

# **What Happens When the Supply Chain Breaks? Implications for the Army Supply Chain Under Attack**

**A Monograph  
by  
Major Steven S. DeBusk  
United States Army**



**School of Advanced Military Studies  
United States Army Command and General Staff College  
Fort Leavenworth, Kansas  
First Term AY 02-03**

Approved for Public Release; Distribution is Unlimited

# REPORT DOCUMENTATION PAGE

Form Approved OMB No.  
0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

<b>1. REPORT DATE (DD-MM-YYYY)</b> 22-05-2003		<b>2. REPORT TYPE</b> monograph		<b>3. DATES COVERED (FROM - TO)</b> 18-06-2002 to 22-05-2003	
<b>4. TITLE AND SUBTITLE</b> What Happens When the Supply Chain Breaks? Implications for the Army Supply Chain Under Attack. Unclassified			<b>5a. CONTRACT NUMBER</b>		
			<b>5b. GRANT NUMBER</b>		
			<b>5c. PROGRAM ELEMENT NUMBER</b>		
			<b>5d. PROJECT NUMBER</b>		
			<b>5e. TASK NUMBER</b>		
			<b>5f. WORK UNIT NUMBER</b>		
<b>6. AUTHOR(S)</b> DeBusk, Steven S. ;			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b> ATZL-SWV		
<b>7. PERFORMING ORGANIZATION NAME AND ADDRESS</b> US Army School of Advanced Military Studies Eisenhower Hall 250 Gibbon Ave Fort Leavenworth, KS66027			<b>10. SPONSOR/MONITOR'S ACRONYM(S)</b>		
<b>9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS</b> ,			<b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b>		
			<b>12. DISTRIBUTION/AVAILABILITY STATEMENT</b> APUBLIC RELEASE ,		
<b>13. SUPPLEMENTARY NOTES</b>					
<b>14. ABSTRACT</b> This monograph answers the question: How should the Army adapt to sudden supply network change? Unexpected catastrophic have significant implications for the strategic-level support provided by the national economic base to the U.S. Army. In a system of tightly linked supply chains consisting of consumers, retailers, suppliers, and manufacturers, a sudden change in their ability to communicate data or distribute product can have a significant effect on the entire organization. Many of the companies who responded well to the September 11, 2001 terrorist attacks had systems and procedures and plans in place that gave them the visibility and agility they needed to shift resources. Because they anticipated disruptions, they designed their organizations so that they could respond. They used the best available technology to help them see ?supply net exceptions? as they were happening allowing them to sense and interpret, and then decide and act on that information. They also protected critical infrastructure, processes, people, and information. They created redundancy by either physically separating resources to mitigate threats and/or they had procedures in place to quickly accommodate or adapt to events by shifting resources where they were needed.					
<b>15. SUBJECT TERMS</b> United States; Army; Supply; Disaster planning; Redundancy; Supply network; Strategic-Level support					
<b>16. SECURITY CLASSIFICATION OF:</b>		<b>17. LIMITATION OF ABSTRACT</b>	<b>18. NUMBER OF PAGES</b>	<b>19. NAME OF RESPONSIBLE PERSON</b>	
		Same as Report (SAR)	56	Buker, Kathy kathy.buker@us.army.mil	
<b>a. REPORT</b> Unclassified		<b>b. ABSTRACT</b> Unclassified	<b>c. THIS PAGE</b> Unclassified	<b>19b. TELEPHONE NUMBER</b> International Area Code Area Code Telephone Number 913758-3138 DSN 585-3138	
				<small>Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39.18</small>	

**SCHOOL OF ADVANCED MILITARY STUDIES  
MONOGRAPH APPROVAL  
Major Steven S. DeBusk**

Title of Monograph: What Happens When the Supply Chain Breaks?  
Implications for the Army Supply Chain Under Attack

Approved by:

\_\_\_\_\_  
COL Brian F. Waters, MMAS

Monograph Director

\_\_\_\_\_  
Robert H. Berlin, Ph.D.

Professor and Director  
Academic Affairs,  
School of Advanced  
Military Studies

\_\_\_\_\_  
Philip J. Brookes, Ph.D.

Director, Graduate Degree  
Program

## Abstract

WHAT HAPPENS WHEN THE SUPPLY CHAIN BREAKS? IMPLICATIONS FOR THE ARMY SUPPLY CHAIN UNDER ATTACK. by MAJ Steven S. DeBusk, U.S. Army, 52 pages.

The September 11th terrorist attacks on the World Trade Center and the Pentagon created tremendous difficulties for manufacturing and retail industries both inside and outside the United States who prided themselves on their tight supply chain management that supported their “Just in Time” approach to logistics. This monograph analyzes case studies of large business organizations to learn how they used their people, processes, and technologies to learn from, anticipate, or adapt to unexpected disruption in their supply chains.

This monograph attempts to answer the question: How should the Army adapt to sudden supply network change? Unexpected catastrophic have significant implications for the strategic-level support provided by the national economic base to the U.S. Army. In a system of tightly linked supply chains consisting of consumers, retailers, suppliers, and manufacturers, a sudden change in their ability to communicate data or distribute product can have a significant effect on the entire organization. Safety stocks are designed to account for variability in supply and demand but do not always account for low probability, high impact events like fire, earthquakes, blizzards, strikes, and terrorist acts. When disruption hits, there is far less time to react and far fewer options. An unexpected or unplanned anomaly causes a “ripple effect” throughout the entire system.

The term “hardening” is a descriptive term prevalent in supply chain related literature to describe actions taken to minimize vulnerability to the unexpected. This monograph highlights those systematic approaches and institutional mechanisms from commercial industry that can be applied to harden the Army’s supply chain. Because of the sudden shift in security procedures across the United States after September 11th, the paradigm that modern supply chains had operated under suddenly changed. The attacks offer a snapshot that can be examined to determine what when right, what when wrong, and why it happened that way. Analysis reveals that critical supply chain vulnerabilities are most commonly associated with contingency planning, information technology, inventory location and availability, transportation, and assured communication.

Many of the companies who responded well to the September 11<sup>th</sup> attacks had systems and procedures and plans in place that gave them the visibility and agility they needed to shift resources. Because they anticipated disruptions, they designed their organizations so that they could respond. They used the best available technology to help them see “supply net exceptions” as they were happening allowing them to sense and interpret, and then decide and act on that information. They also protected critical infrastructure, processes, people, and information. They created redundancy by either physically separating resources to mitigate threats and/or they had procedures in place to quickly accommodate or adapt to events by shifting resources where they were needed.

The Department of Defense supply chain is arguably one of the most complex in the world. Many of the current and planned DoD supply chain best practices are in line with those used by commercial industry. The vast network of supply chain partners outside the depots in commercial industry may have certain vulnerabilities that by extension are shared by all. What may be missing is the formalization of contingency planning and procedures within the entire supply chain to leverage capabilities that already exist. Ongoing Army and Department of Defense initiatives will increasingly harden the defense supply chain against the unexpected. Perhaps the greatest vulnerability is resistance to change itself that keeps an organization from realizing its vision.

## TABLE OF CONTENTS

TABLE OF CONTENTS .....	iii
Chapter 1: Introduction .....	1
Chapter 2: Supply Chain Evolution and Theory .....	5
Chapter 3: The Army Supply Chain .....	11
Process Changes .....	13
Velocity Management Initiative: The Shift Towards Lean Logistics.....	13
Inventory Management.....	15
Strategic Stock Positioning.....	17
Commercial Prime Vendor.....	17
Business Systems Modernization.....	18
Doctrine .....	19
Vision.....	23
Chapter 4: Analysis of The Threat .....	26
Analytical Framework.....	26
Critical Capabilities .....	27
Critical Requirements .....	28
The Nature of the Threat .....	29
Critical Vulnerabilities .....	34
Contingency Planning.....	36
Information Technology.....	37
Inventory .....	39
Transportation .....	41
Assured Communication .....	45
Critical Vulnerabilities Revisited .....	47
Chapter 5: Conclusion.....	48
Bibliography .....	53
Books .....	53
Government Publications .....	53
Articles .....	54
Reports and Unpublished Works.....	55
Other Resources .....	56

## FIGURES

Figure 1: Generic SCOR Model.....	8
Figure 2: The "Ripple Effect".....	9
Figure 3: Define, Measure, Improve Model.....	15
Figure 4: DoD SCOR Model.....	20
Figure 5: The DoD Supply Chain .....	21
Figure 6: Critical Capabilities .....	28
Figure 7: Critical Requirements.....	29
Figure 8: 1993 Mississippi River Flood.....	31
Figure 9: Terrorism in the United States.....	33
Figure 10: September 11, 2001 "Ripple Effect".....	42
Figure 11: Critical Vulnerabilities.....	47

## Chapter 1: Introduction

*The paradox in creating the future is that you cannot predict the future. Success will come from being able to accommodate the unexpected, exploiting opportunity, and working through setbacks. A leader must build flexibility and resilience into the organization, conditioning it not to be surprised so that, when the unexpected occurs, response is prompt, action is deliberate, and the organization stays on course. The organization that is successful is the one that can best deal with surprise.<sup>1</sup>*

Gordon R. Sullivan, CSA (Ret), *Hope Is Not A Method*

As the emotional shock of the terrorist attacks on September 11, 2001 began to set in, a ripple effect occurred out from New York City that would eventually be felt around the world. Almost immediately, air travel within the borders of the United States shut down and would not resume fully for several weeks. Cross border traffic from Canada and Mexico came to a screeching halt as new security measures were put in place. Thousands of shipping containers at ports around the country immediately became suspicious and were delayed until they could be inspected. The circumstances brought on by the September 11th terrorist attack created tremendous difficulties for manufacturing and retail industries both inside and outside the United States who prided themselves on their tight supply chain management that supported their “Just in Time” approach to logistics.

This monograph will answer the question: How should the Army adapt to sudden supply network change? An event like the one described above could have significant implications for the strategic-level support provided by the national economic base to the U.S. Army. It could also yield important lessons for how the Army should be postured to

---

<sup>1</sup> Michael Harper and Gordon Sullivan, *Hope is Not a Method* (New York: Broadway Books, 1996), 231.

anticipate, survive, and respond to unexpected catastrophe be it manmade or natural to ensure uninterrupted logistics support.

James R. Beniger describes the methodical progression of the “Control Revolution” and resulting “information society” as it grew to fill the need to keep up with an increased ability to produce and distribute goods and services. He says a “Crisis of Control” exists when output of manufactured goods, services, and distribution methods exceed the ability to control them efficiently. The crisis that brought on the need for greater supply chain management was purely economic. Large organizations relying on a complex system of suppliers, distributors, and end users were susceptible to maintaining large expensive inventories to consistently meet demand. As competition for market share grew, these inventories had to be brought under control to limit expenses. The aim of supply chain management is to bring these separate systems into harmony through the use of advanced information technology and processes. Can information technology keep a supply chain from being disrupted once an unexpected catastrophic event occurs? The real “crisis of control” for Army logistics in the future may not be the control of large inventories but one of controlling an inventory in motion when sudden changes in distribution capability occur.

Peter M. Senge highlights “systems thinking” as an essential discipline in a “learning organization”. He says, “systems thinking is a conceptual framework, a body of knowledge and tools that have been developed over the past fifty years, to make patterns clearer, and help us to change them effectively.”<sup>2</sup> The Army logistics system is complex and could be described as a system of systems linking hundreds of customer

---

<sup>2</sup> Peter M. Senge, *The Fifth Discipline* (New York: Doubleday, 1990), 7.

units with installation supply support activities and regional depots. These depots, in turn, are linked through a complex distribution system of air, sea, rail, and road networks to suppliers. The suppliers similarly are linked to the manufacturers of component parts or raw materials. A complex web of people, processes, and technologies are used to exchange information between U.S. Army units, Materiel Management Centers, Army Materiel Command, The Defense Logistics Agency, Military Traffic Management Command, and civilian suppliers. In a system of tightly linked supply chains, a sudden change in their ability to communicate data or distribute can have a significant effect on the entire organization.

Current Army doctrine describes combat service support (CSS) reach operations as the operational positioning and efficient use of all available CSS assets and capabilities, from the industrial base to the soldier in the field.<sup>3</sup> Since the Army's institution of the Velocity Management Initiative beginning in 1995, significant reductions have been made with regard to the amount of stocks kept on hand at supply depots in the United States and overseas. Current Army doctrine also supports the use of advanced technology to provide rapid throughput and reduce the CSS footprint. Joint Vision 2020's principle of "focused logistics" will support the Army's ability to deliver the right supplies, at the right place, at the right time. Some argue that as the Army's supply chain tightens and becomes more efficient, it will lose robustness and the agility it needs to respond to the unexpected. While much has been published on disaster preparedness in general, little has been published on how a disaster or unexpected crisis affects a supply chain or how those lessons might be applied. This paper will examine

---

<sup>3</sup> Department of the Army, *FM 3-0, Operations* (Washington D.C.:Government Printing Office, 2001), 12-2.

how a tight supply chain or “lean logistics” can be affected by a catastrophic event. Additionally, it will recommend actions that the Army can take to “harden” its supply chain and minimize the impact.

Dietrich Dorner, Eliot A. Cohen, and John Gooch’s analysis of failure and military misfortune provide several useful insights into how to analyze this problem. Dorner recognizes the tendency of organizations to “economize” analysis of complex problems and omit analysis of undesired second and third order effects. It is possible that the Army’s approach to Supply Chain Management is looking through a misdirected telescope. In its quest for speed and reduction of on-hand stocks (and funds to pay for them), the Army may be neglecting the consequences of sudden change to its supply chain. Dorner says, “In solving problems that involve complex dynamic realities...we must think about problems we may not have at the moment but that may emerge as side effects of our actions.”<sup>4</sup> Cohen and Gooch illustrate that most military misfortunes occur because of a failure to learn, failure to anticipate, failure to adapt, or a combination of all of these.<sup>5</sup> This monograph will analyze case studies of large business organizations to learn how they used their people, processes, and technologies to learn from, anticipate, or adapt to unexpected disruption in their supply chains. This analysis will help to identify possible impacts to the Army logistics system and make recommendations on how to respond to sudden change.

---

<sup>4</sup> Dietrich Dorner, *The Logic Of Failure* (New York: Metropolitan Books, 1996), 190.

<sup>5</sup> Eliot A. Cohen and John Gooch, *Military Misfortune* (New York: The Free Press, 1990), 231-246.

## Chapter 2: Supply Chain Evolution and Theory

The term “Supply Chain” and “Supply Chain Management” trace their beginnings to the early eighties but did not become a regular part of commercial industry lexicon until the 1990s. These concepts had their beginnings in the 1960s with a renewed study of Systems Theory first proposed by Ludwig von Bertalanffy in the 1940s. His theory emphasizes the interactions and interrelationships of the different components of a system.<sup>6</sup>

Before World War II manufacturers drove the pace at which goods reached consumers. They controlled production, marketing and distribution of their products. Vendors or retailers were just an extension of the manufacturer’s distribution channel. In the post World War II era, new advertising media gave new importance to brand recognition. Distribution and logistics, viewed as separate supporting elements, took a back seat to product development, marketing, and brand management.

In the 70s and 80s’ several changes occurred that would bring new importance to an integrated approach to business. A surging U.S. economy created an “Empowered Consumer” with new demands and new expectations.<sup>7</sup> By the late 1980s these consumers had access to information from the internet and other media that enabled them to compare prices and obtain products from several retailers or get delivery direct from a manufacturer. Not only did the number of sources increase, but their expectations of

---

<sup>6</sup> Ludwig von Bertalanffy, *General System Theory* (New York: Penguin University Press, 1975) discussed in Shimon Naveh, *In Pursuit of Military Excellence: Evolution in Operational Theory* (London, Frank Cass & Co., 1997), 3-4.

<sup>7</sup> John J. Coyle and others, *The Management of Business Logistics: A Supply Chain Perspective* (Mason, OH; Thomas Learning, 2003), 3.

quality and quick delivery increased. Another change was the growth of “big box” retailers like Wal-Mart, K-mart, and Home Depot who were able to gain tremendous market share from smaller retailers. In 1967 Wal-Mart reported \$12.6 million in sales, by 1997 sales had increased to \$100 billion.<sup>8</sup> Today Wal-Mart ranks as number 1 on the Fortune 500 list of the top 500 companies in the U.S. with revenues of over \$2.2 billion.<sup>9</sup> These changes shifted control of markets away from manufacturers to retailers and consumers. As competition for market share between retailers increased, profit margins shrank. In order to meet customer’s expectations of lower prices, retailers placed new emphasis on gaining efficiencies in the distribution systems that connected them with their manufacturers. By shrinking their backroom inventories they could save capital. In order to consistently meet demand, however, the distribution system itself had to become cheaper, more efficient, and more reliable. In the past, manufacturers used either a “push” or a “pull” system to accommodate a retailer’s demand. Push systems replenish supply by forecasting future demand, pull systems replenish based on actual demand experienced. Either system was inherently inefficient because it resulted in excess or shortage inventories to the manufacturer or retailer when supply exceeded or failed to meet demand. In order to overcome this inefficiency, both entities had to view themselves as collaborative partners operating in a common system rather than as competing adversaries.

The situation described above illustrates the interdependent relationships in a system consisting of consumers, retailers, suppliers, and manufacturers. In reality, this

---

<sup>8</sup> Walmart website; available from <http://www.walmartstores.com/wmstore/wmstores/HomePage.jsp>; Internet; accessed on 30 November 2002.

<sup>9</sup> Fortune magazine website; available from <http://www.fortune.com/lists/F500/index.html>; Internet; accessed on 30 November 2002.

interdependency extends far beyond the manufacturers to his sources of raw materials and labor. In effect it describes a complex “system of systems” that must perform efficiently and reliably if it is to provide maximum benefit to each entity. Taken together, this system is described as an “enterprise” or a group of strategically aligned companies focused on new market opportunities.

In 1996 several commercial industry leaders formed the Supply Chain Council (SCC) to provide a common supply-chain framework, standard terminology, common metrics with associated benchmarks, and best practices. They describe a supply chain as those actions “encompassing every effort involved in producing and delivering a final product or service, from the supplier's supplier to the customer's customer”. Supply Chain Management includes managing supply and demand, sourcing raw materials and parts, manufacturing and assembly, warehousing and inventory tracking, order entry and order management, distribution across all channels, and delivery to the customer.<sup>10</sup>

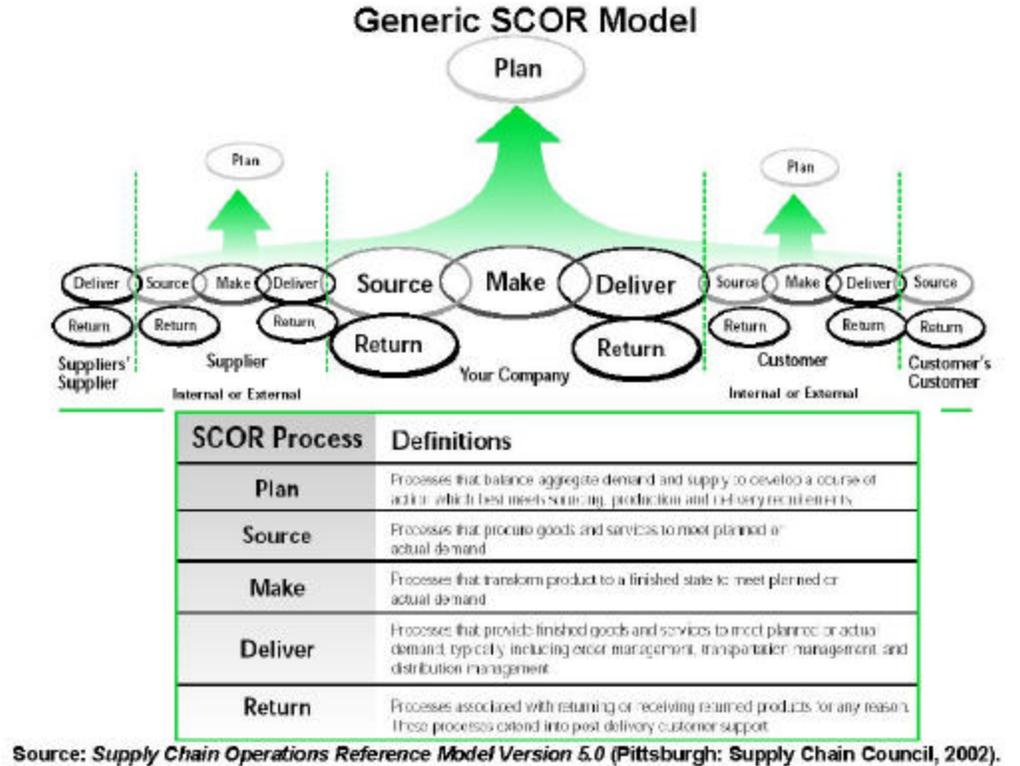
The Supply Chain Council has developed a Supply Chain Operations Reference-model (SCOR). This model is the cross-industry standard for supply chain management. The SCOR-model has been developed to describe the business activities associated with all phases of satisfying a customer's demand. The Model itself contains several sections and is organized around the four primary management processes of Plan, Source, Make, and Deliver. By describing supply chains using these process building blocks, the Model can be used to describe supply chains that are very simple or very complex using a common set of definitions.<sup>11</sup> Figure 1 illustrates how each process is interconnected and

---

<sup>10</sup> Anonymous, *Supply-Chain Operations Reference Model: Overview Version 5.0* (Pittsburgh: Supply Chain Council, 2002); available from <http://www.supply-chain.org/default.htm>; Internet; accessed on 2 December 2002.

<sup>11</sup> Ibid.

interdependent. Integrated planning occurs at all levels and helps to eliminate friction and allow for smooth efficient flow of product.

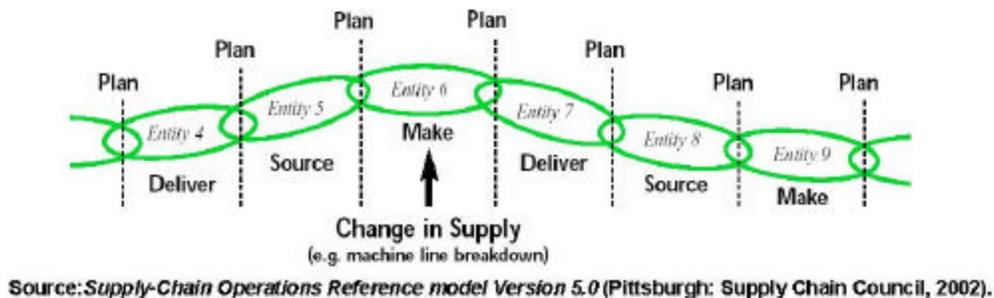


**Figure 1: Generic SCOR Model**

The gradual shift from “vertical” supply chains characterized by complete, in-house management of the end-to-end supply chain to a “leaner” horizontal supply chain characterized by dependent cooperative control was not without risk. Highly volatile market demands and decreasing product cycles made manufacturers far more dependent on timely, reliable deliveries of supplies. The pressure to increase cash flow and reduce inventory significantly reduced or eliminated safety stocks. Safety stocks are designed to account for variability in supply and demand but do not always account for low probability, high impact events like fire, earthquakes, blizzards, strikes, and terrorist acts.

Therefore, when disruption hits, there is far less time to react and far fewer options.<sup>12</sup>

An unexpected or unplanned anomaly causes a “ripple effect” throughout the entire system.



**Figure 2: The "Ripple Effect"**

Navi Radjou of Forrester Research calls these anomalies “supply net exceptions” which he defines as “the lack of a rule-based resolution to the difference between the expectation and result of a supply chain process step.”<sup>13</sup> In simple terms, supply net exceptions are any unexpected event that disrupts the smooth efficient operation of the supply chain. Radjou believes that the non-linear effects of supply net exceptions has amplified over the past decade because of a trend in increased reliance on outsourcing and partnering that has heightened interdependency among different nodes of global supply networks. Net exceptions cause short-term financial impacts because of a failure to balance supply and demand. Manufacturers over-react and increase inventory to meet demand that isn’t there or they fail to fulfill demand and lose profit opportunities. They also tend to necessitate high cost corrective measures because manufacturers lack a systematic approach or institutionalized mechanism to deal with them.

<sup>12</sup> Andre Kuper, “Hardening Vulnerable Links in the Supply Chain,” *Total Supply Chain*, February 2002; available from <http://www.totalsupplychain.com>; Internet; accessed on 20 January 2003.

<sup>13</sup> Navi Radjou and others, *Adapting to Supply Network Change* (Cambridge: Forrester Research, 2002), 2.

The term “hardening” is a descriptive term prevalent in supply chain related literature to describe actions taken to minimize vulnerability to the unexpected. This monograph seeks to highlight those systematic approaches and institutional mechanisms from commercial industry that can be applied to harden the Army’s supply chain.

## Chapter 3: The Army Supply Chain

*Without a transformation in logistics, there will be no transformation in the Army.*<sup>14</sup>

Gen. Eric Shinseki, Army Chief of Staff

*Our ability to adapt to changing conditions and adopt relevant technologies, concepts, and business practices will make us more efficient, more capable, and more responsive to the warfighter's requirements. Logistics is not just a combat multiplier. Rather, it is an absolute war-stopper, a critical part of the Army's muscle. As we transform we must flex our logistics muscle and continue to strengthen it.*<sup>15</sup>

Gen. John G. Coburn, Commander, Army Materiel Command

The post-Desert Storm Army began to experience a major paradigm shift in how it thought about logistics. Prior to and during Desert Storm the Army relied upon a supply-based system designed to support the Cold War force structure. Many have described the Army's logistic management philosophy as an "iron mountain" or "just in case" approach. The Army supported its mission by buying products to meet strict specifications as they were needed. Stocks were received from vendors and maintained in multiple depots at wholesale and retail levels. In 1992 the Department of Defense (DoD) had over \$150 billion in inventory, of which the Army Logistics system had \$40 billion, and one-third of that was in spare parts.<sup>16</sup> In spite of the large investment in repair parts inventories, the supply system was unresponsive to customers' needs.

---

<sup>14</sup> Quoted in Katherine Peters, "Army Chief Says Logistics Reform Is Vital," *Government Executive Magazine*, (4 September 2002).

<sup>15</sup> John Coburn, "Logistics: Flexing Muscle for Army Transformation," *Army Magazine*, (May 2001) 25.

<sup>16</sup> John Dumond and others, *Velocity Management: An Approach for Improving the Responsiveness and Efficiency of Army Logistics Processes* (Santa Monica: RAND, 1994) 2.

Repairs at depots took from three weeks to nine months to complete and requests for repair parts took several days to weeks to reach the source of supply.<sup>17</sup> It became clear that the Army logistics system was far behind what could be expected from industry leaders using commercial best practices. Alarming, based on their experiences during Operations Just Cause, Desert Storm, and Restore Hope, many commanders began to question the reliability of the Army logistics system. John Dumond, director of RAND Arroyo Center's Military Logistics Program said, "These problems persisted despite repeated efforts to remedy them. For this reason, successfully reforming the Army logistics system, much less achieving the transformation that many called for, required a fundamental shift in approach to how the Army thought about logistics and how it thought about change."<sup>18</sup>

In their best-selling book, *Hope is Not a Method*, former Chief of Staff of the Army Gordon Sullivan and Col. (Ret.) Michael Harper discuss how to lead change in an organization based on their experiences with post-Desert Storm Army transformation. They say, "only by clarifying, changing, and growing its critical processes can an organization make fundamental and enduring change."<sup>19</sup> Those critical processes are driven and defined by doctrine representing the "collective understanding of how the Army will fight and conduct operations."<sup>20</sup> Vision is the catalyst for changing doctrine and processes by providing a "sense of the future...an imagined possibility, stretching beyond today's capability, providing an intellectual bridge from today to tomorrow, and

---

<sup>17</sup> Ibid., 3.

<sup>18</sup> John Dumond and others, *Velocity Management: The Business Paradigm That Has Transformed U.S. Army Logistics* (Santa Monica: RAND, 2001) iii.

<sup>19</sup> Harper and Sullivan, *Hope is Not a Method*, 231.

<sup>20</sup> Ibid., 10.

forming a basis for looking ahead, not for affirming the past or status quo.”<sup>21</sup> Below, some of the key process changes, doctrine, and vision that have guided the Army’s current concept of supply chain management are discussed.

## **Process Changes**

### **Velocity Management Initiative: The Shift Towards Lean Logistics**

In 1995, the Army formalized a relationship with RAND’s Arroyo Center that began in the late 1980s by establishing the Velocity Management Initiative. The goal of Velocity Management is to provide the Army with a tailored logistics system that performs as well as a first class commercial supply chain. Velocity Management seeks to replace the Army’s traditional reliance on mass with the modern business concept of high velocity processes tailored to meet evolving customer needs. For the first time, the Army began to view its logistics system as a supply chain of inter-linked processes between suppliers and customers. In order to institute lasting change, senior level logisticians from across the Army and DoD formed the “Velocity Group” (VG) to provide guidance and vision for a program that would cut across several organizations and many different levels. The Velocity Group is co-chaired by the Deputy Chief of Staff, G-4 (DCS, G-4), the Deputy Commanding General of Army Materiel Command (AMC), and the Commanding General of the Combined Arms Support Command (CASCOM). The Velocity Management Vision is to “define, measure, and improve the Army’s logistics processes to and from other services and defense agencies to enhance readiness through the rapid adoption of new business processes so our soldiers know what right looks like

---

<sup>21</sup> Ibid., 79.

and act on that knowledge.”<sup>22</sup> The Velocity Group defined its mission as “investigating, reporting, and where possible implementing Army logistics best business practices focusing on joint logistics to maximize end-to end distribution and repair cycle from national level through the last tactical mile consistent with approved logistics transformation initiatives.”<sup>23</sup>

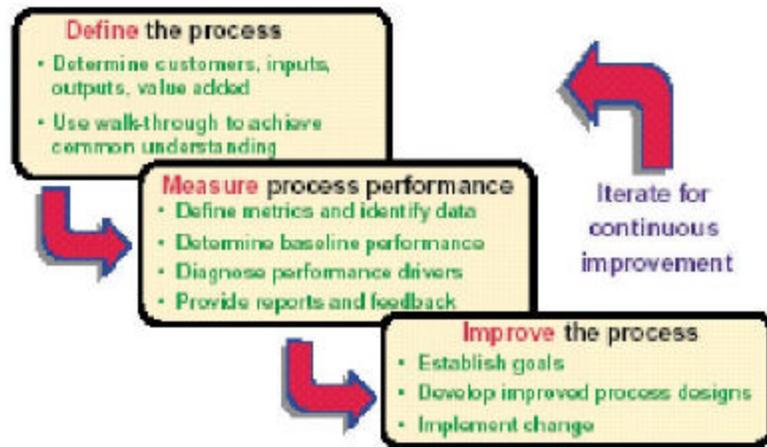
Several teams were organized to drive changes to meet the VM vision. Each installation formed Site Improvement Teams (SITs) comprised of local leaders and technical experts for supply, maintenance, distribution and finance that survey, analyze, and redesign logistic processes at installation or MACOM level. A key enabler in the Velocity Management Program is that local leaders are empowered to implement new procedures identified by SITs on the spot to take advantage of “low hanging fruit”. Process Improvement Teams (PITs) were formed as directed by the VG Board of Directors to focus on broad logistics processes that crossed the functional organizational structure of the Army. PIT Technical experts from various DoD organizations studied logistic processes and identified systemic problems and developed improvement proposals and recommendations for technical implementation of the changes. Currently PITs exist that focus on the distribution process and the repair cycle process, however, new PITs can be formed and dissolved as needed. VG members can appoint “change agents”, usually general officer level equivalents, to act on their behalf while interacting with PITs and SITs to provide feedback and advice.

---

<sup>22</sup> Velocity Management Transformation Brief dated 17 Sep 02; available from <http://www.cascom.army.mil/vm>; Internet; accessed on 14 November 2002.

<sup>23</sup> Ibid.

Taking a cue from successful companies like Toyota, Motorola, and Penske, Velocity Management leaders adopted a “Define, Measure, Improve (DMI)”



Source: Mark Wang, *Accelerated Logistics* (Santa Monica: Rand, 2000), 11.

Figure 3: Define, Measure, Improve Model

methodology to identify and eliminate non-value adding steps in logistic processes and implement changes where needed.<sup>24</sup> By defining “process flows”, establishing metrics to measure performance, and implementing changes to improve a process, SITs and PITs were able to meet or exceed goals established by the VG. The D-M-I methodology is the Army’s version of a commercial change management approach that leads to continuous improvement. Using this methodology, VM has yielded several initiatives that work to save money, improve readiness, shorten customer wait time, and indirectly harden the Army supply chain.

### Inventory Management

Dollar cost banding is a process improvement resulting from the velocity management initiative designed to optimize what the Army stocks for its customers and

<sup>24</sup> Dumond and others, *Velocity Management: The Business Paradigm That Has Transformed U.S. Army Logistics*, 7-12.

where that stock is located. Before dollar cost banding, a supply support activity (SSA) on an Army installation used a “one size fits all” approach to inventory management. By regulation any given item needed nine demands per year to be added to an SSA’s inventory and three demands thereafter to be retained. No consideration was given to the item’s cost, size, or importance to readiness. As a result, equipment that needed repair often was delayed for lengthy periods waiting for inexpensive parts to arrive. Commercial developments in inventory management suggested that better performance could be achieved. Dollar cost banding used an algorithm developed by the RAND Corporation that took into account an item’s criticality, mobility requirements, density and dollar value to create an inventory better designed for the customers it supported.<sup>25</sup> A small inexpensive but critical item could be stocked locally with less demands while bulky more expensive items tended to migrate toward depots further up the supply chain. Dollar cost banding resulted in an increase in readiness because more items were likely to be stocked locally and, because less items were moving in the supply chain, wait time for parts that weren’t in stock decreased. The Army supply chain was becoming leaner and more responsive. A 1994 RAND study points out that the shift from “mass” to “velocity” was not without critics. Many argued that an ideal logistics system would provide both mass and responsiveness. This argument, however, overlooks the fact that responsiveness reduces the need for massive resources while massive resources can slow responsiveness by choking logistics processes.<sup>26</sup>

---

<sup>25</sup> RAND, Research Brief: “Improved Inventory Policy Contributes to Equipment Readiness,” (2001); available from <http://www.rand.org/publications/RB/RB3026/>; Internet; accessed on 27 November 2002.

<sup>26</sup> Dumond and others, *Velocity Management: An Approach for Improving the Responsiveness and Efficiency of Army Logistics Processes*, 3.

## Strategic Stock Positioning

Velocity management was one of many initiatives that have shaped the Army supply chain into what it is today. Much of the supply chain, however, resides outside the confines of service responsibility with other DoD agencies and commercial industry. At the heart of the Army supply chain is the Defense Logistics Agency (DLA) who handle about \$14 billion in sales each year to 17,000 military customer units.<sup>27</sup> DLA and to a lesser extent Army Materiel Command are largely responsible for the procurement and distribution of supplies from regional depots to the SSAs that supply Army units. DLA provides approximately 90 percent of all Army supplies. Beginning in 1997, DLA began to take steps to restructure its distribution depot system. The effort began as a response to a shrinking force structure but also sought to streamline processes, eliminate duplication, reduce overhead costs, and create a more efficient organization. Today DLA operates the Defense Distribution Center at New Cumberland, Pennsylvania that serves 22 distribution depots across the country and in Europe, Hawaii, and Japan. These depots stock over 3.9 million different items and process over 24 million transactions a day. Depots either function in a global support role for general commodities or regional support for local customers. The number of depots in the future is likely to decrease as DLA reduces its stock of low demand items and private industry begins to compete for previously public supply functions under DoD's Strategic Sourcing Program.<sup>28</sup>

## Commercial Prime Vendor

DLA plans to leverage commercial industry by increasing its direct vendor

---

<sup>27</sup> Ellen Messmer, "Defense Logistics Agency on slow march to supply chain modernization," *Network World Fusion*, (7 August 2002); available from <http://www.nwfusion.com>; Internet; accessed on 27 November 2002.

<sup>28</sup> For more information of strategic sourcing see <http://www.dla.mil/j-8/a-76/osdigmstrategic sourcing.html>.

delivery program where supplies bypass depots and are delivered directly from the supplier to the customer.<sup>29</sup> LTG Henry T. Glisson, then Commander of DLA said “prime vendor business arrangements enable us to contract with one full-service distributor of commercial products rather than with hundreds of individual vendors. The prime vendor, under a long-term contract, provides all material in a product line or commodity to a major customer or regional customers on a just-in-time basis. Prime vendor contracting is a win-win situation because it eliminates the middle bureaucracy and puts customers directly in touch with vendors.”<sup>30</sup>

### Business Systems Modernization

In July 2002, in what might represent DLA’s most aggressive shift towards adoption of commercial business practices, DLA implemented its business systems modernization program (BSM). BSM is a DoD-wide effort to replace current legacy software systems with modern commercial off-the- shelf software (COTS). The \$500 million program will phase in COTS for supply chain management through fiscal year 2005. BSM is a key initiative to streamline the DoD supply chain and re-engineer logistics processes to reflect best commercial business practices. BSM includes enterprise resource planning (ERP) software from SAP America, advance planning and scheduling software from Manugistics, and procurement desktop-defense from American Management Systems.<sup>31</sup> This software will replace Standard Automated Materiel Management Systems (SAMMS) and the Defense Integrated Subsistence Management

---

<sup>29</sup> Defense Logistics Agency, *Defense Logistics Agency Strategic Plan 2002-2007*, (Washington D.C.: Government Printing Office, 2002).

<sup>30</sup> Henry Glisson, “Revolution in Military Logistics: Improving Support to the Warfighter,” *Army Logistician* (Jan/Feb 1999), 9.

<sup>31</sup> DLA press release, “DLA Fields First Release of Modernized System,” (6 August 2002); available from <http://www.dla.mil>; Internet; accessed on 12 February 2003.

System (DISMS), both COBOL based mainframe applications. These legacy systems were developed by the Government to meet defense specific needs over 30 years ago and are not able to keep pace with advances in the commercial marketplace. One advantage of the new systems is that they can more easily exchange data with other application allowing greater collaboration. Dave Falvey, DLA's program executive officer says, 'the homegrown systems weren't integrated and able to share data related to procurement, order management, and financials.'<sup>32</sup> Another advantage is that many new applications will be web-based allowing greater access for customers, suppliers, and decision makers. BSM is only in the beginning stages at present but promises to not only change DoD's logistics information technology architecture but will also streamline and eliminate many of the processes and human resources that supported the old system.

## **Doctrine**

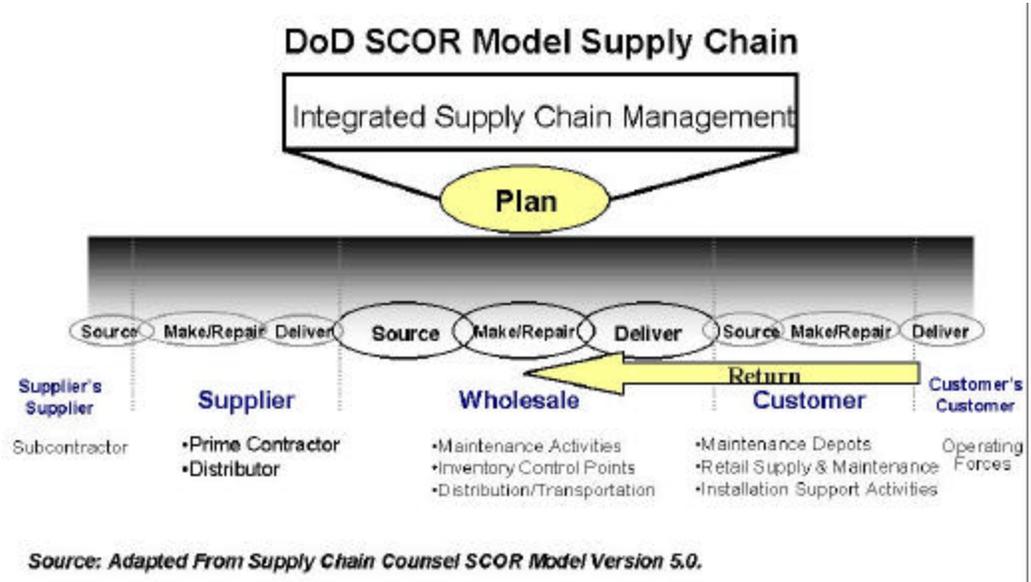
In 2000, DoD established the Supply Chain Integration office with Secretariat level leadership to facilitate DoD Component implementation of supply chain management practices. They also will identify business process changes that can be enabled or strengthened through the implementation of e-business capabilities. They will develop modern supply chain policies in DoD to develop and maintain end-to-end distribution capabilities required to meet 21st century deployment and sustainment requirements. Additionally, they establish policy regarding materiel management and supply distribution, including supply depot operations, storage and issue processing, inventory control, physical inventories, and security.<sup>33</sup> With the publication of DoD

---

<sup>32</sup> Messmer, "Defense Logistics Agency on slow march to supply chain modernization."

<sup>33</sup> Office of the Under Secretary of Defense (Logistics), Supply Chain Integration website; available from <http://www.acq.osd.mil>; Internet; accessed on 23 November 2002.

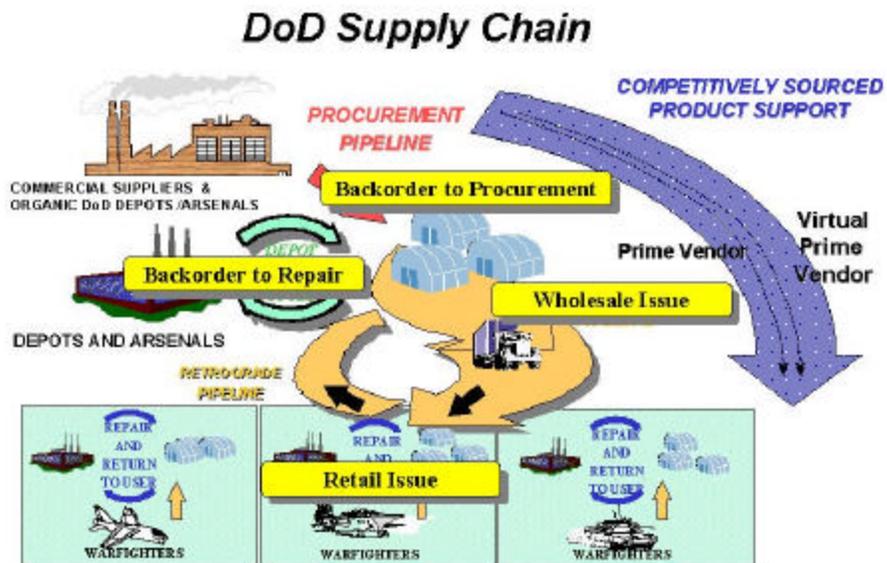
Regulation 4140.1-R in September 2002, the Department of Defense adopted the Supply Chain Operations Reference model as a framework for developing, improving, and conducting materiel management activities.<sup>34</sup> The commercial version of the SCOR model has evolved into an analytical tool for Supply Chain Management for the Defense community. The Model shown in figure 4 reflects terminology aligned with the OSD-defined SCOR model for Defense represented by the Plan, Source, Make/Repair, Deliver,



**Figure 4: DoD SCOR Model**

and Reutilize/Dispose arrows. While most supply chains end with delivery to the customer, this model reflects the unique activities in Department of Defense materiel management that follow certain pieces of equipment throughout their entire lifecycle.

<sup>34</sup> Department of Defense, DoD 4140.1-R, *Supply Chain Materiel Management Regulation*, (Washington: Government Printing Office, 2002), 3.



Source: Army Supply Chain Management Integration Office briefing dated 15 May 2001.

**Figure 5: The DoD Supply Chain**

Like DoD, the Army formed its own Supply Chain Integration Management office under the Deputy Chief of Staff, G-4. Their goal is to achieve a service level that is comparable to a world-class commercial firm. They coordinate closely with the supply chain management (SCM) teams of national providers, Army agencies and other services to optimize the SCM at all levels. They also provide oversight of the Army's Velocity Management (VM) Team, which provides field SCM. They integrate policies, best business practices, and Logistics Information System (LIS) changes into appropriate regulations or pamphlets and provide commanders the necessary tools to identify problem areas through the use of performance based metrics and reports.<sup>35</sup> Their efforts will institutionalize SCM and VM concepts.

<sup>35</sup> Supply Chain Integration Management Office briefing dated 15 May 2002.

The Deputy Chief of Staff, G-4 introduced the Army Supply Chain Management Program with the publication of Army Regulation 711-1. This regulation established Army policies and responsibilities for Supply Chain Management and described the principles that guide it. The Army defines a supply chain as “The material and informational interchanges in the logistical process stretching from the acquisition of raw materials to delivery of finished products to the end user. All vendors, service providers and customers are links in the supply chain.”<sup>36</sup> This definition places emphasis on the fact that a large portion of the military supply chain is found in the commercial sector, especially in the manufacturing and distribution functions.

The Army defines supply chain management as “The management of all internal and external logistics processes, information and functions necessary to satisfy a customer’s requirement. It’s the management of the interdependent logistics processes of customer response, inventory planning and management, warehouse management, transportation, supply, maintenance and reverse logistics.”<sup>37</sup> The Army supply chain management program’s goal is to optimize the Army supply chain for prompt, effective, and efficient support to the customer by identifying, isolating and eliminating non-value adding processes. The Army supply chain management regulation places particular emphasis on structuring logistics procedures and systems to provide an agile response during crises and military operations, collaboration with all elements in the supply chain by sharing information, and making maximum, effective use of competitive, global commercial capabilities.<sup>38</sup>

---

<sup>36</sup> Department of the Army, AR 711-1 *Supply Chain Management*, (Washington: Government Printing Office, 2002), GL-9.

<sup>37</sup> Ibid.

<sup>38</sup> Ibid, 1-3 to 1-5.

## Vision

Several documents provide the vision for Army leaders as they implement supply chain management concepts in support of Army transformation. In Joint Vision 2020, four operational concepts are outlined that include, dominant maneuver, precision engagement, focused logistics, and full dimensional protection. Focused logistics as described in JV 2020 is “the ability to provide the joint force the right personnel, equipment, and supplies in the right place, at the right time, and in the right quantity, across the full range of military operations. This will be made possible through a real-time, web-based information system providing total asset visibility as part of a common relevant operational picture, effectively linking the operator and logistician across Services and support agencies. Through transformational innovations to organizations and processes, focused logistics will provide the joint warfighter with support for all functions.”<sup>39</sup> The DoD Logistics Strategic Plan guides component implementation strategies to meet its objectives. The future end-state characteristics outlined in the plan are establishment of an integrated supply chain, adopting streamlined business processes, using “best value” products and services, supporting joint warfighting, incorporating commercial business practices without losing sight of core functions, and providing access to information by establishing an integrated data environment.<sup>40</sup>

The Army Vision guides logistics transformation that will support capabilities required in the 21<sup>st</sup> Century. This force will be responsive, deployable, agile, lethal,

---

<sup>39</sup> Department of Defense, Joint Chiefs of Staff, *Joint Vision 2020* (Washington D.C.: Government Printing Office, 2000), 24.

<sup>40</sup> Department of Defense, Deputy Under Secretary of Defense for Logistics, *FY2000 Logistics Strategic Plan* (Washington D.C.: Government Printing Office, 1999).

survivable, and sustainable.<sup>41</sup> The *Objective Force 2015 White Paper* outlines the key transformation concepts that will guide Army Transformation efforts to the year 2015. It says that sustainment is characterized by a “Joint Logistics Corporate Enterprise (JLCE) comprised of a seamless architecture from the strategic to the tactical level.”<sup>42</sup> Logistics will be distribution based, fusing supply, transportation, and information functions to speed delivery and reduce the footprint on the ground. Industry is linked with the Army and all other organizations in the supply chain with automated systems that enhance flexibility and agility to support the full spectrum of operations. The Army’s fundamental logistics concepts for the Objective Force are velocity over mass, centralized management, direct delivery, minimum essential stocks, two-way flow of resources, and time definite delivery.

Current Army logistics transformation efforts have already started to realize some of the concepts laid out in DoD and Army visionary documents. Between 1990 and 2000 the Army reduced its stocks by 51 percent. The time it takes to get repair parts to soldiers has been cut by more than 50 percent. CONUS bases have an average order-of-ship time of just 8 days and OCONUS bases average 14. Today 99 percent of Army inventory is visible and can be tracked as it moves through the supply chain.<sup>43</sup> The Army supply chain today can be characterized as a highly automated inventory in motion, much leaner and faster than the Desert Storm era supply chain. Today’s Army supply chain looks much more like commercial industry; minimized inventory, reliant on assured high-speed communication, commercial transportation, and direct delivery from manufacturer to the

---

<sup>41</sup> Department of the Army, *The Army Vision*, (Washington D.C.: Government Printing Office, 1999).

<sup>42</sup> Department of the Army, *Objective Force 2015 White Paper* (Washington D.C.: Government Printing Office, 2002).

<sup>43</sup> Department of Defense, *FY2000 Logistics Strategic Plan*, 3-4.

point of need. The Army supply chain must have the agility to operate lean while maintaining the resiliency and responsiveness to support forces during contingency operations for extended periods of time.

This chapter has outlined the evolution of the Army supply chain and detailed some of the initiatives that drove this process. If the Army supply chain is becoming more and more like the commercial sector, it will be susceptible to the same vulnerabilities that they have experienced during unexpected crisis situations. The next chapter will attempt to describe and categorize these vulnerabilities to guide Army efforts in hardening its supply chain.

## Chapter 4: Analysis of The Threat

*"No theory, no matter what the field, survives in its original form, and business operating philosophies are no exception. Real world testing either forces a discarding or a tweaking. Just-in time seems to fall into the latter category."<sup>44</sup>*

Bill Virgin, Seattle Post-Intelligencer

### Analytical Framework

Joint planning doctrine provides a methodology for translating national and theater strategy into planning actions required to design and synchronize a campaign plan. One of these actions requires that planners identify critical factors with respect to the enemy and himself. Properly identifying these critical factors allows one insight into the key sources of strength and vulnerability from which an adversary gains his power. This process is commonly known as "center of gravity analysis". Joint doctrine defines a center of gravity as "those capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight."<sup>45</sup> Once properly identified, center(s) of gravity can be attacked indirectly or directly to achieve the desired endstate established by the commander for the campaign. Likewise, analysis of a "friendly" center of gravity can identify those key capabilities that must be protected in order to retain freedom of action. In the mid-1990s Dr. Joe Strange of the Marine Corps War College built on the concept of center of gravity by advocating the use of the terms critical capabilities and critical requirements to link the center of gravity with its associated vulnerabilities. Current Joint doctrine has embraced these concepts as part of

---

<sup>44</sup> Bill Virgin, "Port Shutdown shows just-in-time may be past its prime," *Seattle Post Intelligencer*, 10 October 2002.

<sup>45</sup> Department of Defense, JP 5-00.1 *Joint Doctrine for Campaign Planning*, (Washington D.C.: Government Printing Office, 2002), II-6.

an accepted methodology. It defines critical capabilities as those adversary capabilities that are considered crucial enablers for the adversary's center of gravity to function as such and are essential to the accomplishment of the adversary's assumed objectives."<sup>46</sup> It defines critical requirements as "those essential conditions, resources, and means for a critical capability to be fully operational" and critical vulnerabilities as "those aspects or components of the adversary's critical capabilities which are deficient or vulnerable to neutralization, interdiction, or attack in a manner achieving decisive or significant results disproportionate to the military resources applied."<sup>47</sup> While the center of gravity concept was designed to assist in the planning of military campaigns or major operations it offers a useful analytical tool to identify what vulnerabilities may exist with respect to a supply chain whether it be commercial or military. This analysis assumes that the Army supply chain, because it has significant commercial elements, is vulnerable in a similar manner to what historical commercial industry experiences will show. Once identified, action can be taken to mitigate these vulnerabilities and "harden" the Army supply chain.

### **Critical Capabilities**

As noted earlier, the Department of Defense has adopted the Supply Chain Council's Supply Chain Operations Reference Model (SCOR) to describe the key management processes that are part of any supply chain. These processes (plan, source, make, deliver, and return) are critical capabilities that a supply chain must retain in order to function. Figure 6 shows how the supply chain management logistics processes

---

<sup>46</sup> Ibid, II-7.

<sup>47</sup> Ibid.

outlined in Army Regulation 711-1 support this model, however, they are not as inclusive in all respects. In particular, the SCOR model considers planning a continuous aspect of all other processes while the Army planning process outlined in AR 711-1 only considers inventory planning. For this analysis, the SCOR processes are sufficiently broad and well defined to serve as the critical capabilities from which critical requirements can be derived.

<b>Critical Capability (SCOR)</b>	<b>Critical Process (AR 711-1)</b>
<b>Plan:</b> Demand/Supply planning and management (includes management of performance, data collection, inventory, infrastructure, transportation)	<b>Inventory Planning:</b> Proper inventory size and location to best meet demand
<b>Source:</b> Sourcing stocked, make-to-order, and engineer-to-order product	<b>Supply:</b> Requirements determination and procurement from manufacturer
<b>Make:</b> Make-to-Stock, make-to-order, and engineer-to-order product execution from supplier	<b>Supply:</b> Manufacturing
<b>Deliver:</b> Order, warehouse, transportation, and installation management for stocked, make-to-order, and engineer-to order product at supplier and depot level	<b>Transportation:</b> Physically moving material to its destination <b>Customer response:</b> Shortest possible delivery, highest quality, lowest cost <b>Warehousing:</b> receiving, storage and handling, issuing, and shipping from depot
<b>Return:</b> Return of raw materials(to supplier or depot) and receipt of returns of finished goods (from customer), including defective products and excess products	<b>Reverse Logistics:</b> Creating value through serviceable and unserviceable material that has been returned to the logistics system by the customer <b>Maintenance:</b> return of repaired items to customer or supply system

Source: derived from SCOR Model Version 5.0 and AR 711-1 Supply Chain Management.

**Figure 6: Critical Capabilities**

### Critical Requirements

To derive the “essential conditions, resources, and means” that are critical requirements for a supply chain, this analysis pulls from several sources. First, the Supply Chain Council’s description of key management process outlines some of the requirements for each process.

Second, DoD Regulation 4140.1-R and AR 711-1 describe specific requirements and functions that are part of supply chain logistics processes.<sup>48</sup>

Critical Capability	Critical Requirements
<b>Plan</b>	<ul style="list-style-type: none"> <li>•Collaborative environment</li> <li>•Access to shared information</li> <li>•Common understanding of business rules and processes</li> <li>•Common Metrics and data collection capability</li> <li>•Visibility of resources and requirements</li> <li>•Ability to forecast and determine current requirements</li> </ul>
<b>Source</b>	<ul style="list-style-type: none"> <li>•Identification and access to suppliers</li> <li>•Global access and ability to import</li> <li>•Invoice processing and payment</li> </ul>
<b>Make</b>	<ul style="list-style-type: none"> <li>•Access to raw materials</li> <li>•Access to off-shore suppliers</li> <li>•Inventory management</li> <li>•Scheduled production and assured delivery</li> </ul>
<b>Deliver</b>	<ul style="list-style-type: none"> <li>•Global Multi-mode delivery means</li> <li>•In-Transit Visibility</li> <li>•Warehouse receipt, storage, cross-dock, shipping</li> <li>•Inventory management (adequate fill rate to meet customer needs)</li> <li>•Customer request processing/order fulfillment</li> </ul>
<b>Return</b>	<ul style="list-style-type: none"> <li>•Ability to receive/ship unserviceable/serviceable materiel</li> <li>•Ability to inspect, test, service, classify, repair, rebuilding, and reclaim unserviceable supplies</li> <li>•Access to repair parts</li> </ul>

Source: SCOR version 5.0, DoD 4140.1, AR 711-1, JP 4.09

Figure 7: Critical Requirements

### The Nature of the Threat

Before analysis of critical vulnerabilities, we will examine the nature of the threat to supply chains. While these threats take many forms, some are more common than others and may vary with respect to impact on a supply chain. By understanding what crises are most likely, supply chain managers can better allocate resources toward mitigation.

<sup>48</sup> Department of the Army, AR 711-1Supply Chain Management (Washington D.C.: Government Printing Office, 2002), 2-1 to 2-4, 3-1.

While the terrorist attacks on the world trade center have caused many supply chain professionals to reexamine their contingency plans, more benign threats are much more common and can have lasting effects. The U.S. has suffered 54 weather-related disasters over the past 23 years in which overall damages and costs reached or exceeded \$1 Billion. 45 of these disasters occurred during the 1988-2002 period with total damages and costs of nearly \$200 billion. Seven occurred during 1998 alone, the most for any recorded year.<sup>49</sup> In 2001, Tropical Storm Allison brought 30-40 inches of persistent rain that flooded the coastal areas of Texas and Louisiana then moved north flooding the eastern seaboard as far as Pennsylvania.<sup>50</sup> In 1999, Hurricane Floyd, a Category 2 hurricane made landfall in North Carolina destroying property and flooding coastal regions up the east coast as far north as Vermont.<sup>51</sup>

From May through September of 1993 persistent rain caused major flooding across the nation's Midwest. Damages from the floods caused \$15 billion in damages to property and infrastructure.<sup>52</sup> Transportation was severely impacted. Barge traffic on the Missouri and Mississippi Rivers stopped for nearly two months. Bridges were out or not accessible on the Mississippi River from Davenport, Iowa to St. Louis, Missouri. On the Missouri River, bridges were out from Kansas City to St. Charles, Missouri. Numerous state highways and other roads were closed. Ten commercial airports were flooded and railroad traffic in the Midwest was stopped.<sup>53</sup>

---

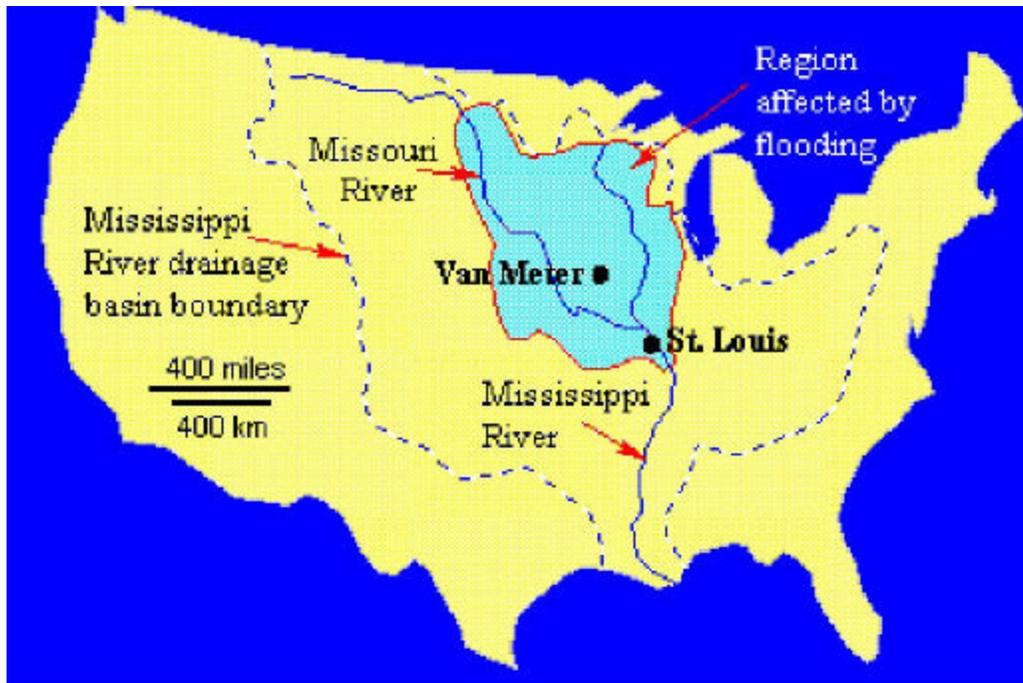
<sup>49</sup> National Climatic Data Center, "Billion Dollar U.S. Weather Disasters," available from <http://www.ncdc.noaa.gov/oa/reports/billionz.html>; Internet; accessed on 13 February 2002.

<sup>50</sup> Ibid.

<sup>51</sup> Ibid.

<sup>52</sup> Lee Larson, *The Great USA Flood of 1993* (Silver Spring: NOAA/National Weather Service, Office of Hydrology, 1996), 1.

<sup>53</sup> Ibid., 1-2.



Source: University of Akron geology department, "Missouri River Flood:1993"; available from [http://lists.uakron.edu/geology/natscigeo/lectures/miss\\_flood.htm](http://lists.uakron.edu/geology/natscigeo/lectures/miss_flood.htm): Internet.

**Figure 8: 1993 Mississippi River Flood**

Storms and floods are not the only natural disasters that can have lasting effects. The 1989 Loma Prieta earthquake, with a magnitude of 7.1, struck 60 miles south of San Francisco. While earthquakes in California are not particularly uncommon, the Loma Prieta earthquake was particularly destructive because of its proximity to the large urban centers around San Francisco and Oakland. Damage from the quake disrupted electrical systems from 24 hours to several weeks. While airports and ports sustained only minor damage, transportation infrastructure was severely disabled for several months and in some cases, years.<sup>54</sup>

<sup>54</sup> Anonymous, *The October 17, 1989 Loma Prieta Earthquake* (Houston: EQE Engineering, 1989).

Natural disasters are not the only catastrophic events that can disrupt a supply chain. On September 29, 2002, the International Longshore and Warehouse Union went on strike, locking out 10,500 unionized longshoremen at 29 ports from San Diego, California to Seattle, Washington. By October 8, an estimated 200 ships waited offshore to be unloaded.<sup>55</sup> The Anderson Economic Group of Lansing, Michigan estimated that the strike had an economic impact of \$1-2 billion.<sup>56</sup> Ten days after it began, President Bush put an end to the strike by requesting that a Federal judge order the longshoremen back to work. While a ten-day shutdown may not seem “catastrophic”, the effects of the port shutdowns on retailers and manufacturers were felt for months after ports were reopened. Honda Motor Company shut its four North American Assembly plants for two days in late October due to lack of necessary parts.<sup>57</sup>

Although most Americans didn't feel particularly vulnerable to terrorist attacks, all that changed on September 11<sup>th</sup>, 2001. While the September 11<sup>th</sup> attacks on the World Trade Center seemed to focus the nation's attention on the threat of terrorism, there was plenty of prior evidence that the U.S. was not insulated from attack. Between 1980 and 1999, the FBI recorded 327 incidents or suspected incidents of terrorism in the United States. Of these, 239 were attributed to domestic terrorists while 88 were determined to be international in nature. During the same period, 130 planned acts of terrorism were prevented. Of these, 83 were domestic plots and 47 were international extremist plots.<sup>58</sup>

---

<sup>55</sup> Tom Ramstack, “Bush Steps In To Halt West Coast Shutdown”, ([The Washington Times](#), 8 October, 2002).

<sup>56</sup> Patrick Anderson, [Lost Earnings Due to the West Coast Port Shutdown](#), (Lansing, Anderson Economic Group, 2002), 2.

<sup>57</sup> Chris Isidore, “Port backlog still ails economy”, (CNN/Money Magazine, 21 October 2002), available at <http://money.cnn.com/2002/10/21/news/companies/ports/index.htm>.

<sup>58</sup> U.S. Department of Justice, *Terrorism in the United States 1999*, (Washington D.C.: Government Printing Office, 2000), 16.

Terrorist incidents from 1980 to 1999 were most numerous in the Northeast region of the United States (140 incidents) followed by the Western region (82 incidents).<sup>59</sup>



**Figure 9: Terrorism in the United States**

The most frequently occurring event was bombings, of which there were 321 followed by assassinations, of which there were 21.<sup>60</sup> Aside from the 1993 bombing of the World Trade Center and the 1995 Oklahoma City Federal Building bombing, most of the recorded bombing incidents between 1980 and 1999 were low yield events directed at specific targets which may have resulted in loss of life but didn't do significant damage to infrastructure or transportation systems. The real destructive effect (as this monograph

<sup>59</sup> Ibid, 28.

<sup>60</sup> Ibid, 41.

will illustrate later) to supply chains is the self-imposed second and third order effects of terrorist attacks.

### **Critical Vulnerabilities**

In July 2001, the Council of Logistics Management commissioned a study by Dr. Omar Helderich and Dr. Robert Cook to assist supply chain professionals in planning for major events that could disrupt a supply chain. Their work, *Securing the Supply Chain*, classifies types of disasters and offers a practical guide for event planning. Steps in their disaster management process include: Planning, Mitigation, Detection, Response, and Recovery. With respect to vulnerability they say:

Many current supply chains are particularly vulnerable to disruption by disasters because of their design characteristics and operating philosophy. First, many supply chains are global in nature, and consequently are susceptible to border crossing disruptions. Second, many current supply chains are complex; involving many partners and therefore must rely on operational support from numerous firms and public entities. Any disruption in operations of one link in the chain can affect supply chain performance. Third, many supply chains rely on highly flexible, quick response operations to meet customer requirements. As a result, any major disruption of electrical power, communications and transportation flow, or destruction of critical supply chain operating capabilities such as employees, inventories or manufacturing plants would have a major negative impact on supply chain performance.<sup>61</sup>

Their white paper accurately identifies why supply chains are vulnerable and offers a valuable disaster classification scheme and framework for developing a disaster plan. While they do present six case studies of how some companies reacted to unplanned event, the primary focus of their work is developing a practical approach to disaster planning. Logistics consultant Roger Kallock, former Deputy Undersecretary of Defense for Logistics and Material Readiness said, "If I were vice president or general manager of

---

<sup>61</sup> Robert Cook and Omar Helderich, *Securing the Supply Chain: Management Report* (Oak Brook: Council of Logistics Management, 2002), 3.

a division of a corporation that had international supply-chain components, I'd want my team coming to me saying 'here is our range of vulnerability that we have as a result of this wake-up-call.' I'd also want to know the range of ways we're responding. Accelerate attention on those improvement programs that will give you better information across the supply chain so you can make decisions quickly and take appropriate action.<sup>62</sup> Mr. Kallock is not alone in his renewed emphasis on assessing the impacts of major crises on a supply chain. A week after the September 11th attacks, 39% of supply chain managers called the disruptions dramatic, 52% reported a slight impact, and only 9% saw no effect on deliveries, according to a survey by Purchasing magazine in Newton, Massachusetts.<sup>63</sup>

While terrorist attacks may not be at the top of the list of potential supply chain disrupters, the 2001 World Trade Center attack was significant enough in magnitude to offer a good test case. Multiple companies with global supply chains shared a common experience with similar results. Because of the horrific nature of the attack, there is significant amount of data with regards to the impacts on commercial industry. Because of the sudden shift in security procedures across the United States, the paradigm that modern supply chains had operated under suddenly changed. The September 11<sup>th</sup> attacks offer a snapshot that can be examined to determine what went right, what went wrong, and why it happened that way. These lessons yield what current and future supply chain best practices might be. A survey of impacts reported by commercial industry in professional journals, published reports, magazine articles, newspapers, and on-line sources reveal that critical supply chain vulnerabilities are most commonly associated

---

<sup>62</sup> Tom Andel, "The New World of Global Distribution," *Material Handling Management*, January 2002, 24.

<sup>63</sup> Mitch Betts, "Just in Case," *Computerworld*, 17 December 2001, 46.

with contingency planning, information technology, inventory location and availability, transportation, and assured communication.

### Contingency Planning

Helferich and Cook's research revealed that only 12 percent of U.S. firms had disaster recovery plans for their entire organization and only 28 percent of executives had crisis management teams in any form.<sup>64</sup> They say, "although the potential risk for business disruption was known to exist prior to September 11<sup>th</sup>, many business organizations still had not developed continuity plans. For those companies that did have continuity or crisis management plans, many focused on information systems failures rather than the full range of potential infrastructure risks."<sup>65</sup> Companies who had well-structured organizations, established and understood procedures and processes, and responsive information technology tools were impacted the least. Sears uses a "contingency cell" consisting of up to 100 people in an "emergency operations center" located in a special room at their headquarters. After the September 11<sup>th</sup> attacks they were able to monitor impacts on delivery routes and communicate with their stores and suppliers to minimize bottlenecks. Retired Army Lieutenant General Gus Pagonis, who led the logistics effort supporting the Persian Gulf War said, "the key to success is to not overreact and not to kill your people. A good leader prepares for crises, so when they occur, they become routine."<sup>66</sup> Yossi Sheffi a logistics and transportation expert from the Massachusetts Institute of Technology recommends creating a "Chief Security Officer"

---

<sup>64</sup> Robert Cook and Omar Helferich, *White Paper: Securing the Supply Chain*, (Oak Brook: Council of Logistics Management, 2002), 19.

<sup>65</sup> Cook and Helferich, *Securing the Supply Chain: Management Report*, 14.

<sup>66</sup> Matt Hicks, "When the Chain Snaps," *Eweek*, 18 February; available from <http://www.eweek.com>; Internet; accessed on 18 August 2002.

position to coordinate business preparedness for crisis situations. Planning teams should be collaborative by nature and should represent all functions of an organization, including suppliers and contractors.<sup>67</sup>

### Information Technology

Many companies have made large investments in their information technology infrastructure since the 1990s. The DLA's \$500 million investment in its business systems modernization plan is an example of that. While most investments were not nearly that large, those companies who took advantage of them reaped the benefits.

Disruptions from the September 11<sup>th</sup> attacks also identified areas that need to be improved or expanded upon. United Parcel Service Logistics Group (UPS LG) lost a key distribution center located 150 yards from the World Trade Center. A second nearby distribution center had to be evacuated and a third was inaccessible because roads were blocked. Because they had invested in a supply chain tracking and visibility system, they were able to locate stock in other distribution centers and route it to their customers with little impact. Lynette McIntire, director of marketing for UPS LG said "Nobody anticipated a facility being destroyed, but we did have the redundancy of product available in the area. We figured out where the parts were and had hourly shuttles...to get them there."<sup>68</sup>

Matt Hicks, a writer for *Eweek* magazine said "Among the lasting effects of September 11<sup>th</sup> has been a growing awareness among IT managers and others of the need to shore up supply chain execution and planning practices and systems so that the chains

---

<sup>67</sup> Yossi Sheffi, "Supply Chain Management un the threat of international Terrorism," *International Journal of Logistics Management*, Vol. 12 No. 2, (2001), 1-11.

<sup>68</sup> Hicks, "When the Chain Snaps," *Eweek*.

can keep operating smoothly, even through disaster...the need to harden supply chains against disaster is motivating many companies to deploy systems that provide them with more real-time visibility into supply networks."<sup>69</sup>

A unique capability at UPS LG is a homegrown program that they call "Global Tracker" that not only tracks a shipment as it moves through the supply chain, but alerts a manager when that shipment misses a pre-established milestone. This capability allows managers to only focus on those shipments that may have problems rather than monitor the entire supply chain. The capability provided by software like Global Tracker is now being described as "supply chain event management" (SCEM) software. SCEM software enables companies to rapidly (and sometimes automatically) respond to unplanned events - without having to completely regenerate plans. SCEM applications accomplish this by notifying supply chain managers when specific "events" occur, e.g., when inventories are depleted, shipments delayed, etc. Data that represent exceptions from plan are red flags. Often times, automated responses can resolve these issues promptly, but in all cases, managers have the opportunity to analyze problems and determine solutions.<sup>70</sup>

Sears is using a program called "SeeCommerce" to provide real-time information about movement of supplies among its 900 stores by linking several of its legacy systems. Currently, during a crisis, managers must monitor over 20 different systems for data.<sup>71</sup> Current trends seem to be aimed at establishing greater visibility of supply chains.

Scott Stephens, Chief Technology Officer at the Supply Chain Council said "[IT departments must build] advanced planning systems and decision support software that enable the supply chain planners to plan for a wider range of conditions. You'll see a

---

<sup>69</sup> Ibid.

<sup>70</sup> Deb Marabotti, "Supply Chain Event Management," *Line 56*, 27 August 2002.

greater emphasis on real-time sharing of demand and inventory and shipping information. If we can react quicker to a disruption, then we carry less inventory, or we have to carry less safety stock."<sup>72</sup> Along with global transportation tracking, event management, and supply chain visibility IT solutions like the ones described above, Steve Banker, a supply chain analyst recommends developing new planning tools to simulate “what if” scenarios. These tools could give supply chain planners better insight into how much safety stock is adequate to mitigate risk.<sup>73</sup>

### Inventory

Current business trends as well as trends within the Department of Defense are to move towards an environment of “lean logistics”. Many companies who took this to the extreme and operated on a “Just-in-Time” (JIT) philosophy where, theoretically, a manufacturer received component parts or materials just as they were needed in the assembly process. JIT allowed only minimal inventory and some safety stock to be on-site saving the manufacturer the expense of carrying expensive inventory.

Andre Kuper, who works as a consultant for innovation at Hewlett Packard said “Like it or not, as manufacturers, we are far more dependent on timely, reliable deliveries of suppliers and logistics providers than was previously thought possible and we have systematically removed buffer inventories from the supply chain.

Safety stock, a statistically determined buffer for measured variability in material flows, does not take into account low probability high impact events like fire,

---

<sup>71</sup> Damir Barlas, “Performance Management for Sears,” *E-Business News*, 27 November 2001.

<sup>72</sup> Anonymous, “Is Just-in-time returning to Just-in-case?” *Modern Materials Handling*, November 2001, 19-20.

<sup>73</sup> Ibid.

earthquakes, blizzards, strikes, and terrorist acts. Therefore, when disruption hits, there is far less time to react and far fewer options."<sup>74</sup>

Small inventories and inadequate safety stock may be the biggest vulnerability in modern supply chains. Profit motives create tension between demand satisfaction and financial performance. JIT practices sometimes have a risky side. Theodore Schereck, president of a transportation research firm said " We have worked with extended supply chains that use time-definite transportation and sophisticated information technology to replace inventories and [minimize] the number of times a widget must be handled from the point of production to the point of consumption but it carries risk, lean inventories and extended supply chains magnify any interruption of flow. This war footing has more impact on a lean supply chain than it does on older models."<sup>75</sup>

Hewlett Packard stores some of its more expensive components like memory chips centrally and delivers them to regional supply centers as they are needed. The weeklong disruption of air traffic after the September 11<sup>th</sup> attacks created disruptions to their manufacturing output. Kuper said "Because of this [normally reliable air transportation], low variability safety stock was minimal and our ability to respond was limited for a time...the circumstances challenged our assumptions about our logistics infrastructure and buffers for uncertainty."<sup>76</sup>

Other companies who operated on JIT principles also suffered the consequences. Ford had to shut down its assembly lines for several days because trucks delivering component parts from Canada and Mexico were delayed at the U.S. border. Similarly,

---

<sup>74</sup> Andre Kuper, "Hardening Vulnerable Links in the Supply Chain," *TOTAL supply chain*, February 2002, 1-2.

<sup>75</sup> James Cooke, "Brave new World", *Logistics Management*, 1 January 2002.

<sup>76</sup> *Ibid*, 2.

Toyota had to stop production at its Indiana plant because one of its suppliers could not get steering sensors shipped by air from Germany.<sup>77</sup>

Ford and Toyota's experiences highlight another critical vulnerability in modern supply chains. Because so many manufacturers rely on offshore production for component parts, they are increasingly susceptible to delays because of regional weather and security regulations. Many companies are beginning to reevaluate where they procure and store their inventory. This also reinforces the principle that a supply chain does not begin at the receiving dock but extends to your supplier and your supplier's supplier.

Dawn Russell, of Penn State's Smeal College of Business said "...inventory stocks may increase to guard against uncertain supply while continuing to meet customer demand for product...to keep these safety stocks to a minimum and maintain flexibility in meeting changing demand, our use of information technology becomes more important than ever. The right information at the right place at the right time is what allows us to make the real-time decisions so crucial to the operating success of any supply chain."<sup>78</sup> JIT does not appear to be a dead concept, however, many business are now moving towards a "Just-Enough" philosophy and rethinking how they calculate safety stocks.

## Transportation

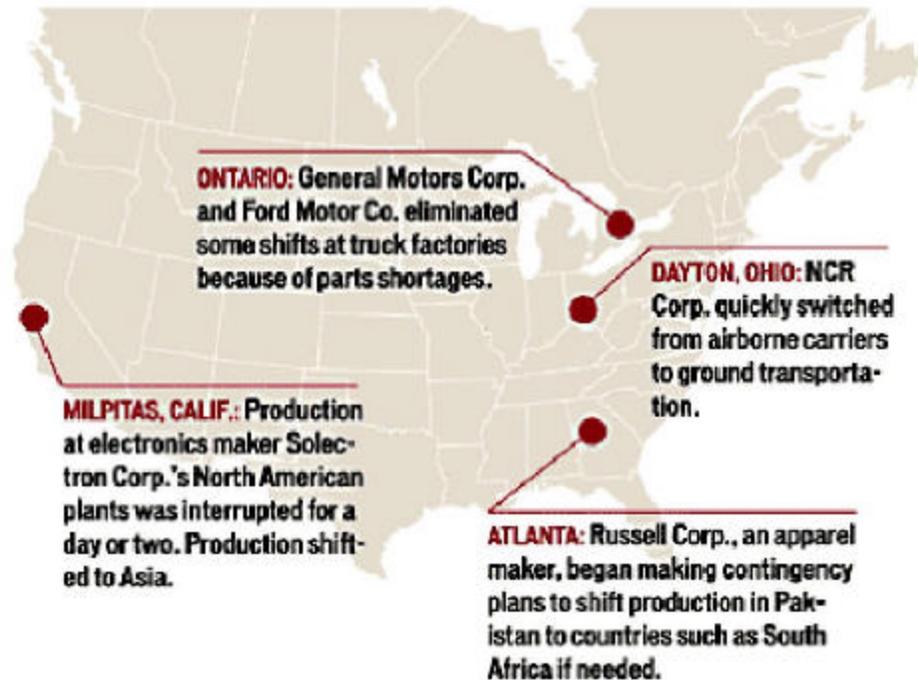
Perhaps the greatest impact on commercial supply chains following the World Trade Center bombing was the disruption of the global transportation network. Increased security measures created long delays at ports and borders and air traffic was grounded

---

<sup>77</sup> Sheffi, "Supply Chain Management and the threat of international Terrorism", 1.

<sup>78</sup> Dawn Russell, "Attacks affect Supply Chains and the Supply Chain Management Profession", (Smeal College of Business, Sep 2001). Available at <http://www.newswise.com/articles/2001/9/supply.scm.html>.

for a week. Just 36 hours after the attack, Daimler-Chrysler announced that it would have to close one of its assembly plants because supplies were stuck in an 18-hour traffic jam at the Canadian border. Ford announced that five of its assembly plants would have to stop production.<sup>79</sup> Airfreight traffic was completely shut down on September 11<sup>th</sup> and 12<sup>th</sup> and didn't return to normal until the 16<sup>th</sup>.



Source: Mitch Betts, "Just in Case," *Computerworld*, 17 December 2003, 46.

**Figure 10: September 11, 2001 "Ripple Effect"**

Companies like Sun Microsystems who ship close to 60 percent of their products by air were impacted the greatest. Sun's Vice President, Hugh Aitken estimates that they ship between \$1 million and \$1.5 million worth of products a day by air.<sup>80</sup> U.S. ports were

<sup>79</sup> Stephen Flynn, "America the Vulnerable", *Foreign Affairs*, Jan/Feb 2002.

<sup>80</sup> Claire Serant and Jennifer Baljko Shah, "Guarding Your Goods In an Uncertain World", *EBN*, 8 July 2002, 23.

shut down initially but most were reopened within a week, although stricter security measures for container inspections were implemented that would slow their clearance from the port. Considering 90 percent of the world's cargo moves in shipping containers, stricter security measures may have a lasting effect on many supply chains that will have to increase stockage levels to compensate for the additional shipping time.<sup>81</sup> Tom White, a spokesperson for the Association of American Railroads said the rail industry faced some restrictions in the Northeast but was back to normal within two days after the attacks.<sup>82</sup> While major transportation delays were relatively short-lived, their effects have caused many companies to rethink the wisdom of relying on a single mode of transportation to ship goods. Future disasters like the 1993 Mississippi floods could have a more lasting effect. Additionally, new security measures and new processes are here to stay. Supply chains will have to adjust to accommodate them.

Many of the companies who responded well to the September 11<sup>th</sup> attacks had systems and procedures in place that gave them the visibility and agility they needed to shift resources. HON, an office furniture manufacturer, that operates 18 factories across the country, used a capacity and supply chain planning application from Synquest that allowed them to reroute shipments to their manufacturing facilities in the Northeast. As a result they were able to cut delivery time from two weeks to five days following the attacks. This transportation visibility tool, along with contingency plans they already had in place, mitigated much of the disruptions experienced by other manufacturers.<sup>83</sup> Dick Metzler, CEO of APL Logistics, a \$4.6 billion a year transportation company, said "In

---

<sup>81</sup> Mike Scott, "Stay Out," *Materials Management and Distribution*, 1 May 2002, 1.

<sup>82</sup> Mike Freeze, "Logistics Leads Response," *Transportation and Distribution*, October 2001, 28.

<sup>83</sup> Jim Ericson, "Supply Chain Interrupted," *Line56*, December 2001, 41-43.

their international supply chains, they [customers] told us that whether they ship by ocean or air, when the finished product or raw material is moving from Asia or Europe, they need to have IT visibility so they can swap modes or destinations on the fly while in transit. Prior to September 11<sup>th</sup>, there just wasn't anybody operating that way."<sup>84</sup>

Scott Stephens, chief technology officer at the Supply Chain Council says, "Supply Chain systems may require redesigns so companies can do a better job of handling 'surge and ebb' situations in product demand and stock availability."<sup>85</sup> Michael Bittner, an analyst at AMR Research said, "Companies should build automated alternative sourcing functions into their systems."<sup>86</sup>

NCR, for example, implemented Y2K contingency plans supported by its supply chain and procurement system to switch from air to ground transportation when the distribution facility it shared with UPS was destroyed.<sup>87</sup> Current best practices seem to indicate that the best mitigators for transportation disruptions are information technology solutions that provide accurate in-transit visibility and redundant transportation modes that can redirect product flow when needed. Well thought out security regulations at ports could also speed container inspections for known shippers and focus on those that fit an established security profile. Collaboration between transportation companies, manufacturers, and the U.S. government will be essential if disruptions to supply chains following a shift in security level are to be minimized.

---

<sup>84</sup> Ibid, 42.

<sup>85</sup> Marc Songini, "Supply Chains face changes after attacks," *Computerworld*, 1 October 2001.

<sup>86</sup> Ibid.

<sup>87</sup> Ibid.

## Assured Communication

While few companies outside of the New York financial district reported disruptions in communications, loss of data transfer capability, or loss of data storage, the effects of a disruption to a communications network can be devastating. Because the attacks knocked out electricity, phone lines, and other basic services, many companies that weren't destroyed by the attack had to relocate operations. Merrill Lynch was initially not able to access its trading floors in the World Financial Center but was able to relocate in accordance with their contingency plans to another location outside of New York. American Express was able to shift operations performed in the World Trade Center to lower Manhattan and New Jersey while its trading operations continued unaffected in Minneapolis.<sup>88</sup>

These companies responded well to the attacks because they kept duplicate computer networks and stored data in sites outside of Manhattan. Other companies did not fare so well. Comdisco, a company who specializes in data storage and disaster recovery helped rebuild networks for six companies who were located inside the World Trade Center and 29 others who were located nearby. One day after the attacks, John Jackson, president of Comdisco's disaster recovery division said "Based on my knowledge of the companies, there is some significant data loss. Anything they've done since the last back-up is lost."<sup>89</sup>

Redundancy seems to be the key. The disruption to financial industry in Manhattan's financial district provides a good example of this. About \$3.5 trillion moves daily through three major payment networks operated by banks and the government and

---

<sup>88</sup> Lisa Singhania, "Financial firms put it together," *USA Today*, 12 September 2001.

<sup>89</sup> Ibid.

converges at 10 data processing centers across the country.<sup>90</sup> The system was designed so that if one of the data processing centers were lost, there would be no disruption.

What was surprising about the September 11<sup>th</sup> attacks are that disruptions to data networks were caused by kinetic means rather than cyber attack. Tim Belcher, Chief Technology Officer for Riptech, a computer security firm said “It was always assumed that a small group of terrorists could do much more damage to the cyberworld than the physical world. There was some surprise that this [first attack] wasn’t a cyberattack.”<sup>91</sup>

It is widely believed that cyberterrorism will be the weapon of choice in the future for trans-national terrorist groups seeking to create disproportional effects after cyberattacks. At a Senate Judiciary subcommittee hearing on cyberterrorism, White House technology adviser Richard Clark said cyber-attacks are almost inevitable because they are cheaper and easier for a foreign country or terrorist group than a physical attack.<sup>92</sup>

Despite spending \$2.7 billion on computer network security many computer security experts still believe that the U.S. Government is not safe from cyberattacks.<sup>93</sup> A survey conducted by the Business Software Alliance released in June 2002 found that among 395 IT professionals responsible for their company’s computer and internet security 59 percent believed that a major attack against the government is likely in the next 12 months.<sup>94</sup> They recommended better cooperation between commercial industry and government and employment of better encryption technologies to prevent access

---

<sup>90</sup> Jim Hopkins, “Electronic financial networks: How safe are they?” *USA Today*, 29 October 2001.

<sup>91</sup> Sharon Gaudin, “Protecting a net in a time of terrorism,” *Network World*, 24 September 2001.

<sup>92</sup> Associated Press, “Cyberattack could result in military response,” *USA Today*, 14 February 2002.

<sup>93</sup> *Ibid.*

<sup>94</sup> U.S. Department of State Press release, “Stronger action needed to prevent cyberattack survey finds,” 25 June 2002; available from <http://usinfo.state.gov>; Internet; accessed on 12 March 2003.

from hackers. While disruptions to computer networks following the September 11<sup>th</sup> attacks may have been localized and short-lived, they may serve as a pointed reminders of the real “Achilles heal” of the modern supply chain.

### Critical Vulnerabilities Revisited

Figure 11 below outlines the key critical vulnerabilities of commercial supply chains as a result of analysis of the September 11<sup>th</sup> terrorist attacks on the World Trade Center.

Category	Critical Vulnerability
<b>Planning</b>	<ul style="list-style-type: none"> <li>• Failure to properly identify and assess threats</li> <li>• Lack of contingency plans that encompass the entire supply chain</li> <li>• Failure to collaborate with all supply chain partners</li> </ul>
<b>Information Technology</b>	<ul style="list-style-type: none"> <li>• Inability to see shipments in the supply chain from end to end</li> <li>• Inability to manage by exception using automated tools (data overload)</li> <li>• Unlinked "legacy" systems</li> <li>• Inability to redirect supplies as they move through the supply chain</li> <li>• Lack of accessibility by all supply chain partners</li> </ul>
<b>Inventory</b>	<ul style="list-style-type: none"> <li>• Lean Inventory and or inadequate safety stocks</li> <li>• Lack of simulation tools to plan and adjust safety stocks</li> <li>• Reliance on off-shore suppliers</li> <li>• Too much inventory the clogs the supply chain and reduces efficiency</li> </ul>
<b>Transportation</b>	<ul style="list-style-type: none"> <li>• Reliance on a single transportation mode for mission critical supplies</li> <li>• Delays at border crossings/ port clearance requirements</li> <li>• Centralized distribution facilities</li> <li>• Competition with other supply chains for transportation resources during crisis</li> </ul>
<b>Assured Communication</b>	<ul style="list-style-type: none"> <li>• Lack of real-time data backup and network perimeter protections</li> <li>• Lack of contingency plans for data recovery</li> <li>• Inability to quickly reestablish or regenerate networks</li> <li>• Localized networks performing multiple critical functions</li> <li>• Lack of data encryption</li> </ul>

**Figure 11: Critical Vulnerabilities**

## Chapter 5: Conclusion

*“Keep your mind open to change all the time. Welcome it. Court it. It is only by examining and re-examining your opinions and ideas that you can progress.”*

Dale Carnegie

*“Change is not an optional thing, we cannot vote and say we want to stop it. In fact, we are changing faster than ever before.”*

Bill Gates

The purpose of this monograph was to describe what happens when a supply chain is disrupted and determine what the implications might be for the Army supply chain under attack. This analysis has shown that modern supply chains face an array of threats both man-made and natural. Examination of these threats shows that significant vulnerabilities existed for those companies who failed to learn from previous crises, failed to anticipate the range of threats to their supply chains, or lacked the agility to adapt once crisis occurred.

The majority of companies that were minimally impacted by the September 11<sup>th</sup> attacks had some type of contingency plan in place. These plans went beyond continuity of operations plans for IT systems and involved arrangements with other partners in the supply chain. Because they anticipated disruptions, they designed their organizations so that they could respond. They developed processes that mitigated disruption through supply chain visibility, redundancy, and agility. They used the best available technology to help them see “supply net exceptions” as they were happening. They were able to sense and interpret, and then decide and act on that information. They were able to decentralize decision-making and execution because many of their systems were web-

based; members within the supply chain could share information and collaborate. Successful companies had good continuity because they protected critical infrastructure, processes, people, and information. They created redundancy by either physically separating resources or functions to mitigate threats and/or they had procedures in place to quickly accommodate or adapt to events by shifting resources where they were needed.

The process changes outlined in chapter three have bore fruit for the Army supply chain. The payoff was evident in how the defense supply chain responded to the events of September 11<sup>th</sup>, 2001. Unlike many of the companies discussed previously, the impact was minimal. Despite a direct attack on the Pentagon, the defense supply chain was able to respond immediately to support disaster relief operations as well as deploying forces to fight the new war on terrorism.

By early October 2001 forces from multiple CONUS bases began to deploy to Afghanistan, Uzbekistan, and multiple other countries for Operation Enduring Freedom. The elastic effect of the defense supply chain was demonstrated as hundred of tons of supplies and equipment were projected halfway around the world into a desolate, landlocked countries.

About five to six thousand requests for supplies from Afghanistan and Uzbekistan were filled each month from November 2001 through August 2002. Critical repair parts were delivered from CONUS depots by air on average in 13 days and less in less than 40 days by surface transportation.<sup>95</sup> In spite of disruptions that caused significant difficulties for many civilian supply chains, the defense supply chain has proven resilient, agile, and responsive.

The Department of Defense supply chain is arguably one of the most complex in

the world. Unlike most commercial supply chains, the DoD supply chain represents a lucrative target for terrorism not only for the symbolic effect of attacking a powerful government but for the lifeline it provides to the military. Additionally, the DoD supply chain extends to hundreds of remote places around the world and can be required at a moment's notice to stretch to new ones.

Many of the current and planned DoD supply chain best practices are in line with those used by commercial industry. DoD's business systems modernization program is beginning to leverage new advances in supply chain IT capabilities. The Global Transportation Network (GTN) system and other feeder systems provide in-transit visibility of items moving in the supply chain. The Army's Combat Service Support Control System (CSSCS) which feeds into the Global Command and Control System (GCCS) provides logistics professionals at the tactical and operational level visibility they need and the ability to manage by exception by building a "Commander's Tracked Items List" of only those mission critical items deemed necessary. Future advancements might track these items all the way to the manufacturer and alert managers when certain parameters are not met in advance of a need.

As part of its Velocity Management Program, the Army has a process in place to examine its critical processes and measure efficiency through established metrics. Although future advancements in IT may better enable managers to establish ideal inventory levels, dollar cost banding represented a giant leap in right-sizing inventory. It brings the added benefit of reducing what is moving in the supply chain so when an unexpected event occurs, the supply chain is more agile and can adapt quickly. Stocks are distributed from strategically located regional depots that have the ability to mutually

---

<sup>95</sup> John Hall, "Afghan Supply Pipeline Performance," *Army Logistician*, (January-February 2003), 8.

support one another should the supported unit move or if a lengthy disruption occurs.

What may be missing is the formalization of contingency planning and procedures within the entire supply chain to leverage capabilities that already exist.

The vast network of supply chain partners outside the depots in commercial industry may have certain vulnerabilities that by extension are shared by all. Suppliers of critical parts who have off-shore suppliers may need to increase buffer stocks to insulate themselves from disruption. Commercial transportation providers may be vulnerable to regional weather phenomena or security requirements. Critical data may be vulnerable to disruption by cyberattacks or because there is a sudden requirement to transmit to a new location on the other side of the world through commercial satellites or foreign networks. A collaborative contingency planning effort between all partners in the DoD supply chain is needed to evaluate specific likely threats and vulnerabilities. Once this is done, processes and procedures can be instituted when necessary to adapt to sudden changes and mitigate the effects.

The aim of this monograph was to present the range of threats to a supply chain and analyze the impacts of a single catastrophic event. Secondly, it sought to focus on how commercial industry responded and what practices best mitigated the threat. Current defense supply chain practices have postured the Army supply chain well to respond to the unexpected. Many of the “best practices” observed in the commercial sector that minimized impacts of the September 11<sup>th</sup> attacks have been in place in the defense supply chain for some time. Given this observation, the Army and DoD could best respond to sudden supply network change by adopting or developing these best practices where they

already exist. The following recommendations are offered for consideration to DoD

supply chain leaders and managers:

- Formalize crisis continuity planning among all partners in the defense supply chain to include tier 1 and 2 level suppliers.
- Ensure that business systems modernization plans include advanced planning systems and decision support software with the capability to simulate “what if” scenarios to determine impacts on the supply chain and provide visibility solutions that alert managers when critical milestones have been missed.
- Increase supply chain visibility and information sharing among partners through web-based applications to allow parallel planning and decentralized decision making.
- Evaluate and account for the role that the defense supply chain might play in supporting homeland security and possible disaster relief operations. Establish a board to facilitate collaboration between other government agencies, emergency relief organizations, and commercial industry.
- Minimize reliance on off-shore suppliers for critical components of vital systems.

The Army Vision has already provided the catalyst for change that supports a resilient, adaptive, responsive supply chain. Ongoing Army and Department of Defense initiatives will increasingly harden the defense supply chain against the unexpected. Perhaps the greatest vulnerability is resistance to change itself that keeps an organization from realizing its vision.

## Bibliography

### Books

Cohen, Eliot A., and John Gooch. *Military Misfortune*. New York: The Free Press, 1990.

Dorner, Dietrich. *The Logic Of Failure*. New York: Metropolitan Books, 1996.

Harper, Michael, and Gordon Sullivan. *Hope is Not a Method*, New York: Broadway Books, 1996.

Naveh, Shimon. *In Pursuit of Military Excellence: Evolution in Operational Theory*. London: Frank Cass & Co, 1997.

Senge, Peter M. *The Fifth Discipline*. New York: Doubleday, 1990.

### Government Publications

U.S. Department of the Army. *The Army Vision*, Washington D.C.: Government Printing Office, 1999.

\_\_\_\_\_. *FM 3-0 Operations*, Washington D.C.: Government Printing Office, 2001.

\_\_\_\_\_. *Objective Force 2015 White Paper*, Washington D.C.: Government Printing Office, 2002.

\_\_\_\_\_. *AR 711-1 Supply Chain Management*, Washington D.C.: Government Printing Office, 2002.

Defense Logistics Agency, *Defense Logistics Agency Strategic Plan 2002-2007*, Washington D.C.: Government Printing Office, 2002.

\_\_\_\_\_. press release “DLA Fields First Release of Modernized System”, 6 August 2002, available from <http://www.dla.mil>.

Department of Defense, Deputy Under Secretary of Defense for Logistics, *FY2000 Logistics Strategic Plan*, Washington D.C.: Government Printing Office, 1999.

Department of Defense, Joint Chiefs of Staff, *Joint Vision 2020*, Washington D.C.: Government Printing Office, 2000.

Department of Defense, DoD 4140.1-R *Supply Chain Materiel Management Regulation*, Washington D.C.: Government Printing Office, 2002.

\_\_\_\_\_. JP 5-00.1 *Joint Doctrine for Campaign Planning*, Washington D.C.: Government Printing Office, 2002.

National Climatic Data Center, "Billion Dollar U.S. Weather Disasters", available from <http://www.ncdc.noaa.gov/oa/reports/billionz.html>

U.S. Department of Justice, *Terrorism in the United States 1999*, Washington D.C.: Government Printing Office, 2000.

U.S. Department of State Press release, "Stronger action needed to prevent cyberattack, survey finds", 25 June 2002, available from <http://usinfo.state.gov>.

## Articles

Anonymous. "Is Just-in-time returning to Just-in-case?," *Modern Materials Handling*, November 2001.

Andel, Tom. "The New World of Global Distribution," *Material Handling Management*, January 2002, 24.

Barlas, Damir. "Performance Management for Sears," *E-Business News*, 27 November 2001.

Betts, Mitch. "Just in Case," *Computerworld*, 17 December 2001, 46.

Cooke, James. "Brave new World," *Logistics Management*, 1 January 2002.

Ericson, Jim. "Supply Chain Interrupted," *Line56*, December 2001, 41-43.

Freeze, Mike. "Logistics Leads Response," *Transportation and Distribution*, October 2001, 28.

Gaudin, Sharon. "Protecting a net in a time of terrorism," *Network World*, 24 September 2001.

Glisson, Henry. "Revolution in Military Logistics: Improving Support to the Warfighter," *Army Logistician*, Jan/Feb 1999.

Hicks, Matt. "When the Chain Snaps," *Eweek*, 19 August 2002, accessed 23 November 2003, available from <http://www.eweek.com>, Internet.

Isidore, Chris. "Port backlog still ails economy," *CNN/Money Magazine*, 21 October

2002, accessed on 4 December 2003, available from <http://money.cnn.com/>, Internet.

Kuper, Andre. "Hardening Vulnerable Links in the Supply Chain," *Total Supply Chain*, February 2002, Accessed on 23 September 2003, available from <http://www.totalsupplychain.com>, Internet.

Marabotti, Deb. "Supply Chain Event Management," *Line 56*, 27 August 2002, accessed on 3 February 2003, available from <http://www.line56.com>, Internet.

Messmer, Ellen. "Defense Logistics Agency on slow march to supply chain modernization," Network World Fusion website, Aug 2002, accessed on 16 January 2003, available from <http://www.nwfusion.com>, Internet.

Scott, Mike. "Stay Out," *Materials Management and Distribution*, 1 May 2002, 1.

Serant, Claire and Jennifer Baljko Shah. "Guarding Your Goods In an Uncertain World," *EBN*, 8 July 2002, 23, accessed on 20 February 2003, available from [http://www.glog.com/glog\\_buzz/files/ebn2002.pdf](http://www.glog.com/glog_buzz/files/ebn2002.pdf), Internet.

Sheffi, Yossi. "Supply Chain Management un the threat of international Terrorism," *International Journal of Logistics Management*, Vol. 12, No. 2, 2001, 1-11.

Songini, Marc. "Supply Chains face changes after attacks," *Computerworld*, 1 October 2001.

## **Reports and Unpublished Works**

Anderson, Patrick. *Lost Earnings Due to the West Coast Port Shutdown*, Lansing: Anderson Economic Group, 2002.

Anonymous. *The October 17, 1989 Loma Prieta Earthquake*, Houston: EQE Engineering, 1989, accessed on 13 March 2003, available from <http://www.eqe.com/publications/lomaprie/introduc.htm>, Internet.

Cook, Robert and Omar Helferich. *Securing the Supply Chain: Management Report*, Oak Brook: Council of Logistics Management, 2002.

Cook, Robert and Omar Helferich. *White Paper: Securing the Supply Chain*, Oak Brook, Council of Logistics Management, 2002.

Coyle, John J. and others. *The Management of Business Logistics: A Supply Chain Perspective*, Mason, OH: Thomas Learning, 2003..

Dumond, John and others. *Velocity Management: An Approach for Improving the*

*Responsiveness and Efficiency of Army Logistics Processes*, Santa Monica: RAND, 1994.

Dumond, John and others. *Velocity Management: The Business Paradigm That Has Transformed U.S. Army Logistics*, Santa Monica: RAND, 2001.

Larson, Lee. *The Great USA Flood of 1993*, Silver Spring: NOAA/National Weather Service, Office of Hydrology, 1996, 1, accessed on 22 January 2003, available from [http://www.nwrfc.noaa.gov/floods/papers/oh\\_2/great.htm](http://www.nwrfc.noaa.gov/floods/papers/oh_2/great.htm), Internet

Radjou, Navi and others. *Adapting to Supply Network Change*, Cambridge: Forrester Research, 2002.

RAND, *Research Brief: Improved Inventory Policy Contributes to Equipment Readiness*, 2001, accessed on 20 January 2003, available from <http://www.rand.org/publications/RB/RB3026/>, Internet.

### **Other Resources**

Anonymous, *Supply Chain Council Operations Reference Model Overview Version 5.0*, Pittsburg: Supply Chain Council, 2002, accessed on 2 December 2002, available from <http://www.supply-chain.org/default.htm>, Internet.