CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
CSC 32 / CCEM 32

EXERCISE/EXERCICE
NEW HORIZONS

SHIPPING CONTAINER SECURITY – OUR ECONOMIC TROJAN HORSE?

By LCdr Douglas McDonald

18 April 2006

ABSTRACT

This paper will argue that despite increased efforts to improve shipping container security, vast portions of the global containerized supply chain remain unprotected and vulnerable to exploitation by criminal elements and terrorists. Even with these vulnerabilities, there is a reluctance to impose truly meaningful security measures due to the fixation of nations on the maintenance of their economic growth and the cut-throat competition within the shipping industry to remain profitable. The global containerized system will be analyzed by breaking down the containerized supply chain into three interdependent and interacting networks: a *physical logistics network*, a *transactional networ*k and an *oversight network*. The paper will conclude that the only viable way to remove the existing security vulnerabilities is to focus on the grassroots development and rapid introduction of security measures that will also provide secondary economic benefits to sea freight customers as well as the companies that move the freight throughout the global containerized supply chain.

> **"The global container supply chain moves cargo rapidly across seas and into ports throughout the world. A well-planned terrorist attack taking advantage of this system could occur anywhere, at any time. The significance of such an attack would be measured in terms of significant loss of life and billions of dollars in economic damages."[1]**

INTRODUCTION

Today's global economy is almost entirely dependent on the sea for the transport of goods from supplier to consumer. It is a worldwide reality that products are no longer manufactured just down the road, markets have expanded to the point that manufacturers spread their products around the world to satisfy global consumer demands. In 2003, well over 90% of worldwide cargo moved via sea containers[2] using a global inventory of approximately 15 million containers. These containers were loaded, shipped and unloaded numerous times around the world, representing a total of approximately 250 million individual container moves during that year.[3] Historically, container security has always been a concern of the maritime shipping industry, but primarily from an anti-theft perspective. However, the events of 11 September 2001 quickly made the world realize that if airliners could be used by terrorists as weapons, why not shipping containers?

The approach taken by this paper in its examination of the global containerized supply chain was to adopt the framework of assessment suggested by Willis and Oritiz in their 2004 RAND technical report.[4] In that report it was suggested that the supply chain

---

[1] RAND Corporation, "Assessing Container Security: A Framework for Measuring Performance of the Global Supply Chain," *RAND Infrastructure, Safety, and Environment* (2005) [Research Brief]; available from http://www.rand.org/pubs/research_briefs/RB9095/index1.html; Internet; accessed 16 February 2006.
[2] Maarten Van de Voort and Kevin A. O'Brien with Adnan Rahman and Lorenzo Valeri, *Seacurity: Improving the Security of the Global Sea-Container Shipping System*, Workshop Report MR-1695-JRC (Santa Monica: RAND Europe, 2003), 1.
[3] Ibid., 12.
[4] Henry H. Willis and David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*, (Santa Monica: RAND Corporation, 2004), ix.

should be viewed as three interdependent and interacting networks: a *physical logistics network*, a *transactional networ*k and an *oversight network*. The *physical logistics network* is comprised of the containers, the ships, the land vehicles and the ports that physically move the goods, the *transactional network* manages the information flows between suppliers, customers, shippers and regulators to procure and distribute the goods and the *oversight network* implements and enforces rules of behaviour within the other two networks through standards, fines and duties.

The analysis presented in this paper will show that despite increased efforts to improve shipping container security, vast portions of the global containerized supply chain remain unprotected and vulnerable to exploitation by criminal elements and terrorists. Even with these vulnerabilities, there is a reluctance to impose truly meaningful security measures due to the fixation of nations on the maintenance of their economic growth and the cut-throat competition within the shipping industry to remain profitable. This paper will argue that the only viable way to remove these vulnerabilities is to focus on the grassroots development and rapid introduction of security measures that will also provide secondary economic benefits to sea freight customers as well as the companies that move the freight throughout the worldwide containerized supply chain.

HISTORICAL PERSPECTIVE

To examine the global containerized supply chain, it is best to start with the most tangible aspect of the supply chain and the one that is most visible and therefore most understandable to the general public: the *physical logistics network*.

Prior to WWII, all cargo that traveled by sea was loaded in bulk, a crate here and sack there, a piece of machinery in the corner. Such an approach required the goods to be packed and repacked at every stop along a trip. Even if a ship only had one destination, to fully unload it the cargo had to be manhandled from the hold into slings, craned onto the jetty, then loaded by hand onto pallets and moved by forklift into warehouses. It was a labour intensive operation employing many longshoremen and it would literally take weeks to unload a ship. Once off-loaded into the warehouses, the goods had to be repacked again into trucks and railcars for transhipment onto their final destinations inland.

As with many innovations, containerization was born out of wartime necessity. First used by the United States government during WWII, containers proved to be the ideal means of quickly and efficiently unloading and distributing vital supplies which needed to be quickly delivered to the troops. Instead of shipping commodities in bulk, army and navy specialists began to mix cargo by loading freight onto pallets then loading the pallets into specially constructed "boxes." Many post-war forward thinkers were heralding this new method of cargo handling as the wave of the future, but the shipping industry was sceptical. The main complaint from industry was that a move to containerization would require a massive worldwide retooling of ships, ports and inland distribution systems.[5] To the sceptics the investment required for a transition to containerization would be too expensive for an industry that operated on such slim profit margins.

---

[5] APL, "APL History – Containerization," http://www.apl.com/history/topics/innovate/contain.htm; Internet; accessed 18 February 2006.

It took until 1958 before one visionary company stepped forward with hopes of revolutionizing the industry. Looking for a competitive advantage, the American President Lines (APL) sent a fact finding team to 26 major ports around the world and their report concluded that switching to containerized freight was indeed economically viable. From that point forward APL began to incorporate containers into their operations and by 1971 a full 58 percent of their shipments were containerized. In 1973 APL again lead the field and took delivery of four fully containerized vessels.[6] Ships could now be unloaded in days rather than weeks. There was no longer a need to repack goods for reshipment inland. Containers were simply loaded directly onto specially designed railcars or trucks and delivered right to the customer. Speed of delivery was improved dramatically, labour costs were substantially reduced and savings could be passed onto the freight customers. All the while, the efficiencies of containerization protected the profit making capacity of the shipping company.

Once the competitive advantage was proven, the rush to containerization was on and the entire industry threw off the shackles of tradition and embraced the revolution of containerization to become efficient and remain competitive.

CANADIAN PERSPECTIVE

Canada was included in the revolution and today boasts two major container ports: Vancouver and Halifax, both operating at close to capacity. The revolution may have begun in the late-60's, but the demand for bigger container ships and larger capacity ports to service them is still growing exponentially. Today there are 140 container ships

[6] APL, "APL History – Innovate," http://www.apl.com/history/topics/innovate/innovate.htm; Internet; accessed 18 February 2006.

in service with capacities of greater than 6,000 TEU[7] and just a few years ago, container ships of 8,000 TEU were considered outlandish. But the confidence of the shipping industry in the economics of containerization has resulted in the present day usage of post-Panamax[8] container ships that have a capacity of 8,500 TEU and firm orders placed with ship builders for 10,000 TEU post-Panamax ships.[9] As stated in a Times Online article published on 7 September 2004:

> "World container trade has been growing at an average annual rate of 9.3 per cent, Drewry says, with volumes rising from 37.1 million TEU in 1993 to almost 91 million TEU last year. This is expected to reach 154 million TEU by 2010, with the main catalyst for growth coming from China."[10]

2005 figures indicate that 1.767 million TEU were shipped through the port of Vancouver[11] and 550,462 TEU were shipped through the port of Halifax[12]. In order to react to the projected growth in container traffic, both Vancouver and Halifax are undertaking aggressive port facility upgrades and the port of Prince Rupert will have completed a brand new container handling facility capable of handling a throughput capacity of 500,000 TEU by the end of 2006 and over two million TEU by the end of 2010.[13]

---

[7] TEU is an abbreviation for "twenty foot equivalent" and is unit of measurement equal to the space occupied by a standard twenty foot container. Used in stating the capacity of container vessel or storage area. For example, one 40 ft. container is equal to two TEU's.
[8] Post-Panamax is a ship size classification designating a ship that is too large to pass through the Panama Canal.
[9] Lloyd's Register, "Container Market Outlook Remains Healthy," *Container Ship Focus*, (London: Lloyd's Register, August 2005), 2.
[10] Times Online, "Lifeblood of the Global Economy," Web posted 07 September 2004, http://business.timesonline.co.uk/article/0,,16791-1245458,00.html; Internet; accessed 19 February 2006.
[11] Port of Vancouver, "Media: Port Facts – 2005 Statistics," http://www.portvancouver.com/media/port_facts.html; Internet; accessed 25 February 2006.
[12] Port of Halifax, "Port of Halifax sets new TEU record," http://www.portofhalifax.ca/AbsPage.aspx?ID=1042&siteid=1&lang=1#jan27; Internet; accessed 25 February 2006.
[13] Prince Rupert Port Authority, "Fairview Terminal: Highly Efficient, Multi-Use Facility," http://www.rupertport.com/container.htm; Internet; accessed 25 February 2006.

Marine transportation accounts for almost a fifth of the volume of Canada's exports to the United States and over 95 percent of the approximately 180 million tonnes of commodities and processed goods Canada exports to other countries annually.[14] It is clear therefore that our major container ports represent critical national infrastructure vital to the economic well-being of Canada. Not only must we protect that critical infrastructure from terrorist threats, but we must also prevent our container ports from being used as unprotected gateways for terrorist attacks against our major inland population centers.

POTENTIAL THREATS

The real threat from containers lies in the fact that they are cheap, they are accessible and they can be launched from a comfortable distance from inspection points. They truly are the "poor man's missile". For a mere $3,000 to $5,000 anyone can lease one of the millions of containers available around the world, pack it with tens of thousands of kilograms of items, close the door and lock it with a 50 cent security seal. With the aid of a less than scrupulous broker, a container enters a transportation system that is dedicated to get it to its destination in the quickest possible time. Of further worry is the fact that accompanying documents usually only describe the contents of the container in general terms and only shows routing information known to the final transportation carrier.[15] A container could start its journey in a central Asian country, travel cross-country into eastern Europe, change land transport company in Germany and

---

[14] Association of Canadian Port Authorities, "Industry Information - Canadian Port Industry," http://www.acpa-ports.net/industry/industry.html; Internet; accessed 25 February 2006.

[15] Stephan Flynn, *America the Vulnerable, How Our Government Is Failing to Protect Us from Terrorism*, (New York: Harper Collins Publishers, 2004), 88.

then end up in a port in the Netherlands to be loaded onto a container ship. Critical information such as the circuitous land routing to get to the container port might not be present in the accompanying documents.

With such a convenient launch system, it could present a tempting opportunity to a potential terrorist to arm his poor man's missile with a selection from any one of the potential warheads at his disposal. Canada or the United States could be targeted with a bomb-in-a-box (high explosives), a nuke-in-a-box (dirty bomb or nuclear warhead), a bug-in-a-box (biological agent) or even bad-guy-in-a-box (terrorist operatives). Each could be devastating in its own right. Such a terrorist weapon in transit could be lost within the noise of the more than 15 million containers that are on the move throughout the world on any given day.[16]

It is not just speculation that such attacks could occur, they have already happened. In March 2003, two Palestinian terrorists infiltrated the Israeli Port of Ashod hidden behind a false wall in a forty foot container containing marble and ceramic tiles. Israeli security personnel had conducted an electronic scan of the container as well as a physical inspection of the interior, but all efforts failed to detect the false wall. The terrorists emerged from the container and detonated their explosive vests killing ten port workers. What made this especially surprising is the fact that Ashdod had long been considered one of the most secure ports facilities in the world because of their policy to physically inspect 100 percent of all incoming cargo containers.[17]

---

[16] Ibid., 83.
[17] Jonathan Howland, "U.S. Starting to Focus on Maritime/Seaborne Terror," JINSA Online, http://www.jinsa.org/articles/articles.html/function/view/categoryid/1701/documentid/2454/history/3,2360,655,1701,2454; Internet: accessed 26 March 2006.

Some might say that North American detection measures would not allow a container hiding a weapon or even terrorists to pass through our portion of the global container supply chain without being discovered. But the security blanket to which they are clinging is more tattered than they realize. For example, analysis indicates that our current targeting and inspection practices would only have about a 10 percent success rate in detecting a device similar to a Soviet nuclear warhead surrounded by shielding material.[18]

Exactly how vulnerable are we and what can we do to better protect ourselves?

VULNERABILITIES

Traditional concepts of Sea Lines of Communications (SLOCs) have changed dramatically since the conversion from bulk to containerized freight. Since the freight is no longer loaded or unloaded at the sea ports, North American SLOCs can now be considered to extend well into the heartland of Canada and the United States. Customs and security personnel basically have to rely upon the information found within the *transactional network* of the global containerized supply chain to assist them in targeting suspect containers for inspection. However, due to the sheer volume of information to be analyzed and the speed at which containers move through the system, a container may well have reached the inland portions of the North American SLOC before it is flagged for inspection.

Whereas SLOCs used to cover the world's oceans like a spider web, the shift to containerization have concentrated those spider webs into thick ropes encompassing the

[18] Stephan Flynn, *America the Vulnerable, How Our Government Is Failing to Protect Us from Terrorism*, (New York: Harper Collins Publishers, 2004), 96.

globe and connecting the world's major ports. This is due to the fact that as container ships have grown in size and capacity, efficiencies and the economy of scale have dictated that more and more containers are processed through fewer and fewer ports. Smaller ports have given up dealing with container traffic due to depth restrictions and need for massive cranes necessary to unload today's post-Panamax container ships. Looking at the combined capacity of Canada and the United States (CANUS), of the 26 million TEU shipped through CANUS in 2004, 92 percent of those containers passed through only 14 ports (Vancouver and Halifax included) and a staggering 35 percent passed through Southern California alone (Los Angeles – five million TEU and Long Beach – four million TEU).[19] Even these figures pale in comparison to the mega-ports that have emerged in the global containerized supply chain. Today, the two largest mega-ports in the world, Hong Kong and Singapore, together handle more than two million TEU each month![20]

The vulnerability that this movement towards mega-ports presents is actually global in scale. With 15 million containers in motion around the world on any given day[21] and the shrinking number of ports being used to load and unload containers, it raises the thorny issues of flexibility and resilience. If any single mega-port or large capacity port were to be knocked out of commission by a major terrorist attack, where would all the container ships go if surrounding container ports are designed to continually operate close to capacity? The current *physical logistics network* is not flexible enough because it does not possess the necessary excess capacity to bypass a damaged node.

---

[19] World Shipping Council, "Industry Info: Through Modern Port Terminal Gateways," http://www.worldshipping.org/ind_4.html; Internet; accessed 18 February 2006.
[20] Stephan Flynn, *America the Vulnerable, How Our Government Is Failing to Protect Us from Terrorism*, (New York: Harper Collins Publishers, 2004), 82.
[21] Ibid., 83.

Industries worldwide that rely upon just-in-time inventories would suffer greatly from the resultant delays and the negative impacts generated from these industries would ripple throughout national economies. To add insult to injury, due to the massive infrastructure in place at mega-ports and large capacity ports, there is significant doubt that these major container ports are resilient enough to rapidly repair themselves and restore operations soon enough to prevent major damage to the global economy.[22]

Although most efforts of the *overview network* have focused upon the security of the nodes within the *physical logistics network* (namely the ports) and most nations have poured resources into improving port security, they all seemed to have overlooked key vulnerabilities within the *physical logistics network* that have remained relatively unprotected. These key vulnerabilities are the relatively unmonitored transits between nodes: the long periods of time when the ships are moving from one port to another and the time spent on the road or railway transiting from the manufacturer to the container port or from the container port to the final destination.

The time spent at sea might be the lesser of the two vulnerabilities, but it cannot be totally discounted. With large post-Panamax ships and the miniscule crews on board to operate them, how sure are we of the security of those containers onboard during the long period of time in the open ocean or while transiting through sparsely populated island chains? All it would take would be one terrorist planted as a crew member or maybe even just one economically disadvantaged crew member willing to take a bribe. Not only could a poor man's missile be launched from a container's original point of departure, perhaps a legitimate container could be tampered with at sea to convert it into

---

[22] Henry H. Willis and David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*, (Santa Monica: RAND Corporation, 2004), 25.

a poor man's missile. However frightening this scenario might be, this method of terrorist attack represents a lesser threat due to the difficulty of bringing a weapon out to sea to be planted in a container and the tremendous challenge of getting into a specific container that may be one of 8,000 tightly packed together on the deck of a post-Panamax container ship.

The second vulnerability, in transit by road or rail, represents the true threat to container security. Although the SLOCs have concentrated at sea due to the overall reduction in container ports, ashore the SLOCs spread out as thinly as ever in all directions. Moving into and out of sea ports, the containers are dispersed; one or two per railcar in a train carrying perhaps 40 or 50 containers or even out on the highway, one container per truck. When comparing the difficulty of tampering with a container in transit at sea, slipping quietly into a container on a deserted rail siding or in a lonely truck stop would be mere child's play. Instructions for opening container doors without disturbing the security seals are readily available on the internet.[23] Choosing the right isolated spot, at the right distance away from the protected container port, a determined terrorist would have little problem hijacking a legitimate container during its land-transit, inserting his nefarious addition to the container's cargo, then relying on the container's

[23]While looking into the issue of tamper proof security seals, a RAND report (*Seacurity: Improving the Security of the Global Sea-Container Shipping System*) from 2003 referred to a website that showed how to break into shipping containers while leaving the security seal intact and undamaged. The particular website immediately did not offer the promised instructions, but instead stated that "Due to the sensitive nature of this information, this section of our website requires access permission." As an exercise in primary research, the author filled out the access application form with the minimum information possible. Hoping to show that the protection of sensitive information had improved since 2003, the author was surprised to receive a reply email within five minutes that included links to a 17 page illustrated guide showing how to breaking into most known types of containers as well as links to three instructional videos. The only effort at security was the following disclaimer at the end of the email: "All we ask is that you share this sensitive material with discretion because our goal is to aid the international business community, not would-be thieves or terrorists."

legitimate documentation to allow its unhampered passage through the rest of the global containerized supply chain.

Unleashing a weapon of mass destruction (WMD) hidden in a single container and detonated at a major population center, during inland transit or even in the container port itself (often located in a major population center) would have a massive psychological and economic impacts similar to similar to those felt immediately following the terrorist attacks of 11 September 2001. It is fairly obvious that the 50 cent security seal on the container door is merely a means of keeping honest people out of a container in transit. What then are the real security measures put in place by the *oversight network* that would protect us from a container-borne terrorist attack?

CURRENT SECURITY MEASURES

The International Maritime Organization (IMO) of the United Nations have established International Ship and Port Security (ISPS) codes, which came into effect 1 July 2004, to fulfill its role within the *oversight network* of setting global standards for marine security. The ISPS codes require ships on international voyages and port facilities that serve them to conduct security assessments, develop security plans, designate security officers, perform training and drills and take appropriate measures to prevent security incidents.[24]

As part of Canada's obligation to meet ISPS codes Canada Border Service Agency (CBSA) has put the Advance Commercial Information (ACI) program in place. This program requires that vessels of greater that 100 gross tonnes bound for Canada

[24] Deloritte Research, "Prospering in the Secure Economy," A Deloitte Research Study (Australia: Deloitte Touche Tohmatsu, 2004), 8.

notify the CBSA twenty four hours before the vessel is loaded in the foreign port of departure. Notification includes information about both cargo and crew.[25] Also complying with the ISPS codes, Transport Canada requires that vessels greater than 100 gross tonnes report detailed information to Canadian authorities as least 96 hours prior to arriving in Canadian waters.[26]

Canada has not gone so far as to replicate the United States Container Security Initiative (CSI) which place U.S. Customs officers in foreign ports to pre-screen containers bound for the United States due to manpower constraints. However, Canada has accepted the reciprocal offer from the United States to place Canada Customs officers in select American ports to pre-screen containers destined for Canada.[27]

The Maritime Security Operations Centers (MSOC) located on each coast are the limited extent of Canadian military involvement in container security. These newly established centers are multi-departmental organizations involving DND, CBSA, Department of Transport, the Canadian Coast Guard and the RCMP. With the aid of systems such as the Automatic Identification System (AIS), mandated for ships greater that 300 gross tonnage by the ISPS Codes, and the High Frequency Surface Radar (HFSR) system, the MOSCs provide a surveillance system that identifies and monitors all ships in Canadian waters.[28] The effectiveness of the MSOC is highly reliant on the information provided by the *transactional network* to the *oversight network* to identify ships that may pose a security risk to Canada. Once this occurs, the Canadian Navy can

---

[25] Standing Senate Committee on National Security and Defence, *Canadian Security Guide Book – 2005 Edition*, (Ottawa: Public Works and Government Services Canada, 2005), 45.
[26] Ibid., 43.
[27] Deloritte Research, "Prospering in the Secure Economy," A Deloitte Research Study (Australia: Deloitte Touche Tohmatsu, 2004), 31.
[28] Standing Senate Committee on National Security and Defence, "Canadian Security Guide Book – 2005 Edition," (Ottawa: Public Works and Government Services Canada, 2005), 49.

then merely act as the tip of the spear if the risk is judged to by high enough to warrant interception and boarding by naval personnel.

Some of the physical security measures that are slowly finding their way into the global containerized supply chain are radiation scanners, X-Ray and Gamma-Ray scanners and Radio-Frequency Identification (RFID) tags. The scanners allow for non-intrusive inspections of containers while in port to either scan the contents of suspect container for misrepresentation of illegal shipments or to detect the presence of a dirty bomb or weapon of mass destruction. The problem with the current state technology for these scanners is that they are mobile units located off the container processing line, they take time to scan and they offer high rates of false-positive detections.[29] The RFID tags allow shippers and carriers to track cargo as it passes by salient portals within the supply chain. The tags can record and transmit information about the container's origin, destination, contents or processing history. They operate at relatively short range, typically within a few meters of a RFID reader.

ECONOMIC BLINDERS

The *oversight network* has made progress in setting standards and establishing regulations to ensure that the *transactional network* is providing the appropriate information to allow the responsible agencies within nations to enforce security regulations. As well, a number of physical security measures are now available to the *physical logistics network* to monitor the security of the containers passing through the supply chain but they are highly inadequate to address the security concerns associated

[29] Henry H. Willis and David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*, (Santa Monica: RAND Corporation, 2004), 6.

with individual containers passing through the unmonitored land-transit portions of the global containerized supply chain. Economic realities are inhibiting the required revolution in maritime security necessary to completely close the gaps in container protection during land transit.

The sea freight industry remains, as it always has been, an enterprise operated on slim profit margins. Moving to satisfy more stringent security measures always comes with an added cost. Individual shipping companies and port authorities are in a stand-off with their competitors. They don't want to be the first one to blink, increase their operating cost and suddenly lose their competitive advantage. Nations are cautious as well, they don't want to push their shipping companies or their port authorities too hard or they risk damaging their own national economies.

As a result of these fiscal concerns, physical inspection rates of containers are kept very low to ensure high throughput of containers. Using an American example, it takes five agents three hours to completely inspect a fully loaded forty-foot container. If the entire daily throughput of containers for the ports of Los Angeles and Long Beach (18,000 containers) were 100 percent inspected, it would require 270,000 man-hours per day, equivalent to three times the United States Customs manpower that exists nationwide.[30] The situation would surely be worse if a similar Canadian comparison were made. As such only five to six percent of containers are fully inspected in the majority of port throughout the world.[31]

---

[30] Stephan Flynn, *America the Vulnerable, How Our Government Is Failing to Protect Us from Terrorism*, (New York: Harper Collins Publishers, 2004), 87.
[31] Henry H. Willis and David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*, (Santa Monica: RAND Corporation, 2004), 6.

In Canada the economic pressures are further multiplied by the fact that port authorities are not government financed institutions but instead must operate as self-financing organizations. The federal government took steps to help the port authorities and the shipping companies to bring themselves in line with ISPS codes. On 22 January 2003, the Department of Transport announced a five-year package worth $172.5 million to improve marine security. [32] It was a start, but it is not nearly enough.

Because of the shortfalls in funding some aspects of the ISPS codes are being addressed very slowly. One such example was pointed out by the Standing Senate Committee on National Security and Defence in 2005[33] when they noted that approximately 40 percent of longshoremen in Canadian ports have criminal records. Ports authorities across Canada are reluctant to push this initiative too hard for fear that a confrontation with the unions would cripple them with labour shutdowns.

Even such a simple physical security measure as the RFID tags encounters resistance on economic grounds. They are not as widely used as would have been hoped; most companies see them as cost prohibitive at $30 to $40 per unit.

By focusing on the dollar rather than the issue of marine security all stakeholders, from the shippers to the port authorities to the national governments are placing their populations and their critical infrastructures at risk. By leaving the door wide open for speedy processing of an overseas container, with our minds set squarely on economic prosperity, we may be instead holding that door open for an "economic" Trojan Horse sent to us be an opportunistic terrorist organization.

---

[32] Transport Canada, "Government of Canada Announces Up To $172.5 Million In New Marine Security Projects," News Release, http://www.tc.gc.ca/mediaroom/releases/nat/2003/03-gc001.htm; Internet: accessed 17 February 2006.

[33] Standing Senate Committee on National Security and Defence, *Canadian Security Guide Book – 2005 Edition*. (Ottawa: Public Works and Government Services Canada, 2005), 125.

REQUIRED SECURITY MEASURES

Even though the previously mentioned security measures are moving forward slowly, at least they are moving forward. However, there remain a number of security measures that are completely lacking. As discussed earlier, the security of containers while in transit is not an issue that is being pursued as vigorously as it should be. Tampering with legitimate containers and placing a weapon of mass destruction within that container while it is in land-transit to or from a container port could defeat the safeguards of a closely monitored *transactional network*. Without knowing the container has been tampered with, there would be nothing within the accompanying paperwork to help identify it as a high risk container. Technologies exist today that could reduce this vulnerability.

Containers could be equipped with electronic monitoring devices with multiple sensors capable of detecting when a container has been opened and recording the time that it was opened. Such an anti-tampering monitor could be linked with the onboard RFID tags. If this type of system were combined with RFID readers mounted on all container unloading cranes, every single container passing through a port would be monitored and any containers indicating a suspicious opening could be immediately segregated for further inspection. An additional secondary economic benefit of such a system is that a container labeled as "RFID Protected" would also reduce instance of in-transit theft.

In-transit monitoring could even be taken one step further. The anti-tampering monitor could be linked to a satellite communication system and report container status, time and GPS location on periodic basis. Cars are often sold with the option of OnStar

service, which allows it to find a car if it is stolen, to alert emergency personnel if the air bag deploys, or to unlock a car if a customer has locked his keys inside. Such a system adapted to a shipping container would likely have a lifetime cost of around $250, if it were widely deployed.[34]

None of these suggested security improvements come cheap and skeptics will argue that the capital investment required to make these changes are too expensive for an industry that operated on such slim profit margins. All of this sounds strangely familiar. Wasn't that the same argument offered by the industry when it was suggested that they should convert from bulk cargo to containerized cargo?

SEARCH FOR AN INDUSTRY LEADER

Many companies are experimenting with some of the technologies mentioned earlier. Wal-Mart, for example has mandated that its suppliers used RFID tags on individual items to increase visibility in the shipping and purchasing process. Drug companies are beginning to employ RFID tags to help combat counterfeiting.[35] As always, innovative companies with a vision for the future are always willing to step up to a challenge if they can see a competitive advantage in the exploitation of new technology.

What the container shipping industry needs is another industry leader to see the economic value of some of this technology, just like APL did back in the late-50s when they recognized the potential of containerization. Well, APL did it once maybe they can do it again.

---

[34] Stephan Flynn, *America the Vulnerable, How Our Government Is Failing to Protect Us from Terrorism*, (New York: Harper Collins Publishers, 2004), 100.
[35] Henry H. Willis and David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*, (Santa Monica: RAND Corporation, 2004), 2.

> "Companies like APL who own fleets of containers can optimize their use to a far greater extent than today. APL owns about 300,000 containers. When they are on a ship, the company knows where they are, but once on land, it does not. It only finds out when customers call to schedule a pick-up once they have emptied out the container. A typical delivery contract allows a company up to ten days to empty a container before incurring additional fees. Most containers are emptied within twenty-four to thirty-six hours, but companies often wait until the last minute to contact APL to come get the box so that it can be put back in circulation. Now imagine if containers had sensors that could indicate precisely when they are empty and send an alert message that includes the box's location to APL. William Hamlin, the man responsible for running APL's operations in North America, believes his company could start routinely recovering its containers within two to three days instead of the typical eight- to ten-day interval. As a result, a container used for just five full loads a year could be used for six instead, a 20 percent increase in productivity."[36]

This is not to say that APL is once again going to be the industry leader, it is just to demonstrate there are companies out there still digging for the next competitive advantage. It is up to the industry as a whole and the governments around the world dedicated to the improvement of their economies, to support this type of forward thinking application of security measures in conjunction with economically beneficial technology developments. Such support will encourage the next industry leader to break free from the pack and lead the next revolution in maritime shipping.

CONCLUSIONS

The maritime shipping industry has undergone radical changes over the last fifty years transforming itself from a tradition-bound, labour-intensive bulk freight enterprise into a highly efficient, cost-saving mover of containers. The transformation was not an easy one. Conservative members of the industry were reluctant to make the capital

---

[36] Stephan Flynn, *America the Vulnerable, How Our Government Is Failing to Protect Us from Terrorism*, (New York: Harper Collins Publishers, 2004), 99.

investments necessary to make the conversion to containers until a forward thinking company from within their ranks recognized the competitive advantage inherent in the change.

Following the events of 11 September 2001, the industry felt the threat to their livelihood and safety. The industry recognized that the containers that had made them so efficient now exposed their critical infrastructure and nations to threats of terrorist attacks. The three levels of interdependent and interacting networks that make up the global containerized supply chain, the *physical logistics network*, the *transactional networ*k and the *oversight network*, have all worked together to manage this new security threat. However, the reality of slim profit margins and fears of damaging economies dependent on international trade have slowed the progress of instituting meaningful security measures.

Technologies exist that could close the vulnerability gaps that still remain in the global containerized supply chain and, as fifty years ago, economic fears are holding back innovation. Prisoners to our economics of trade, we now face the possibility that any container passing through our porous marine transportation security net could turn out to be an economic Trojan Horse delivering a terrorist attack to the very heartland of our nation.

The marine shipping industry operates on dollars and cents and dollars and cents are going to be the mechanism that will rectify its security shortfalls. The only way to move security initiatives forward is to provide technical solutions that also provide complimentary economic benefits to sea freight customers and the companies that provide the container transportation services.

Bibliography

APL. "APL History - Innovate." http://www.apl.com/history/topics/innovate/innovate.htm; Internet; accessed 18 February 2006.

APL. "APL History - Containerization." http://www.apl.com/history/topics/innovate/contain.htm; Internet; accessed 18 February 2006.

Association of Canadian Port Authorities. "Industry Information - Canadian Port Industry." http://www.acpa-ports.net/industry/industry.html; Internet; accessed 25 February 2006.

Deloritte Research. "Prospering in the Secure Economy." A Deloitte Research Study. Australia: Deloitte Touche Tohmatsu, 2004.

Flynn, Stephan. *America the Vulnerable, How Our Government Is Failing to Protect Us from Terrorism*. New York: Harper Collins Publishers, 2004.

Jonathan Howland. "U.S. Starting to Focus on Maritime/Seaborne Terror." JINSA Online. http://www.jinsa.org/articles/articles.html/function/view/categoryid/1701/documentid/2454/history/3,2360,655,1701,2454; Internet: accessed 26 March 2006.

Lloyd's Register. "Container Market Outlook Remains Healthy." *Container Ship Focus*, London: Lloyd's Register, August 2005.

Port of Halifax. "Port of Halifax sets new TEU record." http://www.portofhalifax.ca/AbsPage.aspx?ID=1042&siteid=1&lang=1#jan27; Internet; accessed 25 February 2006.

Port of Vancouver. "Media: Port Facts – 2005 Statistics." http://www.portvancouver.com/media/port_facts.html; Internet; accessed 25 February 2006.

Prince Rupert Port Authority. "Fairview Terminal: Highly Efficient, Multi-Use Facility." http://www.rupertport.com/container.htm; Internet; accessed 25 February 2006.

RAND Corporation. "Assessing Container Security: A Framework for Measuring Performance of the Global Supply Chain." *RAND Infrastructure, Safety, and Environment* (2005). Research Brief; available from http://www.rand.org/pubs/research_briefs/RB9095/index1.html; Internet; accessed 16 February 2006.

Standing Senate Committee on National Security and Defence. *Canadian Security Guide Book – 2005 Edition*. Ottawa: Public Works and Government Services Canada, 2005.

Times Online. "Lifeblood of the Global Economy." Web posted 07 September 2004. http://business.timesonline.co.uk/article/0,,16791-1245458,00.html; Internet; accessed 19 February 2006.

Transport Canada. "Government Of Canada Announces Up To $172.5 Million In New Marine Security Projects." News Release. http://www.tc.gc.ca/mediaroom/releases/nat/2003/03-gc001.htm; Internet: accessed 17 February 2006.

Van de Voort, Maarten and Kevin A. O'Brien with Adnan Rahman and Lorenzo Valeri. *Seacurity: Improving the Security of the Global Sea-Container Shipping System*. Workshop Report MR-1695-JRC. Santa Monica: RAND Europe, 2003.

Willis, Henry H., and David S. Ortiz. *Evaluating the Security of the Global Containerized Supply Chain*. Santa Monica: RAND Corporation, 2004.

World Shipping Council. "Industry Info: Through Modern Port Terminal Gateways." http://www.worldshipping.org/ind_4.html; Internet; accessed 18 February 2006.