UNIVERSITY OF WISCONSIN, PLATTEVILLE

UNITED STATES OF AMERICA

The attached seminar paper, by Michael Smith, entitled Terrorism in Supply Chains, when completed, is to be submitted to the Graduate Faculty of the University of Wisconsin- Platteville in partial fulfillment of the requirements for the (MASTER OF SCIENCE IN INTEGRATED SUPPLY CHAIN MANAGEMENT) degree.

Approved: Mary R. Bartling Date: 8/12/18

Project Advisor

Professor Mary R. Bartling

Suggested content descriptor keywords:

Terrorism, C-TPAT

A Seminar Paper

Submitted to the Graduate Faculty of

the

University of Wisconsin, Platteville By

Michael D. Smith

in Partial Fulfillment for the Degree of

MASTER OF SCIENCE IN INTEGRATED SUPPLY CHAIN MANAGEMENT

Year of Graduation: Summer 2018

Abstract

The subject of this paper will revolve around terrorism, and how it has changed the way the world practices it's supply chain activities. This paper will explore the history of terrorism in order to better understand the mindset of a terrorist, and how a logistician needs to be mindful of how to take action to combat these evil forces. The majority of the literature and references used for this topic are current or published within the last ten years. Terrorism itself has been a problem for society throughout history. While this research paper will explore the origins of terrorism and its roots, the focus of this paper will be on current events and the recent rise in terrorism, its effects on supply chains, and how globalization has brought the world closer together not only for logisticians and supply chains but for terrorist organizations as well.

Table of Contents

I. Introduction

Everyone remembers where they were the morning the twin towers suddenly erupted into a ball of flame. It was a moment that shook not just the United States but the world. In one event the world seemed to become filled with evil men and suddenly terrorism was born. One would have thought terrorism had never existed prior to 9/11. While this isn't true in some ways a new modern terrorism was born on that day. The world was introduced to a new enemy and terrorists were around every corner waiting to strike. The events of 9/11 brought terrorism to the forefront of political debate and set the stage for the beginning of the Global War on Terrorism that the United States and its allies have continued to fight till this day. It soon would become apparent to corporations around the world that this modern age of terrorism would require new methods to combat and protect its business investments. Specifically, its supply chains that are typically most venerable.

Supply chains have exploded since the creation of the internet. The benefits of being globally connected through an online interface changed how companies do business. Specifically, the speed at which supply chains could operate. These effects were felt globally as well. The world became smaller as the effects of globalization took hold on the world. The benefits of globalization can be applied to more than just business and commerce though. Terrorism at its core took advantage of globalism and applied many of its principals to administrating evil around the world. The same tools that made it easier for supply chains to decrease delivery times and improve communication across the world were implemented by

terrorists as well. This speed and open communication changed the way terrorist organizations conducted business. It's because of this threat, logisticians and businesses need to react.

The definition of terrorism according to Merriam Webster is "the systematic use of terror especially as a means of coercion." (Webster, 2018) Terrorism at its core is appalling and disturbing on many levels. Terrorism is the unfortunate cause of thousands of deaths and leaves an aftermath of destruction in its wake. It is the intent of this study to focus on the aftermath of destruction terrorism causes. In this case the damage and destruction terrorism impose on supply chains and businesses around the world. This approach to research may seem callus and dehumanizing but that is not the intent of the study. By determining how terrorism hinders supply chains logisticians, organizations should be able to prevent many acts of terrorism and give terrorist organizations another front to fight.

Statement of the Problem

Supply chains are becoming the target of acts of terrorism across the globe. With an increased need for logistics and billions of dollars of merchandise being moved across the world, supply chains are becoming soft targets for terrorist organizations to target. These attacks cause damage to physical, intellectual, and human life. On top of that successful attacks help terrorist organizations continue to spread their ideologies and help fund the terrorist organizations.

Business, Organizations, and Countries need to come together to address these issues and continue to fight and develop strategies to minimize this threat as much as possible. The more terrorist organizations are kept at bay the harder it is for terrorism to be effective. Developing methods to fight and protect supply chains from terrorist acts needs to be the globally accepted norm and become the gold standard of any supply chain.

Purpose of the Study

The Primary purpose of this study is to explore the history behind terrorism, how its evolved, and how it affects supply chains around the world. This study will explore supply chain security and how the industry has fought terrorism on many different fronts. This paper will explore current and perspective ways supply chains and countries can achieve continued success against terrorist activities.

Significance of the Study

Exploring terrorism and its effects on supply chains in this study will not solve the security issues that supply chains face. The study will allow for a deeper discussion into the topics and issues that supply chains and logisticians face, including possible ways to combat common problems that supply chains face. Terrorism will never be something that society eradicates. It will always be an issue that continues to harass society and needs to be something taken into consideration by logisticians and organizations when developing strategy. This study will act as another medium for supply chains to draw on.

Assumptions

This study adopts the viewpoint that supply chains are severely unprotected and only recently steps have been taken to secure them. The need for heightened security became apparent to the world after the events of 9/11 took place. Since that time businesses have been playing catchup with their security efforts. Corporations have been required to conduct business differently and recently within the last 10 years have begun the beginning steps to improving supply chain security for the world. The problem continues to be ensuring equal protection of supply chains is enforced not only in first world countries but around the world. Terrorism is a global force that can have far reaching effects around the world. Ensuring supply chains are safe

from harm is the next step to fighting terrorism. A fresh awareness to the real dangers imposed on logistics creates the opportunity for new insightful innovations in the security of supply chains and the world.

Delimitation of the Study

This study will stay within the realms of regular acts of terrorism, piracy, and cyber terrorism. There are many forms of terrorism but these three are the largest forms that affect supply chains. The study will discuss ways supply chains and logisticians are currently fighting back and developing security measures to combat terrorism currently and possible ways organizations can fight terrorism moving forward.

Methodology

The primary approach for this project will consist of a secondary data analysis of research and statistics relevant to the topic presented as well as some primary research from nine years of service in the military. This unique approach to researching the effects of terrorism on supply chains is a special opportunity to discover the far reaching affects that supply chains and terrorism have on the world.

II. Literature Review

Terrorism has a long history with varied intensity throughout times past. Terrorism has an "unexpected, shocking and outrageous character." (Lanqueur, 1977, pg1) Even understanding the definition of terrorism, which is "the systematic use of terror especially as a means of coercion." (Webster, 2018) does not shed light on its complexities. Terrorism draws from a variety of backgrounds and ages. Terrorism has a close history with guerilla warfare. Guerilla warfare was often used by people to free themselves from a type of

political oppression. Many of the tactics and strategies of terrorism and guerilla warfare are similar but their end goals are vastly different. History also plays an influence on terrorism and determining how individuals are viewed. Certainly, had Britain won the Revolutionary War the Colonists would have been painted as rebel terrorists. While Webster has their definition of terrorism Lanqueur says it best "No definition of terrorism can possibly cover all the varieties of terrorism that have appeared throughout history: peasant wars and labor disputes and brigandage have been accompanied by systematic terror, and the same is true with regard to general wars, civil wars, revolutionary wars, wars of national liberation and resistance movements against foreign occupiers. In most of these cases, however, terrorism was no more than one of several strategies, and usually a subordinate one." (Lanqueur, 1977, pg5)

It's important to understand these situations can be breeding ground for terrorism and can certainly still affect supply chains. However, these events are typically somewhat predictable and are often the result of past political decisions of one kind or another. There is a trail of breadcrumbs so to speak of where these events started to fester and can often be predicted by historians, politicians, and economist in some shape or fashion. It's important as a logistician that these events are tracked and considered when creating and managing supply chains, but for the purpose of this study the type of terrorism that will be concentrated on will be organizations that use systematic terrorism as their one and only strategy as opposed to a subset of varying strategies. Organizations that use terror as their one and only means to spread their ideologies with no other notion or reason for their act except to spread evil in the world and further their cause.

Terrorism is by no means a new method adapted in the 21 Century. "The Mesopotamian Empire, that of Sargon of Akkad, was founded on terror. The same was later true of antiquity's

first military empire, the Assyrian, whose brutal methods of reprisal were intended to crush the spirit and break the will." (Chaliand, Blin, 2007, vii) In fact Al Qaeda can trace much of its roots back to the ancient civilizations of Assyria which date back to as far to the 23rd century BC. Another example of acts of terrorism come from 12th Century Genghis Khan. Genghis Khan was known for using terror to influence the people of his newly captured cities to stay in line. Genghis Khan would enter a newly captured city and kill all its city officials, appoint new men in charge, and then take the rest of the most educated men into his Army. This allowed his Army to gain new experienced soldiers and artisans and left weaker men with little education and experience in charge who were less likely to rebel against Genghis Khan. One does not have to look far to see terrorism was not just an act used by armies and political ideologies. Piracy was a huge problem between the 1500s and 1800s in the Caribbean. This form of terrorism was typically used by individuals for self-gain and continues to be an issue till this day. Terrorism has been sprinkled throughout history and conducted in many ways. One thing all terrorism has in common is the use of propaganda, intimidation, and the spread of fear and chaos against its enemies.

Terrorism like many things has found ways to transform and evolve over time. Like many things it has adapted and changed in order to find new ways to stay relevant. Terrorisms principal ideology, to use fear as a weapon, remains the same, but the way terrorist organizations go about inflicting fear is different. The three primary forms of terrorism this paper will explore will be traditional terrorism, piracy, and cyber terrorism. These forms of terrorism inflict terror in different ways and all of them can have different effects on businesses and supply chains.

Many of these terrorist organizations are based around radical Islam but there are subsets that are more politically driven that aren't determined by Islam such as the Real Irish Republican Army (RIRA) or the Lord's Resistance Army (LRA) out of Uganda. However, currently according to the Bureaus Foreign Terrorist Organizations the terrorist organizations at large is the Islamic State of Iraq and Syria ISIS. Just this year several subsects of ISIS have broken off and established themselves in the Pacific and Africa. This is one of the first major terrorist organizations that has been able to network itself across the world to this scale and in many ways Globalization is responsible. The ability to communicate across the world through different media outlets has allowed terrorist organizations like ISIS to be able to recruit easily, distribute propaganda via the internet, claim responsibility for terrorist acts, and coordinate terrorist attacks across the world. One of the major uses of internet by ISIS is to build their human trafficking network. "While it is well-understood that ISIS's kidnapping and enslavement of Yazidi women and other female prisoners constitutes human trafficking, less attention has been paid to the prospect that some of ISIS's female recruits from the West, who average 18 years of age, may also be considered victims of entrapment and trafficking because of the techniques used to lure these young women and how they are exploited upon arrival in ISIS-held territory." (Binetti, 2015, pg1). The Internet has made it easier for ISIS to coordinate and communicate within its network. The network ISIS is building around the world has piggy backed off the success of businesses around the globe and they have used this success to help fund piracy, cyber terrorism, and terrorist attacks against the West.

Foreign Terrorist Organizations

2/28/2018	ISIS-Bangladesh
2/28/2018	ISIS-Philippines
2/28/2018	ISIS-West Africa
5/23/2018	ISIS-Greater Sahara

The Modern Terrorist

September 9th, 2001 was a dark day for America and the world. On that day four planes were hijacked and flown into the twin towers and the pentagon, causing 2976 deaths. 9/11 became one of the most coordinated thought out terrorist attacks in Modern history and was the birth of modern terrorism. While there had been terrorist attacks in the past, such as the 1995 Oklahoma City bombing, or the 1988 United States Embassy bombing, nothing to this scale had been successfully accomplished. The 9/11 terrorist attack managed to give Al Qaeda and Osama bin Laden credibility and showed the world they were a viable threat to be considered. The attack on the twin towers had unprecedented effects on the people and the economy of the free world.

The 9/11 terrorist attacks caused a collective growth within the terrorist community. "Al-Qaeda's fortunes began to improve after the coalition's fatwa to kill Americans wherever they might be found. Until then, bin Laden's name and his cause had been obscure outside of Saudi Arabia and Sudan, but news of the fatwa excited a new generation of fighters." (Wright, 2006, pg262) This new unification of Al Qaeda was felt in more than just the US. After 9/11 there were 16 coordinated attacks that were conducted around the world. Most of these attacks were suicide car bombs which quickly became the most popular form of terrorism, but what was unique to these attacks was also the use of bio weapons such as anthrax. This posed major challenges for supply chains because they were inadvertently delivering bio weapons. London was attacked in 2005 when 56 people were killed in the London bombings. India was attacked many times and

suffered hundreds of casualties to suicide bombings. The country that suffered the greatest attacks after 9/11 however was Israel. Ultimately, 9/11 and its subsequent rise of terrorist activity lead to a new War on Terrorism that the United States and its Allies have been fighting to this day.

Terrorism had many effects on the world the upmost of them being the fear it caused. The recent 9/11 attack sent the transportation community into a panic, airports shut down security tightened, ports were temporarily closed and the stock market was shut down for four days. The attack caused the 2001 recession to continue when the stock market was opened on September 17th, 2001. On top of the economic and transportation effects it pulled the country into a war that's spanned 17 years and cost 2.126 trillion dollars. Security across the world was required to change. This hit hardest with Airlines that elevated their security protocols to require more extensive preflight security checks of all passengers and crew. "An economic study from Cornell University in 2007 showed that federal baggage screenings brought about a 6 percent reduction in passenger volume across the board, with a 9 percent reduction in the nation's busiest airports, totaling a nearly $1 billion loss for the airline industry." (Logan, 2018) The 9/11 terrorist attacks and subsequent attacks caused unseen ripple effects outside the immediate attack that many individuals failed to identify.

Modes of transportation became a targeted theme among terrorist organizations. It was around 2004 that African pirates, particularly Somalians, began to target commercial vessels. Piracy along the African coast has been a problem for generations. Piracy was one of the key factors that led America to the war of 1812, and was common place in Africa and the Caribbean in the 1800s. "On October 31, 1803 the United States frigate *Philadelphia* ran aground near Tripoli and was captured by the Tripolitans, who imposed the crew of more than three hundred,

including the ships commander, William Bainbridge. With a modern warship in its possession and hundreds of captives, Tripoli sharply increased its demands for tribute and ransom." (Lambert 2005, pg116) Though piracy had been common place in the past it had become less of a phenomenon in modern history and the resurgence of this terrorist act was a surprise to the Western world in 2006. Somali pirates began to attack commercial business vessels that lacked security. The ships that were being targeted by pirates were large cargo vessels. Typically, the pirates would use small quick boats and would us ladders and pully systems to board the vessel and take the crew hostage. Once the crew was apprehended the pirates would typically do one of two things. Either they would steal the goods and merchandise on the ships, or they would attempt to hold the crew for ransom. "It has been reported that about $1 million in ransom was paid out by ship owners in the region in 2004, with an average ransom fee negotiated at an estimated range between $50,000 to $100,000. In that year, forty sailors were kidnapped in about twenty incidents. Four seafarers were killed because of botched negotiations. By the end of 2005, there were five confirmed ransom-driven kidnappings in the Malacca Straights. The end of 2005 saw the final tally of kidnappings at ten reported incidents." (Gerard, 2006, xxvii) Attacks like this when successful would help fund terrorist organizations, future operations, and increase the scale of the organizations operations in the region. This new rise in attacks cost companies millions in lost merchandise and disruptions in supply chains.

TABLE 3
Quarterly Breakdown of Reported Incidents of Piracy/Armed Robbery At Sea in the Malacca and Singapore Straits, 2004-2006[19]

	2004				2005			2006	
	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter
Malacca Straits	2	3	3	5	2	6	No reports	No reports	2
Singapore Straits	5	1	No reports	No reports	2	4	1	No reports	Not available
Total	7	4	3	5	4	10	1	No reports	2

The threat to supply chains does not stop at just physical attacks on transportation carriers. The 21st century propelled the world into an age of technological advancement previously unknown. The internet and computers allow people to store vast amounts of information and give the ability to share it virtually anywhere in the world. Warehouse Information Systems changed how supply chains were tracked and operated around the globe. Banks and businesses moved many of their systems to digital computer systems and stored banking records and personal information on personal servers instead of in file cabinets. The technological advancement drastically improved efficiencies and helped surge business growth. Businesses were able to create an organization that is interconnected and able to react and adapt quickly. What was difficult to anticipate was how the internet and the move to digital platforms would be threatened by cyber terrorism. The internet that made it so easy to communicate and do business also made it easy for hacking and malicious acts of cyber terrorism. Personal information, bank accounts, and even department of defense systems were being hacked and controlled by individuals across the world. In some cases, the acts were carried out by individuals and in some unique cases they were even carried out by countries such as North Korea. There were growing worries of missile defense systems being hacked and controlled by

foreign enemies and an increase in successful hacks of businesses that stole personal confidential client information. This new threat previously unseen became another front for terrorism and a new battleground for Governments and business to conquer. “In July 2001 the Justice Department announced the formation of ten Computer Hacking and Intellectual Property (CHIP) units based in U.S. attorneys’ offices across the country and dedicated to prosecuting cybercrime. In the aftermath of September 11, the White House announced the appointment of a special advisor for cyberspace security. In addition, the FBI announced an overhaul of its top management that places more emphasis on counterterrorism and cybercrime. Included in this overhaul is the creation of a new division on cybercrime within the Bureau’s criminal investigation section.” (Sherman, 2002, pg1) This new threat with the added attack on the twin towers helped lead to the passing of the controversial Patriot Act. The 9/11 attack also showed the need for cyber security in the airline industry. “Transport and particularly aviation and the related supporting infrastructure, have increasingly been targeted by terrorists,16 and IT strikes at gross stupidity and ineptitude not to envisage a day when aviation will be targeted by a cyberterrorist. Cybersecurity and cyber-terrorism are invariably the current challenges that need to be acknowledged and most importantly collectively reacted to by the international world.” (Fox, 2016, pg196). While 9/11 was a terrible moment in the worlds history it was a pivotal point at which the world realized security and logistics needed to change.

How Terrorism affected Supply Chains

The lack of security became apparent. “Immediately following the September 11 attack, the US had a somewhat uncoordinated response, marked by closed airports and borders. Conflicting government calls to be on the alert, while leading normal life, followed this. In the

months following the attack The US has started to settle into the long-term reality. This reality is marked by added security costs, added administrative costs, and longer, as well as less certain transportation times due to security checks." (Sheffi, 2001, pg140) Osama Bin Laden's 9/11 terrorist attack caused businesses to reevaluate business strategies they were using. One of the strategies that businesses would have to change drastically was their supply chains. This became apparent when the transportation grid simultaneously halted. "Shortly after the September 11th, 2001 terrorist attack, many manufacturers experienced disruptions to the flow of raw material and parts into manufacturing plants. For example, Ford had to idle several of its assembly lines intermittently in the days following the attack, as trucks loaded with parts destined to these production plants were delayed at the Canadian and Mexican borders. As a result, Ford lost 12,000 units of production. And as reported by the wall Street Journal (Ip 2001), Toyota came within 15 hours of halting production at its Sequoia SUV plant in Princeton, IN, since one of its suppliers was waiting for steering sensors, normally imported by plane from Germany, and air travel was shut down." (Sheffi, 2001, pg128) Plants around the US were suffering similar problems, their supply chains had been halted or their inventories were running extremely low.

"The reason that Ford, Toyota, and other leading manufacturers were vulnerable to transportation disruptions is that they operate a "Just-in-Time" (JIT) inventory discipline, keeping just enough material on hand for only a few days and sometimes only a few hours of operation. The system requires frequent deliveries of material and a reliable transportation system." (Sheffi 2003, pg128) Just-in-Time principals drive down inventory levels, help reduce production time, and response time with suppliers. Using Just-in-Time principals are great for cutting costs and improving efficiency but are devastating when there are disruptions. The

problems 9/11 presented manufacturers and logisticians was made apparent that day. Alternate methods of production and transportation were needed to stay competitive and combat the effects of terrorism.

The need for supply chain security was on the forefront of issues businesses were fighting after 2001. The attacks helped to identify weaknesses in their system and provided an opportunity to make a weakness a strength. "Following the September 11 attack, many US companies started re-considering the wisdom of using overseas suppliers. The choice is between a close-by US supplier and international (mostly but not exclusively third world) suppliers. Offshore suppliers may be less expensive but require longer lead-time and may be susceptible to disruptions in the international transportation system. Local suppliers may be more expensive but closer (and, arguably, less vulnerable) and therefore able to respond faster. Instead of choosing one alternative over another, the solution may include both – using offshore suppliers for the bulk of the procurement volume while making sure that a local supplier has the capability to fill the needs, by giving it a fraction of the business." (Sheffi 2003, pg130) This was one of the first steps companies took after 9/11. Increasing the number of suppliers, a business used provided a company with options in the case of an inability to deliver. While this may not seem as important in the case of a company like Ford a hospital dependent on delivery of blood, plasma, or essential surgical equipment must be able to maintain its inventory to stay operational at all times. Modern terrorism threated this ability and forced companies to consider alternative suppliers when creating their supply chain.

Another step organizations took was to move away from Just-in-Time processes. The benefits of Just-in-Time manufacturing were enormous however and abandoning the processes all together was not a wise option. The principal many organizations developed was a mixture of Just-in Time and carrying safety stock. "The temptation is to start accumulating inventories "just-in-case" something happens again. Some companies are looking to ordering parts in larger quantities and creating new safety stocks to keep their assembly lines moving in case their inbound transportation is disrupted. In addition, they plan to keep more finished goods on hand so their customers can be supplied even when the manufacturing process is disrupted." (Sheffi 2003, pg132) This principal was referred to as a dual inventory system. The idea being that companies for all intents and purposes would carry a second safety stock that would only be drawn upon in extreme situations. "To create a dual inventory system logistics manager should designate a certain amount of inventory as "Strategic Emergency Stock." This stock should not be used to buffer the day-to-day fluctuations of the processes it feeds. Instead, it should be managed using an inventory discipline that can be summarized as: "Sell-One-Store-One" With this discipline the reorder quantity of the items in the strategic emergency stock is raised by the number of item required in this inventory. Then this inventory is managed in JIT fashion – when an item is drawn upon, it is replenished immediately regardless of changing daily needs. Furthermore, this inventory can be drawn upon only in case of an extreme disruption, possibly requiring approval at a high level of authority within the organization." (Sheffi 2003, pg133) This dual inventory was originally created for situations like terrorist attacks but could also be used in extreme weather situations that may lead to natural disasters. Such as Hurricane Harvey or Hurricane Sandy.

Security businesses gained massive amounts of market share from the increased terrorist activity. From physical security to digital security companies were realizing the need for increased safekeeping of information and products within their organizations. The transportation field saw massive overhauls as terrorism continued to disrupt travel and logistics. The TSA was created and helped airports in the US crack down on security. It would now take passengers hours to get through a series of security checks, but the US was determined not to let another plane hijacking occur. Companies began to hire physical security for freight ships to combat the resurgence of piracy in the Straits of Hormuz. Ships were also retrofitted with anti-piracy measures like high pressure water cannons to fight off small invading ships. Governments began to implement new cyber terrorism counter measures. Organizations began to implement organic cyber warfare teams that would combat cyber-attacks. The majority of this infrastructure started to defend department of defense computer systems but banks and business organizations began to see the importance of having teams dedicated to securing servers and private information.

Another unique problem terrorism presented the world with was global supply chain security. Importing and exporting products has always been a tricky process that requires large amounts of oversight and security. Ports are typically where products get held up and must be stored for a period of time and consequently it is also the most likely location for terrorist organizations to be able to effect shipments. If not secured properly large amounts of food shipments could be tainted or tampered with causing serious death or injury to thousands of people. Having a system that allows rapid exchange of products was important for maintaining fast delivery times and proper security. On top of this concern there was also a large need for supply chain uniformity among other countries. Globalization had decreased the size of the

world and trade between countries was easier and more attainable than ever before. The problem this presented was the inconsistency of security procedures from country to country. A package from the US may have RFID tags, tough packaging, and several forms of paperwork required to ensure proper safe deliver as opposed to the same product being shipped from Taiwan. The product from Taiwan may have no RFID tag, second rate packaging, and have different paperwork expectations than the US. This presented a large problem with organizations doing business overseas because there was no uniformity of security with imports and exports. What one country required another one didn't.

The larger issue inconformity presented was the threat of nuclear devices being snuck into a country. Exports coming from countries like the United States, England or France were thoroughly checked and secured before being shipped overseas. Third world countries however, had varying expectations and requirements. There was a greater fear that one of these countries would not properly secure its exports and weapons of mass destruction would be smuggled into a city like London, or Los Angeles. While this was becoming a large concern for the supply chain community it was not a large enough issue for the United Nations. It became apparent that a global organization would be needed to incentivize organizations to join and adopt the same standards for dealing with imports and exports. What was created out of this need was an organization called Customs Trade Partnership Against Terrorism C-TPAT.

C-TPAT presented the solution of a unified method of shipping and receiving products from other countries. C-TPAT presented a minimum-security standard that all members must meet with their imports and exports to become a certified affiliate. To incentivize countries and

business organizations into becoming a member of C-TPAT the organization developed a process that allowed for C-TPAT members to have prioritized shipping with customs. Being a C-TPAT member allowed your products to get through customs faster than a non- C-TPAT member and ensured the proper security measures were being followed around the world. "When an entity joins CTPAT, an agreement is made to work with CBP to protect the supply chain, identify security gaps, and implement specific security measures and best practices. Applicants must address a broad range of security topics and present security profiles that list action plans to align security throughout the supply chain." (DHS, 2018). The C-TPAT organization has increased shipment visibility, allows for a unified global shipment system, and helped minimize the threat of terrorism disrupting supply chains. This has not solved all the security problems in the US though. Many organizations choose not to participate in the program. "For a private company there exists a trade-off between the cost of compliance with C-TPAT and the benefit of reduced congestion costs associated with the inspection of its containers. The US government faces a trade-off, between the security benefit derived from increased inspection of incoming containers and the adverse impact of the resulting congestion. The government must also consider the financial burden stemming from the need for additional security infrastructure." (Gans, 2007, pg3) While many businesses have embraced the idea of streamlined uniformed security some private companies aren't willing to foot the bill.

The financial and legal ramifications of fighting terrorism did not come without a price. Many companies were spending large sums of money they previously had never had to spend on security. The airline industry was impacted greatly. "New analysis from Frost & Sullivan, Global Airport Security Technology Market Assessment, finds that the market earned revenues

of $8.22 billion in 2014 and estimates this to reach $12.67 billion by 2023. The study covers the segments of perimeter security, command, control and integration, cybersecurity, communications, surveillance, access control, and screening. Cutting-edge technologies in the screening, big data and integration markets are particularly driving upgrades and new investments in the airport security market. Over the next 20 years, however, cybersecurity spending will rise at the fastest pace." (Security News Desk, 2015) Airports are spending large amounts of money on maintaining security, particularly in cyber security, an industry that continues to have large growth. Since 9/11 the war on terror has cost $2.126 trillion dollars from 2001 to present day. Since the modern terrorist was born businesses and the government have continued to make changes to improve security in the transportation sector. The effects of terrorism have driven innovation and improvement throughout the community.

Discussion How Supply Chains Combat Terrorism

Between the terrorist attacks across the world and the new prolonged wars fighting terrorism organizations, supply chains realized they would need to come together to avert the effects of terrorist attacks. While many realized the risks of terrorism it didn't take long for the new wave of terrorism to become the status quo. Companies that continued to take threats seriously began to build more resilient supply chains that were able to react to sudden changes or threats in the market. In an article about supply chain resiliency the author points out, "To many shippers, Plan B largely means building in more safety stock. Sheffi stresses he is calling for changes in supply chain management, however, not just more inventory. "Companies by and large do not put more redundancy in, do not put more safety stock in, and rightfully so. The good

companies build in flexibility instead of redundancy," Simply having more inventory on hand does not solve the problem of being able to react to an issue. Investing in supplies on multiple continents, building relationships with suppliers, and creating transparent customs and security was how supply chains accomplished this.

One interesting option some companies adopted was the introduction of a Chief Security Officer. The CSO is responsible for keeping the executive team in touch with the threats of the business world. "The CSO will have to be, first and foremost, a *businessperson* who is familiar with the enterprise and in getting things done in a corporate environment. The reason is that every person and organization is subject to a strong temptation to return to normalcy; return to the days when nobody had to worry about terrorism and bio-attacks. The CSO and the security organization will have to continuously fight this temptation. They will face many of the trade-offs mentioned above on daily basis, and will have to create the constituency to follow through with the required investments and changes to corporate life." (Sheffi 2003, pg145) This approach has helped guide executives in their thinking and allowed a voice in strategy meetings to those considering how to direct the business.

A big problem business faced as individual organizations was the lack of support their organizations were getting from the government. Government had long been a necessity for foreign trade. The government determines what countries can be traded with, what items can be traded, and the taxes and tariffs that will be implemented on imports as they come into the country. For this reason, governments run customs and all businesses must go through customs

when doing business outside their country. Business had no say over how customs was run but this needed to change. Perhaps the biggest change that came from this need was C-TPAT.

C-TPAT became the first voluntary program that was built around a cooperative relationship with government and business. "When you're in C-TPAT, you're supposed to try to use other C-TPAT member-certified companies," says Terrie Gleason, a trade regulation and customs attorney for Baker & McKenzie. In Washington, D.C. "So, there can be a funneling of business" toward companies that adhere to the standard. C-TPAT membership also sends a signal to both current and potential customers that a company is serious about security and its relationship with customs authorities. "There is a sense of' good citizenship' in all of this," notes Gleason. (Edwards 2006, pg81) The benefit of fast shipping does not come free though. The C-TPAT programs unique security requirements push organizations that join to improve internal security systems within their organization. The hope is that the incentive to have faster customs will push businesses to practice safe secure practices that improve supply chains and overall business security. The fact that over 7000 companies have joined the program shows that the initiative for better customs security has improved the way logistics has operated. The success of a voluntary joint run organization between business and government is rare. The new system has helped keep supply chains safe since its introduction and C-TPAT continues to push the boundaries of security.

Containers were used long before 9/11 but today it is the main method of shipping product overseas and by rail. In 2004, $423 billion in goods entered the US in 15.8 million containers. Almost half of the $2 trillion in international goods transported through the US in

2000 was shipped in containers, and the international tonnage of trade through the US is expected to double by 2020 (Greenberg et al. 2006). Customs and Border Protection uses risk management techniques to scree these containers for potential anomalies. The issue with some of these techniques is the amount of time it takes to inspect containers. Many of these checks slow down the shipping process. C-TPAT helps prevent some of these issues but searches still must be done. Several ways companies are helping fight issues with container security by using RFID tags and GPS devises. These devices help identify loads and allow logisticians to track containers around the world wherever they are in the shipping process. This is something the United States military does with all its shipments. During one of my rotations overseas we shipped a Brigades worth of vehicles and equipment to South Korea. This task of shipping everything took a about a week and required paperwork for every vehicle and every shipping container being shipped. Most of the time was spent with paperwork. All paperwork had to have five copies. One for inside the vehicle or container, one for the packet on the outside of the container, one for the exporter, and the additional paperwork for documentation. On top of documentation vehicles and containers were sealed and RFID tags were used on every vehicle and shipping container to be able to track its shipping progress throughout the trip. Not only did this allow us to track our shipment but it kept us informed as to when we would be receiving our shipment as well. This was important because a lot of the containers required special security details and our containers and vehicles were not in the railyard unsupervised because we knew when they would be delivered. This technology is relatively new and while it doesn't stop security threats it does keep supply chain managers informed. They can track their goods and know if a shipment is on time or staying on route. This allows a visibility in supply chains previously un heard of.

Despite security increases in supply chains and customs there is still issues with terrorism. ISIS and other criminal organizations continue to test ways they can get around the security systems in place. Increases in security have prevented any major hijackings since 9/11 but there has been an increase other terrorist activity such as car bombs, shootings in busy city centers, and a recent trend of driving vehicles down busy streets and sidewalks. While many of these situations are tragic none have seemed to have quite the effect of 9/11 on supply chains. Many of these attacks have caused issues for the final customers in supply chain. Many of these attacks are also being conducted in the Europe where travel from country to country is easier. "In 2016, there were 346 attacks in just one year — that's an 8.5% rise on the previous year, averaging 6.7 attacks every week." (Hines, 2017) Clearly terrorism is still a threat. In many ways it's an even bigger threat today. Hines expresses that because of the rise of terrorist attacks organizations "must include actions such as diverse footprint, secondary suppliers for the same components, emergency changes on factories set up. These actions are used to compensate losses/disruption of the supply chain flow. "Furthermore, real-time data acquisition, big-data analysis, and effective planning are the key to fast reaction times for corporations once an attack/ disaster happens. The sooner the corporation takes action in order to mitigate disruption, the less its flow will be affected."" (Hines, 2017) Businesses that fail to do these security tasks put their organization at risk for supply chain disruption, and for some supplier's disruption isn't an option.

Many of the strives for better security and diversified business has inadvertently caused transportation to become more secure. The airline industry has had the most overalls since the

implementation of tighter security and has made flying on the airline safer than ever before. While longer security lines are still needed incidents due to lack of security have been few and far between since 9/11. Not only that but the security industry has made leaps and bounds with the technology being used to screen passengers. New x-ray machines make security less invasive and give TSA agents a depth of security tools to pull from. These improvements in technology not only make screening passengers easier but also improve wait times of passengers in line. Airlines themselves also improved their security onboard their flights making it tough to get into the cockpit and training flight attendants the proper way to respond to possible hijackers in the case of an emergency. New screening "for all air cargo destined for a passenger aircraft originating in the United States of being shipped from overseas to the United States" (Cook, 2012, pg3) was also recently instituted. This new law was implemented by the TSA in 2010 and allows all air freight entering the United States to be properly screened before arriving.

Traveling by road has become safer for companies as well. New GPS systems can track truckers on their route and notify logisticians should the truck take the wrong route, drive too long, too fast, or stop for long periods of time. This allows supply chains to develop tight schedules that make it difficult for interference. This system has had some kick back from current truckers on the road but has made the practice safer. This is especially true for companies transporting hazardous waste or products that require tight security. Railways have also become safer for travel and transport in light of terrorism. After the attempted hijacking of a train headed from Amsterdam to Paris trains and train stations implemented increased security measures that helped secured trains from possible hijackings and increased active monitoring systems in train stations across Europe.

Sea travel has also become safer for supply chains. Many of the issues with terrorism and pirate attacks caused shipping companies to overhaul the system. The most important of those being the container security initiative of 2002. “Every year some 200 million sea cargo containers move among the world’s top seaports. In the U.S., nearly 50 percent of the value of all imports arrive via sea container. In January of 2002, U.S. Customs launched the Container Security Initiative (CSI) to help prevent global containerized cargo from being exploited by terrorists. Now within the Department of Homeland Security, Customs and Border Protection (CBP) continues to implement CSI at major ports around the world.” (Cook, 2012, pg279) When importing shipping vessels are also required to adhere to Importers Security Filing Program (ISF) “Customs and Border Protection now requires importers to file advance manifest security information in addition to the carrier requirements outlined in the CSI’s 24 hour manifest rule for carriers. Importers must submit information in a timely and accurate manner to avoid costly fines and penalties and structured at $5000.00 USD per errant or late filing.” (Cook, 2012, pg279) These new regulations make it difficult for ships to sneak on extra cargo which has been essential to security concerns for many in the government. Many organizations in the Government worry of the threat of nuclear or bio weapons being snuck into containers and with 200 million to choose from it is a daunting task to secure every single one and ensure each one is safe to enter the country. Thankfully recent regulations being implemented make it difficult to tamper with commodities. Cargo ships have also begun to hire organizations like Solace Global and Hudson Analytix who specialize in private cargo ship security. These organizations provide expert security for cargo vessels and allow cargo vessels to go through more dangerous waters. This allows ships to save time in shipping and acts as an active deterrent for pirates and terrorist

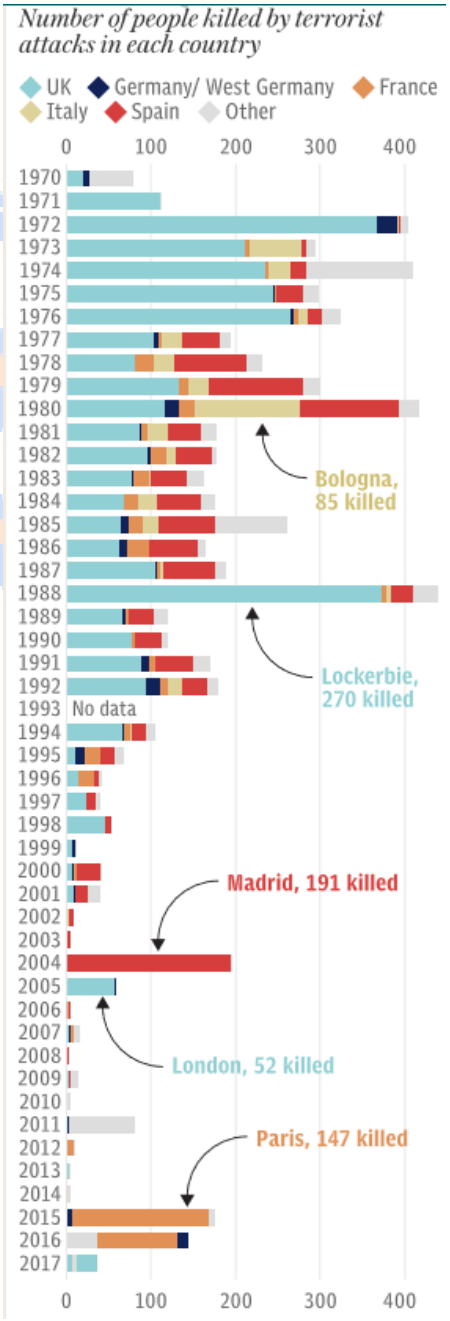
organizations. Many changes have been made to help make maritime transportation a safe secure operation and prevent possible acts of terrorism against it.

These improvements in security show the increased awareness that modern terrorism has brought to the supply chain industry. The industry has made great strides to improve security measures across the many facets of the trade but there is one great risk that must be avoided at all costs if supply chains wish to continue to see success. That risk is complacency. Nothing threatens the industry as a whole more than complacency. History would show that often after a large event like 9/11 there is a huge swing to counteract the threat. The trend after this is to slowly fall back into a state of unpreparedness until the next great catastrophe hits. While the practice of safe secure supply chains continues to be stressed complacency is the one thing that future operations and businesses may forget or see as unnecessary as time goes on.

It is vital that lesson learned registers continue to be passed on to future generations of business managers. Boards and executives must stress security when developing business strategy and help create a culture of preparedness. In doing this organizations can change the mentality of security, and make it necessity instead of an exception. Too often businesses are reactive instead of proactive or preventive. Supply chains need to continue to have a mind towards how they can improve and differentiate themselves from their competitors. Security is an item that can be done to prepare an organization for the unlikely day there is disaster. While it won't seem like the business is accomplishing anything in the event it is needed the supply chain will out preform competitors who are unprepared and allow an organization to gain market share. Security is one of the pillars of any good supply chain and the benefits of conducting good security practices in supply chains far outweigh the downsides, such as extra cost, or

differentiation of suppliers. All supply chains must conduct some sort of cost benefit analysis but cutting on security should be an item supply chains avoid cutting at all costs.

Politically the United States continues to pave the way for security initiatives across the world. C-TPAT has recently had more global recognition with the acceptance of Mexico, Israel, and Singapore as partners in 2014, but more global cooperation is needed to help combat the rise in terrorism. Just in the last three years there has been a resurgence in terrorist activity in Europe. The United States not only drives innovation in security programs but also spends a significant portion of its security budget on maintaining security forces in Eastern Europe. NATO has a commitment that all organizations must meet two percent GDP spent on military spending by 2022 in order to better secure Europe as a whole from terrorist threats and prevent continued aggression in Eastern Europe. As time goes on more universal support will be needed to ensure the terrorist threat is kept at bay. The more countries and businesses can come together to fight terrorism the more difficult it becomes for terrorist organizations like ISIS to gain momentum and build a base to operate. The US continues to lead the way on most large political and economic decisions and will continue to set the standard for supply chain security by pushing businesses and other countries into necessary security compliance.



Conclusion

Terrorism continues to evolve it is unfortunately a threat the world will always face and there is no way to completely avoid it. Eventually there will be another big attack. Countries and businesses must continue to do everything in their power to stay ahead of the threat. 9/11 and the subsequent events that took place shocked the business world. It showed organizations were unprepared for outside threats. Today the world has changed and while terrorism continues in new ways so do the methods of combating it. Organizations must continue to innovate and secure what's most dear to them. There must be corporate responsibility within organizations to secure their organizations against terrorism. The world will not be safe as long as our supply chains are at risk. General Mattis said is best. "There are hunters and there are victims. By your discipline, cunning, obedience and alertness, you will decide if you are a hunter or a victim." While a business is not hunting for a fight it can decide if it will be the victim. The security of the world starts with the security of our supply chains. Only in doing this will the world begin to have success at defeating evil men with terrible intentions, and in so doing protect the ones we love.

Bibliography

1. Nardo, Don. *The History of Terrorism*. Compass Point Books, 2010.

2. Chaliand Gérard. *The History of Terrorism: from Antiquity to Al Qaeda*. Univ. of California Press, 2009.

3. "Foreign Terrorist Organizations." *U.S. Department of State*, U.S. Department of State, www.state.gov/j/ct/rls/other/des/123085.htm.

4. Weatherford, J. McIver. *Genghis Khan and the Making of the Modern World*. Three Rivers Press, 2012.

5. Isis-international-bulletin-no24-women-and-new-technology-sept-1982-39-pp. (n.d.). *Human Rights Documents Online*. doi:10.1163/2210-7975_hrd-1043-0025

6. Wright, L. (2018). *The looming tower: Al-Qaeda and the road to 9/11*. New York: Vintage Books, a division of Random House.

7. Ong-Webb, G. G. (2007). *Piracy, maritime terrorism and securing the Malacca Straits*. Singapore: ISEAS.

8. Shenon, P. (2009). *The Commission: The uncensored history of the 9/11 investigation*. New York: Twelve.

9. Amadeo, Kimberly. "How the 9/11 Attacks Still Damage the Economy Today." *The Balance*, The Balance, www.thebalance.com/how-the-9-11-attacks-still-affect-the-economy-today-3305536.

10. "The Effects of 9/11 on the Airline Industry." *USA Today*, Gannett Satellite Information Network, traveltips.usatoday.com/effects-911-airline-industry-63890.html

11. "Supply Chain Response to Terrorism." *Jon*, web.mit.edu/scresponse/.

12. web-a-ebscohost-com.ezproxy.uwplatt.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=e7b826c8-1592-4977-8f03-1cde91160586@sessionmgr4010

13. "Figure 2f from: Reshchikov A, Van Achterberg K (2014) Review of the Genus Metopheltes Uchida, 1932 (Hymenoptera, Ichneumonidae) with Description of a New Species from Vietnam. Biodiversity Data Journal 2: e1061. Https://Doi.org/10.3897/BDJ.2.e1061." doi:10.3897/bdj.2.e1061.figure2f.

14. search-proquest-com.ezproxy.uwplatt.edu/docview/1831362097?rfr_id=info:xri/sid:primo.

15. Linn, Allison. "Post 9/11, Surveillance Cameras Everywhere." *NBCNews.com*, NBCUniversal News Group, 23 Aug. 2011, www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere#.WzjxR-S0We0.

16. "CTPAT: Customs Trade Partnership Against Terrorism." *Border Patrol Overview | U.S. Customs and Border Protection*, www.cbp.gov/border-security/ports-entry/cargo-security/ctpat.

17. opim.wharton.upenn.edu/risk/library/WP2007-11-19_NB,NG_ContainerSecurity.pdf.

18. "Growing Passenger Volumes and Advanced Threats Spur Global Airport Security." *Security News Desk*, 10 Mar. 2015, www.securitynewsdesk.com/growing-passenger-volumes-and-advanced-threats-spur-global-airport-security/.

19. web-b-ebscohost-com.ezproxy.uwplatt.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=45ad0541-048b-41f4-8c74-7ca0527831d8@pdc-v-sessmgr01.

20. web-a-ebscohost-com.ezproxy.uwplatt.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=6f2a5fb7-ca04-4f22-9e76-d2f12bb58ea7@sessionmgr4010

21. "Terrorism and the Global Supply Chain: A Growing Threat." *Digital and Content Marketing*, 26 Sept. 2017, www.fronetics.com/terrorism-global-supply-chain-growing-threat/.

22. Chrisafis, Angelique. "France Train Attack: Americans Overpower Gunman on Paris Express." *The Guardian*, Guardian News and Media, 22 Aug. 2015, www.theguardian.com/world/2015/aug/21/amsterdam-paris-train-gunman-france.

23. Kirk, Ashley. "How Many People Are Killed by Terrorist Attacks in the UK?" *The Telegraph*, Telegraph Media Group, 24 Mar. 2017, www.telegraph.co.uk/news/0/many-people-killed-terrorist-attacks-uk/.