The Cyber Threat to Military Just-In-Time Logistics: Risk Mitigation and the Return to Forward Basing

A Monograph

by

MAJ Sirius T. Bontea
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2017

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
26-05-2017	Monograph	JUN 2016 - MAY 2017

4. TITLE AND SUBTITLE
The Cyber Threat to Military Just-In-Time Logistics: Risk Mitigation and the Return to Forward Basing

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Sirius T. Bontea

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies, Advanced Military Studies Program

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Logistics is an integral part of military operations, especially in the US Army following World War I as armed conflicts required the military to project power overseas over vast distances. Military logisticians in concert with the private sector developed highly efficient logistics operations over the course of the twentieth century. However, the frequency of cyber-attacks on logistics has increased in over the past decade. The move away from the pre-Operation Desert Storm method of forward-based stockpiles to a cost-reducing and more efficient computer-based "just-in-time" logistics model has exposed military logistics to a multitude of risks from cyber-attacks. Operational commanders need to consider these risks in their logistics plans, and in doing so, have opportunities to evaluate methods that can better safeguard their logistics requirements. Ultimately, the reliance on just-in-time logistics needs to be minimized by way of a partial return to forward basing. Forward basing, though more expensive, has advantages such as redundancy, flexibility, and reduced risk to combat operations.

15. SUBJECT TERMS
Logistics, Just-in-Time, Just-in-Case, Stockpile, Cyber, Cyberspace, Russian New Generation Warfare

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			MAJ Sirius T. Bontea
(U)	(U)	(U)	(U)	48	19b. TELEPHONE NUMBER *(Include area code)*

Reset

Monograph Approval Page

Name of Candidate:	MAJ Sirius T. Bontea
Monograph Title:	The Cyber Threat to Military Just-In-Time Logistics: Risk Mitigation and the Return to Forward Basing

Approved by:

_____, Monograph Director
Melissa A. Thomas, JD, PhD

_____, Seminar Leader
Philipp F. Leyde, COL, AR (German Army)

_____, Director, School of Advanced Military Studies
James C. Markert, COL, IN

Accepted this 26th day of May 2017 by:

_____, Director, Graduate Degree Programs
Prisco R. Hernandez, PhD

Abstract

The Cyber Threat to Military Just-In-Time Logistics: Risk Mitigation and the Return to Forward Basing, by MAJ Sirius T. Bontea, U.S. Army, 48 pages.

Logistics is an integral part of military operations, especially in the US Army following World War I as armed conflicts required the military to project power overseas over vast distances. Military logisticians in concert with the private sector developed highly efficient logistics operations over the course of the twentieth century. However, the frequency of cyber-attacks on logistics has increased in over the past decade. The move away from the pre-Operation Desert Storm method of forward-based stockpiles to a cost-reducing and more efficient computer-based "just-in-time" logistics model has exposed military logistics to a multitude of risks from cyber-attacks. Operational commanders need to consider these risks in their logistics plans, and in doing so, have opportunities to evaluate methods that can better safeguard their logistics requirements. Ultimately, the reliance on just-in-time logistics needs to be minimized by way of a partial return to forward basing. Forward basing, though more expensive, has advantages such as redundancy, flexibility, and reduced risk to combat operations.

Contents

Acknowledgement

This study is dedicated to the logisticians who tirelessly work behind the scenes to ensure that our warfighters always have the “beans, bullets, and fuel” that they need to bring the fight to the enemy and safeguard this great nation. I would like to express my sincere gratitude to all the men and women that served in the military since the Revolutionary War. Without the valiant efforts and sacrifices of the patriots that came before us, the current generation of Soldiers, Airmen, Sailors, and Marines would not exist today. A big thanks also goes to the American public for their continued support of the military, for without their support, we could not effectively do what we need to do on an everyday basis.

My gratitude also goes to the professors at the School of Advanced Military Studies. Dr. Thomas Bruscino, Dr. Stephen Lauer, COL Philipp Leyde, Dr. Peter Schifferle, Dr. Bruce Stanley, and Dr. Melissa Thomas who gave me the tools and valuable insight to help me to understand and think critically about the world around me. Your depth of knowledge, expertise, guidance, and genuine care made this project possible. I will carry these lessons with me for the rest of my life.

Most importantly, I want to thank God for blessing me with my wonderful wife, Laura, and my amazing children, Lily and Bear. To my wife and children, thank you for your love and understanding when I had to put in those extra hours of research and writing after hours. You gave me the motivation to work hard and not give up. You continually give me the inner strength to go the extra mile and to keep fighting the good fight. As President Ronald Reagan eloquently stated, “Freedom is a fragile thing and is never more than one generation away from extinction. It is not ours by inheritance; it must be fought for and defended constantly by each generation, for it comes only once to a people. Those who have known freedom, and then lost it, have never known it again.”

Acronyms

ADP	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
AMC	Army Materiel Command
APICS	American Production and Inventory Control Society
BCS3	Battle Command Sustainment Support System
CAISI	Combat Service Support (CSS) Automated Information Systems Interface
CCSS	Commodity Command Standard System
CERT	Computer Emergency Response Team
CI/KR	Critical Infrastructure and Key Resources
COIN	Counterinsurgency
CONEX	Container Express
COTS	Commercial Off-the-Shelf
CMOS	Cargo Movement Operating System
CSS	Combat Service Support
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DODIN	Department of Defense Information Network
DoS	Denial of Service
DTS	Defense Transportation System
E-ISAC	Electricity-Information Sharing and Analysis Center
ERP	Enterprise Resource Planning
FAR	Federal Acquisition Regulation
FM	Field Manual
GAO	Government Accountability Office

GCSS-Army	Global Combat Support System-Army
GFEBS	General Fund Enterprise Business Systems
ICS-CERT	Industrial Control Systems-Cyber Emergency Response Team
IT	Information Technology
JFC	Joint Force Commander
JIC	Just-in-Case
JIT	Just-in-Time
JP	Joint Publication
LMP	Logistics Modernization Program
MAGTF	Marine Air-Ground Task Force
MIT	Massachusetts Institute of Technology
MTS	Movement Tracking System
NOTM	Networking On-The-Move
OPM	Office of Personnel Management
PBUSE	Property Book Unit Supply Enhanced
RNGW	Russian New Generation Warfare
SALE	Single Army Logistics Enterprise
SAMS-E	Standard Army Maintenance System-Enhanced
SARSS	Standard Army Retail Supply System
SAAS-MOD	Standard Army Ammunition System Modernization
SDS	Standard Depot System
SCADA	Supervisory Control and Data Acquisition
SAP	Systems, Applications & Products in Data Processing
SOA	Service-Oriented Architectures
TC-AIMS II	Transportation Coordinators' Automated Information for Movements System II
ULLS-AE	Unit Level Logistics System-Aviation (Enhanced)
USAID	United States Agency for International Development

USMC	United States Marine Corps

Tables

Introduction

> It is no great matter to change tactical plans in a hurry and to send troops off in new directions. But adjusting supply plans to the altered tactical scheme is far more difficult.
>
> —General Walter Bedell Smith, *Chief of Staff, Supreme HQ Allied Expeditionary Force*

Problem Statement

The US military replaced its traditional stockpile-based logistics model to a fully automated demand-driven logistics model. Since 2008, Russia, using Russian New Generation Warfare (RNGW), which emphasizes the use of offensive cyber capabilities, has routinely launched cyber-attacks against its adversaries to disrupt national-level computer networks for extended periods of time. Currently, US logistics systems and sustainment practices are vulnerable and can be severely degraded by cyber-attacks.

Research Question

Given the inherent vulnerabilities of current military logistics systems and the emergence of cyber capabilities in warfare, is the US Army well served by the demand-driven logistics model?

Thesis

The purpose of this monograph is to argue that the US Army needs to conduct a "hybrid" approach to contingency-based sustainment operations by retaining aspects of demand-driven or "Just-in-Time" (JIT) logistics, and bringing back the concept of traditional large inventory or "Just-in-Case" (JIC) logistics to ensure redundancy.[1]

[1] *Merriam-Webster Dictionary*, s.v. "Just-in-Time," accessed August 31, 2016, http://www.merriam-webster.com/dictionary/just-in-time; Investopedia, "Just in Case," accessed November 16, 2016, http://www.investopedia.com/terms/j/jic.asp. Just-in-Time (JIT) is a manufacturing strategy wherein parts are produced or delivered only as needed. Just-in-Case (JIC) is an inventory strategy in which companies keep large inventories on hand. This type of inventory management strategy aims to minimize the

Background

The US Army's JIT logistics are vulnerable to cyber-attacks that could have dire consequences. Many of these vulnerabilities stem from the fact that the system is reliant on computers, network infrastructure, and private sector systems, and software. The software currently in use by the US Army for logistics is maintained by a single private company, and is, therefore, dependent solely on the company's ability to safeguard its overall logistics systems. If the US Army's logistics infrastructure were disrupted, there is no safety net or alternative means to accomplish sustainment operations. For the US Army to ensure a continued state of readiness, a holistic approach to safeguarding its logistics is imperative.

The use of new technologies and methods within the field of logistics has brought forth many advantages. However, the advantages of the shift from JIC to JIT logistics have also introduced potentially catastrophic vulnerabilities to the military supply system. Simultaneously, the emergence of cyber capabilities has now taken a central role in modern warfare. The Russian Federation has already demonstrated its cyber capabilities as both a stand-alone means, and part of a holistic approach to conduct conventional combat operations by fully integrating cyber. The People's Republic of China has also demonstrated its willingness to use its cyber capabilities in a similar fashion. However, this monograph will focus on Russian cyber capabilities over all other nations, including China, because the Russian use of offensive cyber capabilities has been underway for over a decade. In comparison, China's use of cyber is comparatively immature. As a contingency-based force, the US Army relies heavily on its ability to conduct long-range sustainment operations. Any large-scale disruption in the US Army's ability to supply and equip the force could potentially cripple its capacity to conduct overseas combat operations. However,

probability that a product will sell out of stock. A company practicing this strategy essentially incurs higher inventory holding costs in return for a reduction in the number of sales lost due to sold out inventory.

the many weaknesses of JIT logistics model can be mitigated by returning to the traditional method of forward-based stockpiles.

By using historical examples of how RNGW is applied, this monograph intends to link the following concepts together to advocate for a partial return to traditional forward-basing: JIC logistics for redundancy, JIT logistics for cost-savings, cyber vulnerability mitigation to logistics systems, and modular CONEX configurations that combine JIC and JIT logistics principles. Additionally, there are key questions that affect implementation and transition to a "hybrid" logistics model. What are the current means available to operational level commanders to safeguard military logistics from attacks from the cyber domain? How effective are these means and what possible shortfalls are associated with the present methods employed to protect sustainment systems? Are there any secondary or tertiary effects or risks involved with making changes? What are the opportunities that can potentially surface from attempting to tackle these questions? The tension between cost, efficiency, and capability of projecting military force requires a discourse between operational commanders, strategic policy makers, and the operational artist to chart possible options and opportunities with making changes to the current system, all the while being keenly aware of the risks involved.

In summary, this monograph will advocate for a "hybrid" approach or partial return to traditional forward basing by answering the before-mentioned questions. Recommendations and conclusions will be based on the analysis of similar systems and in certain cases identical systems, within the private sector as well as within the Department of Defense (DOD), Department of Homeland Security (DHS), and Department of Commerce (DOC). Additionally, understanding some of the risks involved in both JIC and JIT logistics models can provide commanders with a framework to evaluate methods to safeguard logistics and to use lessons from the past to augment modern methods and as such, maintain a continued position of advantage. By addressing risk and opportunity, and by answering some key questions regarding cyberspace and military logistics, this

monograph will attempt to creatively respond to the challenges inherent in the modern system as well as the emerging threat of cyber warfare.

The Doctrine of Russian New Generation Warfare (RNGW)

At the heart of RNGW doctrine, the population is the center of gravity in all aspects of war.[2] This mindset is as true to the Russians today as it was to military theorists, such as Sun Tzu and Carl von Clausewitz. On making assessments of the population, Sun Tzu said, "The way (tao) is what brings the thinking of the people in line with their superiors. Hence, you can send them to their deaths or let them live, and they will have no misgivings one way or another."[3] Sun Tzu makes it clear that the population is at the center, and the way to be successful is for political leaders to have popular support and legitimization in the conduct of war. Carl von Clausewitz extends this concept to advocate for attacking the enemy's population for the "duration of the war to bring about a gradual exhaustion of his physical and moral resistance."[4] Similarly, US counterinsurgency (COIN) doctrine places the population at the center of military efforts. US COIN doctrine also stresses that "insurgents often try to use the local narrative to gain popular support and recruits for their cause," and that "insurgent groups adopt an irregular approach because they initially lack the resources required to directly confront the incumbent government in traditional warfare."[5] RNGW doctrine shares this understanding and seeks to gain victory through

[2] Nicholas Fedyk, "Russian 'New Generation' Warfare: Theory, Practice, and Lessons for U.S. Strategists," *Small Wars Journal* (August 25, 2016): 2.

[3] Sunzi, and Roger T. Ames, *Sun-Tzu: The Art of Warfare – the First English Translation Incorporating the Recently Discovered Yin-Ch'üeh-Shan Texts* (New York, NY: Ballantine Books, 1993), 103.

[4] Carl von Clausewitz, *On War, Indexed Edition*, trans. Michael Eliot Howard and Peter Paret, reprint edition (Princeton, NJ: Princeton University Press, 1989), 93.

[5] Joint Publication (JP) 3-24, *Counterinsurgency* (Washington, DC: Government Printing Office, 2013), x.

unconventional, psychological, and information warfare. The following table illustrates the differences between Russia's military traditional doctrine and RNGW doctrine:[6]

Table 1. Changes in the Character of Armed Conflict According to General Valery Gerasimov, Chief of the Russian General Staff

Traditional Military Methods	New Military Methods
• Military action starts after strategic deployment (declaration of war). • Frontal clashes between large units consisting mostly of ground units. • Defeat of manpower, firepower, taking control of regions and borders to gain territorial control. • Destruction of economic power and territorial annexation. • Combat operations on land, air and sea. • Management of troops by rigid hierarchy and governance.	• Military action starts by groups of troops during peacetime (war is not declared at all). • Non-contact clashes between highly maneuverable interspecific fighting groups. • Annihilation of the enemy's military and economic power by short-time precise strikes in strategic military and civilian infrastructure. • Massive use of high-precision weapons and special operations, robotics, and weapons that use new physical principles (direct-energy weapons – lasers, shortwave radiation, etc.) • Use of armed civilians (4 civilians to 1 military). • Simultaneous strike on the enemy's units and facilities in all of the territory. • Simultaneous battle on land, air, sea, and in the informational space. • Use of asymmetric and indirect methods. • Management of troops in a unified informational sphere.

Source: Jānis Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (Riga, Latvia: National Defence Academy of Latvia - Center for Security and Strategic Research, April 2014), 4, accessed March 23, 2017, http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx.

Many doctrinal principles of RNGW were applied directly to the recent conflicts in Estonia, Georgia, and the Ukraine. Furthermore, the indirect nature of RNGW fully exploits the use of cyber capabilities to disable computer networks critical to military logistics. By adopting an irregular approach, Russia is also able to cause significant harm against its enemies without the need to expend substantial resources.

[6] Jānis Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (Riga, Latvia: National Defence Academy of Latvia - Center for Security and Strategic Research, April 2014), 4, accessed March 23, 2017, http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx.

According to Dr. Phillip Karber, RNGW "differs from Western views of hybrid warfare—a blend of conventional, irregular and cyber warfare—in that it combines both low-end hidden state involvement with high-end direct, even braggadocio, superpower involvement."[7] Dr. Karber further distills the RNGW doctrine codified by the Chief of the Russian General Staff into five distinct elements which are political subversion, proxy sanctuary, intervention, coercive deterrence, and negotiated manipulation. Of the five, political subversion and proxy sanctuary employ cyber capabilities to conduct classic "agitprop"[8] information operations and to disrupt and manipulate the flow of information.[9]

RNGW demonstrates the capabilities of cyber-attacks when used in conjunction with conventional military land forces to cripple modern logistics infrastructure preemptively. This new approach to warfare is a holistic approach that incorporates the use of modern technology as well as conventional and covert military forces. From a logistics standpoint, Russia's approach centers on the disruption of its opponent's internal capabilities and systems through the use of a robust cyber-warfare capability.[10] Through cyber-attacks, Russia establishes a de facto "blockade" against its opponents by attacking financial and other capabilities critical to modern sustainment operations. By degrading its enemy's ability to conduct sustainment operations, the flow of

[7] Phillip A. Karber, "Russia's 'New Generation Warfare,'" *National Geospatial-Intelligence Agency*, last modified June 4, 2015, accessed March 23, 2017, https://www.nga.mil/MediaRoom/News/Pages/Russia's-'New-Generation-Warfare'.aspx.

[8] Encyclopædia Britannica, s.v. "Agitprop | Soviet History," accessed March 23, 2017, https://www.britannica.com/topic/agitprop. "Agitprop," abbreviated from Russian "agitatsiya propaganda" (agitation propaganda), is the political strategy in which the techniques of agitation and propaganda are used to influence and mobilize public opinion.

[9] Karber.

[10] Jānis Bērziņš, "The New Generation of Russian Warfare," *The Potomac Foundation*, last modified October 11, 2016, accessed December 20, 2016, http://www.thepotomacfoundation.org/the-new-generation-of-russian-warfare/.

supplies and other computer-based logistics transactions are adversely affected which ultimately hamstrings its enemy's ability to conduct combat operations.[11]

The application of RNGW doctrine has grown over time, reaching its highest point with Russian military intervention within the Ukraine. Russia's war with the Ukraine since 2014 "has moved its evolving operational concepts out of the realm of theory into a brutal practice."[12] The effectiveness of Russia's indirect approach was exemplified by the unprecedented shutdown of the Ukrainian power grid in 2015 by way of cyber-attacks.[13] The US military's doctrine on cyberspace operations acknowledges the potential problems inherent in legacy sustainment systems due to outdated hardware and software.[14] Needless to say, cyber-attacks also pose a clear and present danger to military logistics, especially as many of the legacy systems used by the US Army share similar vulnerabilities.

What is Traditional Forward-Based or "Just-in-Case" Logistics?

Traditional forward-based logistics, often referred to as JIC logistics, is the method of stockpiling supplies and equipment in anticipation of "unforeseen requirements, changing missions, enemy interdiction, and the unpredictability of war."[15] Supplies were prepositioned at the theater level and made readily available to lower echelons down to the company level. This method, often referred to as "stockage," is defined as "the amount of military supplies and

---

[11] Alison Lawlor Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 63–64, accessed December 22, 2016, http://public.eblib.com/choice/publicfullrecord.aspx?p=1810129.

[12] Ibid.

[13] E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Electricity-Information Sharing and Analysis Center, March 18, 2016), iv, accessed March 22, 2017,https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[14] Joint Publication No. 3-12R, *Cyberspace Operations* (Washington, DC: Government Printing Office, 2013), II-11.

[15] Mark E. Solseth, "Distribution and Supply Chain Management: Educating the Army Officer" (Monograph, School of Advanced Military Studies, 2005), 6.

equipment on hand or scheduled to be on hand in controlled quantities in a given place," and was the traditional way of stockpiling supplies and equipment in anticipation of non-specific needs.[16] The purpose of this system was to minimize the length of time required to provide supplies and equipment when needed, and to "create a 'just-in-case' buffer to mitigate risk."[17] Stockage, as an inventory management strategy, incurs higher costs due to storage requirements and the potential for waste if supplies are not used.[18]

Forward-basing was one of the standard means that warfighters, throughout history, planned for anticipated combat operations. Logistics is at the heart of any military operation that requires the projection of military forces, equipment, and supplies over great distances. Throughout history, logistics often dictated the success or failure of not just battles, but also military campaigns. The geography of the United States has routinely forced military commanders to rely on the ability of their logisticians to stretch their supply lines across vast oceans.[19] US military logistics since World War I to present-day conflicts has evolved as new techniques, methods, and technology developed. As technology advanced, so did the volume of supplies and speed of delivery that JIC logistics provided to the theaters in World War II, Korea, and Vietnam.[20] JIC logistics aims to ensure the availability of supplies and equipment, "regardless of the cost or the need for an item of supply."[21] However, the 1991 Persian Gulf War, although

---

[16] *Merriam-Webster Dictionary*, s.v. "Stockage," accessed September 4, 2016, http://www.merriam-webster.com/dictionary/stockage.

[17] Solseth, 6.

[18] Investopedia, "Just In Case – JIC."

[19] Jakub J. Grygiel, *Great Powers and Geopolitical Change* (Baltimore, MD: Johns Hopkins University Press, 2011), 171.

[20] Solseth, 6.

[21] Joseph L. Walden, "Applying Just-In-Time To Army Operations" (Monograph, School of Advanced Military Studies, 2000), 1.

highly successful militarily, revealed massive forward-based stockage to be unreliable, inefficient, and very expensive.[22]

In modern times, military campaign successes and failures are often directly tied to the success or failure of logistics. Logistics has always been a fundamental prerequisite for the United States for waging wars that require the ability to project military force across the oceans. Technology and the presence of a powerful navy enabled US forces to extend supply lines without having the same kinds of risks seen in the past. With the ability to maintain extended supply lines, came the ability to extend *operational reach,* which Joint doctrine defines as "the distance and duration across which a joint force can successfully employ military capabilities."[23] Echoing the verse from George M. Cohen's hit song from World War I, large-scale American wars have always been "over there" from 1917 onwards.[24]

Operational reach is a key strength of the US military, but reliance on the ability to project and sustain military power over long distances can also be a critical vulnerability if not adequately safeguarded. The US Army used to do its supply by way of JIC logistics for all conflicts including and prior Operation Desert Storm. JIC logistics allows the US Army to bring to bear the maximum amount of supplies and equipment into a theater, but it is costly. Modern technology and methods can enable JIC logistics to be used in conjunction with JIT to provide maximum throughput of supplies and equipment into a theater of operations.

---

[22] Solseth, 6-7.

[23] Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Government Printing Office, 2011), GL-15.

[24] George M. Cohan, "Over There: Sheet Music," *Ball State University Digital Media Repository*, accessed November 14, 2016, http://libx.bsu.edu/cdm/ref/collection/ShtMus/id/1273; Peter J. Schifferle, "Evolution of Operational Art - Lesson 16: Joint Operations and the Tenuous End of the Rope: Guadalcanal, 1942" (School of Advanced Military Studies, Fort Leavenworth, KS, October 18, 2016).

What is Demand-Driven or "Just-in-Time" Logistics?

For the US military, demand-driven or JIT logistics is a supply chain model that minimizes the presence of large stockpiles by managing the flow of supplies and equipment by forecasting requirements, and pushing materiel to the end user on a by-need basis.[25] The American Production and Inventory Control Society (APICS) defines JIT as:

> A philosophy of manufacturing based on planned elimination of all waste and on continuous improvement of productivity. It also has been described as an approach with the objective of producing the right part in the right place at the right time (in other words, "just in time").[26]

Additionally, smaller inventories are much easier moved from point A to point B, and the overall flow is much faster than moving large stockpiles. Central to JIT logistics, is an efficient distribution system that differs from forward-basing, where "velocity offsets mass, as echelons of inventory are replaced by managed flows of materiel. . . . The distribution pipeline effectively becomes the . . . warehouse."[27] The speed gained by this process is attractive to military planners.

The JIT method of distribution is accomplished through the use of automated computer systems and database software. When used by manufacturers and other industries, inventory is tracked along all stages in the production chain by automated systems. The goal of avoiding inventory accumulation occurs throughout the manufacturing process. The philosophy behind JIT methodology is "doing only what is necessary when it is necessary and in with the amount that is necessary."[28] This occurs prior to production stage, to avoid an "accumulation of inventory or unfinished products," and after a production stage in order to avoid "delays in serving customers

---

[25] Investopedia, "Just In Time."

[26] APICS Forum, "Just-in-Time Manufacturing," last modified February 8, 2012, accessed March 22, 2017, http://www.apicsforum.com/ebook/10._just-in-time_manufacturing.

[27] Mark O'Konski, "Revolution in Military Logistics: An Overview," *Army Logistician* 31, no. 1 (February 1999): 11, accessed March 21, 2017, http://www.alu.army.mil/alog/1999/janfeb99/pdf/janfeb1999.pdf.

[28] ATOX Sistemas de Almacenaje, "Just-in-Time (JIT) Logistics," last modified July 7, 2015, accessed March 21, 2017, http://www.atoxgrupo.com/website/en/news/just-in-time-logistics.

and the corresponding increase in their dissatisfaction."[29] Parts are ordered or manufactured on a by-need basis with the goal of "eliminating all waste."[30] Furthermore, JIT processes strive to reduce waste by eliminating all tasks that "do not contribute any value to the manufactured product or service."[31] The financial benefit and the reduction in waste from using JIT is what drove the military to adopt this method for logistics.[32] However, the use of automated computer systems and database software is vulnerable to cyber-attacks. US military commanders are already acutely aware of the risks to their computer systems from cyber-attacks from sources such as cyber-terrorists, state-sponsored cyber units, and lone wolf actors.[33]

The Evolution of Military Logistics

> Victory is the beautiful, bright-colored flower. Transport is the stem without which it could never have blossomed.
>
> —Winston Churchill, *The River War, 1899*

The Role of the CONEX Box in Operation Desert Storm

The CONEX, short for "Container Express" emerged in its most rudimentary form in 1948 and underwent continuous refinement and standardization over the years. CONEX boxes are prevalent throughout both commercial and military as the primary means of transporting goods or equipment. Prior to and including Operation Desert Storm, JIC logistics operations used CONEX boxes as its primary means to forward stage large stockpiles of military hardware and supplies for future use. However, military sustainment operations following Operation Desert Storm shifted

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] O'Konski, "Revolution in Military Logistics: An Overview," 10.

[33] Patrick M. Duggan, "U.S. Special Operations Forces in Cyberspace," *The Cyber Defense Review* 1, no. 2 (Fall 2016): 73, accessed January 31, 2017, http://www.cyberdefense review.org/wp-content/uploads/2017/01/CDR-FALL2016.pdf.

almost entirely to a JIT logistics model.[34] By 1990, the lessons learned from Vietnam were used in conjunction with modern computing technology to enhance the ability of the United States to move massive stockpiles of military hardware into Saudi Arabia in anticipation of armed conflict with Iraq. Operation Desert Storm represents the last time the United States projected huge stocks of equipment and supplies into a theater of operations.

Since 1991, the US military logistics model shifted from large forward-based stockpiles to the demand-based model in use by the private sector. This was in direct response to what was seen as excess waste and inefficiency during Operation Desert Storm. After the completion of ground combat operations a mere seven weeks later and soldiers were returning to their home stations, there were "over 27,000 containers on the ground and unopened" and "more than two years of ammunition supplies stored in theater at the completion of the ground war."[35] With this revelation, it was relatively easy to advocate for adopting JIT over JIC. However, with constrained budgets and a push for cost savings, the push towards JIT logistics was the way for military logisticians to meet this requirement.

US military JIT logistics experienced approximately a quarter century of refinement and growth. JIT logistics is largely based on integrated systems of modern computers and database software that tie manufacturers to supply depots and distribution points, all the way to the end user. The unintended side effect of moving away from a model of massive pre-positioned stockpiles is that these systems are susceptible to cyber-attacks. Many of these logistics systems directly mirror their private-sector counterparts. Furthermore, changes in the patterns of manufacturing and trade due to globalization are partially responsible for the shift away from traditional forward-based

[34] Laurel K. Myers, "Eliminating the Iron Mountain," *Army Logistician* 36, no. 4 (August 7, 2004): 40.

[35] Walden, "Applying Just-In-Time To Army Operations," 1.

logistics to an almost entirely JIT logistics model. This aspect of globalization and reduced defense spending since 1991 necessitated moving to the JIT logistics model.

The ability to transport massive quantities of supplies in a manner that can be preconfigured by units before deploying into a war zone was a strength for the US military during Vietnam. The methods were refined throughout the Vietnam War, and further set the stage for the large-scale conflict in the Persian Gulf only a decade and a half later. By the time Operation Desert Storm commenced in 1991, nearly all commercial fleets had used standardized containers and procedures. This fact, coupled with a robust defense budget, ensured that there was little to get in the way of the US Army's ability to stage massive stockpiles of supplies and equipment in Saudi Arabia and Kuwait in preparation for combat operations.

The establishment of massive stockpiles during Operation Desert Storm was an example of the same concept of logistics management that has been in use since World War I. The modern term, JIC logistics, is nothing new for the military. However, this method has been in decline within the private sector for decades before the US Army's shift away from JIC logistics. The JIC inventory strategy used by private sector businesses involves keeping large quantities of inventory on-hand to minimize the probability that a particular product will be sold out. One of the downsides to this strategy is an increase in various costs in its attempt to offset the loss of sales revenue from sold-out or unavailable stock.[36] Ancillary costs associated with retaining large quantities of stock on-hand may include damaged or spoiled goods, storage or warehouse space, labor, utilities, and security.[37]

System redundancy and forward-deployed supply stockpiles are becoming more cost prohibitive given the current trend toward reducing budgets and increasing efficiency. Operation

[36] Investopedia, "Just In Case."

[37] Investopedia, "Holding Costs," accessed October 13, 2016, http://www.investopedia.com/terms/h/holding-costs.asp.

Desert Storm's large-scale use of forward-deployed supplies, the so-called "iron mountains" staged in Kuwait and Saudi Arabia were the result of the Army's traditional approach to mass-based logistics in anticipation of future mission requirements. This scale of supply distribution has not been seen since 1991 as post-Gulf War defense budgets ultimately forced military logisticians to adopt less expensive methods. However, the ability to surge supplies to the front lines to meet requirements for future combat operations remains.

Modular CONEX Boxes for Scalability and Flexibility

Currently, modular CONEX box-based command and control systems are an effective method to balance cost with scalability. The United States Marine Corps (USMC) is at the forefront of experimenting with modular command and control systems. For example, one of the key aspects of the Networking On-The-Move (NOTM) command and control system in use by the USMC is that it is a highly mobile system that fully integrates all elements and capabilities of the Marine Air-Ground Task Force (MAGTF) while remaining truly modular.[38] The effectiveness of the USMC to project force is inherently tied to its ability to maximize the use of limited shipborne cargo space.

The US Army understands the requirement for maximizing use of space when it comes to both strategic airlift and sealift capabilities. This understanding is codified in the US Army's Field Manual (FM) No. 55-80 *Army Container Operations* with the following:

> The transition to a CONUS-based, power projection force increases the need for the Army to be able to rapidly deploy anywhere, anytime. Strategic lift must be maximized to rapidly project power to meet our force projection goals. Strategic lift is supplied by either ocean-going vessels or air transport. Both are limited resources. Having the largest requirement for strategic lift demands that the Army maximize its use of containerization. Containerization increases the types of ships available to support strategic deployment as well as increasing the cargo capacity of other available ships. It also streamlines handling

[38] US Marine Corps Concepts and Programs, "Networking On-The-Move (NOTM)," last modified January 13, 2017, accessed March 14, 2017, https://marinecorpsconceptsandprograms.com/programs/command-and-controlsituational-awareness-c2sa/networking-move-notm.

> requirements within the distribution system. Other added bonuses of containerization are increased protection against shipping damage and safeguards against pilferage.[39]

FM 55-80 goes on to further state that the responsibility within the Defense Transportation System (DTS) is to provide oversight for the employment of containerized systems for joint force. The US Army's stated goal is to have a logistics system that "will meet DOD-wide transportation requirements and result in a fleet of containers designed for common-use among the Services."[40] Additionally, the US Army seeks to further increase container usage in order to improve the efficiency of strategic airlift as well as improve battlefield materiel distribution and field warehousing capabilities.[41]

Preconfigured systems using the CONEX box can provide a level of modularity that enables increased flexibility and the scalability of options for the operational commander. The method using pre-configured CONEX boxes, for use as maintenance shops and offices, was employed in a crude manner during combat operations in Vietnam. However, the overall concept of using pre-configured CONEX boxes is viable if refined and properly planned.[42] Various entrepreneurs have centered their business models on providing customizable solutions for customers using CONEX boxes as mobile workshops and field offices. However, this only addresses part of the solution. Adding more CONEX boxes of a particular configuration is not necessarily sufficient to meet the needs of the warfighter. The military needs to take this one step further by planning for a CONEX box-based system that is scalable and flexible. Ideally, such a system would consist of a relatively small number of pre-configured CONEX boxes that are forward-staged in areas with ongoing combat operations or where conflict is anticipated to occur.

---

[39] Field Manual (FM) 55-80, *Army Container Operations* (Washington, DC: Government Printing Office, 1997), 1–1.

[40] Ibid.

[41] Ibid.

[42] Peppers, 241.

This system needs to be complemented by forward-staged equipment and supplies centered on the concept of modularity and flexibility.

Just-in-Time Logistics

Military Sustainment Operations Following Operation Desert Storm

With regard to human resources and money, the benefits of JIT logistics are significant cost savings. These commercial advantages, not without applicability to their military counterpart, gained support within the DOD as budgets and resources decreased following the Gulf War. However, the computer systems that enable JIT logistics to function are vulnerable to cyber-attacks. First, these systems are located on unclassified networks that are more susceptible to compromise due to their exposure to the Internet when compared to a closed network. Second, the multitude of subsystems that enable JIT logistics is now tied to a centralized database run by a single civilian company. One company being solely responsible for US Army-wide logistics presents a risk of being a single point of failure if the centralized database is compromised. Third, the rapid fabrication of military hardware components by way of additive manufacturing, also known as 3D printing technology, will increase as opposed to having stock on hand due to cost savings. The National Institute for Standards and Technology identified several cyber-related threats to additive manufacturing processes to include software alteration and network disruption.[43]

Logisticians in the DOD met this challenge by standardizing commercial and military logistics metrics and equipment and using real-time stockage information. Standardization improved interoperability between military and commercial equipment and transport. Stockage

[43] Kelley Dempsey and Celia Paulsen, "Risk Management for Replication Devices" (US Department of Commerce, National Institute for Standards and Technology, February 2015), accessed September 4, 2016, http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8023.pdf.

defined as “the amount of military supplies and equipment on hand or scheduled to be on hand in controlled quantities in a given place,” was beginning to be tracked in real-time by way of computer systems and databases.[44] This methodology was modeled after the private sector as it provided cost savings from inventory reduction, leveraging of technology, and the joint use of public assets by the military.[45]

The increase in the use of JIT logistics is juxtaposed against an upward trend in cyber-attacks that specifically target logistics computer systems. Many targeted attacks against both the private sector as well as systems used by the DOD have a level of sophistication that seemed to indicate that they are state-sponsored. Because of these concerns, it is important to explore the possible means that commanders can employ to reduce risk. This inquiry applies to possible changes to the supply model employed, or if changes cannot be made at the operational level, then it is necessary to explore means for commanders to reduce overall risk.

The Impact of Globalization on Military Logistics

JIT logistics, though relatively modern, can be traced back to the 1950s. The JIT logistics model, defined as “a manufacturing strategy wherein parts are produced or delivered only as needed” has many advantages, with cost savings being the primary reason for its adoption by the private sector.[46] One of the first examples comes from Mattel Corporation’s Barbie dolls which relied on a supply chain that was made possible through the efficiency of the standardized shipping containers discussed in the previously.[47] Various components for manufacturing came from all

---

[44] *Merriam-Webster Dictionary*, s.v. “*Stockage*,” accessed September 4, 2016, http://www.merriam-webster.com/dictionary/stockage.

[45] Kristine Lee Leiphart, “Creating a Military Supply Chain Management Model,” *Army Logistician* 33, no. 4 (August 7, 2001): 36.

[46] *Merriam-Webster Dictionary*, s.v. “Just-in-Time,” accessed August 31, 2016, http://www.merriam-webster.com/dictionary/just-in-time.

[47] Levinson, *The Box*, 265.

over the globe in an intertwined and time sensitive network of supply and production. The body was built in China with plastics from Taiwan, using American molds. Machines in the actual manufacturing process originated in Europe and Japan. Clothing fabric from China used pigments that came from America.[48] The overall process was made possible by the efficiency and low-cost of shipping.

Another corporation that took full advantage of the JIT supply model was Toyota Corporation, which by the early 1980s, perfected its ability to implement JIT logistics and reduce its overhead costs by eliminating the need for large inventories.[49] "Before the 1980s, logistics was a military term. By 1985, logistics management—the task of scheduling production, storage, transportation, and delivery—had become a routine business function."[50] As military logistics became increasingly intertwined with commercial shipping, JIT logistics became an integral part of the US Army's supply model and its ability to preposition stock, essentially using JIT to enhance JIC.

Aside from commercial gains from the JIT logistical model, globalization of markets further increased the interdependence of resources from outside of national borders. Not taking into account financial costs, the plastics, dyes, and textiles in the above Barbie doll example could theoretically be produced by Mattel domestically, thereby eliminating dependency on foreign-produced components. Domestic self-sufficiency is an attractive concept if applied to military hardware. Not having to rely on outside resources during a time of war could potentially alleviate problems that may arise from disrupted supply lines or halted component manufacturing in foreign countries.

---

[48] Ibid.

[49] Ibid.

[50] Ibid., 266.

However romantic the notion of having a completely self-reliant military logistics infrastructure and domestically produced hardware, it is simply not realistic. Production of modern electronics in today's society would not just be financially crippling to manufacture without external resources but is in essence, an impossibility. Massachusetts Institute of Technology's (MIT) assessment of the possibility of producing an "All-American iPhone" demonstrates that domestically produced high-end electronics is not feasible without external resources.[51] Suppliers for iPhone components come from twenty-eight different countries.[52] The unfeasibility is not just for components alone, but the raw materials themselves that go into the manufacturing of electronics are simply not available in sufficient quantities to be mined and extracted from US soil.[53] Rare earths, such as neodymium, lanthanum, and hafnium are metals increasingly critical for high-tech as well as for military applications.[54] In light of this, the concept of a domestically self-reliant military is not possible even if the budget variable is removed from the equation.

The interconnected and interdependent nature of global commerce can impact military operations if not considered in its proper context. Understanding the reality of globalization and how it affects military operations is important for any commander who engages in discourse at the strategic level, be it with domestic, coalition partners, or foreign actors. Though much of this interaction occurs at the strategic level, and therefore beyond the scope of most JFCs, it is nevertheless an important part of understanding the operational environment. For example, there are potential long-term implications, especially when considering the effect of sanctions or trade

[51] Konstantin Kakaes, "Making iPhones in the U.S. Might Not Cost as Much as You'd Think," *MIT Technology Review*, accessed December 1, 2016, https://www.technologyreview.com/s/601491/the-all-american-iphone/.

[52] Ibid.

[53] Ibid.

[54] David S. Abraham, *The Elements of Power: Gadgets, Guns, and the Struggle for a Sustainable Future in the Rare Metal Age* (New Haven: Yale University Press, 2015), xiv.

embargoes. Though the United States generally is not on the receiving end of these kinds of measures, sanctions on foreign nations can adversely affect any existing logistics infrastructure a JFC might consider using for combat operations. The degraded logistics infrastructure in Iran, following nearly forty years of economic sanctions, is a clear example of possible effects.[55]

Logistics Vulnerabilities

> The single biggest existential threat that's out there, I think, is cyber. I think we're going to have to focus a lot more on it. We're going to have to put more resources against it. We're going to have to train people better. Because cyber actually, more than theoretically, can attack our infrastructure, our financial systems, etc. It's a space that has no boundaries. It has no rules, and there are people who are very good at it. There are countries who are very good at it.
>
> —Adm. Michael Mullen, Chairman of Joint Chiefs of Staff

The Private Sector's Link to Military Logistics Vulnerabilities

The threat of cyber-attacks against private sector JIT logistics has revealed many of the same potential shortfalls in its military counterpart. In 2014, malware dubbed "Zombie Zero" was introduced into the embedded software of barcode scanners in order to extract financial information and communicate with an external command and control server.[56] This is just one small example of possible risks. In addition to the overlap of military and commercial supply chain methodology and interaction, military logisticians use many of the same Commercial Off-the-Shelf (COTS) equipment. The Federal Acquisition Regulation (FAR) defines COTS as "items offered to the government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace."[57] The risks that private industries

---

[55] Randy Woods, "The Iranian Conundrum: How Sanctions Removal Affects Global Logistics | Air Cargo World," *Air Cargo World*, last modified April 6, 2016, accessed December 1, 2016, http://aircargoworld.com/the-iranian-conundrum-how-sanctions-removal-affects-global-logistics/.

[56] John P. Mello, Jr., "Windows XP Hacked, Supply Chain Poisoned," *Tech News World*, July 16, 2014, accessed September 4, 2016, http://www.technewsworld.com/story/80742.html.

[57] Title 48 Federal Acquisition Regulation System, "Federal Acquisition Regulation," March 2005,

face from cyber-attacks have a direct correlation to their military counterpart, as the equipment itself is required to be unmodified and identical to the civilian version.

Germany-based multinational software company, Systems, Applications & Products in Data Processing (SAP), produces Enterprise Resource Planning (ERP) software for sectors including manufacturing, government, energy, telecommunications, finance, as well as defense.[58] For the US Army, this is especially relevant because the Global Combat Support System-Army (GCSS-Army) runs exclusively on SAP's ERP software for a multitude of functions such as maintenance tracking, supply and equipment tracking, and financial transactions across all military echelons.[59] SAP is a multi-billion dollar company with 345,000 customers in 190 countries, which includes 87 percent of the Forbes Global 2000.[60] This is also relevant for the military in general, due to the fact that all high-end hardware and equipment are produced by the private sector. Though SAP software provides robust security capabilities across the above-mentioned industries and builds critical software patches for their user base on a monthly basis, it is not invulnerable to cyber-attacks.[61]

Business application security provider, ERPScan, provides annual reports on SAP vulnerabilities that have shown an upward trend in cyber-attacks across all industries using SAP enterprise software. SAP routinely produces "several internal advisories called SAP Security Notes

---

accessed September 4, 2016, https://www.acquisition.gov/sites/default/files/current/far/pdf/FAR.pdf.

[58] SAP, "Military, Security & Defense: Industry Software," accessed January 31, 2017, http://www.sap.com/solution/industry/defense-security.html. SAP is also written as "Systeme, Anwendungen und Produkte in der Datenverarbeitung".

[59] GCSS-Army, "Global Combat Support System-Army - System Description," accessed December 28, 2016, http://gcss.army.mil/About/SystemDescription.aspx.

[60] SAP, "SAP Company Information: About SAP," accessed December 28, 2016, http://www.sap.com/corporate/en/company.html.

[61] Mathieu Geli, Darya Maenkova, and Alexander Polyakov, *SAP Cyber Security in Figures (Global Threat Report) 2016* (ERPScan, n.d.), 18, accessed December 28, 2016, https://erpscan.com/wp-content/uploads/publications/Sap-Cyber-Threat-Report.pdf.

to fix security issues, which are often reported by external researchers."[62] Though ERPScan or SAP does not publish specific vulnerabilities to the general public, an inference can be made as to its relevance to GCSS-Army.

The US Government Accountability Office (GAO) findings revealed a multitude of cyber vulnerabilities in logistics systems across all sectors of government, including the US military. In a report in March 2012, the GAO's analysis of unclassified governmental and nongovernmental data identified the following threats to the IT supply chain:

> The installation of malicious logic on hardware or software, installation of counterfeit hardware or software, failure or disruption in the production or distribution of a critical product or service, reliance upon a malicious or unqualified service-provider for the performance of technical services, and the installation of unintentional vulnerabilities on hardware or software.[63]

Keeping up with the pace of innovation is challenging enough in itself for any large organizations such as the DOD. The 2012 GAO report also notes that many of the risks arise from a "reliance on a global supply chain" which provides an avenue for malicious actors such as "foreign intelligence services or counterfeiters—who may exploit vulnerabilities in the supply chain, thus compromising the confidentiality, integrity, or availability of the end-system and the information it contains."[64]

In 2010, Carnegie Mellon University's Software Engineering Institute produced a report about the DOD's supply chain vulnerabilities. The report identified several inherent risks with the use of COTS equipment, especially with the use of newer technologies such as "web services or design patterns including service-oriented architectures (SOAs)."[65] The primary reason behind the

---

[62] Ibid.

[63] Gregory C. Wilshusen, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks* (Washington, DC: US Government Accountability Office, March 2012).

[64] Ibid., 11.

[65] Robert J. Ellison et al., *Evaluating and Mitigating Software Supply Chain Security Risks* (Carnegie Mellon University: Software Engineering Institute, May 2010), 10, accessed March 16, 2017, http://resources.sei.cmu.edu/asset_files/technicalnote/2010_004_001_15176.pdf.

increased risk associated with newer technology is that it has "a short history of known attack patterns and a relatively short list of known coding and design weaknesses compared to more mature technologies."[66] Furthermore, the report also revealed that newer COTS tools used to generate code and develop software applications for use in the DOD's IT supply chain security have vulnerabilities that are difficult to isolate.[67]

The Carnegie Mellon report also revealed that the responsibility for creating software patches for COTS software development tools remained with the civilian contractor. A concern was also raised in the report regarding software quality control, specifically stating that there was "no indication that a continuing review of potential security or supply chain concerns" were conducted because software creation tools were outside the scope of the contracts.[68] Furthermore, there were no established criteria or plans for evaluation of this risk. Exacerbating this problem is the fact that contractors and subcontractors compete directly for government contracts and were reluctant to the share information regarding vulnerabilities with each other. It remains unclear how well vulnerabilities are reported, despite the legal requirement to do so.[69] Though external and independent quality control audits are designed to evaluate any potential software issues, "interviews indicate that Quality Control personnel do not have the knowledge to cover everything."[70]

Newer COTS software and equipment have vulnerabilities, but older legacy software is not without shortfalls. Legacy logistics systems throughout the DOD continue to be on an ongoing challenge for logisticians and cyber security specialists. The 2009 version of Army's FM 4-0

---

[66] Ibid.

[67] Ibid., 30.

[68] Ibid.

[69] Ibid.

[70] Ellison et al.

Sustainment lists various computer and database systems that perform various functions that enable military logistics to take place behind the scenes.[71] In 2012, ADRP 4-0 replaced FM 4-0 and removed the list of logistics systems from the appendix. This is not to imply that these systems no longer exist, but is rather a reflection of the fact that the Army and the DOD, as a whole, were and still are in the process of migrating these legacy systems under the umbrella of GCSS-Army. By definition, GCSS-Army was designed to replace a "variety of legacy tactical-level logistics information systems and automated capabilities such as the Standard Army Retail Supply System (SARSS), the Standard Army Maintenance System-Enhanced (SAMS-E), Unit Level Logistics System-Aviation (Enhanced) (ULLS-AE), and the Property Book Unit Supply Enhanced (PBUSE)."[72] These legacy logistics systems are still in use as of 2017. Furthermore, this list is not a comprehensive list of legacy systems currently in use by the DOD within the field of logistics alone. Joint doctrine acknowledges the challenges this poses in trying to safeguard these systems, especially when it comes to logistics.

There are inherent challenges with modernizing integrated systems, especially within military logistics. JP 3-12R's section on sustainment, mentions that JFCs must not only identify critical cyberspace assets, but must also detect system redundancy, "including non-cyberspace alternatives, and actively exercise continuity of operations plans to respond to outages or adversary actions that degrade or compromise cyberspace access or reliability."[73] JP 3-12R also addresses the challenges of sustainment systems upgrades and states:

> Many critical legacy systems are not built to be easily modified or patched. As a result, many of the risks incurred across DOD are introduced via unpatched (and effectively unpatchable) systems on the Department of Defense Information Network (DODIN).[74]

---

[71] Field Manual (FM) 4-0, *Sustainment* (Washington, DC: Government Printing Office, 2009), A-3.

[72] Ibid.

[73] JP 3-12R, II-11.

[74] Ibid.

These are obvious threats to a JFC's success on the battlefield.

The identification and clear understanding of the various cyber vulnerabilities of US Army logistics systems provide a platform for justifying the reimplementation of the traditional method of JIC logistics as the standard method. The range of risk mitigation options available to a JFC is limited to such measures as increasing operational security (OPSEC) and quality assurance/quality control procedures (QA/QC). However, there is a strong case for implementing change. The private sector can absorb losses if a business goes bankrupt or ceases to exist due to failures in logistics brought on by cyber-attacks. If markets demand a certain product or service, there is always an entrepreneur willing to fill the void in the hopes of making money. The military does not operate this way, and is a "service" that cannot go unfilled without catastrophic risk. Relying purely on JIT logistics is a risky endeavor that the military cannot take lightly. To change the entire military logistics model from its current state would require the DOD to convince the US Congress that the extra expense is not only justifiable, but is imperative to national security.

Responding to Cyber Vulnerabilities in Military Logistics

The whole of government addresses cyber vulnerabilities with capabilities aimed at protecting networks and rapidly restoring compromised systems. The DOD has cyber-defense programs embedded within all branches of service. The Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, Department of Homeland Security, and other governmental organizations have cyber capabilities that monitor and prevent cyber-attacks from degrading mission critical systems. US cyber defenses are arguably the best in the world, but despite this, US networks are not immune to compromise. The Office of Personnel Management (OPM) network was compromised resulting in the theft of massive amounts of data affecting

approximately 80 million people.[75] US military logistics systems, safeguarded by the same government agencies, are still vulnerable to cyber-attacks.

The integration of logistics software from the private sector, as well as computer systems and other COTS equipment, has benefited the military's current supply distribution. Specifically, *economy* is listed as one of the key principles of logistics and refers to the "minimum amount of resources required to bring about or create a specific outcome."[76] The concept of using the minimum amount of resources necessary is echoed in the US Army's sustainment doctrine. Army Doctrine Reference Publication (ADRP) 4-0 *Sustainment* adds, "economy may be achieved by contracting for support or using host nation resources that reduce or eliminate the use of limited military resources."[77] ADRP 4-0 also adds that, "economy is further achieved by eliminating redundancies and capitalizing on joint interdependencies."[78] However, one of the unintended side effects of integration with the private sector is the potential risk of disruption from cyber-attacks.

Joint doctrine on *Cyberspace Operations* addresses the tension between incorporating new technologies and cyber capabilities with operational requirements and the potential for increased risk.[79] It specifically addresses the private sector in that "many of DOD's critical functions and operations rely on commercial assets, including Internet service providers and global supply chains, over which DOD has no direct authority to mitigate risk effectively."[80] One of the ways to reduce cyber risk to the DOD's mission critical information technology (IT) infrastructure is

---

[75] Brendan I. Koerner, "Inside the OPM Hack, the Cyberattack That Shocked the US Government," *Wired Magazine*, last modified October 23, 2016, accessed December 28, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[76] Ibid.

[77] Army Doctrine Reference Publication (ADRP) 4-0, *Sustainment* (Washington, DC: Government Printing Office, 2012), 1–3.

[78] Ibid.

[79] JP 3-12R, II-11.

[80] Ibid., I-8.

through “public-private sector cooperation.”[81] Collaboration between the public and the private sector does yield positive results. However, between the planning stage and implementation, the overall process can take several years.

JP 3-12R’s section on sustainment mentions that JFCs must not only identify critical cyberspace assets, but must also detect system redundancy, “including non-cyberspace alternatives, and actively exercise continuity of operations plans to respond to outages or adversary actions that degrade or compromise cyberspace access or reliability.”[82] JP 3-12R also addresses the challenges of sustainment systems upgrades and states, “Many critical legacy systems are not built to be easily modified or patched. As a result, many of the risks incurred across DOD are introduced via unpatched (and effectively unpatchable) systems on the Department of Defense Information Network (DODIN).”[83] These threats are ongoing and are fixed slowly, partly because of the time it takes to upgrade equipment and the unhurried pace of innovation within the DOD, all of which has the adverse side effect of causing obsolescence throughout the DOD.

The Application of Russian New Generation Warfare Doctrine

> In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces.
>
> —Nikolai Kuryanovich, Russian State Duma deputy and member of the Security Committee, in a 2006 letter of appreciation to hackers against Israeli websites

The GAO and private security firms recognize that cyber-attacks could cause catastrophic impact against US military logistics and present a high risk to national security. Thus far, crippling of the US military logistics chain thankfully remains only theoretical. However, an inference can be made by examining the resultant effects of cyber-attacks in Georgia in 2008 and the Ukraine

[81] Ibid.

[82] JP 3-12R, II-11.

[83] Ibid.

since 2014 by the Russian Federation, that military logistics systems used by the United States also share similar vulnerabilities. Likewise, the Estonian government alleged that Russia engaged in countrywide cyber-attacks against Estonian government internet services and the financial sector in 2007. However, Estonia's blame of Russia remains the subject of debate due to the lack of solid evidence. The three before-mentioned examples illustrate that cyber capabilities can be wielded as a stand-alone method as seen in Estonia, or be fully integrated with conventional military forces as seen in Georgia, or can be a means to augment an insurgency as seen in the Ukraine. These examples reveal that the risks associated with cyber-attacks against US interests, both directly or indirectly, are a real possibility, and are potentially disastrous if not countered. Similar to a traditional military blockade involving warships or ground units, cyber-attacks can accomplish similar purposes such as "to create financial constraints, isolate the adversary politically, create discomfort for society in order to influence political decision making, and demonstrate power and capabilities in the international system."[84] In Estonia, Georgia, and the Ukraine, cyber-attacks resulted in a de facto blockade that severed informational lines of communication, and crippled financial institutions and infrastructure, all of which are critical components to the success employment of military JIT logistics.

Cyber-Attacks Against Estonia in 2007

On April 27, 2007, Estonia experienced countrywide cyber-attacks in the form of DoS and DDoS attacks.[85] Furthermore, attackers hired expensive black market botnets to spam Estonian networks, resulting in a shutdown of many systems in the government, telecommunications, and

[84] Ibid., 62–63.

[85] Russell, 154. DoS attack (denial-of-service attack): an attack that sends a flood of traffic to overwhelm a computer system or consume bandwidth, thereby interrupting the normal flow of traffic to and from the site. DDoS attack (distributed denial-of-service attack): a coordinated effort that instructs multiple computers to launch simultaneous DoS attacks directed at the same target.

financial sectors.[86] Initially, the cyber-attacks were small-scale and amateurish in nature but later grew more sophisticated with their use of large computer networks as a means to propagate the attacks.[87] These cyber-attacks occurred when tensions were high in the political arena between Estonia and Russia over the breakdown of negotiations concerning the relocation of the Soviet-era Soldier of Tallin memorial and associated graves.[88] Ethnic Russians also began protesting in the streets within Estonia during this period.[89] As diplomatic relations continued to degrade, Russian rhetoric against Estonia also intensified. Though harsh rhetoric and posturing by the Russian government is nothing new, especially in the Baltic states, the timing of the cyber-attacks against Estonia indicated that a new type of cross-border attack was not only possible, but also proved to be effective without the use of traditional military arms.

Specifically, the cyber-attacks against Estonia specifically targeted government websites such as the Estonian presidency and its parliament, nearly all of the country's government ministries, and political parties. Furthermore, these cyber-attacks also targeted three of the country's largest news media outlets, two of the largest banks, and various firms specializing in communications services.[90] These attacks caused immediate disruption to the ability of Estonians to communicate outside of their country. The long-term effects were the disruption to industrial

---

[86] *The Economist*, "War in the Fifth Domain," July 1, 2010, accessed March 16, 2017, http://www.economist.com/node/16478792.

[87] Russell, 76.

[88] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 16, 2007, sec. World news, accessed March 16, 2017, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

[89] Maailm, "New York Times: Eesti tuli küberrünnakutega hästi toime," *Postimees*, last modified May 29, 2007, accessed March 16, 2017, http://maailm.postimees.ee/1666071/new-york-times-eesti-tuli-kueberruennakutega-haesti-toime. "Kui Eesti võimud asusid Tallinnas teisaldama nõukogude sõduritele pühendatud pronkskuju, võisid nad eeldada et kohalikud vene päritolu inimesed tulevad tänavatele meelt avaldama." [When Estonian authorities began to move the bronze statue dedicated to Soviet soldiers in Tallin, they could assume that the local people of Russian origin would come to the streets in protest.]

[90] Traynor.

and commercial transactions, which resulted in financial losses.[91] These cyber-attacks were especially painful for Estonians as their society is one of the most wired in Europe as Estonia was one of the earlier pioneers of web-based public administrative services or "e-government" systems.[92] Estonia's heavy reliance on internet-based systems "for everything from voting and paying taxes, to paying for parking," made the country especially vulnerable to cyber-attacks.[93]

Estonian Prime Minister Andrus Ansip and Minister of Justice Rein Lang publically announced that the Russian government was responsible for the cyber-attacks against their country.[94] The cyber-attack timeline coincided with anti-Estonian protests in front of the Estonian Embassy in Moscow and public displays of pro-Russian extremist activities.[95] Ene Ergma, a member of the Estonian parliament, stated that the "gang hooliganism in Tallin in late April, was not a random coincidence, but a systematic and coordinated hostility."[96] Additionally, Merit Kopli,

---

[91] Russell, 69.

[92] Traynor.

[93] M. Dee Dubroff, "Russia's Innovative Cyber-War on Estonia," *InventorSpot.com*, last modified March 13, 2009, accessed March 16, 2017, http://inventorspot.com/articles/russias_innovative_cyberwar_estonia_25100.

[94] Postimees, "Ansip Ja Lang: Küberrünnakud Tulid Otse Putini Administratsioonist," *Postimees*, last modified June 7, 2007, accessed March 17, 2017, http://www.postimees.ee/1669315/ansip-ja-lang-kueberruennakud-tulid-otse-putini-administratsioonist. "Peaminister Andrus Ansip ja justiitsminister Rein Lang kinnitasid täna, et Eesti vastu aprilli lõpus ja mai alguses suunatud ulatuslikud küberrünnakud tulid muu hulgas ka Vene presidendi administratsiooni IP-aadressitelt." [Prime Minister Andrus Ansip and Minister of Justice Rein Lang confirmed today that in Estonia in late April and early May, large-scale cyber attacks came from the Russian presidential administration IP addresses.]

[95] Mihhail Lotman, "Mihhail Lotman: Miks Venemaa seda teeb?" *Postimees*, last modified June 2, 2007, accessed March 16, 2017, http://www.postimees.ee/1667557/mihhail-lotman-miks-venemaa-seda-teeb. "Olemasolu vandenõu Eesti vastu on ka raske vaidlustada: ajakirjanduses on juba antud Vene saatkonnas, samuti tegevust erinevate äärmusrühmituste juuresolekul esindajad 26-27. Aprillisündmuste ajal, samuti selge märk, et sündmused Tõnismäel ja Eesti saatkond Moskvas olid kooskõlastatud. See peaks lisama veelgi küberrünnakud, massiivse Eesti-vastase kampaania Vene meedia jne." [The existence of a conspiracy against Estonia is also difficult to dispute: the press has already conceded to the Russian embassy. There is a clear indication that there was coordination of activities by various extremist groups in the presence of the wider public in Tõnismäel and the Estonian embassy in Moscow during the 26-27 April events. This should add further evidence that cyber-attacks were part of a massive anti-Estonian campaign in the Russian media, etc.]

[96] Martin Mutov, "Ergma arvates võivad küberrünnakud korduda," *Postimees*, last modified May 25, 2007, accessed March 16, 2017, http://www.postimees.ee/1664961/ergma-arvates-voivad-kueberruennakud-korduda. "Riigikogu esimees tõi esile, et küberrünnakud, mis algasid samaaegselt

editor of Postimees, one of the two primary newspapers in Estonia stated, "The cyber-attacks are from Russia. There is no question. It's political. This is the first time this has happened, and it is very important that we've had this type of attack. We've been able to learn from it."[97]

Russian authorities denied the allegations that the attacks originated in Russia or from the Russian government.[98] The over one million "zombie computers," computers used without the knowledge of their owners, which the attackers used to disrupt government and banking services within Estonia, came from countries such as Peru, Vietnam, and the United States. However, IT experts "found that instructions on when and how to execute the DDoS attack were posted on Russian-language websites, leading Estonia to accuse Russia of involvement in the attacks."[99] Regardless of who was ultimately responsible for the cyber-attacks in Estonia, the attacks are indicative of a new form of warfare where the use of a "botnet threatened the national security of an entire nation."[100]

Estonia, despite its robust network security, was susceptible to wide-scale disruption lasting 22 days. Furthermore, the cyber-attacks in Estonia fit the model of RNGW by following the principle of going "from a direct clash to a contactless war" to achieve Russian political aims.[101] The cyber-attacks in Estonia also teach us that secure computer networks, such those within the governmental and financial sectors, are vulnerable.[102] The US Army's logistics systems rely on

---

ülesässitatud sovjetimeelsete jõukude huligaanitsemisega Tallinnas aprilli lõpus, ei ole juhuslik kokkulangevus, vaid on süsteemne ja koordineeritud vaenutegevus." [The Chairman of the State pointed out that the cyber attacks that began at the same time as the gang hooliganism in Tallin in late April, are not a random coincidence, but are systematic and coordinated hostilities.]

[97] Dubroff.

[98] Traynor.

[99] Russell, 76.

[100] Ibid., 78.

[101] Berzinš, "The New Generation of Russian Warfare."

[102] Russell, 78.

very similar networks. GCSS-Army depends on financial transactions on a daily basis in order to effectively manage maintenance and the ordering of spare parts. Furthermore, GCSS-Army systems rely on the Internet for all of their other financial transactions including the tracking of supplies and organizational equipment.[103] GCSS-Army computer systems share many of the same vulnerabilities as the systems that were attacked in Estonia.[104] The need to safeguard GCSS-Army and its subsystems remains paramount, but more importantly, a mechanism to provide overall logistical redundancy should be established in order to mitigate the effects of network and financial system disruption.

The 2008 Russo-Georgian War

As part of its effort to support pro-Russian separatist movements in South Ossetia and Abkhazia, the Russian Federation began a full-scale invasion of the Republic of Georgia. On 8 August 2008, Russian warplanes entered into Georgian airspace and attacked various targets in the immediate vicinity of the Georgian capital of Tbilisi. Simultaneously, Russia through the use advanced cyber-attacks disrupted various Georgian websites that were "vital to the distribution of information by governmental and independent media agencies."[105] Of note, US Agency for International Development (USAID)-supported news site *Civil Georgia* was also "rendered inaccessible during the first days of the war."[106]

---

[103] GCSS-Army, "Global Combat Support System-Army - System Description."

[104] GCSS-Army, "FY15 Army Programs - Global Combat Support System-Army (GCSS-Army)" (Director, Operational Test and Evaluation (DOT&E), 2015), accessed 28 December 2016, http://www.dote.osd.mil/pub/reports/FY2015/pdf/army/2015gcssa.pdf.

[105] S. Frederick Starr and Svante E. Cornell, *The Guns of August 2008: Russia's War in Georgia*, Studies of Central Asia and the Caucasus (Armonk, NY: M. E. Sharpe Incorporated, 2009), 152.

[106] Ibid.

Approximately three weeks prior to armed hostilities between Russia and Georgia, cyber-attacks against Georgian websites were already taking place.[107] By the onset of armed conflict, the use of cyber capabilities became a key component in a four-pronged approach used by the Russians. The use of conventional infantry and armored forces, bombing sorties by the Russian Air Force, and a naval blockade were all synchronized with cyber-attacks.[108] Specifically, these cyber-attacks targeted networks that were related to telecommunications, finance, and government.[109] Network degradation of government and news media outlets "hampered Tbilisi's ability to disseminate information during the first days of hostilities."[110] Of note, the Russian government denied attacking against Georgia from the cyber domain, despite telltale signs that these attacks were of Russian origin.[111]

To Russia's advantage, cyber-attacks not only damaged Georgia's logistical capacity by degrading government and financial networks but also hindered Georgia's ability to disseminate information within its borders and to the outside world.[112] Georgian government officials attempted to block "websites on the .ru domain as part of the information war with Russia" with failed results.[113] Georgian hackers also attempted to disable Russian news networks through DDoS

---

[107] Noah Shachtman, "Top Georgian Official: Moscow Cyber Attacked Us - We Just Can't Prove It," *Wired Magazine*, last modified March 11, 2009, accessed March 19, 2017, https://www.wired.com/2009/03/georgia-blames/.

[108] Ibid.

[109] Jon Oltsik, "Russian Cyber Attack on Georgia: Lessons Learned?," *Network World*, last modified August 17, 2009, accessed March 19, 2017, http://www.networkworld.com/article/2236816/cisco-subnet/russian-cyber-attack-on-georgia---lessons-learned-.html.

[110] Starr and Cornell, 154.

[111] John Leyden, "Bear Prints Found on Georgian Cyber-Attacks," *The Register – Biting the Hand That Feeds IT*, last modified August 14, 2008, accessed March 19, 2017, https://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/.

[112] David M. Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* (January 11, 2011): 2-3, accessed March 19, 2017, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

[113] Civil Georgia, "Georgia Eases Restrictions on Russian Websites," last modified September 10, 2008, accessed March 19, 2017, http://www.civil.ge/eng/article.php?id=19459.

attacks, but with limited success.[114] Within the cyber domain, Russia clearly outmatched Georgia during this conflict. Russia's use of cyber capabilities in coordination with conventional military means is in line with concepts within RNGW in that conflict is changed "from war in the physical environment to a war in the human consciousness and in cyberspace."[115]

The fact that Russia fully integrates and synchronizes its cyber capabilities with its conventional military forces, has direct implications for US military JIT logistics. Critical to the function of network-centric logistics, Russia specifically targeted and successfully disrupted Georgia's government and financial networks during this conflict. What is known is that Russia "prepositioned logistics in Abkhazia; and built a railroad there to connect it to its own military and logistic bases."[116] Whether Russia prestaged its equipment as standard practice, or as a means to mitigate risk in anticipation of Georgian cyber-attacks against their military networks, is debatable. However, the lesson is clear that Russia was prepared well in advance of the onset of the armed conflict.

Russian Military Intervention in the Ukraine

The application of RNGW doctrine within the Ukraine is an ongoing activity by Russian forces. Similar to Estonia and Georgia, the doctrine includes indirect methods such as subversion and propaganda messaging through the use of cyber capabilities against the government, military, industry, and the local population. However, what makes the application of RNGW doctrine unique to the Ukraine is the use of cyber capabilities to shut down part of the national power grid. The implication is that risk to the US power grid infrastructure is no longer in the realm of theory, but is now a reality. Furthermore, many of the legacy military logistics systems use software and

---

[114] Gregg Keizer, "Russian Hacker 'Militia' Mobilizes to Attack Georgia," *Network World*, last modified August 12, 2008, accessed March 19, 2017, http://www.networkworld.com/article/2274800/lan-wan/russian-hacker--militia--mobilizes-to-attack-georgia.html.

[115] Bērziņš, "The New Generation of Russian Warfare."

[116] Starr and Cornell, 117-118.

hardware that is as old and outdated as those used by the electrical power companies. This was primarily due to severe post-Soviet era budget constraints, which resulted in modernization and maintenance being a luxury. Of note, "higher-level logistics infrastructure was cut to the bone," resulting in problems that manifested years later.[117] Despite such vulnerabilities, such systems are still used today because they are still functional.[118]

On December 23, 2015, the regional power distribution company, Ukrainian Kyivoblenergo, initially reported a power outage that disrupted power for approximately 80,000 Ukrainians. It was detrmined that the power disruption was caused by a cyber-attack. Shortly after the initial assessment, it was revealed that cyber-attacks successfully targeted three power distribution companies, resulting in power being disrupted for roughly 225,000 customers across various areas.[119] Experts within the Ukraine concluded that the cause was an external computer virus that targeted SCADA units with instructions to disconnect the power station from the grid.[120]

Though power was restored a few hours later, this particular use of cyber was unprecedented. Cyber-attacks against the power grid had long been theorized, but this incident

---

[117] Phillip A. Karber, *Lessons Learned from the Russo-Ukrainian War* (Vienna, VA: The Potomac Foundation, July 8, 2015), 30, accessed December 20, 2016, https://prodev2go.files.wordpress.com/2015/10/rus-ukr-lessons-draft.pdf.

[118] Richard Campbell, *Testimony – Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?* (Washington, DC: Congressional Research Service, April 11, 2016), 2, accessed March 30, 2017, http://transportation.house.gov/uploadedfiles/2016-04-14-campbell.pdf.

[119] Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, DC: Electricity-Information Sharing and Analysis Center, March 18, 2016), v, accessed March 22, 2017, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[120] Televizionnaya Sluzhba Novostey (TCH), "Prichinoju vchorashn'ogo znestrumlennja polovini Ivano-Frankivshhini bula hakers'ka ataka," last modified December 24, 2015, accessed March 30, 2017, https://tsn.ua/bin/player/iframe/385164683. [According to experts, hackers broke into the robotic control system. More than half of the region itself and part of Ivano-Frankivsk were left without electricity for a few hours. According to a spokesman for the power companies, the running of an "outside-in" virus suddenly began to disconnect power from the substation. Currently, power has been restored everywhere. However, power does not hide the fact that power companies are doing this in the so-called "manual mode" because the system is still disabled, and experts are trying to overcome the running virus.]

showed inherent weaknesses in legacy systems within CI/KR, especially systems that use SCADA units. Furthermore, many of these legacy systems directly interface with the Internet while running outdated operating systems such as Windows 2000 and Windows XP.[121] SCADA units are used throughout the logistics supply chain to include docks, airports, and rail. These SCADA systems are critical to properly functioning logistics, and are highly susceptible to cyber-attacks that introduce malicious code such as Trojan horses and viruses for the purpose of disrupting system functionality.[122] The implication is that US legacy logistics systems are just as vulnerable to cyber-attacks as their Ukrainian counterparts.

Conclusion and Recommendations

> God punishes those that don't have a backup plan.
>
> —Command Sgt. Maj. Ricky Richardson, 15th Regimental Signal Brigade

JIC versus JIT: The Ongoing Debate between Logisticians

As previously mentioned, the primary drivers for military sustainment to move from JIC to JIT logistics were to reduce cost and improve efficiency. Before the Army implemented its Logistics Modernization Program (LMP), the Army Materiel Command (AMC) "depended on ponderous, 30-year-old systems to manage its logistics operations and supply critical equipment and repair parts to the soldier."[123] Two of the largest systems, the Commodity Command Standard System (CCSS) and the Standard Depot System (SDS), "evolved into a complex web of software

---

[121] Honeywell, *Mitigating Cyber Security Risks in Legacy Process Control Systems*, White Paper (Houston, TX: Honeywell Process Solutions, November 2014), 3, accessed March 30, 2017, https://www.honeywellprocess.com/library/marketing/whitepapers/cyber-security-legacy-systems.pdf.

[122] InfoSec Resources, "Cyber Security Risk in Supply Chain Management: Part 1," last modified March 12, 2015, accessed March 30, 2017, http://resources.infosecinstitute.com/cyber-security-in-supply-chain-management-part-1/.

[123] Kevin Carroll, and David W. Coker, "Logistics Modernization Program: A Cornerstone of Army Transformation," *Army Logistician* 39, no. 1 (February 2007), accessed March 24, 2017, http://www.almc.army.mil/alog/issues/JanFeb07/lmp_cornerstone.html.

solutions that were difficult to maintain and almost impossible to update to address the Army's rapidly expanding supply needs."[124] The issue of having a decades-old system that grew burdensome in its complexity, yet was not able to sufficiently meet the needs of the US Army, was justification enough for modernizing the military logistics systems.

Ground combat during Operation Desert Storm lasted just over five weeks before victory was declared.[125] In addition to the troop surge, it took approximately six months for US forces and coalition partners to build up stockpiles of supplies and equipment in Kuwait and Saudi Arabia.[126] Stockpiles of ammunition to sustain two years of combat, as well as over 27,000 unopened containers in theater, raised concerns for budget analysts, especially seeing that the ground war only lasted just over a month.[127] Furthermore, the contents of many of these containers were not "known until they were opened and physically inventoried, an obviously resource intensive and inefficient process that illustrates that having a stockpile forward does not necessarily make the system responsive."[128]

Using these circumstances, one could make the case that forward stockpiling is not efficient and is wasteful. Leading up to Operation Desert Strom, Iraq possessed the fourth largest army in the world, and had soldiers that were seasoned veterans of the eight-year Iran-Iraq War only a few years prior. US military planners expected war with Iraq could be protracted. In hindsight, knowing the length of the war in advance makes it easy to critique the military planners of the day. The fact there was stockage in the theater to sustain two years of combat operations is

---

[124] Ibid.

[125] Ash McCall, "A Timeline of Operation Desert Storm," *Army Live*, last modified February 26, 2013, accessed March 24, 2017, http://armylive.dodlive.mil/index.php/2013/02/operation-desert-storm/.

[126] Mark E. Solseth, "Distribution and Supply Chain Management: Educating the Army Officer" (Monograph, School of Advanced Military Studies, 2005), 6–7.

[127] Joseph L. Walden, "Applying Just-In-Time To Army Operations" (Monograph, School of Advanced Military Studies, 2000), 1.

[128] Solseth, "Distribution and Supply Chain Management: Educating the Army Officer," 7.

not an indictment against JIC. Instead, it demonstrates that JIC logistics was able to provide sufficient sustainment needs for long-term combat operations. Regardless of the war's outcome, modernization of logistics systems and processes were necessary.

Once efforts were underway to modernize military sustainment practices and transition to JIT logistics, cost savings were starting to show. However, roughly a decade following Operation Desert Storm, the US Navy expressed concerns that JIT logistics were "requirements set by Joint Vision 2010 to fight two nearly simultaneous major theater wars."[129] Concerns centered on JIT logistics being unable to "respond to shifting requirements, that there are enough transportation resources, and that support is too shallow, and, when equipment breaks in the heat of battle, there will be enough spare parts to draw on because they have not been manufactured yet."[130] However, the US Navy also understood problems of traditional JIC logistics. Many of the US Navy's component requirements have "items that were time sensitive, the older the inventory got, the more likely it was that some of the items would fail when issued, contributing even more to the problem of poor inventory quality, along with the inability to find items."[131] As the US Army continues to increase its use of advanced weapon systems, it will share the same issues concerning time-sensitive parts as the US Navy does.

Since 2003, the LMP has been able to fulfill "warfighter requirements on a daily basis."[132] At the center of the LMP, is GCSS-Army as one of the largest implementers of ERP technology by SAP. The US Army benefits greatly from LMP as it streamlines supply chain processes and

[129] Ernest D. Harden II, "Just-in-Time Logistics: Does It Fulfill the Surface Navy's Requirements to Support the National Military Strategy?" (Thesis, US Army Command and General Staff College, 2001), 2, accessed March 24, 2017, http://www.dtic.mil/jv2010/jv2010.pdf.

[130] Ibid.

[131] Ibid., 3.

[132] Carroll and Coker.

employs an IT platforms to improve overall performance.[133] Furthermore, by centralizing all data functions into LMP and GCSS-Army, the US Army is able to "eliminate many costly and outdated legacy data systems."[134] From an operational perspective, federating data into a centralized database facilitates faster decision making as all are synchronized when an update to the database is made.[135] The downside is that "federating data also makes the overall system more vulnerable to cyber-attacks."[136]

The Committee on Force Multiplying Technologies for Logistics Support to Military Operations reported there is a sizable system security risk from cyber-attacks:

> Having a single federated ERP data and/or execution system magnifies the Army's vulnerability to cyber-attack. A successful cyberattack could shut down the entire GCSS-Army and LMP systems, which could easily bring the Army's logistics system to a halt. The military is the target of a tremendous number of cyber-attacks on a daily basis. Because SAP has thousands of ERP implementations all over the world, it is possible that a potential enemy may have already determined how to breach the GCSS-Army and LMP systems.[137]

Furthermore, this committee warned that an international hacking enterprise exists to exploit commercial SAP-ERP systems.[138] Despite these concerns about cyber vulnerabilities with JIT logistics systems, a potential shutdown of military logistics from cyber-attacks has yet to be prevented.

Conclusion

Despite its vulnerabilities, JIT logistics is here to stay. Historical examples might imply that a full reversal of JIT logistics to JIC logistics is better for overall system redundancy. Though

---

[133] Ibid.

[134] National Research Council (US) et al., *Force Multiplying Technologies for Logistics Support to Military Operations* (Washington, DC: The National Academies Press, 2014), 110.

[135] Ibid.

[136] Ibid.

[137] Ibid., 111–112.

[138] Ibid., 112.

this is true in many respects, the benefits are too great to justify a complete reversal. The US military is utterly dependent on its logistics, more so than many other nations. A failure in logistics would mean a failure in a military campaign. Such a failure could cost tremendous amounts of blood and treasure, more so than the cost of reimplementing JIC logistics.

Currently, the United States is well served by using the JIT logistics model, but only if nothing bad happens to the system. By employing a "hybrid" approach to logistics, the military retains the many cost-saving advantages of JIT logistics. On the other hand, by also incorporating JIC logistics, this provides a sound foundation for a much-needed safety net that is currently lacking in the present system. Using both logistics methodologies is likely to be more expensive, but safeguarding military logistics is imperative to the national security of the United States as well as its allies.

Recommendations

As JIT logistics is the currently used method for daily supply chain transactions, a hybrid system is prone to failure if commanders do not to exercise and train the JIC element. The temptation to fill CONEX boxes with materiel and forget about it until an emergency happens is foolish. If history is to serve as a guide, Operation Desert Storm teaches us that JIC logistics has potential downsides such as vast quantities of containers being filled with supplies and equipment, coupled with poor tracking and inventory practices, resulted in the containers' contents being unknown. However, this particular problem is more procedural rather than an inherent characteristic of the philosophy behind JIC logistics.

If a "hybrid" approach is adopted, some initial growing pains are expected. Any large-scale change in procedures and training practices can be planned for, but upon execution of a plan of this magnitude, it will need refinements along the way. In the end, the CONEX box would continue to serve a key role in logistics. The speed and throughput capacity provided by JIT logistics enable CONEX boxes to be placed anywhere in the world in sufficient quantities and with

sufficient speed. The future of preconfigured CONEX boxes will expand on current concepts such as providing a base for telecommunications and modular power generation. In light of the philosophy behind RNGW and the likelihood of using high-tech solutions such as electromagnetic pulse (EMP) weapons to achieve tremendous results through indirect means, the CONEX box already provides protection. A CONEX box already has the characteristics of a Faraday cage, which would provide protection against new EMP weapons. Future preconfigured CONEX boxes might also feature additive manufacturing such as 3d printing facilities that could provide some manner of JIT logistics capability close to the front lines. These facilities should be modular, whereby merely increasing the number of preconfigured CONEX boxes is scalable to the echelon and requirements of the units using them. This type of scalability already exists with diesel power generators as preconfigured CONEX boxes.

Furthermore, networks with only enough bandwidth to meet daily requirements are not enough. DDoS attacks can flood a system, regardless of its cyber security features. One effective way to combat DDoS attacks and other similar flood type attacks is to use cloud-based networks with very high, distributed bandwidth, thus being able to absorb DDoS attacks effectively and prevent network shutdown.[139] The DOD is notorious for having networks with low bandwidth due to cost-savings. General Fund Enterprise Business Systems (GFEBS), which is an integral part of JIT logistics and of GCSS-Army, handles nearly all the financial transactions relating to supply. GFEBS already suffers from low bandwidth during regular usage. The committee led by the National Research Council recommended that military sustainment systems use the best networks and technology available rather than going with systems produced by the "lowest bidder." The committee specifically recommended the following:

> This is an area of considerable risk to DOD, and anything less than an effort comparable to the one made to protect the US financial system would be inadvisable. The financial

[139] Sean Leach, "Four Ways to Defend against DDoS Attacks," *Network World*, last modified September 17, 2013, accessed March 30, 2017, http://www.networkworld.com/article/2170051/tech-primers/tech-primers-four-ways-to-defend-against-ddos-attacks.html.

> systems of the United States are protected with multiple data backups in case of a catastrophic event, and the Army needs nothing less. When it is at war, the Army's security requirements are as important as those of Wall Street. Once the Army fully implements GCSS-Army and LMP and depends on it operationally, the entire Army logistics system will incur the attendant risks of a federated ERP database, including catastrophic failure of the system due to enemy activity.[140]

It is imperative that commanders train as they would fight. Otherwise, there is a risk of being caught off guard and ill-prepared. The enemy knows US doctrine, and JP 3-0 speaks to creating multiple dilemmas on the battlefield.[141] Losing the capacity to conduct logistics, by itself, will create multiple dilemmas for US military forces. Adding several layers of complexity, such as having to contend with known actors, as well as unknown actors that might emerge later to exploit a weakness such as a disabled logistics system, is not a favorable position for the US military. Not being in a position of relative advantage increases the cost of warfare in terms of both blood and treasure.

[140] National Research Council (US) et al., *Force Multiplying Technologies for Logistics Support to Military Operations* (Washington, DC: The National Academies Press, 2014), 112.

[141] JP 3-0, V-45.

Bibliography

Abraham, David S. *The Elements of Power: Gadgets, Guns, and the Struggle for a Sustainable Future in the Rare Metal Age*. New Haven: Yale University Press, 2015.

Andrews, Evan. "8 Ways Roads Helped Rome Rule the Ancient World - History Lists." History.com. Accessed November 16, 2016. http://www.history.com/news/history-lists/8-ways-roads-helped-rome-rule-the-ancient-world.

APICS Forum. "Just-in-Time Manufacturing." Last modified February 8, 2012. Accessed March 22, 2017. http://www.apicsforum.com/ebook/10._just-in-time_manufacturing.

Army Doctrine Reference Publication (ADRP) 3-0, *Operations*. Washington, DC: Government Printing Office, 2016.

Army Doctrine Reference Publication (ADRP) 4-0, *Sustainment*. Washington, DC: Government Printing Office, 2012.

ATOX Sistemas de Almacenaje. "Just-in-Time (JIT) Logistics." Last modified July 7, 2015. Accessed March 21, 2017. http://www.atoxgrupo.com/website/en/news/just-in-time-logistics.

Bērziņš, Jānis. "The New Generation of Russian Warfare." The Potomac Foundation. Last modified October 11, 2016. Accessed December 20, 2016. http://www.thepotomac foundation.org/the-new-generation-of-russian-warfare/.

Bērziņš, Jānis. *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (Riga, Latvia: National Defence Academy of Latvia - Center for Security and Strategic Research, April 2014). Accessed March 23, 2017. http://www.naa.mil.lv/~/ media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx.

Campbell, Richard. *Testimony – Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?* Washington, DC: Congressional Research Service. April 11, 2016. Accessed March 30, 2017. http://transportation.house.gov/ uploadedfiles/2016-04-14-campbell.pdf.

Carroll, Kevin, and David W. Coker. "Logistics Modernization Program: A Cornerstone of Army Transformation." *Army Logistician* 39, no. 1 (February 2007). Accessed March 24, 2017. http://www.almc.army.mil/alog/issues/JanFeb07/lmp_cornerstone.html.

Civil Georgia. "Georgia Eases Restrictions on Russian Websites." Last modified September 10, 2008. Accessed March 19, 2017. http://www.civil.ge/eng/article.php?id=19459.

Clausewitz, Carl von. *On War, Indexed Edition*. Trans. Michael Eliot Howard and Peter Paret. Reprint edition. Princeton, NJ: Princeton University Press, 1989.

Cohan, George M. "Over There: Sheet Music." Ball State University Digital Media Repository. Accessed November 14, 2016. http://libx.bsu.edu/cdm/ref/collection/ShtMus/id/1273.

Comey, James B. "Homeland Threats and the FBI's Response." Testimony. *Federal Bureau of Investigation*. Last modified November 14, 2013. Accessed December 21, 2016. https://www.fbi.gov/news/testimony/homeland-threats-and-the-fbis-response.

Dempsey, Kelley, and Celia Paulsen. "Risk Management for Replication Devices." US Department of Commerce, National Institute for Standards and Technology, February 2015. Accessed September 4, 2016. http://nvlpubs.nist.gov/nistpubs/ir/2015/ NIST.IR.8023.pdf.

Dubroff, M. Dee. “Russia’s Innovative Cyber-War on Estonia.” Inventor Spot. Last modified March 13, 2009. Accessed March 16, 2017. http://inventorspot.com/articles/russias_innovative_cyberwar_estonia_25100.

Duggan, Patrick M. “U.S. Special Operations Forces in Cyberspace.” *The Cyber Defense Review* 1, no. 2 (Fall 2016). Accessed January 31, 2017. http://www.cyberdefensereview.org/wp-content/uploads/2017/01/CDR-FALL2016.pdf.

Economist. “War in the Fifth Domain.” July 1, 2010. Accessed March 16, 2017. http://www.economist.com/node/16478792.

E-ISAC. *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Electricity-Information Sharing and Analysis Center, March 18, 2016. iv. Accessed March 22, 2017. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Ellison, Robert J., John B. Goodenough, Charles B. Weinstock, and Carol Woody. *Evaluating and Mitigating Software Supply Chain Security Risks*. Carnegie Mellon University: Software Engineering Institute, May 2010. Accessed March 16, 2017. http://resources.sei.cmu.edu/asset_files/technicalnote/2010_004_001_15176.pdf.

Engels, Donald W. *Alexander the Great and the Logistics of the Macedonian Army*. Berkeley: University of California Press, 1978.

Federal Acquisition Regulation System. *Code of Federal Regulations*. title 48 (2005): 52.209-6(a)(1)(iii) 1270. Accessed September 4, 2016, https://www.acquisition.gov/sites/default/files/current/far/pdf/FAR.pdf.

Fedyk, Nicholas. “Russian ‘New Generation’ Warfare: Theory, Practice, and Lessons for U.S. Strategists.” *Small Wars Journal* (August 25, 2016): 2-8.

Field Manual (FM) 4-0, *Sustainment*. Washington, DC: Government Printing Office, 2009.

Field Manual (FM) 55-80, *Army Container Operations*. Washington, DC: Government Printing Office, 1997.

GCSS-Army. “FY15 Army Programs - Global Combat Support System-Army (GCSS-Army)” (Director, Operational Test and Evaluation (DOT&E), 2015). Accessed 28 December 2016. http://www.dote.osd.mil/pub/reports/FY2015/pdf/army/2015gcssa.pdf.

GCSS-Army. “Global Combat Support System-Army – System Description.” Accessed December 28, 2016. http://gcss.army.mil/About/SystemDescription.aspx.

Geli, Mathieu, Darya Maenkova, and Alexander Polyakov. *SAP Cyber Security in Figures (Global Threat Report) 2016*. ERPScan, n.d. Accessed December 28, 2016. https://erpscan.com/wp-content/uploads/publications/Sap-Cyber-Threat-Report.pdf.

Grygiel, Jakub J. *Great Powers and Geopolitical Change*. Baltimore, MD: Johns Hopkins University Press, 2011.

Harden II, Ernest D. “Just-in-Time Logistics: Does It Fulfill the Surface Navy’s Requirements to Support the National Military Strategy?” Thesis, US Army Command and General Staff College, 2001. Accessed March 24, 2017. http://www.dtic.mil/jv2010/jv2010.pdf.

Hollis, David M. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal* (January 11, 2011). Accessed March 19, 2017. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Honeywell. *Mitigating Cyber Security Risks in Legacy Process Control Systems*. White Paper.

Houston, TX: Honeywell Process Solutions. November 2014. Accessed March 30, 2017. https://www.honeywellprocess.com/library/marketing/whitepapers/cyber-security-legacy-systems.pdf.

Hugos, Michael H. “Alexander the Great Needed Great Supply Chains.” March 17, 2014. Accessed March 21, 2017. http://blog.scmglobe.com/?p=385.

InfoSec Resources. “Cyber Security Risk in Supply Chain Management: Part 1.” Last modified March 12, 2015. Accessed March 30, 2017. http://resources.infosecinstitute.com/cyber-security-in-supply-chain-management-part-1/.

Investopedia. “Holding Costs.” Accessed October 13, 2016. http://www.investopedia.com/terms/h/holding-costs.asp.

Investopedia. “Just in Case.” Accessed November 16, 2016. http://www.investopedia.com/terms/j/jic.asp.

Investopedia. “Just In Time - JIT.” Last modified November 23, 2003. Accessed March 21, 2017. http://www.investopedia.com/terms/j/jit.asp.

Joint Publication 3-0, *Joint Operations*. Washington, DC: Government Printing Office, 2011.

Joint Publication 3-12R, *Cyberspace Operations*. Washington, DC: Government Printing Office, 2013.

Joint Publication 3-17, *Air Mobility Operations*. Washington, DC: Government Printing Office, 2013.

Joint Publication 3-24, *Counterinsurgency*. Washington, DC: Government Printing Office, 2013.

Joint Publication 4-0, *Joint Logistics*. Washington, DC: Government Printing Office, 2013.

Joint Publication 4-01, *The Defense Transportation System*. Washington, DC: Government Printing Office, 2013.

Kakaes, Konstantin. “Making iPhones in the U.S. Might Not Cost as Much as You’d Think.” *MIT Technology Review*. Accessed December 1, 2016. https://www.technologyreview.com/s/601491/the-all-american-iphone/.

Karber, Phillip A. “Russia’s ‘New Generation Warfare.’” National Geospatial-Intelligence Agency. Last modified June 4, 2015. Accessed March 23, 2017. https://www.nga.mil/MediaRoom/News/Pages/Russia’s-’New-Generation-Warfare’.aspx.

Karber, Phillip A. *Lessons Learned from the Russo-Ukrainian War*. Vienna, VA: The Potomac Foundation. July 8, 2015. Accessed December 20, 2016. https://prodev2go.files.wordpress.com/2015/10/rus-ukr-lessons-draft.pdf.

Keizer, Gregg. “Russian Hacker ‘Militia’ Mobilizes to Attack Georgia.” Network World. Last modified August 12, 2008. Accessed March 19, 2017. http://www.networkworld.com/article/2274800/lan-wan/russian-hacker--militia--mobilizes-to-attack-georgia.html.

Koerner, Brendan I. “Inside the OPM Hack, the Cyberattack That Shocked the US Government.” *Wired Magazine*. Last modified October 23, 2016. Accessed December 28, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

Leach, Sean. “Four Ways to Defend Against DDoS Attacks.” Network World. Last modified September 17, 2013. Accessed March 30, 2017. http://www.networkworld.com/article/2170051/tech-primers/tech-primers-four-ways-to-defend-against-ddos-attacks.html.

Lee, Robert M., Michael J. Assante, and Tim Conway. *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Washington, DC: Electricity-Information Sharing and Analysis Center. March 18, 2016. Accessed March 22, 2017. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Leiphart, Kristine Lee. "Creating a Military Supply Chain Management Model." *Army Logistician* 33, no. 4 (August 7, 2001): 36-39.

Levinson, Marc. "The Box That Changed Asia and the World." *Forbes*. Accessed January 24, 2017. http://www.forbes.com/global/2006/0313/030.html.

Levinson, Marc. *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger*. Princeton, NJ: Princeton University Press, 2006.

Leyden, John. "Bear Prints Found on Georgian Cyber-Attacks." *The Register - Biting the Hand That Feeds IT*. Last modified August 14, 2008. Accessed March 19, 2017. https://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/.

Lotman, Mihhail. "Mihhail Lotman: Miks Venemaa seda teeb?" *Postimees*. Last modified June 2, 2007. Accessed March 16, 2017. http://www.postimees.ee/1667557/mihhail-lotman-miks-venemaa-seda-teeb.

Maailm. "New York Times: Eesti tuli küberrünnakutega hästi toime." *Postimees*. Last modified May 29, 2007. Accessed March 16, 2017. http://maailm.postimees.ee/1666071/new-york-times-eesti-tuli-kueberruennakutega-haesti-toime.

McCall, Ash. "A Timeline of Operation Desert Storm." *Army Live*. Last modified February 26, 2013. Accessed March 24, 2017. http://armylive.dodlive.mil/index.php/2013/02/operation-desert-storm/.

Mello, John P. Jr. "Windows XP Hacked, Supply Chain Poisoned | Malware | TechNewsWorld." *Tech News World*. Last modified July 16, 2014. Accessed November 16, 2016. http://www.technewsworld.com/story/80742.html.

Muradian, Vago. "Adm. Michael Mullen - Chairman, U.S. Joint Chiefs of Staff." *Defense News*. Last modified July 10, 2011. Accessed December 21, 2016. http://archive.defensenews.com/article/20110710/DEFFEAT03/107100301/Adm-Michael-Mullen.

Mutov, Martin. "Ergma arvates võivad küberrünnakud korduda." *Postimees*. Last modified May 25, 2007. Accessed March 16, 2017. http://www.postimees.ee/1664961/ergma-arvates-voivad-kueberruennakud-korduda.

Myers, Laurel K. "Eliminating the Iron Mountain." *Army Logistician* 36, no. 4 (August 7, 2004): 40-57.

National Research Council (US), Committee on Force Multiplying Technologies for Logistics Support to Military Operations, Board on Army Science and Technology, Division on Engineering and Physical Sciences, *Force Multiplying Technologies for Logistics Support to Military Operations.* Washington, DC: The National Academies Press, 2014.

O'Konski, Mark. "Revolution in Military Logistics: An Overview." *Army Logistician* 31, no. 1 (February 1999). Accessed March 21, 2017. http://www.alu.army.mil/alog/1999/jan feb99/pdf/janfeb1999.pdf.

Oltsik, Jon. “Russian Cyber Attack on Georgia: Lessons Learned?” *Network World*. Last modified August 17, 2009. Accessed March 19, 2017. http://www.networkworld.com/article/2236816/cisco-subnet/russian-cyber-attack-on-georgia---lessons-learned-.html.

Peppers, Jerome G. *History of the United States Military Logistics, 1935-1985: A Brief Review*. Huntsville, AL: Society of Logistics Engineers, 1988.

Postimees. “Ansip ja lang: küberrünnakud tulid otse putini administratsioonist.” Last modified June 7, 2007. Accessed March 17, 2017. http://www.postimees.ee/1669315/ansip-ja-lang-kueberruennakud-tulid-otse-putini-administratsioonist.

Rosenstein, Nathan, and J. S. Richardson. *Rome and the Mediterranean 290 to 146 BC: The Imperial Republic*. Edinburgh: Edinburgh University Press, 2014.

Russell, Alison Lawlor. *Cyber Blockades*. Washington, DC: Georgetown University Press, 2014. Accessed December 22, 2016. http://public.eblib.com/choice/publicfullrecord.aspx?p=1810129.

SAP. “Military, Security & Defense: Industry Software.” Accessed January 31, 2017. http://www.sap.com/solution/industry/defense-security.html.

SAP. “SAP Company Information: About SAP.” Accessed December 28, 2016. http://www.sap.com/corporate/en/company.html.

Schifferle, Peter J. “Evolution of Operational Art - Lesson 16: Joint Operations and the Tenuous End of the Rope: Guadalcanal, 1942,” School of Advanced Military Studies, Fort Leavenworth, KS, October 18, 2016.

Shachtman, Noah. “Top Georgian Official: Moscow Cyber Attacked Us – We Just Can’t Prove It.” *Wired Magazine*. Last modified March 11, 2009. Accessed March 19, 2017. https://www.wired.com/2009/03/georgia-blames/.

Solseth, Mark E. “Distribution and Supply Chain Management: Educating the Army Officer.” Monograph, School of Advanced Military Studies, 2005.

Starr, S. Frederick, and Svante E. Cornell. *The Guns of August 2008: Russia’s War in Georgia*. Studies of Central Asia and the Caucasus. Armonk, NY: M. E. Sharpe Incorporated, 2009.

Sunzi, and Roger T. Ames. *Sun-Tzu: The Art of Warfare - the First English Translation Incorporating the Recently Discovered Yin-Ch‘üeh-Shan Texts*. New York, NY: Ballantine Books, 1993.

Televizionnaya Sluzhba Novostey (TCH). “Причиною вчорашнього знеструмлення половини Івано-Франківщини була хакерська атака.” Last modified December 24, 2015. Accessed March 30, 2017. https://tsn.ua/bin/player/iframe/385164683.

Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” *The Guardian*, May 16, 2007, Accessed March 16, 2017. https://www.theguardian.com/world/2007/may/17/topstories3.russia.

US Marine Corps Concepts and Programs. “Networking On-The-Move (NOTM).” Last modified January 13, 2017. Accessed March 14, 2017. https://marinecorpsconceptsandprograms.com/programs/command-and-controlsituational-awareness-c2sa/networking-move-notm.

Van Creveld, Martin. *Supplying War: Logistics from Wallenstein to Patton*. Cambridge: Cambridge University Press, 1977.

Walden, Joseph L. “Applying Just-In-Time To Army Operations.” Monograph, School of Advanced Military Studies, 2000.

Wilshusen, Gregory C. *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*. Washington, DC: US Government Accountability Office, March 2012.

Woods, Randy. “The Iranian Conundrum: How Sanctions Removal Affects Global Logistics | Air Cargo World.” *Air Cargo World*. Last modified April 6, 2016. Accessed December 1, 2016. http://aircargoworld.com/the-iranian-conundrum-how-sanctions-removal-affects-global-logistics/.