

Revista Sextante

ISSN : 2665-3923

Vol: 30 No: 01 (2024)

Risk Assessment and Operational Continuity in Military Logistics and Defense Supply Networks

Kofi A. Mensah-Boateng

Department of Defence Logistics and Resilience Studies, Gold Coast Institute for Strategic Logistics, Accra, Ghana

Article History

Received June, 07th , 2024

Accepted June, 08th , 2024

Published June, 09th, 2024



© 2024 The Authors. This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution(CC-BY)license

<https://creativecommons.org/licenses/by/4.0>

Abstract

Military operations depend on supply networks that move fuel, munitions, spare parts, food, medical supplies, and equipment from industrial sources to forces in the field and at sea. Disruption of these networks can undermine operational capability more quickly than the loss of combat power. This article examines risk assessment and operational continuity in military logistics and defence supply networks. It describes the logic of continuity in defence supply, classifies sources of logistic risk, and reviews frameworks and methods for assessing risk, including criticality, dependency, and vulnerability analysis. It then considers continuity planning, resilience strategies based on redundancy, flexibility, and agility, and the special problems of contested logistics in which an adversary deliberately targets supply. The article also discusses governance, metrics, and organisational learning. Drawing on research in supply chain risk management, resilience, and continuity management, the analysis finds that effective continuity depends on understanding dependencies across the whole network, assessing risk in operational rather than purely financial terms, and preparing adaptive responses in advance. It concludes with recommendations for defence organisations seeking to protect the continuity of operations against a wide spectrum of disruption.

Keywords: military logistics, risk assessment, operational continuity, supply network resilience, contested logistics

INTRODUCTION

Armed forces have long recognised that logistics shapes what operations are possible. Armies and fleets have been halted not only by enemy action but by shortages of food, fuel, and ammunition, and by the failure of supply lines. Kress, in his study of operational logistics, describes military sustainment as a system of interacting processes whose

design determines the endurance and tempo of operations (Kress, 2016). In modern conditions, this system extends from global industrial suppliers through ports, depots, and transport fleets to the individual unit. Supply networks today are more complex, more global, and more dependent on digital systems than in the past. Tang observed that supply chains face a wide range of risks, from supply and demand uncertainty to disruptions caused by natural disasters, labour disputes, supplier failures, and terrorism, and that managing these risks requires deliberate strategies rather than reliance on efficiency alone (Tang, 2006). Defence supply networks inherit these civil vulnerabilities and add others arising from conflict, in which adversaries may deliberately attack the means of sustainment. Operational continuity refers to the ability of an organisation to continue delivering essential functions during and after disruption. For a military force, this means maintaining the flow of critical supplies and services so that operations can proceed. Risk assessment is the process of identifying and evaluating threats and vulnerabilities to that flow, so that resources can be directed to the most significant exposures. Together, they form the basis of resilient logistics. This article examines how risk assessment and continuity planning can be applied to military logistics and defence supply networks. It proceeds through nine thematic sections covering the logic of continuity, sources of risk, assessment frameworks, dependency analysis, continuity planning, resilience strategies, contested logistics, governance and learning, and recommendations. A summary and a list of references follow.

Defence Supply Networks and the Logic of Continuity:

A defence supply network is a system of organisations, facilities, transport links, and information flows through which materiel and services reach the user. It includes industrial suppliers and subcontractors, government depots and warehouses, ports and airfields, commercial and military transport, and the units that consume supplies. It is typically multi tiered, with many suppliers at the lower tiers whose identity may not be fully known to the end customer. Continuity is central because the cost of failure is measured in operational capability rather than money. A missing part can ground an aircraft or immobilise a ship, and an interrupted fuel supply can stop a campaign. Because demand in conflict may rise suddenly and unpredictably, networks designed for peacetime efficiency may lack the capacity to surge. Logistic feasibility defines the range of strategic possibilities, which means that continuity cannot be treated as a secondary concern (Kress, 2016). The logic of continuity differs from that of commercial supply chains in several respects. Commercial firms balance cost and service, and may accept occasional stockouts if the cost of avoiding them is high. Defence organisations accept higher costs to ensure availability of critical items, because failure may be unacceptable. Defence networks also face deliberate adversaries, not just accidents. And they must function in austere and degraded conditions, away from developed infrastructure. Understanding continuity requires attention to the whole network, not just to individual links. A resilient depot is of little value if the transport route to the unit is cut, and a stockpile of parts is useless if the data systems that track it fail. Christopher and Peck argued that resilience must be considered across the end to end supply chain, since weaknesses at any point can undermine the whole (Christopher and Peck, 2004).

Sources and Taxonomy of Logistic Risk:

Risks to defence supply networks can be classified by origin. Supply risks arise from the failure of suppliers, shortages of critical materials, quality problems, and dependence on single or foreign sources. Demand risks arise from unforeseen surges or shifts in requirements, as when an operation consumes munitions or spares at rates far above planning assumptions. Process and transport risks arise from delays, capacity shortfalls, accidents, and failures at ports or depots. External risks include natural hazards such as storms, floods, and earthquakes, pandemics that disrupt labour and production, and geopolitical shocks such as sanctions, trade restrictions, and conflict. Cyber risks arise from attacks on information systems used for planning, tracking, and control. Kleindorfer and Saad proposed a framework for managing disruption risks in supply chains that distinguishes operational contingencies from disruptions, and emphasises the need to assess both the likelihood and the consequence of low probability, high impact events (Kleindorfer and Saad, 2005). Craighead and colleagues found that the severity of supply chain disruptions depends on design characteristics, such as density of nodes, complexity of the network, and node criticality, as well as on mitigation capabilities such as recovery ability and warning systems (Craighead et al., 2007). This finding is helpful for defence logisticians, since it suggests that network structure can be improved to reduce the impact of disruption, and that early warning and rapid recovery are valuable. In the military context, adversary action constitutes a distinct category. Hostile forces may attack ports, lines of communication, and logistic ships, conduct cyber operations against transport and inventory systems, interfere with navigation and communications, and exploit supply chain weaknesses through sabotage or the introduction of counterfeit components. Perrow argued that tightly coupled and complex systems are prone to accidents in which small failures cascade, and such coupling is evident in highly optimised logistic networks (Perrow, 1984). The figure below presents an illustrative comparison of the relative composite risk rating of several categories of logistic risk, as discussed in the literature, expressed on a standardised index from zero to one hundred. The values are stylised to show relative magnitude and should not be read as measured data.

Risk Assessment Frameworks and Methods for Supply Networks:

Risk assessment seeks to answer the questions of what can go wrong, how likely it is, and what the consequences would be, a formulation set out by Kaplan and Garrick that remains foundational (Kaplan and Garrick, 1981). Aven later stressed that assessments should also report the strength of knowledge on which judgements are based, since risk concerns uncertainty and not only probability (Aven, 2016). These principles apply directly to logistics, where data may be incomplete and adversary behaviour is uncertain. A typical assessment process begins with mapping the network, identifying key nodes, links, and flows. It then identifies hazards and threats, analyses vulnerabilities, estimates likelihood and impact, and evaluates risk against criteria. Treatment options, such as reducing, transferring, accepting, or avoiding risk, are then selected and implemented, and results are monitored. Pettit, Fiksel, and Croxton developed a conceptual framework for ensuring supply chain resilience that links vulnerabilities and capabilities, suggesting that organisations should assess both their exposure and their ability to anticipate and respond (Pettit et al., 2010). Methods range from qualitative workshops and risk matrices to quantitative models. Failure mode and effects analysis identifies how components or processes may fail and the effects of failure. Scenario analysis explores plausible disruptions and their consequences. Simulation models represent the network and test how it behaves under stress, including surges in demand or loss of nodes. Network analysis identifies nodes whose removal would most severely disrupt flows. In defence settings, assessments should express consequences in operational terms, such as days of supply, mission capable rates, or time to restore a capability, not only in financial terms. Operational planners need to know how a disruption would affect the ability to conduct missions. Assessments should also consider the interplay of multiple simultaneous disruptions and the possibility that adversaries will exploit identified weaknesses.

Criticality, Dependency, and Vulnerability Analysis:

Prioritising effort requires distinguishing what matters most. Criticality analysis identifies the items, suppliers, facilities, and links whose loss would have the greatest effect on operational capability. Items may be critical because they are essential to mission success, have long lead times, lack substitutes, or come from a single source. Facilities may be critical because they handle a large share of flows or provide unique capabilities. Dependency analysis explores how elements rely on each other. Rinaldi, Peerenboom, and Kelly examined the identification and analysis of critical infrastructure interdependencies and showed that infrastructures are linked through physical, cyber, geographic, and logical connections, so that failure in one may cascade to others (Rinaldi et al., 2001). For defence logistics, this means that a port depends on power, communications, and road or rail links, and that logistic information systems depend on networks and software that may be shared with civil users. Vulnerability analysis examines how susceptible critical elements are to specific threats. It considers physical exposure to attack or natural hazard, concentration in a single location, reliance on a single transport mode, lack of redundancy, weak cyber defences, and limited recovery capacity. The combination of high criticality and high vulnerability identifies priorities for protection or redundancy. Deep tier visibility is a persistent challenge. Many risks lie several tiers below the prime contractor, in the supply of materials, components, and software that the customer may not see. Mapping sub tier suppliers, tracking sources of critical materials, and monitoring financial and geopolitical risk indicators are therefore important tasks. Digital tools can assist but require cooperation from industry and sharing of sensitive commercial information under appropriate protections.

Business Continuity and Operational Continuity Planning:

Continuity planning prepares an organisation to maintain essential functions through disruption. The international standard for business continuity management systems describes a cycle of understanding the organisation and its context, analysing impacts, determining strategies, developing plans, exercising and testing them, and continually improving (International Organization for Standardization, 2019). Although designed for civil organisations, its principles have been adopted in many defence settings. A central step is the business impact analysis, which identifies the essential functions of the organisation, the resources they depend upon, and the effects of their interruption over time. In military logistics, this translates into identifying the supply and support functions that are vital to operations, such as fuel distribution, ammunition resupply, aircraft and ship maintenance, and medical support, and determining the maximum tolerable period of disruption for each. These time thresholds guide the level of investment in redundancy and recovery. Continuity strategies then specify how functions will be sustained or restored. They may include alternative suppliers and transport routes, pre positioned stocks, dispersed storage, backup facilities, mobile support units, manual workarounds for digital systems, and agreements with civil providers. Plans should assign roles, define triggers and decision authorities, establish communication arrangements, and describe the sequence of actions for recovery. Plans are only valuable if they are tested. Exercises, ranging from tabletop discussions to full scale simulations, reveal gaps, build familiarity, and refine procedures. Realistic exercises should include degraded communications, loss of key nodes, and adversary interference. Lessons identified must be recorded and implemented. Because networks and threats change, plans need regular review and updating, and they must be integrated with operational planning so that logistic continuity measures are part of the campaign design rather than a separate concern.

Resilience Strategies of Redundancy, Flexibility, and Agility:

Continuity plans draw on several resilience strategies. Redundancy involves holding extra capacity, whether in the form of inventory, spare transport, alternate facilities, or multiple suppliers. It provides buffers against disruption and time to adapt. Its cost, however, can be high, and excess stock may become obsolete. Decisions on where to hold reserves should be guided by criticality and vulnerability analysis, focusing on items and nodes whose loss would be most damaging. Flexibility refers to the ability to change sources, routes, modes, or production methods quickly. It can be built through qualifying multiple suppliers, using standardised and interchangeable components, designing transport plans with alternative paths, and maintaining relationships with civil carriers. Sheffi and Rice argued that flexibility and a culture of readiness often yield more resilience at lower cost than redundancy alone, because they allow organisations to respond to a wide range of disruptions (Sheffi and Rice, 2005). Agility, the ability to sense and respond rapidly to change, depends on information and decision speed. Visibility of stocks and flows, early warning of disruption, and delegated authority to reroute or reallocate resources shorten reaction time. Christopher and Peck emphasised that supply chain agility and the capacity for collaboration among partners are key elements of resilience (Christopher and Peck, 2004). In the military context, agile logistics supports manoeuvre and tempo by allowing support to follow changes in operational plans. Other strategies include dispersion, which reduces the consequences of attack on any single location, and hardening, which protects critical facilities. Simplification reduces complexity and coupling, thereby lowering the chance of cascading failures, a point consistent with Perrow's analysis of tightly coupled systems (Perrow, 1984). Standardisation of equipment and spare parts across services and allies increases the pool of available resources. Investment in repair capacity, local manufacturing, and the ability to cannibalise or adapt equipment provides further adaptive capability when resupply is interrupted. No single strategy suffices. A balanced portfolio, tailored to risks and costs, offers the best resilience. Efficiency need not be abandoned, but it should not be pursued at the expense of the ability to continue operating under stress.

Contested Logistics and Adversary Action:

In conflict, an opponent will attempt to disrupt sustainment. Contested logistics refers to conditions in which supply lines, bases, and facilities are subject to attack or interference, and in which logistic activities must be conducted under threat. This is a significant departure from peacetime assumptions of secure rear areas and reliable transport. Adversaries can target logistic assets through kinetic means, such as attacks on ports, airfields, depots, and supply ships, and through non kinetic means such as cyber operations, electronic warfare, and disruption of navigation and communications. They may also exploit civil vulnerabilities, such as dependence on commercial shipping, privately owned ports, and civil infrastructure. Long, predictable, and concentrated supply lines are especially vulnerable. Risk assessment in this setting must account for adaptive and intelligent opponents. Unlike natural hazards, adversaries observe defences and choose their targets, which means that visible weaknesses invite attack. Assessments should therefore adopt an adversary perspective, using red teaming and wargaming to identify how logistic networks could be disrupted most effectively. Kaplan and Garrick's scenario based view of risk, in which each scenario has likelihood and consequences, can be applied by building scenarios of adversary action (Kaplan and Garrick, 1981). Responses include dispersing stocks and distributing capacity so that no single strike is decisive, protecting key nodes with active and passive defences, diversifying routes and modes, using deception and emission control to reduce visibility, and preparing to operate with reduced and austere support. Forward positioning of critical supplies, mobile and modular support, local production, and prepared fallback bases improve endurance. Convoy and escort arrangements, and the security of sea lanes, remain vital for naval supply. Close coordination with allies and civil operators ensures that protection and alternatives are available when needed.

Governance, Metrics, and Organisational Learning:

Effective continuity management requires clear governance. Responsibility for logistic risk should be assigned to accountable leaders with authority across organisational boundaries, since supply networks span services, agencies, and industry. Risk appetite, meaning the level of risk the organisation is willing to accept, should be defined by senior leadership and translated into thresholds and criteria that guide decisions. Metrics make resilience measurable. Useful indicators include days of supply for critical items, the proportion of items with qualified alternative sources, time to recover from simulated disruption, mission capable rates, order fulfilment times, and the share of suppliers with mapped sub tier visibility. Craighead and colleagues' emphasis on recovery capability and early warning suggests indicators such as detection time and recovery time (Craighead et al., 2007). Metrics should be used with care to avoid distorting behaviour, and they should be complemented by qualitative review. Organisational learning is vital. Disruptions, exercises, and near misses provide information about weaknesses and the effectiveness of responses. Structured after action reviews, shared lessons across services and allies, and feedback into planning and doctrine convert experience into improvement. Culture matters, since personnel must feel free to report problems and to challenge assumptions without fear of blame. Aven's call for transparent communication of uncertainty and the strength of knowledge supports honest reporting of limitations in risk assessments (Aven, 2016). Industry partnership forms part

of governance. Contracts and agreements should include requirements for supply chain visibility, risk reporting, cyber security, and continuity planning by suppliers, together with mechanisms for surge and priority access. Regular engagement with key suppliers, including joint exercises and information sharing, builds trust and shared understanding of risks.

Recommendations and Future Directions:

Several recommendations arise from the analysis. First, defence organisations should map their supply networks end to end, including deep tier suppliers, and identify critical items, nodes, and dependencies. Second, they should assess risk in operational terms, linking disruptions to effects on mission capability and expressing results in measures that commanders can use. Third, they should prioritise mitigation according to criticality and vulnerability, using a mixture of redundancy, flexibility, agility, dispersion, and protection. Fourth, they should develop and exercise continuity plans that include degraded digital conditions and adversary interference, and that integrate logistic considerations into operational planning. Fifth, they should strengthen governance by assigning accountability, defining risk appetite, setting metrics, and embedding learning mechanisms. Sixth, they should cooperate with allies and industry, aligning standards, sharing information, and agreeing arrangements for surge and priority supply. Looking ahead, several trends will shape the field. Digital tools, including advanced analytics, sensors, and digital twins of supply networks, will improve visibility and simulation of disruptions, though they will also create new cyber dependencies. Additive manufacturing and distributed production may reduce reliance on long supply lines for some items. Climate change, geopolitical competition, and the fragility of global supply chains for critical materials will keep risk high. Autonomous systems may reduce exposure of personnel but present new vulnerabilities. Research should evaluate the effectiveness of different resilience strategies under realistic conditions, develop methods for assessing risks in deep tier networks and for modelling adversary behaviour, and examine how to balance efficiency and resilience in constrained budgets. The central conclusion is that operational continuity is achieved through deliberate design, honest assessment, and continuous preparation rather than through luck or the assumption that supply lines will remain open.



Summary:

This article has examined risk assessment and operational continuity in military logistics and defence supply networks. Defence supply networks are multi tiered, global, and increasingly digital, and their disruption can undermine operational capability. Risks arise from supply, demand, process, external, cyber, and adversary sources, and they can be assessed through frameworks that combine criticality, dependency, and vulnerability analysis with scenario and simulation methods. Continuity planning, based on impact analysis, defined strategies, and regular exercises, prepares organisations to sustain essential functions. Resilience is strengthened through redundancy, flexibility, agility,

dispersion, and protection, and contested logistics demands special attention to adversary action. Governance, metrics, and organisational learning sustain improvement. Defence organisations that map their networks, assess risk in operational terms, plan and test continuity measures, and collaborate with allies and industry are best placed to keep operations supplied under pressure.

References:

- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13.
- Christopher, M., and Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management*, 15(2), 1–14.
- Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., and Handfield, R. B. (2007). The severity of supply chain disruptions: Design characteristics and mitigation capabilities. *Decision Sciences*, 38(1), 131–156.
- International Organization for Standardization. (2019). ISO 22301:2019 Security and Resilience: Business Continuity Management Systems: Requirements. Geneva: ISO.
- Kaplan, S., and Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, 1(1), 11–27.
- Kleindorfer, P. R., and Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management*, 14(1), 53–68.
- Kress, M. (2016). *Operational Logistics: The Art and Science of Sustaining Military Operations* (2nd ed.). Cham: Springer.
- Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.
- Pettit, T. J., Fiksel, J., and Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. *Journal of Business Logistics*, 31(1), 1–21.
- Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11–25.
- Sheffi, Y., and Rice, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review*, 47(1), 41–48.
- Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics*, 103(2), 451–488.