

AI-Enabled Self-Healing Supply Chain for Contested Logistics

WRITTEN BY
Willow Yang, Ph.D.
Pamela Zelbst, Ph.D.
William Ellegood, Ph.D.

2026



**INSTITUTE FOR
HOMELAND SECURITY**
SAM HOUSTON STATE UNIVERSITY



AI-Enabled Self-Healing Supply Chain for Contested Logistics

Willow Yang, Ph.D., Pamela Zelbst, Ph.D., and William Ellegood, Ph.D.
College of Business Administration, Sam Houston State University

EXECUTIVE SUMMARY

Modern logistics systems depend heavily on timely and reliable information, yet major disruptions, cyber incidents, communication failures, and deliberate information manipulation can undermine both data quality and decision-making. This whitepaper proposes an AI-enabled self-healing supply chain framework designed to maintain decision continuity when information is incomplete, uncertain, or contested.

The framework integrates three interdependent functions: Sense, Trust, and Adapt. Sense monitors network conditions and emerging disruptions. Trust evaluates the reliability of available information and determines the confidence appropriate for a specific decision. Adapt uses this information to generate feasible response options through predictive analytics, optimization, simulation, operating rules, and human judgment. Together, these functions form a governed feedback loop that supports continuous observation, evaluation, response, and adjustment.

The proposed framework offers a practical research foundation for improving logistics resilience in homeland security and other critical operational settings. Its central contribution is a decision architecture that combines situational awareness, information reliability, and adaptive response while preserving human oversight and operational control.

Table of Contents

EXECUTIVE SUMMARY.....	1
1. INTRODUCTION	3
2. AI-ENABLED SELF-HEALING SUPPLY CHAIN FRAMEWORK.....	3
2.1 Sense: Establishing Operational Awareness	4
2.2 Trust: Establishing Decision-Quality Information.....	5
2.3 Adapt: Generating and Executing Feasible Responses.....	6
2.4 Closed-Loop and Governed Adaptation.....	7
3. DIGITAL TWIN RESEARCH PLATFORM.....	8
3.1 Platform Design	9
3.2 Platform Evaluation	9
4. FUTURE RESEARCH AND IMPLEMENTATION ROADMAP.....	10
4.1 Phase 1 Concept and Design.....	11
4.2 Phase 2 Prototype Development	11
4.3 Phase 3 Framework Integration and Proof of Concept.....	11
4.4 Phase 4 Partner-Informed Validation	11
4.5 Phase 5 Pilot Implementation and Expansion.....	12
5. STRATEGIC IMPACT AND CAPACITY BUILDING	12
5.1 Institutional and Research Capacity.....	12
5.2 Government and Industry Engagement	12
5.3 Education and Workforce Development	13
6. REFERENCES	13

1. INTRODUCTION

For more than a decade, supply chain modernization has been emphasizing visibility. Organizations have invested heavily in tracking systems, control towers, dashboards, sensor networks, and enterprise platforms to improve awareness of inventory, shipments, assets, and operating conditions. These capabilities are essential, but visibility alone does not ensure resilience. A dashboard may identify a failed transportation route without providing a feasible alternative; a sensor may report a disruption while transmitting inaccurate, delayed, or manipulated data; and a centralized planning platform may maintain an accurate network model but lose connectivity with remote operations precisely when its guidance is most needed. Research on supply chain digitalization similarly suggests that real-time visibility creates value when it supports predictive and responsive decisions rather than simply displaying network conditions (Ivanov & Dolgui, 2021).

The gap between recognizing a disruption and responding effectively is especially important within the homeland security enterprise, where logistics resilience is closely tied to mission continuity. Emergency response, critical infrastructure restoration, healthcare operations, and defense support all depend on the ability to move essential resources despite damaged infrastructure, constrained capacity, and uncertain information. When this capability deteriorates, the effects can spread quickly across interconnected systems.

Contested logistics refers to the planning and execution of supply operations in environments where an adversary can deliberately disrupt, degrade, or manipulate the physical and information networks on which logistics depends (Hughes, 2024). Unlike conventional disruptions caused by natural hazards, equipment failures, or unexpected demand, contested conditions may involve coordinated and adaptive interference directed at transportation corridors, distribution facilities, suppliers, communication systems, or operational data (Sand, 2024). Physical disruption may also occur alongside cyber interference, leaving decision-makers uncertain whether reported conditions reflect actual failures, delayed information, or deliberate manipulation (Petratos & Faccia, 2023). Under these conditions, maintaining effective logistics operations requires decision-makers to continue assessing conditions and adapting plans even when information and communications are degraded. An AI-enabled self-healing supply chain provides a structured approach to this challenge by integrating sensing, information validation, and adaptive decision support.

2. AI-ENABLED SELF-HEALING SUPPLY CHAIN FRAMEWORK

An AI-enabled self-healing supply chain is a governed logistics system capable of detecting disruptions, assessing the reliability of available information, generating feasible response alternatives, and reconfiguring operations to preserve critical supply functions. In this context, *self-healing* does not imply that the system can eliminate disruptions, physically repair damaged infrastructure, or operate independently of human authority. Rather, it refers to the ability to

maintain or restore logistics performance by adjusting supply flows, inventory allocations, sourcing arrangements, transportation plans, operating priorities, or decision authority as conditions change.

Self-healing may involve both anticipatory and responsive action. When warning signals indicate an emerging threat, the system may support the pre-positioning of inventory, reservation of transportation capacity, or activation of alternative suppliers before performance deteriorates. During an active disruption, it may reroute shipments, reallocate scarce resources, modify delivery priorities, or shift selected decisions to regional operators when centralized communication is unavailable. Because conditions may continue to evolve after an initial response, the system must also monitor the consequences of its actions and revise earlier decisions when assumptions no longer hold.

To support this form of adaptation, a logistics system must answer three fundamental questions. First, *what is happening across the network?* Second, *which available information is sufficiently reliable to support a decision?* Third, *what feasible action should be taken given current mission priorities, constraints, and uncertainty?* These three questions are fundamental to the proposed **Sense–Trust–Adapt** framework.

2.1 Sense: Establishing Operational Awareness

The Sense function develops an operational picture of the logistics network by tracking inventory, transportation assets, infrastructure conditions, supplier status, demand, resource availability, and emerging disruptions. It may draw on sources such as enterprise systems, vehicle telematics, asset-tracking technologies, IIoT devices, machine vision, infrastructure sensors, weather and traffic data, cybersecurity alerts, supplier reports, and observations from field personnel. The goal, however, is not simply to collect more data. In contested environments, additional data may do little to improve decisions if it is delayed, inaccurate, inaccessible, or irrelevant. The Sense function must therefore interpret raw observations and determine what they mean for current operations. This includes detecting departures from expected conditions, identifying potential failures, estimating their severity, and determining which routes, facilities, resources, and missions may be affected.

Sensing must also account for incomplete information. Losing communication with a facility, for example, does not necessarily mean that the facility has stopped operating, just as the absence of a disruption report does not confirm that conditions are normal. The system must distinguish between what is known and what is simply unobserved. When direct information is unavailable, the Sense function may use related indicators, historical patterns, independent sources, or local observations to estimate the most likely network condition. This makes redundancy essential. Critical decisions should not depend on a single sensor, organization, database, or communication channel. Where possible, the system should compare multiple observations, flag inconsistencies, and preserve local monitoring when broader connectivity is lost. The output of

the Sense function is a structured view of observed conditions together with the uncertainty surrounding them.

2.2 Trust: Establishing Decision-Quality Information

The Trust function evaluates the reliability of available information and determines how much confidence decision-makers should place in it for a particular operational decision. Reliability depends on factors such as source identity, data integrity, timeliness, completeness, and corroboration. Confidence, however, is decision-specific because reliable information may still be insufficient for a particular use. For example, a vehicle location that is several minutes old may be adequate for regional planning but insufficient for authorizing entry into a secure facility. Similarly, an unconfirmed report of a route closure may justify caution without warranting the immediate diversion of all traffic. The level of confidence required depends on the urgency of the decision, the consequences of error, and whether the resulting action can be reversed.

To evaluate information reliability and confidence systematically, the Trust function considers five core dimensions of information quality:

- Source identity and authorization: verifying who or what produced the information and whether the source was authorized to do so;
- Data integrity and provenance: determining whether the information has been altered and tracing where it originated;
- Timeliness and completeness: assessing whether the information remains current and contains enough detail for the decision;
- Consistency and corroboration: comparing the information with independent sources and known operating conditions;
- Historical reliability: considering the source's previous record of accuracy and dependability.

In contested environments, this approach is consistent with zero-trust principles, which reject implicit confidence based solely on network location or organizational ownership (Rose et al., 2020). Information can be protected and verified through measures such as access controls, cryptographic safeguards, anomaly detection, and, when multi-organizational auditing is required, permissioned ledgers (Yaga et al., 2019). These tools can strengthen the integrity and traceability of information, but they cannot guarantee that the original physical observation was accurate. The framework therefore does not depend on blockchain or any single verification technology. Instead, it combines technical safeguards with plausibility checks, corroboration, and human verification.

The Trust function may assign explicit confidence levels, such as High, Moderate, or Low, rather than relying on simple pass/fail classifications. High-confidence information may support more autonomous response options within established governance limits, moderate-confidence information may trigger contingency planning or additional verification, and low-confidence

information may be isolated or escalated for human review. Making confidence explicit reduces the risk that automated decision processes amplify corrupted, misleading, or adversarial data.

2.3 Adapt: Generating and Executing Feasible Responses

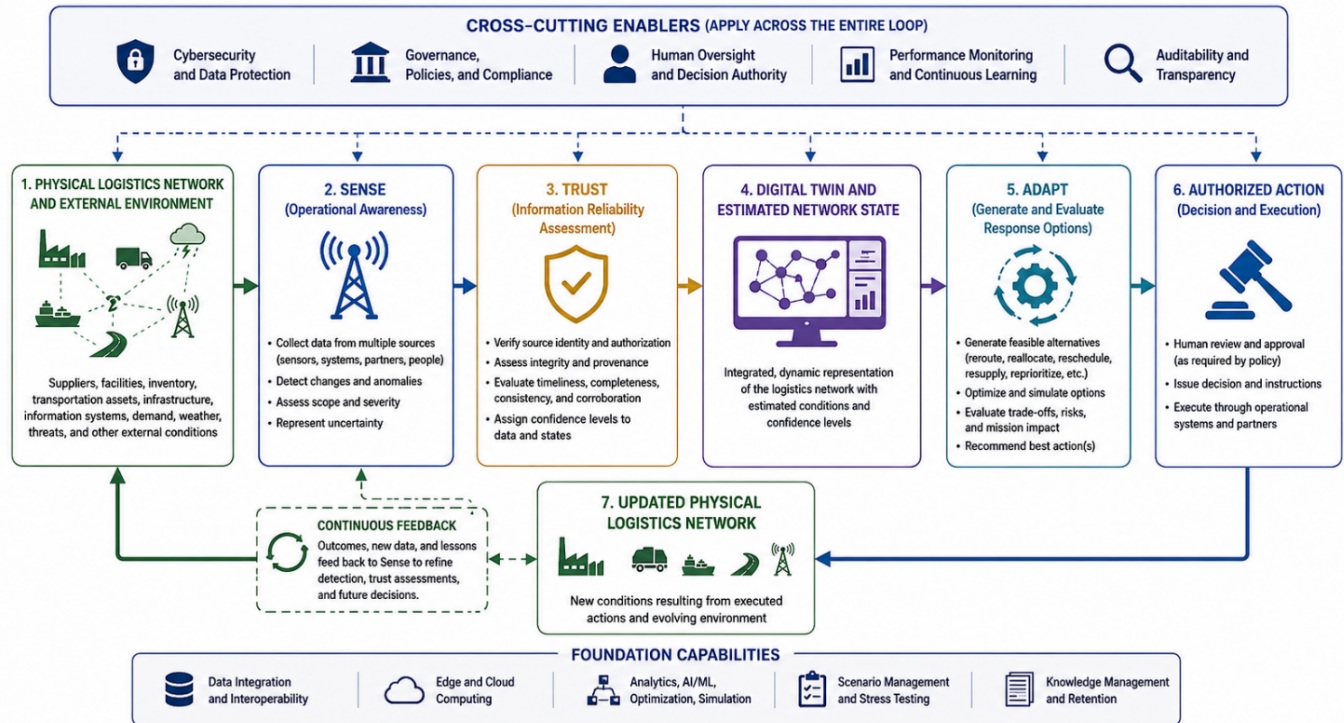
The Adapt function converts the estimated network state, informed by the Trust function, into actionable operational responses. Rather than pursuing a single solution optimized against one fixed objective, its purpose is to sustain critical logistics functions within dynamic operational, security, temporal, and resource constraints. Adaptation may include *operational changes*, such as rerouting shipments, reallocating inventory, switching transportation modes, or reprioritizing competing demands, as well as *procedural adjustments* involving decision authority and operating rules. For instance, if communication with central command is disrupted, regional or tactical units may be granted temporary authority to execute predefined contingency actions using locally available data.

Contested logistics decisions are inherently multi-objective. A response that minimizes transit cost may cause mission-critical delays; rapid rerouting may increase security exposure; and stockpiling inventory may improve readiness while increasing storage costs and vulnerability. The Adapt function must therefore evaluate response options across multi criteria, including mission effectiveness, responsiveness, resilience, security, cost, and operational risk, with priorities adjusted to the circumstances of the decision. This requires prediction, optimization, and evaluation under uncertainty. Because no single analytical method can address every operational scenario, these capabilities should be integrated within a hybrid decision architecture:

- Machine learning and predictive models: forecasting demand, estimating emerging operational risks, and assessing the likelihood of node and link failures;
- Deterministic and stochastic optimization models: identifying and comparing feasible routing, allocation, and scheduling solutions under capacity constraints and uncertainty;
- Simulation: testing proposed responses in a simulated environment to identify queuing, congestion, and cascading effects under dynamic conditions.

Within this architecture, automated tools help generate, compare, and stress-test response options, while human decision-makers such as central planners or tactical commanders evaluate the resulting operational trade-offs and authorize high-consequence actions. Lower-risk or reversible actions may be executed more autonomously when they fall within predefined governance limits.

Figure 1. Conceptual Sense–Trust–Adapt Decision Loop for Contested Logistics



2.4 Closed-Loop and Governed Adaptation

Figure 1 illustrates a conceptual Sense–Trust–Adapt decision loop for contested logistics. Sense, Trust, and Adapt are interdependent functions within a continuing decision process. Sensing without Trust may accelerate the use of inaccurate or manipulated information. Trust without Adapt may establish confidence in available information without improving the operational response. Adaptation without sufficient awareness may produce technically sophisticated decisions based on an incomplete or outdated representation of the network. The value of the framework therefore lies in integrating the three functions into a dynamic, bidirectional feedback loop that supports continuous observation, evaluation, response, and reassessment.

This feedback process operates at two critical stages. In the *pre-decision targeted sensing stage*, the Trust and Adapt functions may determine that uncertainty in a key variable, such as bridge integrity or warehouse inventory, disproportionately affects the recommended response. Rather than passively accepting available information, the framework can direct sensing assets to reduce uncertainty in the variables most critical to the decision. For example, it may task additional sensors, reconnaissance assets, or personnel to verify critical information before an action is authorized. In the *post-execution continuous adjustment stage*, once an action is implemented, its real-world effects are monitored through Sense, re-evaluated through Trust, and used by Adapt to revise the response. If a rerouted convoy encounters unexpected congestion or an alternative facility becomes unavailable, the framework can adjust the response as conditions change. This

continuing reassessment distinguishes a self-healing operational system from a static contingency plan.

The framework is supported by a digital twin that maintains a dynamic representation of the logistics network. The digital twin receives observations from the Sense function, incorporates confidence assessments from the Trust function, and provides the operational model through which the Adapt function evaluates potential actions. It also incorporates the observed effects of implemented actions to update the represented network state. Digital supply chain twins can combine real-time network representation with disruption modeling, simulation, and performance analysis to support predictive and responsive decision-making (Ivanov & Dolgui, 2021).

To ensure safe and effective operation, the degree of decision automation should consider factors such as the consequences of error, action reversibility, decision urgency, data confidence, and system authority. Low-risk, highly reversible actions may be automated within predefined parameters. Conversely, high-consequence decisions involving critical assets, sensitive locations, or ambiguous data must remain subject to human authorization. During periods of degraded communication, local systems may execute preauthorized contingency measures, but these actions remain bounded by established operational priorities and governance rules.

This tiered control model aligns with the NIST AI Risk Management Framework, which emphasizes that AI systems should remain valid, safe, secure, resilient, transparent, and appropriately governed throughout their life cycle (Tabassi, 2023). The objective is not unrestricted autonomy, but rather governed adaptability: improving the speed and quality of logistics decision-making while preserving human oversight, accountability, and operational control. Section 3 provides a more detailed discussion of the digital twin platform that supports this governed feedback process.

3. DIGITAL TWIN RESEARCH PLATFORM

A digital twin provides a virtual environment in which the Sense-Trust-Adapt framework can be represented, tested, and refined. In this whitepaper, the platform is conceived as a dynamic digital representation of a logistics network that captures its structure, resources, operating conditions, and disruptions. Unlike a static analytical model, the platform is designed to update as conditions change, enabling decision-makers to evaluate how alternative actions may affect subsequent network performance.

The initial platform is not intended to replicate an entire national or defense logistics system. Instead, it focuses on a bounded network that is sufficiently realistic to evaluate decision continuity while remaining practical to construct and validate. Within this bounded scope, the appropriate level of detail depends on the decisions being studied. For example, a routing experiment may require detailed transportation capacity and travel-time information but only an aggregated representation of warehouse operations, whereas an inventory-allocation study may

require greater detail regarding inventory availability, demand priorities, and replenishment lead times.

3.1 Platform Design

The platform is designed to represent major logistics network components, including suppliers, production or repair facilities, warehouses, transportation corridors, ports, transfer points, and demand locations. Each node and link would include key operational attributes such as capacity, inventory, operating status, travel time, and infrastructure dependencies. A data-ingestion layer integrates information from operational systems, sensors, partner reports, public sources, and simulated events. These inputs would be processed through the Sense and Trust functions to update the estimated network state and assign confidence levels to critical variables.

A decision engine would combine optimization, simulation, AI, and predefined operating rules to evaluate response alternatives under both normal and disrupted conditions. A human decision interface would present recommended actions together with their supporting evidence, confidence levels, and operational trade-offs. The platform would also log observations, trust evaluations, decisions, and outcomes to support model validation, after-action review, and continuous improvement. Together, these capabilities would support stress testing, resilience analysis, and what-if experimentation before actions are implemented (Ivanov & Dolgui, 2021; Shao & Helu, 2020).

Using this architecture, initial prototype scenarios should represent disruptions common to homeland security and contested logistics, including transportation corridor failures, facility outages, supplier disruptions, cyber incidents, communication loss, and manipulated information. Experiments based on these scenarios would assess not only whether the framework can generate feasible responses but also how sensing quality, information confidence, and human decision authority influence operational outcomes. Initial platform development and validation could rely on synthetic and publicly available data describing facility capacities, transportation networks, demand patterns, infrastructure, weather, and disruption events. As the platform matures, operational partners may contribute anonymized parameters, such as capacity ranges, delay distributions, recovery times, and decision policies, without disclosing detailed transactional records. Subsequent operational pilots may incorporate additional data under appropriate governance, cybersecurity, and data-sharing agreements. Throughout this progression, engagement with operational partners would help validate modeling assumptions, identify realistic use cases, and support eventual technology transition.

3.2 Platform Evaluation

Platform evaluation would focus on whether the Sense–Trust–Adapt framework improves decision quality and operational continuity under degraded conditions. Primary metrics may include mission effectiveness, response time, recovery time, resource utilization, unmet demand, and operational constraint violations. Additional metrics may assess information quality, including the accuracy of confidence assessments and resilience to manipulated or incomplete

data, as well as human factors such as recommendation acceptance rates, operator workload, and operator trust in the system.

Comparative experiments should evaluate four distinct approaches: (a) a conventional static plan, (b) a visibility-only system, (c) an adaptive system without an explicit Trust function, and (d) the complete Sense–Trust–Adapt framework. These comparisons would help isolate the contribution of each architectural component and identify the conditions under which the proposed framework delivers the greatest operational benefit.

4. FUTURE RESEARCH AND IMPLEMENTATION ROADMAP

Development of the proposed capability should follow an incremental, phased roadmap. This approach allows the research team to demonstrate value, identify limitations, and refine the scope before moving into more complex or data-intensive applications.

Phase	Primary Purpose	Key Activities	Principal Outputs
Phase 1: Concept and Design	Translate the framework into a testable research architecture	Define use cases, network boundaries, decision rights, data requirements, performance measures, and preliminary scenarios	Detailed architecture, research questions, data dictionary, and experimental plan
Phase 2: Prototype Development	Build a functional digital twin using synthetic and publicly available data	Model the logistics network, implement disruption scenarios, develop baseline optimization and simulation capabilities, and create a basic decision interface	Executable prototype, scenario library, baseline models, and technical documentation
Phase 3: Framework Integration and Proof of Concept	Integrate and test the Sense, Trust, and Adapt functions	Simulate real-time data, introduce missing and manipulated information, develop confidence assessments, connect information quality to decisions, and compare system configurations	Integrated framework, proof-of-concept results, revised models, and evaluation report
Phase 4: Partner-Informed Validation	Increase operational realism through practitioner input	Incorporate anonymized parameters, validate constraints and scenarios, conduct tabletop or simulation exercises, and obtain structured feedback	Validated assumptions, refined prototype, exercise findings, and recommended pilot design
Phase 5: Bounded Pilot Implementation and Expansion	Demonstrate the framework in a specific logistics setting and assess its potential for expansion	Apply the platform to a defined regional or organizational use case, compare existing procedures with digital-twin-supported decisions, and assess usability	Pilot demonstration, implementation findings, training materials, and scalability assessment

		and implementation requirements	
--	--	---------------------------------	--

4.1 Phase 1 Concept and Design

The first phase should identify a limited number of high-value use cases rather than attempting to model every aspect of contested logistics. Potential applications include emergency commodity distribution, infrastructure-repair logistics, medical supply allocation, regional fuel distribution, and the movement of critical replacement parts. For each use case, the research team should define the key decisions to be supported, the relevant decision-makers, required information, available response actions, operational constraints, consequences of delay, and the appropriate level of automation. This phase should also establish performance measures and the criteria for advancing to prototype development.

4.2 Phase 2 Prototype Development

The second phase should develop a working digital-twin prototype for a simplified logistics network. The initial model may include several supply and storage locations, multiple demand nodes, constrained transportation capacity, different priority classes, and a limited set of disruption scenarios. The objective at this stage is not to achieve high fidelity, but to establish a network that can be represented, disrupted, and reconfigured through controlled and repeatable experiments. Baseline routing and resource-allocation models should also be developed to support later comparisons between the integrated Sense–Trust–Adapt framework and conventional static or visibility-based planning approaches.

4.3 Phase 3 Framework Integration and Proof of Concept

The third phase should introduce degraded-information conditions, including delayed observations, missing data, conflicting reports, and manipulated information. Confidence assessments should then be incorporated into the decision models so that uncertainty in the estimated network state influences the recommended actions. A successful proof of concept should demonstrate that the integrated framework can (a) detect or represent a disruption, (b) recognize uncertainty in the available information, (c) generate feasible response alternatives and explain the principal trade-offs, and (d) outperform a static or visibility-only baseline in selected scenarios. The evaluation should also identify conditions under which the framework fails or provides limited benefit.

4.4 Phase 4 Partner-Informed Validation

With a functional prototype established, the focus should shift to grounding the platform in real-world operations. Practitioners and domain experts should review the model's assumptions, constraints, scenarios, and outputs. Synthetic parameters can then be refined through expert judgment or replaced with anonymized operational parameters. Through tabletop exercises and simulation runs, the research team should assess whether the framework's recommendations are

practical, understandable, and actionable for operational users. This phase should result in a clearly bounded pilot design focused on a specific decision problem, a defined group of participants, manageable data requirements, and a measurable operational outcome.

4.5 Phase 5 Pilot Implementation and Expansion

The fifth phase should move the framework into a bounded operational pilot, such as emergency commodity distribution, medical logistics, infrastructure restoration, port-to-inland movement, or another application identified through partner engagement. The primary objective is to determine whether the framework improves decision speed, the feasibility of recommended actions, coordination, and resilience relative to existing procedures. The pilot should also assess organizational requirements, including data access, system integration, cybersecurity, user training, governance, and long-term platform maintenance. Findings from this phase would inform whether the platform should be expanded to additional commodities, transportation modes, organizations, or disruption types.

5. STRATEGIC IMPACT AND CAPACITY BUILDING

The proposed initiative would establish a distinctive research capability at the intersection of homeland security, supply chain management, artificial intelligence, operations research, cybersecurity, and critical infrastructure resilience. Its strategic value lies not in any individual technology but in integrating these fields to address a critical homeland security challenge: *maintaining trustworthy and feasible logistics decisions during disruptions*.

5.1 Institutional and Research Capacity

Developing the Sense–Trust–Adapt framework and an initial digital twin prototype would provide IHS with a foundation for applied research, scenario analysis, partner demonstrations, and future pilot projects. Because the framework is not tied to a single organization or type of disruption, it could be adapted over time to a range of logistics and critical infrastructure settings.

The initiative could also support interdisciplinary research on information reliability, AI-assisted decision-making, optimization under degraded conditions, and cross-sector interdependencies. By providing common scenarios and consistent evaluation measures, the platform would allow researchers to compare alternative analytical and decision-support approaches under controlled conditions.

5.2 Government and Industry Engagement

Government agencies, emergency management organizations, infrastructure operators, healthcare systems, transportation providers, logistics companies, and defense-related industries could contribute to scenario development, assumption validation, tabletop exercises, and bounded pilot activities. Their involvement would help ensure that the research addresses operationally meaningful problems without requiring immediate access to sensitive data or live systems. These partnerships could also deepen understanding of the interdependencies among

transportation, energy, communications, healthcare, and supply networks. This understanding could help identify shared vulnerabilities, resource constraints, and coordination gaps before they are exposed during an actual disruption.

5.3 Education and Workforce Development

The initiative could create hands-on learning opportunities for undergraduate and graduate students through research assistantships, capstone projects, simulation modeling, and tabletop exercises. These activities would help students understand how technical analysis must be combined with operational constraints, cybersecurity, governance, and human judgment while preparing them to work in logistics, emergency management, and critical infrastructure settings. As the initiative develops and new partners and research questions emerge, it could provide continuing opportunities for student involvement, interdisciplinary faculty research, and future IHS projects.

6. REFERENCES

- Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning & Control*, 32(9), 775-788.
- Hughes, Z. S. (2024). Giving our "paper tiger" real teeth: Fixing the U.S. military's plans for contested logistics against China. *Joint Force Quarterly*, 115(3), 114–125. National Defense University Press. <https://digitalcommons.ndu.edu/joint-force-quarterly/vol115/iss3/20/>
- Petratos, P. N., & Faccia, A. (2023). Fake news, misinformation, disinformation and supply chain risks and disruptions: Risk management and resilience using blockchain. *Annals of Operations Research*, 327(2), 735–762. <https://doi.org/10.1007/s10479-023-05242-4>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST special publication*, 800(207), 1-52.
- Sand, E. (2024). Fighting to supply the fight—Assessing approaches for overcoming contested logistics. *Naval War College Review*, 77(2), 6. <https://digital-commons.usnwc.edu/nwc-review/vol77/iss2/6/>
- Shao, G., & Helu, M. (2020). Framework for a digital twin in manufacturing: Scope and requirements. *Manufacturing letters*, 24, 105-107.
- Tabassi, E. (2023). Artificial intelligence risk management framework (AI RMF 1.0).
- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

[Institute for Homeland Security](#)

[Sam Houston State University](#)

© 2026 The Sam Houston State University Institute for Homeland Security.

Yang, W., Zelbst, P. & Ellegood, W. (2026). AI-Enabled Self-Healing Supply Chain for Contested Logistics. (Report No. 2026-1034). The Sam Houston State University Institute for Homeland Security.
<https://doi.org/10.17605/OSF.IO/Y6KJA>



**INSTITUTE FOR
HOMELAND SECURITY**
SAM HOUSTON STATE UNIVERSITY

