but it can exert pressure on systems through which U.S. power and policy operate.

Strategic adjacency is rarely symmetric. Networked warfare does not erase underlying power inequalities; it changes the mechanisms through which weaker actors can exploit limited access. The relevant measure is therefore not parity in damage, but leverage: the capacity to raise the marginal cost of intervention, delay operations, consume scarce inventories, complicate coalition management, or increase political uncertainty.

4. From Territorial Homeland to System Homeland

The homeland remains a territorial and legal concept grounded in sovereignty, political authority, and the state's responsibility to protect its population. That foundation is not displaced by networked warfare. However, contemporary national power depends increasingly on functions located outside sovereign territory: overseas bases and logistics hubs sustain military readiness; orbital infrastructure supports navigation and communications; multinational suppliers support defense production; maritime routes support energy and trade; international payment systems sustain finance; and public institutions rely increasingly on privately operated digital infrastructure.

The territorial homeland and the functional homeland are therefore no longer fully congruent. This article defines the system homeland as the distributed infrastructures, institutions, networks, and functional relationships through which a state's political authority, military capability, economic continuity, and capacity for regeneration are sustained.

The concept is functional rather than juridical. It does not extend sovereignty over foreign infrastructure, nor does dependency create a legal entitlement to control external assets. Its analytical purpose is narrower: to identify systems whose sustained degradation would materially impair essential national functions and for which timely substitution is limited.

The system homeland can be organized into five overlapping layers. The operational layer includes bases, transportation, communications, intelligence, and logistics networks; the industrial layer includes production facilities, suppliers, skilled labor, specialized components, maintenance systems, and energy inputs; the digital and informational layer includes cloud services, software, data systems, satellite communications, digital platforms, and information environments; the economic and financial layer includes payment systems, insurance, investment, shipping finance, energy markets, and commercial infrastructure; and the political and alliance layer includes diplomatic coordination, host-state access, intelligence sharing, interoperability, and the legitimacy required to sustain long-term action.

These layers are interdependent. A shipping disruption can create industrial shortages; a cyber incident can affect logistics and finance; political disagreement can restrict base access; and industrial bottlenecks can reduce military readiness. The system homeland is therefore defined by functional relationships rather than by an inventory of isolated assets. A port matters because of the flows it supports, a satellite because of the services it provides, and a factory because of the supplier, labor, energy, and transport systems through which production is sustained (Rinaldi et al., 2001).

Proposition 3. The functional homeland expands beyond sovereign territory when essential national capabilities depend on distributed external systems.

This proposition requires a demanding threshold. Not every disruption to an overseas interest is homeland-relevant. The concept should apply only where degradation produces material consequences for essential political, military, economic, or social functions within the state, or materially reduces the state's capacity to exercise national power. This boundary is necessary to prevent the concept from collapsing ordinary interdependence into homeland security.

4.1 Homeland Effects Without Territorial Penetration

A transmitted homeland effect arises when an action outside the target state materially changes domestic capability, decision-making, economic continuity, or political stability. Examples include reduced readiness caused by overseas logistics disruption; production delays caused by supply-chain interruption; domestic price or availability shocks linked to maritime insecurity; degradation of communications or navigation through attacks on external infrastructure; political pressure arising from casualties or prolonged overseas deployments; loss of public confidence associated with cyber or information operations; and alliance divergence that constrains national strategy.

These effects vary greatly in severity and should not be equated automatically with kinetic attacks on civilians or sovereign territory. The distinction is analytical rather than legal or moral: the geography of consequence can differ from the geography of violence.

5. Iran and Asymmetric Effect Projection

Iran is analytically useful because the limits of its conventional intercontinental reach are clear. It does not possess a demonstrated capability to conduct a sustained conventional strike campaign against the continental United States, and it has not tested or deployed a missile capable of striking the United States (Missile Defense Project, 2026). Its broader strategy instead relies on regionally ranged missiles and unmanned systems, maritime pressure, dispersed capabilities, cyber activity, political relationships, and other mechanisms intended to increase the costs and uncertainty of intervention (ODNI, 2026; Wu, 2026c).This approach reflects a cost-imposition logic. Iran need not defeat the United States conventionally to influence U.S. decisions; it must preserve sufficient retaliatory and disruptive capacity to raise the marginal cost and political difficulty of continued pressure. Repeated missile and drone attacks can compel defenders to consume high-value interceptors, reinforce bases, sustain deployments, and protect commercial routes. Individual attacks may therefore produce limited tactical effects while contributing to cumulative pressure on inventories, logistics, and decision-making (Schelling, 1966; Wu, 2026c).The strategic logic is to pressure the systems that sustain superior military power rather than to reproduce that power symmetrically (Wu, 2026c, 2026e).

5.1 Maritime Uncertainty

The Strait of Hormuz provides the clearest illustration. The conventional question is whether Iran can close the strait, treating closure as a binary military outcome. Effect projection operates before that threshold. Threats, seizures, limited attacks, warnings, selective restrictions, and persistent uncertainty can alter shipping behavior even when traffic continues (EIA, 2026a, 2026b; Wu, 2026g).

Commercial operators may delay transit, reroute vessels, increase insurance coverage, reduce exposure, or demand higher prices. Governments may deploy naval forces, expand escorts, reposition surveillance assets, and devote diplomatic attention to preserving navigation. Energy markets may price risk before physical supply losses become severe. The strategic effect is therefore transmitted through expectations, commercial responses, and defensive allocation as well as through physical denial (EIA, 2026a, 2026b).

Iranian leverage in the strait lies not only in the capacity to stop vessels, but also in the capacity to alter expectations surrounding passage. A chokepoint can become strategically consequential before it becomes physically impassable, transforming a bilateral confrontation into a broader problem involving shipping, insurance, energy markets, neutral states, and maritime governance. Persistent uncertainty may therefore generate leverage without requiring complete closure (EIA, 2026a, 2026b; Wu, 2026g).

5.2 Cyber and Information Pressure

Cyber operations provide another pathway of effect projection. Iran does not need to paralyze the United States nationally to impose costs. Temporary disruption, defensive mobilization, investigation, restoration, regulatory response, and public concern can acquire strategic significance even where immediate physical damage is limited (Cybersecurity and Infrastructure Security Agency et al., 2026; NIST, 2021).

This pathway is no longer merely hypothetical. In July 2026, U.S. federal authorities warned that Iranian-affiliated cyber actors were exploiting programmable logic controllers and other internet-connected operational technologies across U.S. critical infrastructure. Such assessments establish a plausible and officially recognized pathway of access; they do not justify attributing subsequent incidents to Iran without incident-specific evidence (Cybersecurity and Infrastructure Security Agency et al., 2026).

The mechanism is cumulative. Repeated operations can compel institutions to allocate resources, harden systems, isolate networks, revise procedures, and manage public communication. Information operations can reinforce these effects by amplifying uncertainty, undermining confidence in official reporting, or increasing the political salience of limited incidents. Their strategic significance is greatest when informational amplification interacts with material events such as cyber incidents, maritime seizures, infrastructure failures, or military casualties.

A late-August 2026 refrigeration disruption across multiple U.S. military commissaries illustrates the analytical significance of shared control layers. Several geographically dispersed installations reported refrigeration failures within a narrow time window, and military investigative agencies opened inquiries. No cyber cause or responsible actor had been publicly established as of early September. The episode nevertheless demonstrates the structural vulnerability created when dispersed facilities depend on common remote-management, maintenance, or control architectures: physical dispersion does not necessarily produce functional or strategic separation (Thayer, 2026a, 2026b).

5.3 Pressure on External Operational Nodes

The United States projects power through a globally distributed operational network of overseas bases, allied facilities, tanker aircraft, naval deployments, radar systems, logistics hubs, communications infrastructure, and host-state permissions. Iran's regional capabilities cannot directly reach most of the continental United States, but they can threaten parts of the external network through which U.S. military power is organized and sustained (Hurley, 2017; U.S. Department of Defense, 2022; Wu, 2026e).

Such pressure becomes homeland-relevant when it causes casualties, consumes inventories, requires reinforcement, constrains force availability elsewhere, or generates domestic political and fiscal costs. The physical action may occur in the Gulf while consequences accumulate in U.S. readiness, budgets, industrial demand, alliance politics, and public debate. The objective of the weaker actor is therefore not to match the stronger actor's total capacity, but to increase the marginal and cumulative costs of employing it.

5.4 Cross-Theater Transmission

Effect projection also operates through cross-theater competition. Military resources are finite: interceptors, tanker aircraft, naval forces, intelligence platforms, precision munitions, maintenance capacity, industrial output, and political attention committed to one theater may become less available elsewhere. Regional conflicts can therefore influence one another without unified command or common war aims (U.S. Department of Defense, 2024; Wu, 2026d).

Personnel, bases, logistics, maritime incidents, production lines, shared inventories, and support infrastructure create cross-theater coupling. This wider environment also reveals different forms of functional centrality. The United States remains a principal operational-control center capable of integrating alliances, intelligence, bases, and high-end forces across theaters. China increasingly occupies influential positions across production, trade, logistics, infrastructure, and selected energy networks. These forms of centrality generate different advantages: operational integration supports rapid concentration of force, while systemic connectivity can support endurance, substitution, rerouting, and regeneration under prolonged pressure.

Iranian pressure in the Gulf can consequently affect a broader allocation environment by requiring the United States to commit scarce assets, reassure partners, protect commerce, replenish defensive inventories, and expand production. These consequences are not equivalent to a successful attack on U.S. territory, but they remain relevant to U.S. military readiness and national power (U.S. Department of Defense, 2024; Wu, 2026d).

5.5 Limits of the Iranian Case

Iran's effect-projection capacity remains constrained by U.S. military and intelligence advantages, sanctions, limited global access, internal economic pressure, and the risk of overwhelming retaliation. Disruptive actions may also alienate third parties, weaken diplomatic support, interrupt Iran's own trade, and impose substantial domestic costs (Office of the Director of National Intelligence [ODNI], 2026).

Networked warfare therefore provides mechanisms of resistance, delay, and cost imposition, not automatic compellence. Political statements should not be treated as evidence of operational capability, and downstream market or infrastructure effects should not automatically be attributed to deliberate Iranian strategy. Iran matters analytically because limited intercontinental firepower does not eliminate all pathways through which a geographically distant and conventionally weaker actor can generate homeland-relevant effects. Its significance lies in leverage, not parity.

6. From Territorial Defense to System Defense

If essential national functions depend on distributed systems, homeland defense must extend beyond territorial protection. Missile defense, border security, air defense, maritime surveillance, law enforcement, and domestic critical-infrastructure protection remain indispensable, but they address only part of the problem. Modern national power also depends on systems that cannot be secured through territorial control alone.

System defense is defined here as the capacity to maintain, restore, reroute, substitute, and regenerate essential national functions across interconnected military, economic, technological, logistical, and informational systems. Its objective is not invulnerability, which is unattainable in complex networks, but the denial of lasting strategic value to disruption. Four capabilities are central: continuity, redundancy, recovery, and regeneration (NIST, 2021).

6.1 Continuity

Continuity is the capacity to maintain essential functions during disruption. Individual assets may fail without producing functional collapse if communications can shift to alternative networks, logistics can move through different ports or corridors, command structures can disperse, or commercial providers can supplement government systems.

The August 2026 cyberattack on Suisun City, California, illustrates this distinction. Malicious software disrupted municipal IT systems, including 911 routing and police and fire dispatch, prompting the city to shut down its network. Emergency calls were rerouted through the Solano County dispatch center while police and fire response continued. The incident demonstrates that node or network failure does not necessarily produce function failure when substitute pathways preserve the underlying service (City of Suisun City, 2026).

The relevant metric is therefore functional continuity rather than universal node survival. This principle becomes increasingly important as conflict shifts from the destruction of prominent fixed assets toward the distributed functions sustaining operational continuity.

6.2 Redundancy

Redundancy reduces dependence on individual nodes, suppliers, routes, or platforms. Logistics resilience requires alternative corridors, diversified ports, multiple transport modes, reserve capacity, and compatible systems. Digital resilience requires segmented networks, backup communications, distributed data storage, and multiple service providers. Industrial resilience requires alternative suppliers, spare tooling, accessible designs, and inventories of specialized components (NIST, 2021).

Redundancy imposes peacetime costs and may appear inefficient under normal conditions, but optimization around a single pathway can become fragility under strategic pressure. Its value lies in preserving choice when the primary pathway fails. Eastward and northward logistics alternatives under Hormuz pressure illustrate this logic: Eurasian rail, road, and Caspian routes cannot replace Persian Gulf maritime scale, but they can preserve selected flows and reduce complete dependence on a single chokepoint (Wu, 2026a).

6.3 Recovery

Recovery is the capacity to restore disrupted functions rapidly. Traditional assessments often emphasize the number of assets destroyed; system defense places greater weight on restoration time and functional recovery. A damaged port that resumes partial operations quickly may retain greater strategic value than an intact port isolated from transportation, communications, or supporting services (NIST, 2021).

Recovery depends on trained personnel, repair capacity, spare parts, emergency procedures, modular systems, and institutional coordination. It contributes directly to strategic resilience by shortening the period during which disruption produces leverage.

6.4 Regeneration

Regeneration concerns the production and replacement of capacity over time. Short conflicts may reward sophisticated inventories and high operational tempo; protracted conflicts place increasing weight on the ability to manufacture munitions, replace platforms, repair infrastructure, train personnel, and adapt organizations and supply chains (U.S. Department of Defense, 2024).

Military superiority that cannot be regenerated may erode under repeated pressure. Conversely, an actor able to sustain lower-cost systems, substitute components, preserve logistics, and restore institutional performance may retain influence despite substantial physical damage. Strategic endurance therefore depends on the relative capacity to replace inventories, restore functions, adapt supply chains, preserve alliance cohesion, and sustain political support under prolonged uncertainty.

6.5 System Defense and Deterrence

System defense contributes to deterrence by reducing the expected value of disruption. Traditional deterrence operates primarily through punishment or denial: punishment threatens retaliation, while denial seeks to convince an adversary that an attack will fail. Resilience adds a related mechanism by reducing the duration and strategic utility of disruption even when some attacks succeed (NIST, 2021; Schelling, 1966).

Proposition 4. The coercive value of systemic disruption declines as the target's capacity for continuity, redundancy, recovery, and regeneration increases.

Resilience does not eliminate the need for active defense or retaliation. It changes the attacker's expected return by making disruption less durable and therefore less useful for coercion. System defense consequently seeks not to prevent every disruption, but to prevent disruption from producing sustained strategic advantage.

7. Implications for Deterrence and Strategic Theory

The partial decoupling of geographic and strategic distance has several implications for the analysis of power, deterrence, and homeland defense.

7.1 Military Superiority Does Not Guarantee Systemic Control

A state may dominate conventional operations while remaining exposed to persistent pressure across logistics, industry, finance, information, and alliance politics. Battlefield superiority remains strategically important because it creates access, protects infrastructure, deters escalation, and shapes bargaining. Its political conversion, however, depends on the wider systems through which operational advantage is sustained and translated into durable outcomes.

The U.S.–Iran conflict illustrates this distinction. The United States has retained major operational advantages, yet prolonged confrontation can generate pressure through defense expenditure, maritime insecurity, coalition constraints, bargaining complexity, and cross-theater commitments. Operational success and strategic control are therefore related but not identical (Wu, 2026c).

7.2 Connectivity Produces Power and Exposure

Connectivity is a source of influence. Highly connected states can organize alliances, coordinate finance, move forces, establish standards, and shape industrial and technological systems. The same connectivity can create dependence on bases, transport routes, communications, commercial providers, host-state access, and industrial replenishment. Power and exposure can therefore arise from the same network position (Farrell & Newman, 2019; Wu, 2026f).

The strategic objective is not isolation, which would sacrifice influence and capacity, but the management of concentration, dependency, redundancy, substitution, and failure propagation. The relevant question is not how extensively a state is connected, but whether essential functions can continue when critical nodes, routes, or relationships are disrupted.

7.3 Deterrence Must Address Effects as Well as Attacks

Traditional deterrence often focuses on identifiable acts such as missile launches, invasions, or attacks on national territory. Effect projection may be more ambiguous because strategic consequences can propagate beyond the initiating action. Maritime incidents can generate market effects beyond the immediate event; cyber operations can cascade through interconnected providers; information amplification can shape perceptions before facts are established; and shared control layers can transmit disruption across multiple physical sites (Cybersecurity and Infrastructure Security Agency et al., 2026; EIA, 2026a, 2026b; Rinaldi et al., 2001).

Deterrence must therefore address both intentional attacks and the transmission mechanisms through which their effects expand. This requires clearer thresholds, stronger attribution, crisis communication, public-private coordination, and better understanding of cross-domain propagation.

7.4 Defense Must Protect Relationships, Not Only Assets

Critical-infrastructure protection often focuses on individual facilities. Networked warfare requires equal attention to the relationships connecting them. A port without rail access, communications, fuel, insurance, or customs coordination may remain physically intact but functionally degraded; a military base without replenishment or host-state support may retain assets while losing operational value; and a factory without specialized components or skilled personnel may remain undamaged while ceasing meaningful production (NIST, 2021; Rinaldi et al., 2001).

System defense should therefore map dependencies, substitution possibilities, restoration times, shared control layers, and cross-sector relationships rather than relying primarily on asset counts.

7.5 Homeland Defense Begins Outside the Homeland

Because essential national functions are globally distributed, some measures relevant to homeland defense must occur abroad. Protecting maritime corridors, strengthening allied infrastructure, diversifying suppliers, maintaining overseas repair capacity, coordinating cyber defense, and improving partner resilience can reduce domestic exposure. This does not make every external interest part of the homeland; it means that external systems become homeland-relevant when their disruption materially affects essential national functions and timely substitution is limited (NIST, 2021; U.S. Department of Defense, 2022).

7.6 Networked Warfare Requires Conceptual Restraint

Extending homeland-security analysis into systemic domains also creates risks of conceptual overreach. Governments may over-securitize ordinary commerce, classify routine economic competition as warfare, or justify excessive control over private infrastructure. The system-homeland concept becomes analytically unhelpful if it expands to include every external commercial interest.

Three constraints should therefore govern its application. Systemic dependence must be significant rather than incidental; disruption must materially affect essential national functions or the state’s capacity to exercise power; and hostile intent or strategic exploitation should be distinguished from ordinary commercial volatility, technical failure, and unrelated externalities whenever evidence permits. Networked warfare expands the field of strategic analysis, but it should not erase the distinction between conflict and normal interdependence.

8. Limitations

The framework has three principal limitations. First, effect projection may be difficult to distinguish from ordinary spillover, particularly where attribution and intent remain uncertain. Second, the boundaries of the system homeland are contingent because dependency, substitutability, and criticality vary across sectors and conflict conditions. Third, Iran is an illustrative rather than representative case, and the framework still requires comparative testing and quantitative operationalization before broader generalization.

Conclusion

Strategic thought has long treated geographic distance as a central constraint on military reach. That logic remains valid, but it is increasingly insufficient for explaining how strategic effects are generated in highly interconnected conflict environments. Networked warfare adds a second strategic space formed by military, industrial, logistical, digital, economic, maritime, and informational systems, allowing consequences to propagate beyond the immediate range of military force. The resulting transformation is not the disappearance of geography, but the partial decoupling of geographic distance from strategic distance.

Effect projection captures this shift by focusing on the transmission of strategic consequences through connected systems rather than on the movement of force alone. Actors unable to conduct sustained conventional strikes against distant territory may nevertheless affect military readiness, economic continuity, political decision-making, or public confidence when they possess access to systems on which those functions depend. Strategic distance therefore reflects not only physical separation, but also connectivity, dependency, substitutability, and resilience.

This transformation also complicates the relationship between territory and homeland security. Sovereign territory remains the legal and political foundation of the state, but essential national functions increasingly depend on distributed infrastructures, external operational nodes, commercial networks, supply chains, and digital services extending beyond national borders. The territorial homeland and the system homeland therefore overlap without being identical, making continuity, redundancy, rerouting, substitution, recovery, and regeneration increasingly important components of defense.

Iran illustrates these mechanisms without independently validating the theory. Although Tehran lacks a demonstrated capability to conduct a sustained conventional strike campaign against the continental United States, it retains pathways for generating homeland-relevant effects through maritime uncertainty, cyber and informational pressure, external operational nodes, and cumulative demands on U.S. logistics, inventories, alliances, markets, and political attention. These mechanisms do not imply strategic parity; they demonstrate that limited conventional range does not eliminate strategically consequential leverage. The broader implication is that strategic reach can no longer be assessed solely by how far military force can travel, but also by how far disruption can propagate through the systems that sustain national power.

Working Paper

References

Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). *Network centric warfare: Developing and leveraging information superiority* (2nd ed.). Command and Control Research Program. https://apps.dtic.mil/sti/tr/pdf/ADA406255.pdf

Cebrowski, A. K., & Garstka, J. J. (1998). Network-centric warfare: Its origin and future. *Proceedings, 124*(1), 28–35. https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future

City of Suisun City. (2026, August 8). *Suisun City Council declares state of emergency in response to cybersecurity incident*. https://www.suisun.com/News-articles/Suisun-City-Council-Declares-State-of-Emergency-in-response-to-Cybersecurity-Incident

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency, U.S. Environmental Protection Agency, U.S. Department of Energy, U.S. Cyber Command–Cyber National Mission Force, & U.S. Department of the Treasury. (2026, July 22). *Iranian-affiliated cyber actors exploit programmable logic controllers across US critical infrastructure* (AA26-097A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

Douhet, G. (2019). *The command of the air* (D. Ferrari, Trans.). Air University Press. (Original work published 1921). https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0160_DOUHET_THE_COMMAND_OF_THE_AIR.pdf

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Hurley, P. C., Jr. (2017, August 29). *Force projection and force reception doctrine update*. U.S. Army. https://www.army.mil/article/192631/force_projection_and_force_reception_doctrine_update

Mackinder, H. J. (1904). The geographical pivot of history. *The Geographical Journal, 23*(4), 421–437. https://doi.org/10.2307/1775498

Mahan, A. T. (1890). *The influence of sea power upon history, 1660–1783*. Little, Brown and Company. https://archive.org/details/cu31924095147611

Missile Defense Project. (2026, June 17). *Missiles of Iran*. Center for Strategic and International Studies. https://missilethreat.csis.org/country/iran/

National Institute of Standards and Technology. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2, Rev. 1). https://doi.org/10.6028/NIST.SP.800-160v2r1

Office of the Director of National Intelligence. (2026, March 18). *Annual threat assessment of the U.S. intelligence community*. https://www.odni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf

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. https://doi.org/10.1109/37.969131

Schelling, T. C. (1966). *Arms and influence*. Yale University Press. https://yalebooks.yale.edu/book/9780300002218/arms-and-influence

Thayer, R. L. (2026a, August 28). Commissaries across the US affected by refrigeration outages. *Stars and Stripes*. https://www.stripes.com/theaters/us/2026-08-28/refrigeration-outages-multiple-us-commissaries-22684428.html

Thayer, R. L. (2026b, September 1). Army, Air Force special agents investigate refrigerator outages affecting several commissary stores. *Stars and Stripes*. https://www.stripes.com/theaters/us/2026-09-01/army-cid-investigates-commissary-refrigerator-outages-22721718.html

U.S. Department of Defense. (2022, October 27). *2022 national defense strategy of the United States of America*. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

U.S. Department of Defense. (2024, January). *National defense industrial strategy*. https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf

U.S. Energy Information Administration. (2026a, March 3). *World oil transit chokepoints*. https://www.eia.gov/international/analysis/special-topics/World_Oil_Transit_Chokepoints

U.S. Energy Information Administration. (2026b, March 26). Middle East crude oil tanker rates reached a multi-decade high in March. *Today in Energy*. https://www.eia.gov/todayinenergy/detail.php?id=67386

Wu, S. (2026a). *A preliminary assessment of eastward and northward logistics alternatives under Hormuz pressure: The China–Russia–Central Asia–Caspian network* (EPINOVA Policy Brief No. EPINOVA–2026–PB–63). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.67037/epinova.pb.2026.063

Wu, S. (2026b). *Beyond the battlefield: From strike to system disruption in the Caspian logistics network* (EPINOVA Policy Brief No. EPINOVA–2026–PB–37). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.5281/zenodo.19681411

Wu, S. (2026c). *Deterrence under cost pressure: From overmatch to cost imposition in the U.S.–Iran conflict* (EPINOVA Policy Brief No. EPINOVA–2026–PB–16). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.5281/zenodo.19210002

Wu, S. (2026d). *From separate wars to linked battlefields: The emerging risk of continentalized conflict* (EPINOVA Policy Brief No. EPINOVA–2026–PB–64). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.67037/epinova.pb.2026.064

Wu, S. (2026e). *Industrial war and network war: Operational logics in the Russia–Ukraine war and the U.S.–Israel–Iran conflict* (EPINOVA Working Paper No. EPINOVA–WP–F–2026–06). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.5281/zenodo.18972327

Wu, S. (2026f). *Operational control versus systemic connectivity: The emerging structure of U.S.–China competition under networked warfare* (EPINOVA Policy Brief No. EPINOVA–2026–PB–65). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.67037/epinova.pb.2026.065

Wu, S. (2026g). *Rerouting the Gulf: Bypass infrastructure and the changing strategic value of the Strait of Hormuz* (EPINOVA Policy Brief No. EPINOVA–2026–PB–67). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.67037/epinova.pb.2026.067

Wu, S. (2026h). *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