Systemy Logistyczne Wojsk
Zeszyt 65(2026)
s. 133-148

Instytut Logistyki
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna w Warszawie

Military Logistics Systems
Volume 65(2026)
pp. 133-148

Institute of Logistics
Faculty of Security, Logistics and Management
Military University of Technology in Warsaw

DOI: 10.37055/slw/242083
Article type: Original research article

ISSN 1508-5430
eISSN 2719-7689

A ZERO-TRUST ARCHITECTURE FOR MULTINATIONAL MILITARY LOGISTICS DATA EXCHANGE: A BREACH-PROPAGATION MODEL OF COALITION CYBER RESILIENCE

Artur Chlebicki
contact@chlebicki.art; ORCID: 0009-0009-7304-0138
Independent Researcher, Gdańsk, Poland

Abstract.
Multinational military operations depend on the exchange of logistics data across coalition partners whose information systems differ in assurance and whose mutual trust is necessarily incomplete. The research problem is that the prevailing perimeter model grants broad implicit trust once a partner is authenticated: a stolen credential, a compromised partner system or an insider can then move laterally across the shared logistics fabric towards the consolidated logistics picture. Policy asserts that a zero-trust architecture reduces this risk, but the size of the reduction has never been quantified for coalition logistics. The aim of the article is to measure the reduction in breach impact that zero-trust delivers in a coalition logistics data-exchange network, and how it depends on attacker capability. The method is a breach-propagation Monte-Carlo simulation of a six-nation network in which an adversary compromises one partner node and spreads; perimeter trust, microsegmentation and zero-trust are compared across a swept attacker-capability parameter. Zero-trust contains the breach: where the perimeter blast radius rises from 55% to 97% of nodes as the attacker improves, zero-trust holds it between 7% and 16%; the probability of reaching the critical consolidated store falls from up to 94% to below 6%; and the breach stays within roughly the originating nation instead of three to six of them. The contribution to logistics is quantified evidence that zero-trust turns a coalition-wide breach into a contained local incident, protecting the continuity of the shared logistics picture on which multinational sustainment depends, and the advantage grows as the adversary improves.

Keywords:
zero trust; military logistics; coalition interoperability; supply-chain cybersecurity; data exchange

Introduction

Modern coalition operations run on shared logistics. Allied forces pool movement plans, stock balances, demand signals, maintenance data and consignment tracking so that a multinational force can be sustained as if it were one. That pooling is a data-exchange problem before it is a transport problem: the common logistics picture is assembled from feeds owned by many nations, each with its own enterprise resource planning (ERP) and movement-control systems, its own security policy and its own level of assurance. The exchange happens over federated networks that connect partners of unequal maturity, often at speed and under operational pressure.

The dominant way of securing such exchange has been the perimeter model. A partner that authenticates at the boundary is admitted to a trusted zone and thereafter treated as friendly; controls concentrate at the edge, and traffic inside the zone is lightly inspected. This model assumes that the inside is safe, which in a coalition is precisely the assumption that cannot hold. The weakest partner sets the security of the whole. A credential stolen from any partner, or an insider anywhere in the federation, lands the adversary inside the trusted zone, from which lateral movement across the shared logistics fabric is comparatively easy. A local compromise can therefore become a coalition-wide breach, and the consolidated data store that makes the common picture valuable becomes the natural objective. Figure 1 shows the arrangement: national ERP and movement-control systems joined through gateways into an implicitly trusted federation, with the consolidated store at its centre.

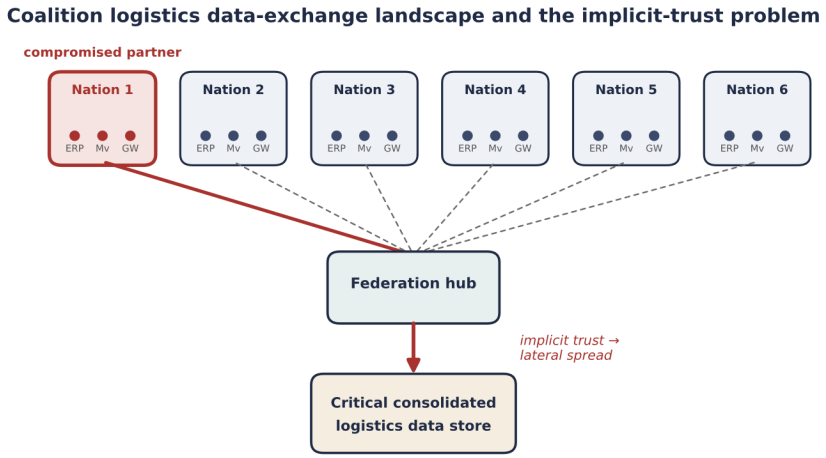


Figure 1. Coalition logistics data-exchange landscape, in which a compromised partner can move laterally through an implicitly trusted federation towards the shared critical data store

Source: own elaboration

Zero-trust security inverts the perimeter assumption. Its principle, often summarised as never trust, always verify, is that no request is trusted on the basis of its origin; every access to every resource is authenticated, authorised against policy and continuously evaluated, regardless of whether it comes from inside or outside any boundary (Rose et al. 2020). The approach is now defence policy in several nations (U.S. Department of Defense 2022), yet its value for the specific problem of multinational logistics data exchange has not been quantified. Practitioners assume the approach should help; how much it helps, and against what kind of adversary, has not been measured.

Research aim and problem

This article provides such a measure. The aim is to quantify the reduction in breach impact that a zero-trust architecture delivers in a coalition logistics data-exchange network, and to show how that reduction varies with the capability of the attacker. Three research questions follow. First, how does the architecture (perimeter, microsegmentation or zero-trust) change the blast radius of a breach that begins at a single compromised partner? Second, does the protective benefit of zero-trust grow or shrink as the adversary becomes more capable? Third, how is the coalition-specific risk, the spread of a breach from one nation to others and the exposure of the shared critical store, affected by the choice of architecture? The first two questions are answered by the simulation presented in the Results and Analysis section; the third is addressed in the parts of the analysis concerning the critical store, cross-national spread and the mapping of controls to coalition logistics threats. The intended contribution is to logistics rather than to network engineering: what the model measures is the survivability of the data exchange on which multinational sustainment planning, stock visibility and movement control rest.

Scope and structure

The scope is deliberately bounded. The study models the data-exchange and access-control layer of coalition logistics, not the physical movement of materiel, and it treats breach propagation through that layer rather than the exploitation of any specific vulnerability. The architectures are represented at the level of the trust decision, which is where they differ, and not at the level of product configuration. The article first reviews zero-trust and the coalition logistics context, then describes the model, reports the results, discusses implications and limitations, and closes with conclusions.

Literature Review and State of Research

Three strands of work meet in this study: the development of zero-trust security, the doctrine and practice of coalition logistics information exchange, and the analysis of supply-chain and coalition cyber risk.

From perimeter defence to zero trust

The intellectual roots of zero-trust lie in the principle of least privilege and the rejection of implicit trust, articulated long before the term existed (Saltzer and Schroeder 1975). The label and its network framing were introduced by Kindervag (2010), who argued that the distinction between a trusted inside and an untrusted outside was itself the vulnerability. The approach was consolidated into a reference model by the National Institute of Standards and Technology, whose Special Publication 800-207 defines zero-trust around per-request authorisation by a policy decision point (PDP) and enforcement by a policy enforcement point (PEP), informed by identity, device state and continuously updated risk (Rose et al. 2020). Subsequent surveys have mapped the design space and the gaps between principle and practice (Buck et al. 2021; Syed et al. 2022), and maturity models now guide phased adoption (Cybersecurity and Infrastructure Security Agency 2023). The common finding is that zero-trust is an architecture and an operating discipline rather than a product, and that its benefit is realised through the containment of movement after an inevitable initial compromise.

Coalition logistics information exchange

Allied sustainment doctrine treats interoperability and the timely exchange of logistic information as a precondition for multinational sustainment (NATO Standardization Office 2026). Achieving it requires federating data across national systems of differing classification and releasability, which is as much a trust-management problem as a technical one. The releasability of a data item to a particular partner is an attribute that must be enforced at the point of access, a requirement that maps naturally onto attribute-based access control (ABAC) within a zero-trust model. In alliance practice this exchange runs through dedicated systems: the Logistics Functional Area Services (LOGFAS) suite, through which nations plan deployments and movements and report stocks, and the logistic reporting (LOGREP) arrangements that feed the shared logistics picture (NATO 2012). Whatever secures coalition logistics data exchange must in the end secure systems of this kind. The literature on coalition information sharing has long recognised the tension between the need

to share and the need to protect, but it has rarely been connected to a quantified model of how architectural choices change the outcome of a breach. The closest work, by Schmitt et al. (2025), identifies the requirements and key components of a tactical zero-trust architecture for a coalition environment and evaluates a prototype implementation against those requirements in a virtual testbed. That study establishes that such an architecture is feasible and what it must contain, but it is a requirements-and-prototype evaluation rather than a quantified analysis of risk. The present article supplies what is missing: a six-nation breach-propagation Monte-Carlo model of coalition logistics data exchange that quantifies blast radius, the probability of reaching the critical consolidated store, and cross-national spread across an attacker-capability sweep, and so measures how much a zero-trust architecture reduces breach impact rather than only confirming that one can be built.

Supply-chain and coalition cyber risk

The risk that a trusted third party becomes the route of compromise is now central to cybersecurity practice. Guidance on cyber supply-chain risk management stresses that an organisation inherits the risk of its partners and dependencies (Boyens et al. 2024), and threat reporting documents the growth of attacks that reach their target through a weaker connected party (European Union Agency for Cybersecurity 2021). The systems-security-engineering literature reframes the objective from prevention to resilience, that is, limiting the damage of compromises that will occur and recovering from them (Ross et al. 2021). A coalition is a supply chain of trust, and its logistics data exchange is exactly the kind of densely interconnected, unevenly assured environment in which these concerns are sharpest. The gap addressed here is the absence of a quantitative link between the architectural choice and the coalition-level consequences of a breach.

Materials and Methods
Model overview and assumptions

A breach-propagation Monte-Carlo model was constructed. The coalition is represented as a graph of twenty nodes: six partner nations, each contributing an ERP node, a movement-control node and a gateway, together with a shared federation hub and the critical consolidated logistics data store that the hub fronts. Within each nation the three systems are interconnected; each national gateway connects to the hub; and the hub alone connects to the critical store. This is the topology of Figure 1.

An attack begins with the compromise of a single partner node, representing a stolen credential, a compromised partner system or an insider. The breach then

propagates: from any compromised node the adversary attempts to move to each adjacent node, and each attempt succeeds with a probability that depends on the edge it crosses and on the architecture in force. Three edge classes are distinguished: movement within a national enclave; movement from a gateway across the federation to the hub; and movement from the hub to the critical store, which is the most strongly defended. How hard each class is to cross under each architecture is set by the probabilities described in the simulation procedure and parameters subsection.

Four assumptions bound the model, stated here so that the results can be read against them. The initial compromise is taken as given, because credential theft and partner compromise cannot be excluded from any real federation. Each attempted move is an independent Bernoulli trial; there is no learning and no time dimension, so detection and eviction are not represented. The three architectures differ only in the probabilities they assign, which isolates the trust decision from every other design difference. And the controls are assumed to work as specified, an assumption revisited in the discussion of the model's limitations. The parameter values are representative rather than measured: they encode the ordering that movement is easiest inside a flat enclave, harder across segment boundaries and hardest against a per-request decision, so the analysis rests on the direction and relative size of the differences between architectures rather than on absolute point values.

The three architectures

The three architectures express the trust decision differently. Perimeter trust permits easy lateral movement once a node is inside the federation, so its base probabilities are high. Microsegmentation partitions the network and so lowers the probability of lateral movement between segments. Zero-trust applies the logic of Figure 2, in which a policy enforcement point intercepts every request and a policy decision point authorises it per request against identity, device posture and the releasability attributes of the data, with continuous monitoring feeding a risk score that can trigger denial or session eviction. The per-request authorisation flow is shown in Figure 3. Because every hop is re-evaluated and the critical store is additionally protected by ABAC, zero-trust assigns the lowest probabilities and the lowest caps, so that even a highly capable adversary cannot move freely.

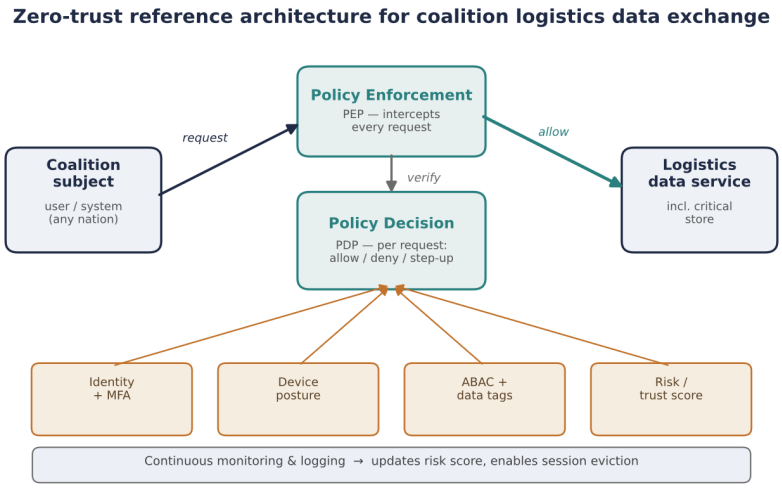


Figure 2. Zero-trust reference architecture for coalition logistics data exchange: a policy enforcement point intercepts every request and a policy decision point authorises it per request using identity, device posture, attribute-based access control and a continuously updated risk score

Source: own elaboration

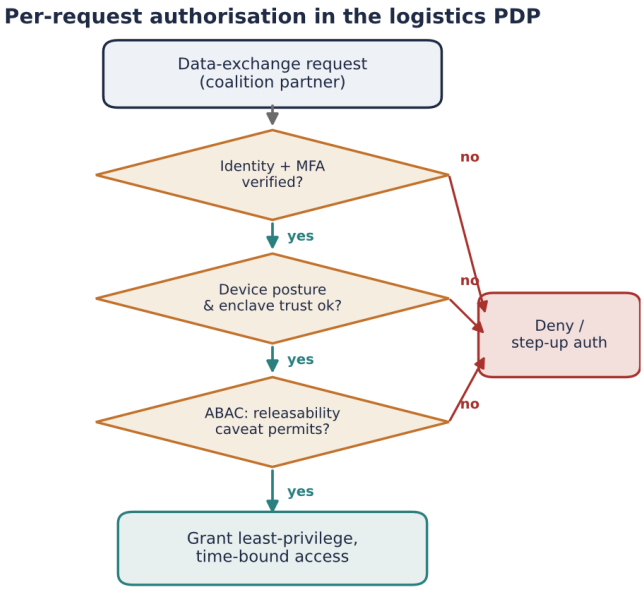


Figure 3. Per-request authorisation in the policy decision point: identity, device posture and releasability attributes are checked on every access, and only a least-privilege, time-bound grant is issued

Source: own elaboration

Simulation procedure and parameters

Each run of the simulation proceeds in four steps. First, the twenty-node graph described in the model overview is built. Second, an entry point is drawn uniformly at random from the eighteen national nodes; the hub and the store are never entry points. Third, the breach spreads in breadth-first order: every compromised node attempts to move to each neighbour not yet compromised, each attempt succeeds with the probability defined below, and a node that resists one attempt can still fall to a later attempt from another compromised neighbour. Propagation stops when no compromised node has an uncompromised neighbour left to try. Fourth, four outcomes are recorded: the blast radius, defined as the fraction of the twenty nodes compromised; whether the critical store was reached; the number of distinct nations with at least one compromised node; and, where the store fell, the number of hops from the entry point.

For an edge of class c under architecture a, a single movement attempt succeeds with probability $p(a, c, \alpha) = \text{base}(a, c) + \alpha \cdot (\text{cap}(a, c) - \text{base}(a, c))$, which rises linearly from the base value at $\alpha = 0$, a low-capability adversary, to the cap at $\alpha = 1$, a near-omnipotent one. The capability parameter is swept from 0.0 to 1.0 in steps of 0.1, and each of the 33 combinations of architecture and capability level is replicated 3,000 times; reported values are means over the replications. Table 1 lists every parameter value, including the caps for each edge class.

The model is implemented in Python, using only the standard library. Propagation is realised as a breadth-first search over the graph, and each replication of each experimental cell draws its pseudo-random numbers from a generator seeded with a fixed function of the replication index, the capability level and the architecture, so every run, and therefore every value reported in the results section, is exactly reproducible. The description in this section, together with Table 1, is sufficient to reimplement the simulation independently; at 3,000 replications the standard error of every reported proportion is below one percentage point. The code and the generated result files are available from the corresponding author (see the Data Availability Statement).

Table 1. Model parameters and per-architecture lateral-movement probabilities

Parameter	Value
Partner nations	6
Nodes per nation (ERP, movement, gateway)	3
Shared nodes (federation hub, critical store)	2
Total nodes	20
Monte-Carlo replications per point	3000
Attacker capability α (swept)	0.0 – 1.0 in steps of 0.1

Table 1 (continued)

Parameter	Value
Perimeter base → cap (intra / federation / critical)	0.85 → 1.00 / 0.70 → 0.98 / 0.60 → 0.95
Microsegmentation base → cap (intra / fed. / critical)	0.45 → 0.85 / 0.30 → 0.70 / 0.25 → 0.60
Zero-trust base → cap (intra / federation / critical)	0.12 → 0.45 / 0.08 → 0.35 / 0.04 → 0.22

Source: own elaboration

Results and Analysis
Blast radius and attacker capability

Figure 4 shows the blast radius as a function of attacker capability. Under perimeter trust the breach is extensive even against a weak adversary, compromising about 55% of nodes at the lowest capability, and it grows almost linearly to 97% as the attacker improves. Microsegmentation lowers the whole curve, from about 16% to 55%, but the breach still expands substantially with capability. Zero-trust both lowers and flattens the curve, holding the blast radius between roughly 7% and 16% across the entire capability range. The vertical distance between the perimeter and zero-trust curves, marked in the figure as the containment gap, is the share of the network that zero-trust keeps the adversary out of, and it widens as the adversary becomes more capable. The mechanism is that perimeter exposure compounds, because each successful hop opens further easy hops, whereas under zero-trust every hop is independently re-evaluated and most attempts fail, so the breach cannot snowball.

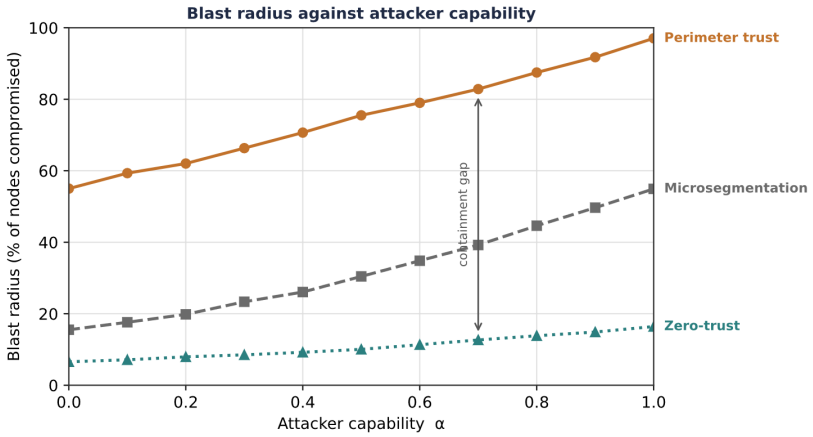


Figure 4. Blast radius against attacker capability. Zero-trust both lowers and flattens the curve, so the containment gap relative to perimeter trust widens as the adversary improves

Source: own elaboration

The critical store and cross-national spread

The outcomes of greatest operational interest are whether the adversary reaches the consolidated data store and how many partner nations are drawn into the breach. Under perimeter trust the probability of reaching the critical store rises from 43% to 94% across the capability range, and the breach spreads to between 3.4 and 5.8 of the six nations; a local compromise reliably becomes a coalition-wide loss of the most sensitive data. Microsegmentation reduces both figures appreciably but not decisively. Zero-trust changes the picture in kind rather than degree: the probability of reaching the critical store stays below 6% even against the most capable adversary, and the breach is confined to about one nation throughout, rising only to 1.4 nations at maximum capability. Figure 5 traces the store-reach probability across the whole capability range.

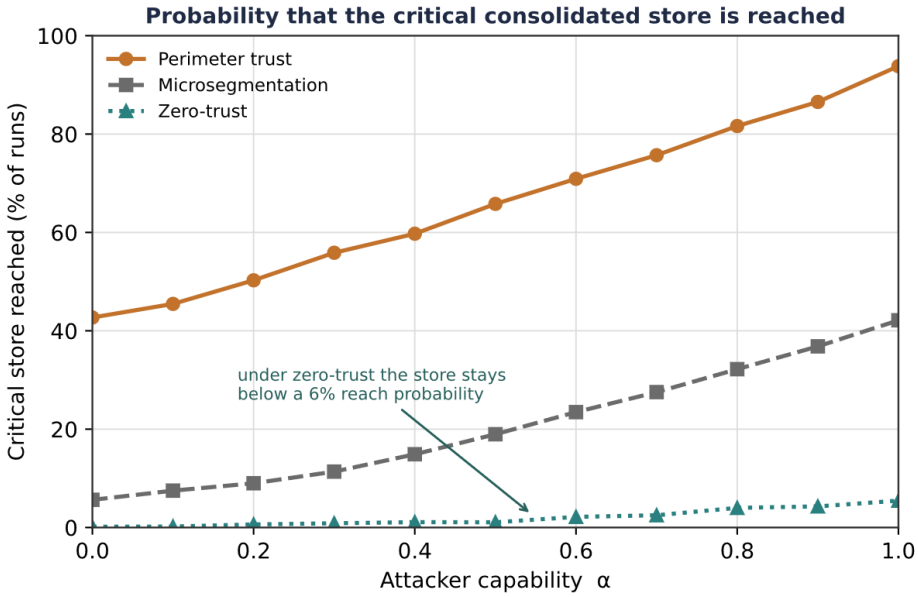


Figure 5. Probability that the critical consolidated logistics data store is reached, against attacker capability, by architecture

Source: own elaboration

Figure 6 gathers the three outcome measures at a representative capable-adversary level (α = 0.5); Table 2 lists the values, and Table 3 extends the two headline metrics to a weak (α = 0.1) and an advanced (α = 0.9) adversary.

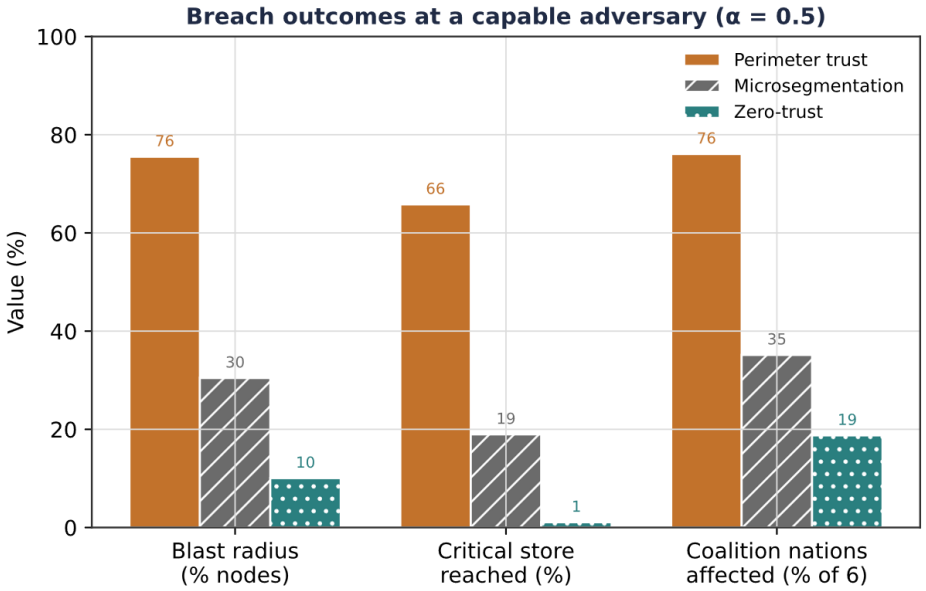


Figure 6. Breach outcomes at a capable adversary (α = 0.5): blast radius, probability the critical store is reached, and the share of coalition nations affected, by architecture

Source: own elaboration

Table 2. Breach outcomes at a capable adversary (α = 0.5)

Metric	Perimeter	Microsegmentation	Zero-trust
Blast radius (% of nodes)	75.5%	30.4%	10.0%
Critical store reached	65.8%	19.0%	1.1%
Coalition nations affected (of 6)	4.6	2.1	1.1
Mean hops to critical store	2.71	2.70	2.50

Source: own elaboration

The coalition reading of these numbers is the important one. Zero-trust changes the character of the breach as well as its size: an incident that would have propagated across partners and exposed shared sensitive data stays close to its point of origin instead. For a coalition, that is the difference between a single nation managing a contained intrusion and the alliance as a whole losing its common logistics picture. Table 3 shows that this holds across the capability range, and that the distance between the architectures widens as the adversary improves.

Table 3. Blast radius and critical-store exposure at three attacker-capability levels

Metric	α	Perimeter	Microsegmentation	Zero-trust
Blast radius (% of nodes)	0.1	59.3%	17.6%	7.1%
	0.5	75.5%	30.4%	10.0%
	0.9	91.8%	49.7%	14.9%
Critical store reached	0.1	45.5%	7.5%	0.2%
	0.5	65.8%	19.0%	1.1%
	0.9	86.5%	36.8%	4.3%

Source: own elaboration

Mapping controls to coalition logistics threats

The containment in the simulation is produced by the combination of zero-trust controls rather than by any single one. Figure 7 maps the principal controls to the threats that matter for coalition logistics, scoring the strength of each control against each threat. Identity and multi-factor authentication (MFA), together with continuous monitoring, bear most directly on stolen-credential and insider threats; microsegmentation and per-request authorisation contain lateral movement; and ABAC with data tagging, supported by encryption, does most to protect the releasability of the consolidated store against exfiltration. No single control is sufficient on its own; the result comes from the architecture operating as a whole.

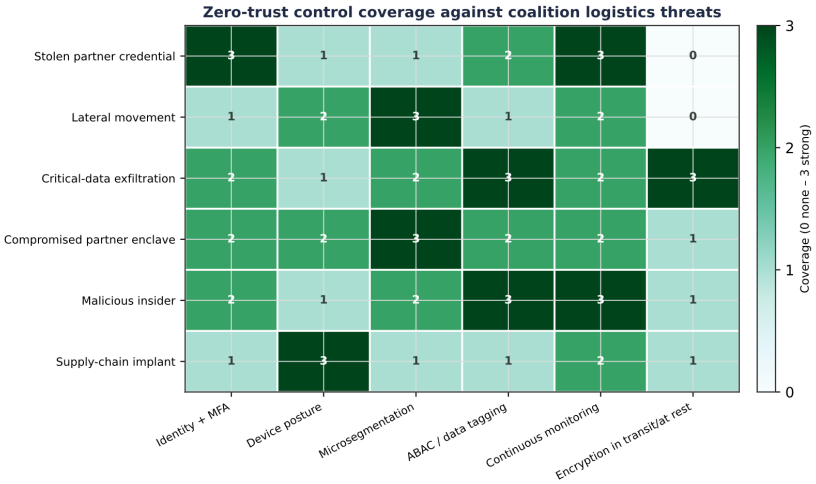


Figure 7. Coverage of zero-trust controls against coalition logistics threats, scored from none to strong

Source: own elaboration

Discussion
Limitations of the model

The model is intentionally simple, and its limitations bound the claims. It represents breach propagation as independent per-edge successes and does not model specific vulnerabilities, detection latency or the time dimension of an intrusion; a fuller treatment would represent dwell time and the race between attacker movement and defender eviction. The parameters were not calibrated against a real coalition network, so the absolute percentages should be read as indicative and the comparative pattern as the result. The model also assumes that the zero-trust controls function as designed, whereas in practice their value depends on the quality of identity federation across nations, on consistent device-posture signals from partners of differing maturity, and on agreed data-tagging and releasability schemes. These dependencies are themselves coalition problems, and a poorly federated identity layer would erode the benefit shown here.

The model against real allied logistics systems

The abstraction maps onto named systems. The federation hub and the consolidated store stand where shared logistics functional services stand in NATO practice: the LOGFAS suite, with its deployment and movement planning and its stock reporting, and the LOGREP arrangements that populate the recognised logistics picture (NATO 2012). The national ERP and movement-control nodes are the systems from which those feeds originate. The traffic in question is mundane and constant: stock and readiness reports, movement bids, port and airfield throughput, host-nation support requests. Every crossing of a national boundary is an access decision. The model counts what follows when those decisions carry implicit trust and when they do not.

The cost of losing such an environment is documented, not hypothetical. In 2017 the NotPetya malware entered A.P. Møller-Maersk through the compromised update channel of a Ukrainian accounting package, a trusted connection, and within hours had disabled the booking and terminal systems of a carrier handling close to a fifth of the world's container shipping capacity; recovery took about ten days and cost the company roughly 300 million dollars (Greenberg 2018). Military sustainment leans on exactly such civilian carriers and on reporting environments with the same trust structure. In the model's terms NotPetya travelled on perimeter assumptions, and the zero-trust rows of Tables 2 and 3 state how far an equivalent intrusion gets when every hop must be re-authorised.

Design implications for coalitions

Within those bounds the implications are clear and, the author argues, robust. The coalition investment that changes the outcome is the removal of implicit trust from the interior, ahead of any further strengthening of the perimeter: once no partner is trusted by default, a compromised partner cannot become a coalition-wide incident. The enabling work is organisational as much as technical: a federated identity scheme that partners of differing maturity can join, an agreed ABAC and data-tagging model that encodes releasability, and continuous monitoring whose signals are shared sufficiently to drive a common risk score. These findings are consistent with the resilience-oriented view of Ross et al. (2021) and with the policy direction of recent defence zero-trust strategies (U.S. Department of Defense 2022), and they extend that direction by quantifying, for logistics data exchange specifically, how the protective benefit scales with the capability of the adversary. None of this requires nations to rebuild their ERP or movement-control systems, because zero-trust changes what a request must prove when it crosses between them; an environment of the LOGFAS kind can be brought under such an architecture incrementally, gateway by gateway.

Conclusions

This article modelled the cyber resilience of multinational military logistics data exchange under three trust architectures, and reached three conclusions. First, zero-trust contains the blast radius of a breach: where perimeter trust allows a single compromise to spread from about 55% to 97% of the network as the attacker improves, zero-trust holds the spread between 7% and 16%. Second, the protective benefit grows with the threat, because the containment gap widens as the adversary becomes more capable, so zero-trust is most valuable against precisely the sophisticated adversary that a peer conflict implies. Third, and most important for a coalition, zero-trust keeps the probability of reaching the shared critical store below 6% and confines the breach to roughly its originating nation, where under perimeter trust the same intrusion would have grown into an alliance-wide loss of the common logistics picture.

The broader implication is that the security of coalition logistics should be built on the assumption that any partner may be compromised, and engineered so that such a compromise stays local. In logistics terms what that buys is continuity: sustainment planning, stock visibility and movement control keep working through a partner's compromise because the data exchange beneath them survives it. Future work should add a temporal dimension to the model, incorporating detection and

eviction, calibrate it against the topology of a real federated logistics network, and examine the federation of identity and data-releasability attributes across partners of differing assurance, which the present analysis identifies as the binding enabler of the benefit it measures.

References

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A. and Fallon, M., 2024. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST Special Publication 800-161 Rev. 1 (Update 1). Gaithersburg, MD: National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-161r1-upd1.

Buck, C., Olenberger, C., Schweizer, A., Völter, F. and Eymann, T., 2021. Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, 110, 102436. DOI: https://doi.org/10.1016/j.cose.2021.102436.

Cybersecurity and Infrastructure Security Agency, 2023. Zero Trust Maturity Model, Version 2.0 [online]. Washington, DC: CISA. Available from: https://www.cisa.gov/zero-trust-maturity-model [Accessed: 4 July 2026].

European Union Agency for Cybersecurity, 2021. ENISA Threat Landscape for Supply Chain Attacks [online]. Athens: ENISA. Available from: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks [Accessed: 4 July 2026].

Greenberg, A., 2018. The untold story of NotPetya, the most devastating cyberattack in history. Wired [online], 22 August. Available from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Accessed: 5 September 2026].

Kindervag, J., 2010. Build Security into Your Network's DNA: The Zero Trust Network Architecture. Cambridge, MA: Forrester Research.

NATO, 2012. NATO Logistics Handbook [online]. Brussels: NATO Headquarters. Available from: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/pdf_2016_03/20160303_2012-logistics_hndbk-en.pdf [Accessed: 5 September 2026].

NATO Standardization Office, 2026. Allied Joint Doctrine for Sustainment of Operations (AJP-4, Edition C, Version 1) [online]. Brussels: North Atlantic Treaty Organization. Available from: https://www.gov.uk/government/publications/allied-joint-doctrine-for-sustainment-of-operations-ajp-4 [Accessed: 4 July 2026].

Rose, S., Borchert, O., Mitchell, S. and Connelly, S., 2020. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-207.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. and McQuaid, R., 2021. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160 Vol. 2 Rev. 1. Gaithersburg, MD: National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-160v2r1.

Saltzer, J.H. and Schroeder, M.D., 1975. The protection of information in computer systems. Proceedings of the IEEE, 63 (9), 1278–1308. DOI: https://doi.org/10.1109/PROC.1975.9939.

Schmitt, T., Shaffer, A. and Singh, G., 2025. Tactical zero trust architectures in a coalition environment. In: Arabnia, H.R., Deligiannidis, L., Shenavarmasouleh, F., Amirian, S. and Ghareh Mohammadi, F., eds. Computational Science and Computational Intelligence (CSCI 2024). Communications in Computer and Information Science, vol.

2510. Cham: Springer Nature Switzerland, 3–17. DOI: https://doi.org/10.1007/978-3-031-94956-2_1.
Syed, N.F., Shah, S.W., Shaghaghi, A., Anwar, A., Baig, Z. and Doss, R., 2022. Zero trust architecture (ZTA): a comprehensive survey. IEEE Access, 10, 57143–57179. DOI: https://doi.org/10.1109/ACCESS.2022.3174679.
U.S. Department of Defense, 2022. Department of Defense Zero Trust Reference Architecture, Version 2.0 [online]. Washington, DC: Defense Information Systems Agency and National Security Agency. Available from: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf [Accessed: 4 July 2026].

Author Contributions
The author is the sole author of this article and is solely responsible for its conceptualisation, methodology, software, formal analysis and writing.

Funding
This research received no external funding.

Data Availability Statement
The simulation code and the generated result files supporting the figures are available from the corresponding author upon reasonable request.

Conflict of Interest Statement
The author declares no conflict of interest.

Use of AI Tools
The author used DeepL, an AI-based language translation tool that uses machine-learning technology, during the preparation of the manuscript to assist with translation and to polish the language and phrasing to a natural, publication-appropriate level of English. All content, including the scientific analysis, methodological choices, interpretation of the results, and final wording, was reviewed and verified by the author, who takes full responsibility for the content of the manuscript.

Ethics Approval / Consent
Not applicable.

Received: 4.07.2026
Accepted: 24.10.2026

© Artur Chlebicki, 2026. This article is published in «*Systemy Logistyczne Wojsk*" / "*Military Logistics Systems*" under the Creative Commons Attribution 4.0 International licence (CC BY 4.0).