Review Draft. Do not quote, copy or cite without author's permission.

Harnessing a Trojan Horse: Aligning Security Investments with Commercial Trajectories in Cargo Container Shipping

By

Jay Stowsky
University of California, Berkeley

Prepared for the Public Policy Institute of California (PPIC) project on port security. Additional funding for this research provided by a gift from John Gage and Linda Schacht-Gage to the Richard and Rhoda Goldman School of Public Policy at the University of California, Berkeley

March 21, 2005

Policy efforts to induce the private sector to improve the security of cargo container shipping will benefit from careful consideration of where such improvements can also enhance the economic efficiency of the typical shipping supply chain. Impolitic as it may be to observe, the fact is that a major terrorist attack on a US port (perhaps in a shipping container) may never come. If it does come, it may turn out to be a fairly isolated, albeit economically and psychologically devastating event. In either case, a massive security investment not offset by the concurrent achievement of the largest possible social or economic benefit will have represented a colossal missed opportunity, a waste of economic resources that could have been artfully invested to create technologies that were by nature dual use, that is, valuable for both homeland security and commercial purposes.

This chapter characterizes the private sector's early response to the increased awareness of potential security threats to cargo container shipping that dawned in the awful wake of the terrorist attacks of September 11, 2001. It is motivated by the conviction that profit-seeking investments by private sector shippers, carriers and port operators to enhance the efficiency of the global containerized supply chain may do more to prevent terrorist groups from using container shipping as a conveyer of weapons of mass destruction (WMD) than investments targeted at the outset specifically to the security threat. It is motivated, as well, by a belief that lack of due attention to the opportunities for dual use technology development may impede the growth of the civilian economy and the competitive fortunes of American industry in international competition without doing very much to improve homeland security. This would replicate one of the costliest aspects of America's involvement in the forty-year Cold War, when military-led technology development sometimes benefited the civilian economy, but sometimes also distorted the country's economic and technological development with only negligible effects on the nation's security (Stowsky, 2004).

The best opportunities for dual use investment are in the area of improving the transparency of the global container supply chain. Technologies that make container tracking easier while making tampering or breaching the container harder are the most lucrative from a purely private sector perspective and thus have already attracted the lion's share of private investment. For both security and supply chain efficiency, the ideal system is one that enables interested parties (those with no malicious intent) to track the containers as they move from link to link in the system. Available Global Positioning System (GPS) and radio frequency identification (RFID) technology can already record snapshots of a container's journey, enabling human interrogators to check at key points along the way for evidence of tampering or even WMD. Both shippers and security officials have an interest in developing the capability to track containers continuously and in real time, but it is would be imprudent to put off investments in existing technology that can already improve both efficiency and security to a significant extent (Flynn, 2004).

Such investments were already underway before 9/11 for purely commercial reasons, though they were not being made as quickly or comprehensively as security officials would prefer. Through a judicious balance of standard setting and procurement the federal government could encourage this trend without dampening market signals and without distorting the trajectory of technological development with too many security-specific performance requirements. History suggests that the wisest approach is for the government to let private sector solutions emerge in response to private sector problems, and then provide inducements for private suppliers to ‘spin on’ commercial technology to security applications, rather than funding those applications directly with the hope (often more hype than hope) that commercial spin offs will rapidly emerge in the opposite direction.

Investments that would enable the supply chain to operate through a terrorist attack, or to quickly recover in the event of one, promise less immediate commercial benefit and so have attracted much less private investment. Yet this is an area where the potential for dual use is also great, even if it the scope of the potential returns becomes clear only in retrospect. This is an area of technological development where the federal government should be willing to invest more heavily, in partnership with private investors who will be able to appropriate some of the returns to such investments in supply chain resilience as a purely commercial matter and so should be willing to put a significant portion of their own funds at risk. The largest share of public-led investment should target research and technological development in the areas of remote sensing of chemical, biological, radiological and nuclear agents. This is an area fraught with technological and practical impediments, both of which have, and will continue to, impede private sector investment. But it is also an area where a breakthrough could produce exceptionally dramatic returns, both commercially and in terms of homeland security.

The Case for Integrating Commercial and Homeland Security Technology Development

Since the late-1970s, a security centered approach to developing dual-use technology has not prevented superior, commercially derived versions of security technologies from reaching open global markets, where they quickly become accessible to allies and adversaries alike. Most homeland defense technology, especially information technology, now has commercial roots, and these roots extend across the globe. It is impractical, if not impossible, to prevent these technologies from ever diffusing to potential enemies. Homeland security cannot be made to depend, therefore, on how well a system of export and publication controls maintains exclusive access to any particular technology over time.

Moreover, homeland security research and development projects that are isolated from the demands of potential users in mainstream commercial markets are apt to produce dual-use technology that is inferior in quality and price to that which will be available commercially. This is the lesson of significant numbers of dual use technologies developed during the Cold War—NC machine tools, very high speed integrated circuits, artificial intelligence software, flat panel displays, intelligent transportation systems, and encryption. In each case, the US sponsored military specific versions of the underlying technology, which were eventually overtaken by less costly commercial applications of equivalent or superior quality and functionality. In contrast, the involvement of military, intelligence and homeland security agencies in an open and collaborative development process can actually enhance prospects for commercialization of dual use technology. This is the lesson of several other technologies developed by the United States during the Cold War—solid-state transistors and integrated circuits, VLSI circuits and computer-aided design tools, semiconductor production equipment, and the Internet.

Can the agencies responsible for port security gain access to the most promising dual-use technology from researchers at universities and commercial enterprises yet still maintain a technological-edge over opponents who have access to the same technology? They can if they focus more of their own investment spending on the front-end activities of basic research and exploratory development, where projects focus on investigating and advancing a technology's general state of the art capabilities. And they should focus more internal resources on technology adoption and insertion, so that contractors are rewarded for quicker absorption of commercial technology in their security systems.

The first change will attract more participation from leading research universities and commercial firms, particularly when they are permitted to control the intellectual property that results. The second change depends on whether the US Department of Homeland Security adopts procurement practices that encourage program officers to buy commercial technology off the shelf. In this environment the underlying technologies are not secret, but security applications—systems architectures—can be. The point is to resist the tendency to specialize for security applications as long as possible, and also to adopt commercial technology for use in security systems as quickly as possible, more rapidly than potential opponents can.

Third, these R&D policies must be supported by a reformed system of export controls that is rooted in a realistic appreciation of the extent to which security technology now derives from a global commercial technology base. This will require an acknowledgment by all governments that there are likely to be commercial sales of sensitive items outside of their country of origin. Better procedures will be required to assess what kinds of technology are already widely available and stronger agreements among the nations that manufacture these sensitive items about which foreign destinations they will attempt to proscribe. But more and more items will be electronically disseminated and difficult to control. A real security price will be paid.

A shift toward more reliance on external R&D places commercial producers and research universities, as well as foreign nationals, at the center of the US security apparatus. This obviously creates significant new security challenges for the United States. But, in a global economy, policies aimed at restricting participation in technology development and keeping the results secret are counterproductive. Commercial producers in excluded countries will find alternate technology sources and will, when they can, invest to develop the technologies themselves. The fact that many of these technologies (and much of the information about them) can be digitized and disseminated electronically means that their propagation will be increasingly difficult to monitor and control. In the digital age, the best approach to conducting security centered R&D is an approach that embraces openness.

How has the Private Sector Responded to the Terrorist Threat to Shipping and Ports?

Like most commercial firms in the first years after the September 11th attacks, companies in the cargo container shipping business initially assumed an attitude of "watch and wait." Private spending for supply chain security increased, but at a rate not dramatically inconsistent with a decade-long trend toward higher spending on security that began well before 9/11. For the most part, the first post-9/11 expenditures purchased security technology that was already available off the shelf.

Subsequently, as new generations of security products and services have started to emerge from corporate and government labs, corporate boards have begun to view investments in security as a necessary form of insurance against terrorism and other sources of operational instability and disruption. The mandates provided by the US Maritime Transportation Security Act (MTSA) of 2002 and the International Maritime Organization's updated Security Code are also compelling port operators, shippers and carriers to take action. As a result, new product and services markets for maritime and port security are coming into sharper focus, in terms of supply and demand, and in terms of overall size.

When one examines this still-developing market, a couple of characteristics stand out. First, the 2001 terrorist attacks did not generate a brand new market. Rather, they amplified and accelerated an on-going 'digital transformation' of cargo container shipping with respect to both security and supply chain management. Before 9/11, advances in digital electronics hardware and software had already started to multiply the actual and potential interconnections among the dozens of players involved in cargo container shipping. Companies that had been content before to rely on separate vendors for security guards and surveillance cameras, electric fences and electronic firewalls, had already started to seek suppliers who could offer more integrated, end-to-end security solutions. Thus a segment of the market had already started to consolidate in the form of new security services firms offering to integrate different security products and solutions. The main effect of 9/11 was to accelerate this pre-existing trend.

This turn of what was previously a set of stand-alone product markets into a single consolidated market for integrated, information technology-based solutions to overall security and supply chain management is the key competitive dynamic driving the continued expansion of security spending in the maritime and port sector. As in all advanced technology markets characterized by network scale economies, commercial success, as measured by market share, may depend more on the size of a company's portfolio of complementary products and services than on the technical performance of the company's point-targeted security solutions. Companies with superior products may struggle against competitors with larger partner networks or against companies that already have a large established base of installed products and after-sales services.

The Co-Existence of Successive Technology Generations

A second significant feature of this burgeoning market for port and maritime security technology is the extent to which the market is segmented into distinct but concurrent technological generations, as well as by product or security function. To analyze the competitive dynamics of any particular product segment, one must first understand whether the product in question represents a mature technology, a technology just coming to market, or a technology still being tested in corporate, university or government labs. The prospects for different technological generations might vary dramatically in response to different levels or styles of government regulation, for example. The main point to understand is that different generations of port and maritime security technology are installed simultaneously and will need to be able to interconnect and inter-operate for the foreseeable future.

As previously noted, the initial reaction of commercial shippers, suppliers and port operators to 9/11 was to expand purchases of security products and services that were already on the market or just coming to market prior to the terrorist attacks. These products constitute a first generation of maritime and port security technology and make up the majority of the sectors' current installed technology base. First generation security products include such things as metal detectors and handheld radiation detectors, building or area access control systems, and fingerprint recognition software.

As a consequence, a common desire among many commercial shippers, importers, suppliers and port operators contemplating new security technology is for new products and services that will enable them to integrate the disparate technologies in their installed ‘first generation’ product base. These represent a substantial sunk investment, and the ports and shippers are not in any rush to replace or entirely upgrade it. For companies and investors on the supply side of this market, first generation technologies are a low risk but still profitable investment, offering a steady stream of revenue, although one that has passed its peak. These products are starting to be replaced, albeit gradually, as second generation products and systems start to come to market.

Most of the new or “second” generation maritime and port security services and products have been designed at inception to offer a broader and more integrated set of security solutions. They tend to comprise ‘suites’ of services and functions based on technologies that were under development before September 11th but which may not have been offered commercially prior to the attacks. In some cases, these products represent the repurposing of technologies that were under development prior to 9/11 but which had targeted other, sometimes non-security-related applications. As one would expect, many of them are designed to interconnect with first generation applications so that suppliers do not have to try to overcome customer resistance to replacing an entire installed base of first generation security products.

Second generation products include such things as screening or imaging technologies that can perceive plastic and ceramic explosive devices hidden in luggage or under clothing and various ‘smart surveillance’ technologies that match images captured by security cameras to databases designed to trigger an alarm and further investigation. This is the generation of products that has probably benefited most from increased federal funding for new technology deployment, mainly in the form of pilot or demonstration projects such as the US Department of Homeland Security’s Operation Safe Commerce (OSC). This market segment is the site of considerable new venture development, but also a great deal of acquisition activity, as larger, established security, logistics and enterprise software suppliers attempt to keep up with the latest available product offerings.

Many firms selling products in this market have adopted a strategy that focuses on bundling their products with complementary products from other companies whose technologies aim at securing other points along the supply chain. Others are partnering with logistics companies attempting to succeed as the providers of integrated end-to-end security solutions. Consequently, this is a market where competition will be tough over the establishment of intellectual property rights and industry standards, which in some cases will require customers to replace installed equipment. As suites of complementary products develop, in other words, competition in this sector is likely to center on contests between rival technology platforms.

Finally, breathless press accounts have focused much attention on the next or “third” generation of port and maritime security technology, a set of products and services that still have not emerged from the research lab. This generation of technology is characterized by cutting edge applications of developing fields such as nanotechnology that hold out the promise—but still only a promise—of dramatic leaps in both operational efficiency and security within and across the entire transportation supply chain. Some of this technology is just now beginning to be integrated into the most advanced versions of currently available security products and services.

This market segment is still dominated by privately-held start ups, many of which are rooted in university or government laboratories. They are focusing their research on areas where a breakthrough might be expected to create new capabilities across a broad range of security needs, for example, in the area of remote sensing equipment that might detect a wide range of potentially dangerous agents. This is the place where "disruptive" innovations might be expected to emerge, with either price or performance attributes improving dramatically enough to induce customers to abandon their loyalties to previous generations of security technology.

Other Factors Shaping the Private Sector Response

Besides the overall shift toward integrated rather than stand-alone solutions and the simultaneous presence of three generations of technology, the private sector response to security threats in the cargo container shipping sector is shaped by at least five additional factors. These include: (1) the need for technical standards; (2) the "public goods" nature of investments in port and maritime security; (3) liability issues; (4) the trade-off, embodied in many security products, between security and other important societal values, particularly privacy; and (5) the extreme sensitivity of this market to unpredictable external events.

A. The Need for Standards

The 20-foot and 40-foot cargo container is itself a technical standard, first developed during the Second World War to speed the movement of military equipment to the front line without diverting too many soldiers to the task of loading and unloading ships. A typical shipment of cargo by container today involves 25 or more organizations. With some 21,000 containers arriving at US docks each day, and tens of thousands traversing ports across the rest of the globe, the opportunities for theft, fraud, smuggling and terrorist infiltration are enormous.

Current security solutions, such as electronic anti-tamper seals, chemical, radiological and biological sensors, tracking technologies of various types, and encrypted data transmission, tend to secure the nodes of the supply network rather than providing true end-to-end security along the entire supply chain. To achieve that, industry and government agencies will have to agree on technical standards for interoperability and interconnection. Commercial suppliers, shippers and port operators cannot afford to maintain multiple technical platforms, infrastructure, or communications protocols all the way from the cargo suppliers' facilities to the final receiving location.

So far the US government is relying mainly on industry self-regulation to bring standardization about. The shipper and carrier industries have been responsive, but only to a point. A regulated security system offers many benefits to commercial shippers and carriers, as it is likely to speed the movement of cargo more rapidly through the world's ports, freeing ships up more quickly for the next load. The Customs Service, now part of the US Department of Homeland Security, has issued some new rules, most prominently a requirement that shippers must file a manifest, electronically, twenty-four hours before a cargo container bound for the United States is loaded at a foreign port. But the US government has wielded more carrots than sticks.

The Customs-Trade Partnership against Terrorism (C-TPAT) is a voluntary program that shippers and carriers can enter to assure the Customs Service that they have adopted best practices for the secure packing, tracking and distribution of all goods and services bound for the United States. In return, Customs rewards C-TPAT qualified shippers and carriers with fewer inspections and expedited processing (A newer program enables them to dispense with inspections entirely). Similarly, Operation Safe Commerce (OSC) is a publicly-subsidized collaboration among shippers, carriers and port operators at a small group of the most active US ports, to promote testing, evaluation and fielding of container scanning and tracking technologies and best practices for the safe movement of containerized cargo.

Still, a number of essential process questions remain to be settled, by industry consensus, government mandates, or both: What are the minimum documents required for transmission and when? What baseline encryption standards are necessary at each point along the supply chain? What constitutes a security breach, and what types of exceptions are allowable? Who needs to report a security breach, and to whom? What is the procedure to mitigate the risk of such breaches? Furthermore, when information on risk and security is shared between corporate entities and government agencies, questions of data ownership often arise. Who owns what data? With whom can the data be shared? Where should security profile data be stored—with individual shippers or federal agencies?

B. "Public Good" Aspects of Maritime and Port Security

Analysts have argued that the private sector will be willing to bear most of the cost of building a more terrorist-deterring system of maritime transportation because the resultant commercial benefits of improved inventory control and fast-track shipping will more than pay for the private costs of assisting the national security project. This may not be clear to any particular commercial firm before the fact, however. There are clearly incentives for firms to free ride on the investments of others, as they will benefit from system-wide increases in efficiency and security whether they pay for them or not.

Most cost estimates for cargo container security put the bill at around $500 per container; shippers typically generate only $100 of profit for each container (though many are reluctant to admit they make any profit at all). In any case, shippers do not generate enough revenue to pay for the new integrated security solutions on their own. For the economic and security benefits of such investments to come about, therefore, the industry will have to act collectively to establish the requisite standards and spread the costs among all of the potential beneficiaries. The US government, indirectly through its enormous purchasing power or more directly through regulatory mandates, may be required to facilitate this process.

Moreover, for an individual firm or port, the added benefit from an investment in better container tracking is easier to measure (and thus easier to justify in terms of positive net present value) than the extra value of investments in the system's overall capacity to operate through and after a terrorist attack. Just as the US government may want to subsidize or accelerate investments in container shipping transparency that the industry was starting to make on its own before the September 11th attacks, it may want to focus its investment of public resources (in research and development, for example) on those areas of collective benefit that any individual firm might be harder pressed to justify. Investments to enhance the resilience of the overall system of international containerized shipping fall squarely in this category.

C. Liability Issues

As the cargo container shipping business starts to operate more like a vast computer-managed network, it will have to come to grips with some the same information security challenges that have made computer security so difficult to achieve in the Internet age (Varian, 2000). One of these challenges is the creation of incentives for the private sector to invest in security products and procedures by assigning liability for security failures to the companies best positioned to avoid them. As it stands no one entity is accountable for security breaches anywhere along the supply chain. With more than two dozen parties involved in a typical end-to-end shipment, such clear assignment of responsibility is unlikely ever to occur, though the best candidates for that role would probably be the logistics companies currently campaigning to provide integrated security and supply chain solutions to shippers, carriers and ports (and inter-modal solutions encompassing trucking and rail as well).

The fundamental economic principle here is that liability should be assigned to the party that can do the best job of managing the inherent risks. Careful analyses must be done to locate the weak points in the overall supply chain, from point of origin to final destination, at each point a different party might be best positioned to strengthen them. The need is to create the appropriate risk management incentives by assigning liability for security breaches to the parties best equipped, at each stage, to control the risk.

Once this is accomplished, shippers, carriers, port operators and/or systems integrators will want to insure themselves against the risks for which they are liable. Insurers, who are only beginning to serve this market, will then have an incentive to alert their clients to industry best practices. This may be the easiest way to create a vibrant market for new maritime security technology, as companies compete to get their products (or integrated product suites) certified by insurers who will then give their clients reduced rates for installing them. This process will not become self-sustaining, however, unless legal liability is clearly assigned to responsible parties at each point of the supply chain.

D. Trade-Offs Between Security and Other Societal Values

Many of the tracking, screening and surveillance technologies proposed (or already in use) for securing port facilities and container shipping could require a sacrifice of individual privacy and/or subject innocent individuals to various forms of profiling, ethnic, racial and otherwise. Both of these concerns have already caused some consumer resistance to the deployment and continued development of certain security technologies. In addition, some civil liberties activists have campaigned for restrictions on the permissible range of use of the new technologies that could stifle technological innovation unnecessarily.

The concerns of consumers and civil libertarians are not without basis, however. For example, the standardized radio frequency identification (RFID) chips that are on track to replace the familiar Universal Product Code (UPC) bar codes on all manner of products and shipping containers can be hidden from sight, as can the devices that read them. Various proposals to require consumer notification when the chips or readers are present in products, stores or public places, have been resisted by retailers. So have proposals that consumers be given the right (as well as the ability) to remove or deactivate the tags at will. Industry groups have developed guidelines about the use of RFID technology, but they are voluntary.

The dilemma here is a common one with respect to all of the new digital security technologies. Use restrictions such as those that have been proposed for RFID devices would be frustrating (and in some cases costly), but not fatal to widespread commercial adoption of the technology. Yet much of the private response by industry to even the most reasonable expressions of concern has been so dismissive that it has had the effect of pushing more people into the arms of those who would prefer to hobble or prevent deployment of the technology altogether. Aside from the commercial efficiency benefits foregone, this could end up undermining security efforts at many levels, not just efforts to help prevent terrorist attacks (e.g., the installation of RFID chips in car keys, smart cards and steering columns can help to prevent auto theft).

There are, however, some areas of real divergence between the wishes of security officials and the needs of commercial retailers. Whereas commercial interests probably could live with a regulatory regime that enabled consumers to know when tracking devices (chips and readers) are present, and even a regime that would enable consumers to deactivate them at will, security officials are not likely to want to so weaken the capabilities that these new technologies afford them. As muted as the public debate has been about the use of these new devices for commerce, however, debate about their use for homeland security purposes has been virtually nonexistent. Just as the Congressional uproar over US Defense Department plans to develop better data mining software may have complicated private sector efforts to develop that technology for purely commercial use, the lack of widespread debate over the costs and benefits of various tracking technologies, from the standpoint both of the economy and homeland security may end up unnecessarily hampering both.

E. The Special Sensitivity of the Security Market to Terrorist Events

The use by the September 11th terrorists of hijacked commercial airplanes understandably focused the attention of US government officials on aviation security. Legislation to improve security at ports was introduced, but funded at levels significantly below what would be needed to make the system of cargo container shipping even reasonably safe. Bills to expand funding for railway security were similarly under-funded or stalled in the first years after the September 11th attacks, despite their clear vulnerability to assault. This changed on March 11, 2004, with the devastating railway bombings in Madrid, Spain. Within weeks, the US Congress had appropriated an additional $100 million in railway security grants for FY2005. Any analysis of the private sector response to the security threat at ports and on the high seas should make room for the possibility that a successful terrorist attack via cargo container would significantly reshape expectations on both the demand and supply side of the security product and services market.

Key Technologies

Six key technologies cut across the markets for improved security and supply chain management at ports and in the cargo container shipping industry. They are:

1. Sensor technologies
2. Identification and authentication technologies
3. screening technologies
4. surveillance technologies
5. anti-tamper, tracking and inspection technologies
6. integrated solution and data analysis technologies

1. Sensor technologies

A great deal of scientific attention is focused on the development of new generations of sensors to detect chemical, biological, radiological or nuclear weapons of mass destruction, any of which would otherwise be relatively easy to conceal aboard a cargo container. The bottom line is that sensors capable of detecting any of these agents in the form and at the scale at which they would need to be detected to secure a port (or to prevent the transport of WMD inland by truck or train) do not exist. Furthermore, the development of such sensors, particularly with respect to harmful biological agents, constitutes an enormous scientific and technological challenge.

Bio-sensors would need to be able to detect a wide array of pathogens, preferably prior to an attack, but essentially during the initial stages of an attack when countermeasures might still be able to significantly contain the damage. To be useful in the real world, however, bio-sensors would also need to be able to distinguish harmful biological agents from the millions of naturally occurring airborne viruses and spores that share the environment we inhabit. There is a similar issue with respect to radiation, as there are all sorts of objects, from bananas to ceramic tile, which emit harmless radiation naturally and would need to be distinguished from devices loaded maliciously onto container ships by groups or individuals aiming to cause harm.

Because remote sensors with the capabilities described would be breakthrough technologies for homeland security, efforts to create them are heavily concentrated in government laboratories. For private investors willing to bear the risk, the payoff to the successful development of a deployable multi-threat sensor technology would be exceptional.[1] In addition, such sensors represent a major opportunity for the creation of dual-use technology, as they would be useful for the rapid identification and containment of accidental or naturally-occurring releases of biological, chemical and/or radiological agents into the atmosphere near industrial facilities, for example, or in emergency rooms. With respect to cargo container shipping, however, sensors are not perceived to have many uses beyond their essential security role; they will not enhance supply chain efficiency, though they might be useful in helping to get supply chains up and running more quickly after an attack if they can be used to reassure people that cargo and facilities can be considered safe.

2. Identification and Authentication Technologies

[1] Vendors developing remote sensors include Alexeter Technologies, CombiMatrix, Cepheid, MesoSystems Technology, Nanosphere, Universal Detection Technology.

Much private sector research and development is focused on technologies that would be used to identify and authenticate individuals who come into contact with cargo containers from stuffing the boxes to unloading them at their final destination. Such technologies, which include increasingly familiar products such as smart cards, include optical memory and biometrics, for example, iris scanning and facial recognition. Private companies and government agencies have already been using such technologies for some time to identify their employees and to permit their entry (and in some cases exit) from the workplace.[2] The issue of tracking when an employee exits the workplace (the loading dock, for instance) as well as when he or she enters has been a matter of some contention.

Other contentious issues in this regard include the high potential for false positive rates, particularly with the use of immature technologies such as facial recognition systems. The extent to which high false positive rates cause significant supply chain delays, however, depends as much on the human systems put in place to deal with positive readings as it does on the capabilities of the current generation of technology. More difficult to solve may be the need for significant back-end infrastructure to store data against which various physical identifiers can be matched. The potential civil liberties implications of any centralized biometric data warehousing are likely to raise significant obstacles to the widespread deployment of technology designed in this particular form, especially those linked to DNA sampling.

[2] Vendors in this category include A4 Vision, Acsys Biometrics, ActivCard, Bioscrypt, ChoicePoint, Cross Match Technologies, Digimarc, Drexler Technology, Identix, LG, Motorola, NEC, SAGEM, Schlumberger, and Viisage.

3. Screening Technologies

In the area of screening technologies, work currently is focused on two issues. First, there is the issue of reducing the costs of screening cargo containers by increasing cycle time or throughput. This is a particularly pressing concern for ports and represents the major trade-off between enhanced security and improved efficiency from advances in transparency (tracking) along the supply chain. Container screening adds time to the processing of containers; port operators or customs inspectors must also bear the significant cost of the scanning equipment. Current leading technologies for screening cargo containers include x-ray and radiological/nuclear screening systems, and systems geared to explosive and explosive trace detection.[3]

The research emphasis in screening technology is in the area of so-called 'smart screening' systems. The idea here is to arm the screening machines with software that can detect anomalies and then automatically alert human operators to the need for further inspection and, perhaps, the need to instigate countermeasures. Vendors would like to improve the efficiency of screening machines by making them more broadly effective across the entire range of threatening agents, which include chemical, biological, radiological, and nuclear (CBRN) weapons. Screening machines are likely to incorporate advanced sensors to detect these and other potential threats, including also new types of explosives.

[3] Vendors in this category include American Science and Engineering, InVision (General Electric), L-3 Technologies, OSI Systems, SAIC, and Smiths Detection.

Scanning equipment is expected to enhance security by enabling the detection of weapons at ports of entry, thereby preventing their transport onto the mainland by truck or train. The expectation is that better screening technologies will also reduce commercial losses from fraud by enabling the quicker detection of illegal and/or dangerous goods and their removal from the supply chain.

4. Surveillance Technologies

Surveillance technologies are among the most controversial of the products being marketed to achieve better security, particularly in large urban areas where they are being deployed to cover larger and larger areas, such as Times Square in New York City or the National Mall in Washington DC. Established surveillance technologies include infra-red and motion detection camera systems and monitoring systems designed for radiological detection.

New generation 'smart surveillance' technologies incorporate software that can flag anomalous activity and alert human operators to the need for further inspection. Current research is aimed at the even more controversial objective of linking systems of surveillance to databases stocked with information on dangerous individuals or on characteristics of behavior, demeanor and appearance thought to be suspicious or associated with malicious intent.[4]

[4] Vendors in this category include CRS Technologies, InteliTrac, NEC, Northrop Grumman, ObjectVideo, and Vistascape.

5. Anti-Tamper Seals and Tracking and Inspection Technologies

A new class of electronic seals is being affixed to the main latch of most cargo shipping containers.[5] These seals serve as radio frequency identification devices (RFIDs), automatically signaling the container's location as it passes fixed points outfitted with tag readings along the supply chain (e.g., loading cranes, port gates). Moreover, the newest tags come equipped with intrusion detection technology. There is a magnetic field around each seal, and interruptions are recorded on a memory chip that notes the time of the event. So-called "smart" containers, currently under development, will go further, using on-board sensors to detect radiation or chemical residue, but also light and pressure changes that might indicate someone has attempted to cut or drill an opening through the side of the box. These anomalies would then either sound an immediate alarm or gets picked up the next time the container passes a tag reader, alerting human operators to the need for further inspection.

Private sector competition has driven the adoption of technologies for tracking goods as they move through the supply chain, including RFID, bar-coding, GPS and Wi-Fi.[6] The expectation is that tracking will render the supply chain more transparent, enabling both shippers and carriers to pinpoint the location of their goods anywhere in the shipping sequence from port of origin to final destination. From a commercial standpoint, the

[5] Commercial vendors working on this segment of the shipping security product market include Savi Technology, NaviTag Technologies, and IsoTag.

[6] Vendors in this category include Alien Technology, Intermec, Matrics Technology, Qualcomm, Savi Technology, Symbol Technologies, TransCore and Zebra Technologies.

major objective is to be able to rapidly locate bottlenecks if and when they occur so that shipping routes can be redirected and optimized.

From a security standpoint, the ideal system would enable continuous communication and tracking. This can be accomplished if seals are connected to transponders that can exchange signals with orbital satellites. This sort of continuous real-time communication will be quite expensive, however; this is one area where security needs may diverge from the needs of most customers in the commercial marketplace. The exceptions to this will probably be for cargo that is itself high risk (such as explosive chemicals) or high value (such as advanced computer chips). For these types of shipments, the desires of government security agents may match the investment incentives of commercial shippers.

Enhanced tracking promises other commercial advantages; it can assist in the early identification of damaged, misrouted or unapproved goods, reducing losses from both shipping damage and fraud. More so than the other technologies discussed in the context of maritime and port security, tracking technology can also help to mitigate the negative impact of supply chain disruptions, by giving shippers and carriers an added capability to quickly locate shipments en route and then reroute them around major breaks.

For security officials, the use of tracking technology to verify goods as they move through the supply chain is expected to be a major tool for preventing the transport of weapons of mass destruction (WMD) via cargo container. But technology does not currently exist with the ability to detect what is generally regarded as the greatest threat for transport via cargo container: a nuclear bomb or a radioactive "dirty bomb." There is still no technological substitute for good security procedures and well-trained human inspectors. But technology can help. Laboratory scientists are currently developing gamma ray detectors, equipped with imaging components which can reveal the shape of materials that are emitting radioactivity from inside the box. But the technology is not yet refined enough to prevent economically unacceptable numbers of "false positive" readings, from innocent materials such as ceramic tile that naturally emit small amounts of radiation.

Tracking technology presents a key opportunity for dual-use investment by the public and private sectors. Attention will need to be paid to the points at which security demands exceed the performance needs (and thus the investment justification) of commercial shippers. Too much reliance on security-driven investment might lead to the development of technology that is more specialized and expensive than commercial shippers, carriers or port operators will be willing to install. (Willing, or perhaps able—it has been estimated that the security community's dream of outfitting key points (e.g., border crossings) along the transportation route supply chain with gamma ray sensors might cost as much as $10 billion. So this is a technology area where the distance between security and commercial needs for development and deployment will have to be carefully calibrated, and the mix of public/private investment arranged accordingly.

6. Integrated Solution and Data Analysis technologies

As previously described, the market for shipping and port security technology has evolved from a market for stand-alone product solutions for security issues at specific points along the supply chain to an integrated system and services market in which companies compete to offer holistic security end-to-end security solutions that also promise to enhance the efficiency (i.e., profitability) of the entire supply chain network. Not only does a typical end-to-end shipment involve two dozen or more separate parties or organizations. It also involves 35 to 40 separate shipping documents. For a ship carrying, say, 3,000 containers, this would mean more than 100,000 separate documents that would have to be managed and secured in some way.

The foundation of such systems and services includes an array of data mining and access control technologies that propose to help human intelligence personnel see patterns or "connect dots" that would normally be obscured in the daily blizzard of data and communications. These technologies are a focus of development in the private sector, and also in the public sector, despite their having caused a major uproar in the context of the US Defense Department's aborted Technology Information Awareness (TIA) program.[7]

This market is certain to develop as companies engaged in cargo container shipping and port operations struggle to manage the proliferation of security products described in this chapter. Particularly challenging will be the need for vendors who can aggregate and

[7] Vendors in this category include BAE Systems, Boeing, Computer Sciences Corporation, General Dynamics (Veridian), Lockheed Martin, Northrop Grumman, Raytheon, and Verint Systems.

integrate point security solutions of both different vendors and different technology generations, as managers will be resistant, because of sunk costs, to completely abandoning security systems built up piecemeal over the years, no matter how seamless and turnkey the available solutions become.[8]

Most importantly, again, the extent to which the private sector invests in new integrated security solutions on its own will depend critically on the extent to which these solutions also enable them to aggregate and analyze data on cargo in transit. This is what will enable them to use these systems to enhance supply chain efficiency and thus improve the bottom line. The dilemma is that this same information might be considered highly sensitive from an intelligence or law enforcement perspective—this makes resolution of the data ownership and information sharing protocols even more urgent.

Conclusions

Technologies that can make cargo container shipping more secure already exist and are available off the shelf, or nearly so. The technologies that can track the containers as they move from link to link in the supply chain are the same technologies that private sector shippers, carriers and port operators were already pursuing prior to September 11, 2001 to improve the efficiency of their supply chain operations. A key policy objective

[8] Companies attempting to develop and provide integrated security solutions for maritime and port security include Unisys, Computer Associates, Allergent Technology Group, Hewlett Packard, and IBM.

now should be to allow these companies to continue to make the investments that they would want to make anyway for their own profit-seeking reasons.

A second objective would be to create market-based incentives to get these companies to internalize the costs of improving security all along the supply chain. This is a classic negative externality. The transformation of ships into floating warehouses, a consequence of just-in-time manufacturing strategies combined with the digital transformation of supply chain management, has also rendered societies more vulnerable to terrorist attack.

There are areas where security and commercial objectives conflict. It is essential to exploit opportunities for public-private collaboration to leverage emerging technologies for multiple uses (that is, both commercial and security applications). It is essential, as well, that such collaboration be structured in such a way that market signals (and the trajectory of technological development) are not unduly distorted by desires from security officials for expensive bells and whistles that really are not essential for improving security. The impact on supply chain security may be negligible, but the impact on supply chain efficiency may be quite damaging if over-specialized security demands render some of this new technology too complex and expensive for commercial use.

Another possibility is that US-based companies, more likely to win technology development contracts from the US Department of Homeland Security than their counterparts based in Asia or Europe, will end up being disadvantaged in international competition as shippers, carriers and port operators start to prefer less expensive, more commercially-relevant products offered by foreign suppliers. This will create new headaches for US security officials, with effects that could clearly spill over to negotiations involving the removal of restrictions on international trade.

In the end, as was often the case in the latter decades of the Cold War, simpler commercial technology may prove more effective and less expensive for security applications when it is allowed to "spin on" to those applications, instead of reliance on technologies developed from their inception with specialized security needs in mind. From the standpoint of American homeland security officials, it would no doubt be preferable for that commercially-developed spin-on technology to come from suppliers based in the United States.

References

Atkinson, Helen. "More Things to Worry About." *DC Velocity* (June 2004).

Avashi, Amitabh. "Containing Terror." *Technology Review* (September 2003).

Fickes, Michael. "Fighting Terror with Technology," *Government Security* (October 1, 2004).

Flynn, Stephen E. *America the Vulnerable* (New York: Harper Collins, 2004).

Flynn, Stephen E. "Beyond Border Control." *Foreign Affairs* (vol. 79, no. 6, 2000).

Garfinkel, Simson. "RFID Rights." *Technology Review* (November 3, 2004).

Garfinkel, Simson. "Unwrapping the Biometric Present." *Technology Review* (January 18, 2005).

General Accounting Office, "Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors." Washington, DC: GAO-03-770, 2003.

Gerin, Roseanne. "Security Opens New Doors: Guarding Nation's Ports and Commerce Sparks Growing IT Market." *Washington Technology* (September 13, 2004).

Koch, Christopher, "Remarks before the Journal of Commerce's 4th Annual Trans-Pacific Maritime Conference. Long Beach, CA: March 9, 2004.

Koch, Randy. "Secure Commerce: Securing Your Global Supply Chain." Unisys White Paper, Unisys Corporation, 2004.

Kurtz, Rod. "Small Biz Braces for Life on the High (Priced) Seas." *Inc.* (September 2004).

Lee, Hau L., and Michael Wolfe. "Supply Chain Security Without Tears." *Supply Chain Management Review* (January 1, 2003).

Lok, Corie. "Cargo Security." *Technology Review* (June 2004).

Powell, Peter H., Sr. "Testimony before the Subcommittee on Trade of the House Committee on Ways and Means," (June 15, 2004).

Rutner, Stephen, Matthew A. Waller, and John T. Mentzer. "A Practical Look at RFID." *Supply Chain Management Review* (September 1, 2004).

Scalet, Sarah D. "Sea Change." *CSO Magazine* (September 2003).

Seideman, Tony. "Freight Forwarding Heads into a World of Change." *World Trade Magazine* (January 13, 2005).

Sheffy, Yossi. "Supply Chain Management." *Defense Transportation Journal*, vol. 58, (September-October 2002).

Stowsky, Jay. "Secrets to Shield or Share? New Dilemma for Military R&D Policy in the Digital Age." *Research Policy*, vol. 33, no. 2 (March 2004).

"The Trojan Box: the Threat from Containers." *The Economist* (February 9, 2002).

Uchitelle, Louis and John Markoff. "Terrorbusters, Inc." *New York Times* (October 17, 2004).

Varian, Hal. "Managing Online Security Risks." *New York Times* (June 1, 2000).

Wasem, Ellen, Jennifer Lake, Lisa Seghetti, James Monke, and Stephen Vina. "Border Security: Inspections Practices, Policies, and Issues." (Washington, DC: Congressional Research Service, 2004).

"When Trade and Security Clash: Container Trade." *The Economist* (April 6, 2002).

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

Woodard, Kelby. "A Strategy of Trust: What will it take to Secure our Global Supply Chain?" *Loss Prevention* (November-December 2004).