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.

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/.