2-2002

Global Trade: America's Achilles' Heel

James M. Loy

Robert G. Ross

Defense Horizons

Number 7

A publication of the
Center for Technology and National Security Policy
National Defense University

FEBRUARY 2002

Global Trade: America's Achilles' Heel

by James M. Loy and Robert G. Ross

Overview

Much has been written in the aftermath of September 11 on the porosity of America's borders and the failure of various agencies to share, fuse, analyze, and exploit available information to stop foreign threats before they enter the country. The resources and methods available to U.S. border control agencies appear to be no match for the myriad threats that could arrive from outside the country. Nowhere is the gap between vulnerability and capability greater than along the Nation's sea borders. Asymmetrical military and terrorist threats have a natural gateway into America via the marine transportation system.

In the uncertainty following the September attacks, the immediate response of security services around the country—the Coast Guard included—was to shut down the systems under their control until measures were taken to ensure that additional attacks were not already in progress. These system stoppages were generally short-lived because the economic impacts were intolerable, not only in dollar costs but also in potential loss of access to the essentials of daily American life. The United States is a trading nation, both domestically and globally, and relatively unimpeded movement of goods and people is necessary for its economy to function. Transportation is our social and economic cardiovascular system, and ensuring its continuation is vital. The post-attack shutdowns were a tourniquet to control bleeding but had to be released quickly to preserve the patient.

Given the importance of international goods and materials to the American economy, closing our borders for more than a short period is infeasible. Furthermore, with our growing reliance on just-in-time delivery of foreign goods, even slowing the flow long enough to inspect either all or a statistically significant random selection of imports would be economically intolerable. However, the transportation system, especially the maritime component, remains highly vulnerable to attack or other exploitation by terrorists. Thus, a major challenge facing the responsible agencies in the post-September 11 "new normalcy" is to develop border controls and transportation security measures that reduce the threat of the national transportation system's being used either as a weapon or as an essential logistic link in some other kind of attack.[1] Moreover, we must develop ways to better protect the Nation without sacrificing economic vitality or overwhelming the Federal, state, local, and corporate budgets.

Information is the key. Our national ability to detect potential threats in or to transportation can be significantly improved through effective use of information that, to a great extent, is already available. With sufficient advance information on inbound ships, cargoes, crews, and passengers, the various border control agencies will be better able to separate the good from the bad and intercept the bad before it becomes a problem for the country. This notion—exploiting available information to discern threats and concentrate resources to stop them—is at the heart of the maritime domain awareness (MDA) concept.

Center for Technology and National Security Policy

The National Defense University (NDU) established the Center for Technology and National Security Policy in June 2001 to study the implications of technological innovation for U.S. national security policy and military planning. The center combines scientific and technical assessments with analyses of current strategic and defense policy issues. Its major initial areas of focus include: (1) technologies and concepts that encourage and/or enable the transformation of the Armed Forces, (2) developments by defense laboratories, (3) investments in research, development, and acquisition and improvements to their processes, (4) relationships among the Department of Defense, the industrial sector, and academe, and (5) social science techniques that enhance the detection and prevention of conflict. The staff is led by two senior analysts who hold the Roosevelt Chair of National Security Policy and the Edison Chair of Science and Technology and who can call on the expertise of the NDU community and colleagues at institutions nationwide. The papers published in the *Defense Horizons* series present key research and analysis conducted by the center and its associate members.

Maritime domain awareness is the effective knowledge of all activities and elements in the maritime domain that could represent threats to the safety, security, or environment of the United States or its citizens. The objective is timely delivery of actionable information, drawn from all available sources, to the appropriate law enforcement agency or military command. A properly conceived system could be built so that it actually expedites cargoes carried by participating responsible shippers, thus facilitating commerce rather than impeding it.

In an earlier paper, we offered a more comprehensive view of the homeland security challenge facing the Nation and suggested that a truly national strategy should be both broad and based on risk management principles.[2] We also suggested that—in addition to using the traditional national security tools of military power, diplomatic influence, and economic power—the Nation will have to use civil authority at the Federal, state, and local levels in ways not seen before in this country. Further, because so much of our critical infrastructure is privately owned and operated, significant action also will be required from the private sector. We commented briefly on the need for maritime domain awareness as one of many essential tools for dealing with transborder threats. This paper builds on that suggestion and provides a more detailed examination of the MDA concept, emphasizing commercial shipping and international cargoes, especially containerized cargo.[3] Achieving MDA will require all involved to move beyond traditional thinking, traditional agency boundaries and functions, and even traditional distinctions between public and private information.

maritime domain awareness is the effective knowledge of all activities and elements in the maritime domain that could represent threats to the safety, security, or environment of the United States

The Maritime Threat

America is connected to the global economy not by aviation and the Internet but by maritime commerce. More than 95 percent by volume of our non-North American foreign trade (and 100 percent of certain commodities, such as foreign oil on which we are heavily dependent) arrives by ship.[4] Approximately 8,000 ships carrying multinational crews and cargoes from around the globe make more than 51,000 U.S. port calls each year. More than 7.5 million containers enter the country annually.[5]

This tremendous traffic creates a real vulnerability. Drugs and illegal aliens are routinely smuggled into this country, not only in small boats but also hidden among otherwise legitimate cargoes on large commercial ships. These same pathways are available for exploitation by a terrorist organization or any nation wishing to attack us surreptitiously. As immigration controls at the legitimate entry points are tightened, illegal entrants move into the illegal migrant flows to escape detection. In mid-October 2001, for instance, Italian inspectors found a suspected Al Qaeda member hiding in a shipping container equipped with a bed, a makeshift bathroom, and other amenities. The container was bound for Toronto, and its occupant, an Egyptian, had with him a Canadian passport, a satellite phone, two computers, a number of airport maps, security passes for airports in three countries, and papers identifying him as an aircraft mechanic.[6] Authorities do not know if this potential "terrorist in a box" was a singular event, but we do know that smuggling of illegal migrants in containers is increasing.

According to documents and court testimony, Osama bin Laden, through associates using flags of convenience, controls a number of cargo ships. One of these vessels was reportedly used to deliver explosives to a Kenyan port in 1998. Al Qaeda used these same explosives several weeks later to destroy U.S. embassies in Kenya and Tanzania.[7] However, ship registry practices in a number of countries facilitate hiding true ownership interests and the identities of interested parties. Moreover, hidden ownership is not just a problem on the security front. For example, in the 1999 Tankship ERIKA oil spill in France, inability to quickly identify the ship's true owners hampered spill-response activities.

Means of delivery is a significant consideration in addressing the potential for attacks using weapons of mass destruction (WMD). Although a rogue state might threaten or attack the United States using an intercontinental ballistic missile (ICBM) armed with a nuclear or other WMD warhead, other delivery means are available, some of which offer important tactical advantages over the ICBM. Among these are cruise missiles and smuggling, either via legitimate trade or clandestinely. Many types of cruise missiles could be launched, with relatively little risk of detection, from hundreds of miles at sea by small freight vessels or possibly from larger fishing vessels. Some 70,000 cruise missiles are reportedly in arsenals around the world, and, unlike ICBMs, the technology is both affordable and widely available. As to smuggling, millions of sealed containers enter this country each year, only a small percentage of which are ever inspected.

Technological and economic entry barriers to warhead delivery by commercial shipping are even lower than with cruise missiles, and the potential for identifying the perpetrator is practically nil. Because attribution risks and entry costs are small, some analysts have concluded that these non-ICBM delivery avenues represent significantly greater risks than do ICBMs, whether the potential perpetrator is a rogue state or a nonstate actor. In fact, Albert Einstein, in a letter to President Franklin Roosevelt in the early 1940s, noted that "a single [nuclear] bomb . . . carried by boat and exploded in a port, might very well destroy the whole port together with some of the surrounding territory."[8] The most significant difference between then and now might be the ease with which even a less developed nation

Admiral James M. Loy is Commandant of the United States Coast Guard. He may be contacted via Captain Ross. Captain Robert G. Ross, USCG, is Chief of the Office of Strategic Analysis at Coast Guard Headquarters, where he may be reached at rgross@comdt.uscg.mil.

is able to acquire nuclear devices. The number of opportunities for surreptitious entry into this country has increased at the same time that WMD have proliferated.

Container Terrorism

To understand the extent of America's economic and security vulnerability growing out of international trade, one must first understand the size and complexity of that trade and the role it plays in the Nation's economy. Of the 7.5 million loaded intermodal containers that enter this country every year by ship, approximately 2 percent are physically inspected in full for contraband, improperly identified trade goods, improperly packaged or marked hazardous materials, or illegal weapons.[9]

Current customs procedures were developed for economic protection. Final papers are not required to be submitted for a container shipped under customs bond until after the container arrives at its official port of entry, which can be as many as 30 days after it enters the country. Containers shipped under customs bond and bound for a final destination outside the United States never officially enter the country for purposes of commerce. Landbridge containers may undergo even less scrutiny than containers bound for an inland port of entry.[10] Under these kinds of minimal security safeguards, a container could be used quite easily for WMD transport into the United States for an attack. Of course, as experienced in Oklahoma City and other truck bombings, a device need not be a true WMD to have horrific consequences.

Absent the kind of threats predicted by recent blue-ribbon panels such as the Hart-Rudman and Gilmore Commissions[11]—threats made real by the actions of Al Qaeda—this minimalist approach to border scrutiny of trade makes good economic sense. Certainly, the economic benefits of growing global trade and the growing reliance on just-in-time delivery to replace warehousing were major factors in the productivity growth of the 1990s. However, the fragility of just-in-time delivery was illustrated by recent events at the Ambassador Bridge between Detroit and Windsor, Ontario. This bridge was the world's busiest commercial border crossing until shortly after September 11. Previously, some 5,000 trucks crossed this bridge every day; customs agents had on average just 2 minutes to process each truck. Significant delays caused by more complete physical inspections would have caused backups and effectively closed the border. The border was in fact closed on September 11, and the economic consequences were painful, particularly for companies and communities dependent on crossborder trade and travel.

under these kinds of minimal security safeguards, a container could be used quite easily for WMD transport into the United States for an attack

Prior to the security crackdown, American manufacturers relied on Canadian suppliers to deliver parts in as few as 6 hours of an order's being placed. Within a few days of September 11, the backup at the border was 11 hours. Six automobile plants in the Detroit area were shut down due to the interruption in flow across the Ambassador Bridge. Although the time between order and delivery is much longer in transoceanic trade, the principles are much the same. Consumers have reaped the benefits of productivity improvements made possible by replacing warehoused inventory with in-transit inventory. If security procedures impede trade, the economic impacts will be worldwide and could easily lengthen or deepen a global recession. If, on the other hand, economic and other factors result in a return to business as usual and the Nation then suffered a major attack in which insecure international shipping played an important role, the resulting shutdown of trade would have catastrophic and long-term domestic and international consequences.

The challenge for the United States and its foreign trading partners is to maximize security while minimizing delays. A critical component of an overall solution lies in taking advantage of the same information technologies that make just-in-time delivery possible. Easy access to accurate data on container contents, shippers, consignees, and even near-real-time container location is what makes just-in-time systems possible. Information generated for commercial purposes can also be used to support a security regime. The shipping community and supply chain/value chain managers from commercial sector giants, such as Ford, Wal-Mart, and General Motors, should be enlisted to keep national and international distribution networks functioning.

Risk Management

Risk is a function of both probability and consequence. Accordingly, risk management has historically focused both on reducing the probability of adverse events (prevention) and on mitigating the effects of those that occur (consequence management). Prior to the advent of automated information systems, it simply was not possible to compile and analyze large bodies of data to identify and track information that would alert safety authorities to higher-risk ships. Thus, ship safety programs were designed to treat all ships of a given type as if they presented equal potential for an accident, even though experience and instinct indicated otherwise.

Automated systems now permit safety authorities to track the records of owners and operators as well as the histories of their vessels to determine which owners and operators give conscientious attention to safe operations. Historically irresponsible operators are subjected to far more stringent safety scrutiny than are those with good track records. This historical tracking also extends to flag states and the classification societies to which various governments routinely delegate their authority to issue ship safety certificates, certificates of registry, and other required documents.

A principle underlying the MDA concept is that access to the right kinds of information will allow security authorities to better target prevention and security enforcement efforts. While normal to the national security, military, and law enforcement communities, this concept is relatively new to transportation safety and security enterprises, where inspection strategies have been based more on engineering principles than on human behavior. Despite

the newness of this approach, it has been used effectively by the Coast Guard in its program to drive substandard ships from U.S. waters and by customs and port safety authorities in Rotterdam to screen and identify suspect cargoes.

The Coast Guard is using vessel history and advance notices of arrival in its Port State Control Program to target substandard ships with the stated goal of driving such ships out of U.S. waters entirely. Every merchant vessel over 300 gross tons arriving in the United States from a foreign port must provide advance notice of arrival to the Coast Guard. Coast Guard captains of the port access Coast Guard and other databases to determine vessel history, flag affiliation, and ownership history. Based on this information, the vessel is prioritized for a Coast Guard boarding focused on safety and environmental protection issues. In some cases, vessels are boarded offshore before they enter port, and, in extreme cases, they can be denied permission to enter U.S. waters. In an era of scarce resources, this approach allows the Coast Guard to make better use of its limited inspector pool while also creating incentives for vessel operators to act responsibly: responsible operators spend less time dealing with the Coast Guard. The Port State Control Program is largely a success, as are similar efforts in Europe and among the more developed Pacific Rim nations.

much of the information needed for security purposes is already collected by the private sector and can contribute to a high degree of situation awareness

As currently configured, the Port State Control Program is of little utility for direct application to the security problem because it is focused on the ship itself and lacks appropriate security information. Far more pertinent is the Port of Rotterdam's experience with container ships. Several days before their arrival, ships inbound to Rotterdam must provide detailed cargo information to an integrated port safety and customs authority. Using a number of different screening techniques and criteria, officials search for indications of potential safety problems, untaxed goods, and contraband—such as illegal weapons, diseased agricultural products, and counterfeit merchandise. Rotterdam officials consider many inspection criteria, including compliance history of a given shipper. Anomalies in manifests and cargo documentation are also considered. Suspect cargoes and containers are identified and examined in detail as they are unloaded from the ship and before they leave the port. Problems are discovered in approximately 10 percent of the containers subjected to detailed examination. Precleared cargoes, on the other hand, are given expedited handling and quickly depart the port for their ultimate destinations. Some low-probability containers also are inspected as a quality control and integrity assurance measure.[12]

The Rotterdam experience demonstrates the feasibility of using information to target safety and security problems. Information technologies now available—including artificial intelligence, data-mining techniques, and large-scale databases—are well suited to this kind of task. Much of the required information also already exists—it is a necessity for just-in-time logistics systems to function. Other information is collected by various government agencies as well, albeit in a disjointed and sometimes untimely manner. The obstacles preventing U.S. border control agencies from deploying this approach have more to do with statutory restrictions, Government priorities aimed at yesterday's needs rather than today's threat, interagency turf fights, and, most significantly, inadequate resources.

The MDA Concept

The concept of maritime domain awareness first appeared in the Coast Guard's 1999 Strategic Plan, which reads in part: "The Coast Guard will achieve the ability to acquire, track, and identify in real time vessels and aircraft entering America's maritime domain."[13] This goal was not well defined, however, and much work was required to refine the concept further. Since the publication of the Strategic Plan—driven by the reports of the Hart-Rudman Commission, the Gilmore Commission, and the Graham Seaport Security Commission[14]—the Coast Guard has gained a far greater understanding of the information needed to support the MDA concept properly. In particular, Coast Guard planners began to understand the importance of having timely access to detailed information on vessels, cargoes, passengers, crews, and historical vessel and cargo itineraries.

While these commissions were working, the Coast Guard, in concert with the Maritime Administration and other agencies, embarked on the Marine Transportation System (MTS) Initiative. The MTS Initiative was established to address growing concern over the ability of the Nation's ports, waterways, and intermodal land/sea connections to meet future needs and to improve cooperation among the various Federal agencies and other entities delivering essential port and maritime services. As part of the problem-definition phase for the MTS Initiative, listening sessions were held around the country to allow the maritime industry and others to express their concerns. Some of the most frequent complaints concerned information collection and access. Specific objections included the multiplicity of different and partially overlapping advance notice requirements imposed by various Federal agencies and port authorities; the need to undergo multiple boardings once in port; the lack of real-time port status and navigation safety information; and the failure of agencies to provide Web-based means for providing required information.

As a result of the MTS Initiative, agencies became increasingly aware that the ability to move and process information rapidly had grown in importance to the Nation's overall transportation system. In a modern container port, more people move information than cargo. Just-in-time delivery requires in-transit visibility of cargo moving through the system to reduce inventory costs and improve productivity. The implications for MDA from these realizations are that much of the information needed for security purposes is already collected by the private sector and can contribute to a high degree of situation awareness.

Stephen Flynn, a fellow at the Council on Foreign Relations, provided further understanding of the challenges and benefits in making the MDA concept operational. Dr. Flynn, who is also an

active-duty commander on the permanent commissioned teaching staff at the Coast Guard Academy, has studied the security implications of globalized trade and has developed important insights on the potential threats implicit in that trade. According to Dr. Flynn, heavy or exclusive reliance on tight security measures at our borders is a strategy doomed to failure. Realities of global trade preclude ensuring security through border inspections without restricting flow to the point where the economic consequences would be intolerable. At the same time, both the United States and other nations retain vital interests in controlling people and cargo crossing their respective borders. For the United States, security is the most immediate objective. Broader, long-term objectives may include protecting the fiscal integrity of an emerging nation's government and stopping the flow of illegal migrants, drugs, and other contraband. Thus, while a unilateral approach could be pursued, the more attractive alternative is to take advantage of shared interests of overseas trading partners to build security into the international trading system.[15]

The maritime domain awareness idea, having started from the Coast Guard's initial relatively limited goal, has matured. The Coast Guard recognizes maritime domain awareness as a necessary national, and even international, capability.

Interagency Coalition

Achieving MDA is beyond the capability of a single agency or government. The process is simply too complicated. Thus, the desired MDA capability will require a combination of discrete technologies, interoperability between numerous stand-alone systems, and the information analysis capability to take full advantage of that interoperability. The Coast Guard, recognizing that it was not in a position to achieve MDA in isolation, presented the concept to a number of other agencies that appeared to be natural partners in an MDA effort. The MDA concept was also presented to the staff of the National Security Council (NSC), who readily recognized and seized upon its potential.

achieving MDA is beyond the capability of a single agency or government

Under NSC sponsorship, interagency discussions began in mid-2000 and ultimately led to an interagency memorandum of agreement signed on January 12, 2001, by the Department of Defense, the Immigration and Naturalization Service (INS), the Coast Guard, and the Bureau of Consular Affairs in the Department of State. The objectives of the memorandum are to create a maritime fusion center through extensive interagency cooperation and to exploit the expertise and data-mining capabilities of the signatories. The existing Coast Guard Intelligence Coordination Center, collocated at the National Maritime Intelligence Center in Suitland, Maryland, was selected to serve as the initial organizational foundation for the fusion center.

The MDA fusion center has been busy from its inception, but the level of activity has increased dramatically since September 11 and will increase further as MDA capability grows. The Coast Guard has already extended its advance notice of arrival requirement from 24 to 96 hours and significantly increased the amount of information that it requires. Lookout lists from the INS and other agencies are now cross-checked against crew and passenger lists, and Customs and INS are working to place the Advance Passenger Information System in the MDA fusion center. Some advance scrutiny of cargo information is also occurring. The analytic processes now being used are largely manual, but those involved are learning much that will be invaluable in the design of automated processes to handle significantly more data.

Extending U.S. Security Borders

Detecting a containerized WMD at its port of entry is clearly not the best outcome. Identifying and intercepting it as far from its intended target as possible would be preferable. Thus, creating additional offshore security perimeters (sometimes called extending our borders outward) is one of several objectives in the MDA concept. This goal is not a question of violating the sovereignty of America's trading partners. Rather, the idea is to create mutually beneficial layered defenses/security perimeters, with the first layer ideally at the points of origin, both here and there. Another objective is to improve transparency of every key component, player, and transaction in the larger international shipping system. The United States cannot achieve these objectives acting unilaterally. Therefore, we should not hesitate to ask our trading partners to participate in a cooperative effort to build appropriate safeguards into international shipping.

One of the first steps in pushing our security perimeters outward would be to obtain the cooperation of our North American Free Trade Agreement partners, Canada and Mexico, in creating comparable security measures at all North American ports of entry. Another step would be to expand existing trusted shipper programs to address security, thus allowing cargoes to move across borders without the kinds of delays that were experienced at the Ambassador Bridge after September 11. Details of such a system have not been developed, but both point-of-origin requirements and in-transit integrity protections are likely features.

Cooperative information exchanges between American and foreign customs services should be another key element in the future system. Confidence in the quality of the information could be enhanced through regular and continuous sharing, thus facilitating better enforcement of safety, security, and revenue laws at both ends of the trade route. For example, declared cargo identities would be less likely to change mid-voyage, as cargo verification could happen at both ends of the trade route. In addition to improving the U.S. domestic threat situation, this could also improve the international environment. Historically, ineffective border security and lack of governmental fiscal integrity—exacerbated by smuggling to avoid customs duties—have been major factors in the failure of emerging states. Failed states, such as Afghanistan under the Taliban, invariably become security threats to their neighbors and, by providing breeding grounds for discontent and terrorist impulses, to the larger global community. Reducing the potential for failure of emerging states is a worthy national and international goal, and MDA will be beneficial in efforts of that kind.[16]

The International Maritime Organization (IMO), a specialized body of the United Nations, sets international standards for ship construction, environmental protection, vessel traffic control, and the like. IMO should develop international standards on transparency in vessel ownership and the identification of parties involved with or having a controlling interest in a ship. Additionally, IMO should be an active participant in developing a system to track containers and other cargoes after they have been accepted for sea transport. This would help protect against the diversion of cargoes to unintended recipients or the substitution of an illegitimate cargo in a container at a trans-shipment point. Depending on the degree of cooperation by foreign customs services, an overseas presence by the U.S. Customs Service may be required to verify cargoes at the point of origin or possibly at the port of origin. The possibility also exists of creating an international system for vetting shippers and carriers, either under IMO sponsorship or as an International Organization for Standardization standard.

MDA will require cooperative efforts across multiple government and commercial systems and entities

The U.S. delegation voiced the need for IMO to become involved in improving international shipping security at the November 2001 meeting of the IMO Assembly. The U.S. position was strongly supported by IMO Secretary-General William O'Neil and received further support from 48 nations. The organization agreed to add maritime security to its work program, and a special meeting has already been scheduled for February 2002.

Finally, cooperative foreign information exchange is being used in national intelligence and law enforcement; this information also should be made available within the context of MDA. Information on suspect individuals and organizations could easily be correlated with information on parties involved with specific ships and cargoes.

Acting Globally *and* Locally

Local domain awareness is MDA at the tactical level, at sea or in port, where security and safety enforcement operations take place. Data needs and uses at this level are different from those at the national level, where large-scale data fusion and analysis will take place. Most locally generated data will be either relatively static (port facility data) or highly dynamic (vessel positions) and of limited use at higher levels. Local security forces should have some degree of reach-through capability to source data needed in the event of an emergency (for example, cargo data while responding to an accident) and should be provided with warning notices or flags for suspicious inbound cargo or ships.

Clearly, MDA will require more than honest cargo declarations by law-abiding shippers. In keeping with a Russian saying famously quoted by former President Ronald Reagan—"Trust, but verify"—a significant degree of compliance inspection will be required. Some of this will necessarily be performed at sea by Coast Guard boarding teams, but much will also be done in port by various border control agencies. One possibility raised in the MTS Initiative is of joint or multiagency port safety and security operations centers directing multiagency inspection teams. These teams could easily be structured to address the full range of border control and port safety concerns while simultaneously expediting business for vessels in full compliance. These proposals are compatible with not only the desire of the marine industry for single-point reporting for all agencies but also the elimination of multiple boardings by enforcement agencies. Finally, new sensor and detection systems must be included to screen cargoes at sea and in port without appreciably slowing flow.

As also revealed in the MTS Initiative, ships have grown significantly larger over the last half decade, but ports and channels have not grown correspondingly larger and deeper. Thus, real-time information, such as water depth and currents, is becoming increasingly important for navigation safety. At best, such information might seem tangential from a security perspective; however, having these facts would be extremely important for responding to chemical and radiological incidents in U.S. ports and waterways. The Physical Oceanographic Real-Time System (PORTS), developed by the National Oceanic and Atmospheric Administration, would, if adequately funded, meet this need.[17]

Technical Attributes

Maritime domain awareness remains at the conceptual stage, and many of the technical details remain undetermined. Already clear, however, is that MDA will require cooperative efforts across multiple government and commercial systems and entities. Key elements for successful MDA implementation will likely include:

- a data architecture that transcends agency and national lines to provide standardized and simplified data for multisource correlation and analysis
- a system allowing multiple databases to be accessed by appropriate entities without violating the statutory safeguards that govern most government databases
- development of algorithms that would permit machine-based threat analyses based on large data sets.

Pieces of the data architecture are already in place but are not yet robust enough to function as intended. For example, ships engaged in international trade are required to have a unique numeric identifier called a Mobile Maritime Service Identifier (MMSI). The MMSI is, in essence, a ship's phone number for both the Global Maritime Distress and Safety System and for Automatic Identification System (AIS) transponders. As a unique ship identifier, MMSI has great potential for tracking specific ships across multiple databases. Another unique identifier is the Lloyd's Registry number.[18] This number has the advantage of being carried by a ship for life; unlike an MMSI, it does not change as a ship changes flag state registration. Neither of these ship identifiers provides 100 percent coverage, but they do provide starting points.

The International Maritime Dangerous Goods Code, promulgated by IMO to facilitate accurate identification of hazardous materials in transport, could serve as the basis for an expanded cargo classification scheme to standardize cargo reporting for security purposes. A national or international scheme for assigning identification codes

to licensed shippers, freight consolidators, and freight forwarders also could be easily developed and used as the basis for tracking historical compliance with all applicable safety and security requirements. The Customs Service is planning the Automated Commercial Environment (ACE), which might provide an excellent host database for shipper and freight consolidator/forwarder compliance histories. This would provide a shipper-focused counterpart to the Marine Information for Safety and Law Enforcement system, which is the Coast Guard database on ship and ship-owner/operator compliance records.

International or bilateral systems for identification of individuals, such as machine-readable passports required under the Visa Waiver Program (P.L. 106–396), also could play a role in maritime domain awareness. Similarly, an international identity system for the merchant mariners of the world would help address both the potential for terrorist infiltration of a ship's crew and the existing global problem of fraudulent merchant mariner licenses and documents. This system would be especially valuable when combined with appropriate national and international suspect lookout lists, such as the State Department Consular Lookout and Support System and the INS National Automated Immigration Lookout System II.

The extent to which any existing and future databases could be merged might be limited. National privacy laws and the need for legitimate businesses to protect proprietary data will dictate some limits on information sharing. For that reason, a means to provide the appropriate degree of access to users with differing authorizations is required. Good models already exist, such as Pennsylvania's Web-enabled statewide criminal Justice Network (JNET), which is the result of an initiative undertaken by former Governor Tom Ridge.

JNET provides a virtual single system based on open Internet technologies with standards that link information from diverse, seemingly incompatible systems of 16 different criminal justice agencies. The system enables agencies to share information but does not affect independent operating environments. As required by certain confidentiality statutes, each agency can determine the extent to which the others have access to its data. JNET is a secure extranet providing a secure *publish and subscribe* architecture featuring encryption and digital user/server authentication certificates. Appropriate and probably extensive security protocols will have to be in place before the intelligence community is willing, or even allowed, to participate in the MDA effort.[19]

Major differences between the MDA concept and JNET approach will impact any MDA technical architecture significantly. These differences include both the level of predictive analysis and correlation across multiple databases called for in the MDA concept and the need to deal with literally hundreds of millions of separate ship, cargo, passenger, and crew data entries. Several of the databases on which MDA will be built, especially the U.S. Customs ACE system, are far larger than anything in JNET. Thus, MDA will undoubtedly require use of artificial intelligence, sophisticated data-mining techniques, and appropriate risk identification algorithms.

Emerging information technologies show promise in providing significant security benefits. Knowing where a given shipment is at any moment can be critically important from an economic perspective. Cargo-tracking systems, such as container transponders and bar code systems of the type used by United Parcel Service, are now being used to track certain high-value cargoes. Bar code systems update custody and location information every time the cargo changes hands. Container transponders, in contrast, use satellite communications and the GPS (global positioning system) to generate a position update to a ground station at periodic intervals. Cargo-tracking systems of these kinds could be particularly well suited for ensuring that in-transit cargoes do not fall into the wrong hands and are not diverted from their legitimate itinerary, whether through simple theft or substitution of a contraband cargo for a legal one.

cargo-tracking systems could be particularly well suited for ensuring that in-transit cargoes do not fall into the wrong hands

Transponders also can be placed on vessels with clear MDA implications. Two vessel transponder systems, designed with specific MDA use in mind, are entering service now. Both provide specific kinds of information, such as vessel name, a unique vessel identification number, and vessel position. Depending on the system, other information also may be available. Vessel Monitoring Systems (VMS) are being employed in fishery enforcement operations in several countries. VMS is not the name of a single system. Rather, it is a generic term used to describe any of a number of asset management systems using long-distance communications. VMS reporting rates are set at no greater frequency than required for the specific fisheries enforcement purpose. Typically, these range from once every 15 to 30 minutes to once every 24 hours. A number of U.S. fisheries already

MDA Concept: Building Security into International Shipping

- Focus on potential threats—for example, vessels, cargoes, crews, and passengers.
- Develop a common, integrated data architecture.
- Fuse traditional intelligence with information from public, private, commercial, and international sources.
- Develop risk indicators based on fused, multisource data.
- Push security perimeters out, ideally to the points of origin.
- Ensure transparency in international shipping.
- Foster active participation by U.S. trading partners—that is, achieve an *international* solution.
- Foster cooperation and integration across agency, national, public/private, and data system boundaries.
- Ensure shipper and carrier involvement in building maritime domain awareness.
- Provide incentives for cooperation by shippers and carriers.
- Protect proprietary commercial data.
- Trust, but verify. Rigorously verify shipper and carrier compliance.
- Execute cued military or law enforcement responses to threats.

have adopted VMS requirements for fishery enforcement purposes, but broader national security or law enforcement purposes are generally prohibited at the present time.

The other vessel transponder with MDA potential is the Automatic Identification System (AIS). AIS is primarily a navigation safety and collision avoidance tool and differs significantly from VMS. First, AIS operates at a much higher reporting rate—as frequently as once every 2 seconds (radar sweep rates)—and is tightly controlled by technical standards to ensure interoperability across brand names. AIS employs a relatively short-range, VHF–FM line-of-sight communications protocol that operates without any satellite or land-based infrastructure. However, land, air, and possibly even satellite-based receivers can receive AIS signals, making it useful for MDA purposes. The actual range depends on power output and antenna height, but ship-shore ranges over 100 miles have been obtained with the shore antenna located at about 1,500 feet. AIS carriage requirements have been adopted by IMO and will be phased in beginning in 2003. IMO, however, may decide to accelerate this schedule. AIS carriage requirements ultimately will extend to merchant vessels over 300 gross tons on international voyages and over 500 gross tons on domestic voyages. Flag and coastal states are free to set AIS carriage requirements for smaller domestic vessels and fishing vessels as they see fit.

Conclusion

True maritime domain awareness will arise from the combination of historical data on ships, shippers, and involved parties of many types; advance-voyage-specific data on cargo, passengers, and crew; and systems to track the location of both individual containers in-transit and vessels at sea. This level of awareness, augmented by powerful analysis, will yield the kind of understanding necessary to improve the collective ability of the border control agencies to separate the good from the bad—to stop the bad while facilitating the good.

While there are no guarantees that the maritime transportation system will not be used to harm U.S. domestic interests, achieving the level of domain awareness described above will decrease the likelihood significantly. The MDA concept, solidly based on both civil authority and practical application of proven risk-management techniques, is a best-value measure for securing the homeland. Maritime domain awareness is an idea whose time has come.

Notes

[1] The primary agencies responsible for border control are the Customs Service, the Immigration and Naturalization Service, the Coast Guard, and the Department of Agriculture. The Aviation and Transportation Security Act (P.L. 107–71) created the Transportation Security Administration (TSA) under the Department of Transportation. In addition to its aviation security functions, TSA is responsible for overseeing the adequacy of cargo security in transportation. How this responsibility will be carried out remains to be determined.

[2] James M. Loy and Robert G. Ross, "Meeting the Homeland Security Challenge: A Principal Strategy for a Balanced and Practical Response," in *Journal of Homeland Security*, September 2001; accessed at <http://www.homelandsecurity.org/journal/Articles/article.cfm?article=22>

[3] Traditional Coast Guard concerns—such as drugs, illegal migrants, fishery enforcement, domestic maritime commerce, domestic hazardous materials transport and storage, and even search and rescue—are also part of the MDA picture. Full treatment of these issues is outside the scope of this paper.

[4] Department of Transportation, "An Assessment of the Marine Transportation System: A Report to Congress," September 1999, 2.

[5] Container figures can be confusing. Containers come in several common lengths, including 20, 40, and 45 feet, but are counted in 20-foot equivalent units (TEUs). Total inbound and outbound TEU in 2000 was a little over 29 million, both loaded and empty. The actual number of containers is approximately 60 percent of total TEU. Inbound and outbound container numbers are equal, with many more outbound containers empty due to the U.S. import-export imbalance.

[6] Susan Kelleher, "Big Hole in Nation's Defense: Our Ports," *The Seattle Times*, October 28, 2001.

[7] Ibid.

[8] Quoted in Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer, *America's Achilles' Heel* (Cambridge: MIT Press, 1999), 213.

[9] While the overall container inspection rate is less than 2 percent, the number of containers inspected is higher for certain trade routes. As proposed in this paper, the Customs Service selects containers for inspection based on a review of available shipping documents. Concerns with current practice are tied to timeliness, completeness, and accuracy of information now available.

[10] *Landbridge* is the term used to describe the movement of containers by train across the United States to be reloaded on ships to complete the Europe-to-Asia or Asia-to-Europe transit.

[11] The Hart-Rudman Commission was officially known as the Commission on National Security Strategy/21st Century. Its reports can be accessed at <http://www.homelandsecurity.org/research.cfm>. The Gilmore Commission was officially known as the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Its reports can be accessed at <http://www.rand.org/nsrd/terrpanel/>.

[12] Department of Transportation/Volpe National Transportation Systems Center study of foreign port best practices, unpublished results. The Rotterdam visit occurred in spring 2001.

[13] United States Coast Guard Strategic Plan 1999, 14.

[14] The Graham Seaport Security Commission was officially known as the Interagency Commission on Crime and Security in U.S. Seaports. Its report can be accessed at <http://www.uscg.mil/vtm/pages/july2000portspdfversion.pdf>.

[15] For more detailed presentations of Dr. Flynn's ideas, see Stephen E. Flynn, "Beyond Border Control," *Foreign Affairs* (November-December 2000) and "A Transportation Security Agenda for the 21st Century," *TR News* 211(November-December 2000), 3–7.

[16] As a historical note, the Revenue Cutter Service, one of two principal ancestors of the modern Coast Guard, was founded for the explicit purpose of securing revenue for the newly formed United States. Seemingly, some societal needs endure.

[17] National Oceanic and Atmospheric Administration and the U.S. Coast Guard, "Real Time Tide and Current Data Systems in United States Ports: A Report to Congress," July 2000. This report can be viewed at <http://www.uscg.mil/vtm/pages/july2000portspdfversion.pdf.>

[18] The Lloyd's Register is, in itself, an invaluable source of technical information on the world's merchant fleet.

[19] JNET information is from KPMG Consulting, which developed this system under contract to the Commonwealth of Pennsylvania.

Defense Horizons *is published by the Center for Technology and National Security Policy through the Publication Directorate of the Institute for National Strategic Studies, National Defense University.* **Defense Horizons** *and other National Defense University publications are available online at http://www.ndu.edu/inss/press/nduphp.html.*

Center for Technology and National Security Policy

Hans Binnendijk
Director