2004-11-04

Preventing Armageddon I: Enhancing America's Border & Port Security After 9/11; Strategic Insights, v. 3 issue 11 (November 2004)

Zellen, Barry S.

Monterey, CA; Naval Postgraduate School

Strategic Insights, v.3, issue 11 (November 2004)
https://hdl.handle.net/10945/11483

Preventing Armageddon I: Enhancing America's Border & Port Security After 9/11

Strategic Insights, Volume III, Issue 11 (November 2004)

by Barry S. Zellen

Introduction

9/11 radically redefined America's perception of the world beyond its borders and the dangers it faces at home. Ever since, the United States has sought to reinvigorate its efforts to secure not only its long land frontiers with Mexico and Canada, but also it hundreds of seaports that are scattered along its thousands of miles of coastline.

Once, America felt secure and isolated from the world, protected by the vast Atlantic and Pacific oceans off both its shores. But now, America feels uniquely exposed to the world's dangers, with long, porous borders and seaports that appear, in hindsight, remarkably unprotected—and which now are proving exceedingly difficult to secure and defend from the new array of threats in the post 9/11 world, ranging from nuclear and radiological attack to bio/chemical attack.

With an increasingly globalizing world economy crying out for more open markets, more international trade and commerce, America's economic vitality demands more and more openness. Yet America's post 9/11 security requirements demand greater vigilance, greater scrutiny of the commerce that sustains America's, and most of the world's, economy. How do we juggle the competing requirements of security and economic vitality in this new world? The answer comes down to two words: vigilance, and innovation.

In the months since 9/11, there's been a veritable Manhattan Project of innovation going on, from university campuses to the research and development labs at technology companies all across America, as technologists seek to innovate their way through this crisis of historical proportions, and find a way to harness new technologies and government programs to bolster America's border security—so that its ports can remain open, enabling the international commerce upon which it depends to continue even as new threats and dangers emerge.

Securing America's Seaports

When Homeland Security Secretary Tom Ridge spoke about America 's new security challenges at the Port of Newark, New Jersey last year, he announced a new series of programs to bolster America's port security.[1] In his speech, Ridge announced that America's security would be cobbled together by an ambitious series of interconnecting programs that include "smart borders to protect our shores and waterways, tough international container standards, highly trained screeners at our airports, intensive measures to protect our physical and cyber infrastructures, an early warning network of sensors to detect a biological attack, [and] resources to prepare our public health systems in the event of an attack." He added that over $4 billion US has been distributed to America's first responders "to help them train and ready for any threat, whether a force of nature or a force of evil."

Ridge observed that "from the sea-faring borders of our homeland, to the innermost quarters of our heartland, we're doing everything possible, using every means possible, to ensure that the facilitation of trade moves ever forward—with no disruption and no danger to our economy, our people and our way of life." Balancing the need for security with the need for commerce is proving to be a big challenge, but Ridge and his department continue to plug away at their seemingly impossible mission to secure America's immense, and largely unprotected, borders.

The Container Security Initiative (CSI)

During his June 12th speech, Ridge announced a series of new port security initiatives and investments "designed to strengthen port protections through increased international cooperation, new technology and the necessary funding needed to meet these new security enhancements, at strategic ports located around the world." In particular, he announced the Container Security Initiative (CSI), Operation Safe Commerce, the Maritime Transportation Security Act, and new Port Security Grants "to provide added layers of security that build on a comprehensive port security." Ridge added that "these layers—greater information sharing with our international partners, increased levels of inspection, state-of-the-art technology and added intelligence on the crews, cargo and vessels long before they reach our shores—are allowing us to screen and board 100 percent of high-risk vessels coming into our ports."

Ridge noted that phase 2 of the CSI had just begun, a measure spearheaded by Department of Homeland Security's Bureau of Customs and Border Protection with four core components:

- Identifying "high-risk" containers, through the use of advance information, before they are loaded onto board vessels destined for America.
- Pre-screening the "high-risk" containers at the foreign CSI port before being shipped to the United States.
- Using detection technology to pre-screen high-risk containers, including radiation detectors and large-scale x-ray imaging equipment so that security inspections can be done quickly, without slowing down the flow of legitimate cargo.
- Using smarter, "tamper-evident" containers at the port of arrival that indicate to U.S. Customs and Border Protection officers whether cargo has been tampered with after security screening overseas.

Ridge explained that CSI "involves stationing U.S. Customs and Border Protection officers at foreign seaports to do the actual targeting and identification of high-risk containers," enabling America to "extend our zone of security outward, so that American seaports and borders become the last line of defense, not the first," as "we can't afford to focus exclusively on domestic ports." Ridge noted that around 90 percent of all world cargo moves by container and that in the U.S., almost half of incoming trade (by value) arrives by container ships—and "that means that almost 7 million cargo containers arrive and are offloaded at U.S. seaports each year."

Ridge noted that phase 1 of CSI “focused on implementing the program at the top 20 foreign ports,” accounting for 68 percent of all cargo containers arriving at U.S. ports. He added that CSI is now operational at 13 ports worldwide and will soon become operational at the remaining 7 ports. According to Ridge, “CSI has emerged as a formidable tool for protecting America from the threat of terrorism.” With phase 2 underway, Ridge added that the U.S. will be able “to extend port security protection from 68 percent of container traffic to more than 80 percent—casting the safety net of CSI far and wide.”

Bolstering CSI, Ridge said there will be “a significant level of program and funding support,” including Operation Safe Commerce, a “pilot program, designed in conjunction with the Department of Transportation and the Bureau of Customs and Border Protection” that functions “much like a venture capital fund, the program will prompt private businesses, ports, and federal, state and local authorities to develop new technologies that can monitor the movement and integrity of containers as they move through the supply chain.” Ridge said that that “true maritime security demands that government and industry work together—which is why we are continually collaborating with industry, states, and local authorities to secure our ports and waterways.”

IT on the Border

Since its inception on January 24, 2003, DHS’s Border and Transportation Security (BTS) Directorate has initiated a major reorganization of its component agencies, creating two new bureaus: the Bureau of Immigration and Customs Enforcement (BICE), and the Bureau of Customs and Border Protection (BCBP); deployed new technologies and tools at land, air and sea borders; expedited distribution of billions of dollars in grant monies to states and cities—with more to come; and created a 24-hour Radiation/WMD Hotline to assist BCBP and BICE officers with scientific and technical needs regarding Chemical, Biological, Radiological and Nuclear (CBRN) alerts along the border.

BCBP “is implementing the Free and Secure Trade Initiative (FAST),” as Asa Hutchinson, the Under-Secretary of Homeland Security, testified on June 25, 2003 to the House Select Committee on Homeland Security. FAST will enable BCBP “to focus its security efforts and inspections on high-risk commerce while making sure legitimate, low-risk commerce faces no unnecessary and costly delays.” [2] BTS was in its first phase of developing the US-VISIT system, with its initial deployment at air and sea ports of entry scheduled to be completed by December 31, 2003. It was designed to be capable of tracking the entry and exit of foreign visitors who require a visa to the U.S., and will make entry easier for legitimate travelers and more difficult for illegal entrants through the use of biometrically authenticated documents.

Accenture's recent DHS contract win should further bolster these capabilities with better systems integration. As reported by *Silicon.com's* Ed Frauenheim, DHS announced on June 1st that "it had awarded Accenture a contract worth up to $10bn for help in upgrading the nation's system for tracking visitors," and to "provide a range of services including strategic support, design and integration activities, training and 'organizational change management.'" [3] The Bermuda-based IT services giant will "become the prime contractor for a federal programme called US-VISIT" which is designed to "capture and share data—including biometric data—on foreign visitors." DHS undersecretary of border and transportation security Asa Hutchinson told *Silicon.com* that "this award marks an important milestone in the history of Homeland Security and the US-VISIT Program," and "by harnessing the power of the best minds in the private sector, we have taken a major step toward accomplishing our goals of enhancing the security of our country while increasing efficiency at our borders."

BCBP deploys multiple technologies to support our layered inspection process, using various technologies in different combinations to detect the adversary who might defeat a single sensor or device. Over 250 “non-intrusive” inspection systems and/or portal radiation detection devices

have been deployed to detect - and deter - the entry of radiological material into the country. BCBP has provided all of its front-line (BCBP) inspectors across the country with personal radiation detectors that alert them to the presence of radioactive material. BCBP is also implementing of the Customs-Trade Partnership Against Terrorism (C-TPAT), a public-private partnership aimed at securing the global supply-chain against terrorism, while also facilitating legitimate trade.

And along with CSI, BCBP began enforcing the new 24-hour rule in February, requiring submission of electronic advance cargo manifests by sea carriers 24 hours before U.S. bound cargo is loaded aboard the vessel at a foreign port.

The information obtained is used as a factor in determining which containers are high-risk, in an effort to preclude a risk from ever arriving in the USA. BCBP continues to coordinate with the Coast Guard to have expanded Passenger Analysis Units at seaports around the country to target and identify high-risk travelers and immediately react to threats. BCBP cross checks advance notice of arrival information provided to the USCG 96-hours prior to arrival at U.S. ports, rather than the previous 24-hour notice—for potentially dangerous crew, passengers and cargo, thus allowing USCG to act appropriately prior to arrival in the U.S. port.

Mark Willoughby of *Computer World* ("IT to provide multifaceted security at U.S. borders," June 19, 2003) reported that the BCBP is working to "secure the nation's borders with a state-of-the-art [IT] architecture," and its goal is to provide "a single face at the border' for fast and efficient decision-making on the millions of visitors and billions of imports crossing U.S. borders every week." [4] The result of this ambitious effort is large-scale effort to "encrypt information in storage and transit, authenticate users and provide rules-based authorization policies, single sign-on, radio frequency identification (RFID), content X-ray, and radiation detection with outsourced Internet threat monitoring and detection." DHS is taking what Willoughby describes as "a top-down, architectural approach to integrating disparate IT organizations," and that "security priorities extend from customs inspectors and border patrol agents in the field to foreign manufacturing plants and ports shipping goods to the U.S., and the layers of infrastructure required to support them."

To help secure against threats originating at foreign ports, those "foreign points of origin for goods to be imported into the U.S. are now viewed as an extension of U.S. Customs jurisdiction, so that shipping containers can be inspected and sealed at the source. Containers then will be tracked and authenticated via RFID and other technologies. Insecure containers will be X-rayed and checked for radiation." DHS has decided to use public-key infrastructure (PKI) to help deal with the chaos and risk of integrating encrypted and non-encrypted data resulting from the multiple sources of customs information emanating from this globally reaching extended border security program. As well, smart cards are being deployed by DHS to "provide multiple factor authentication and authorization for department personnel," supporting "a planned single sign-on system that will give a single view of data from multiple applications," enabling "agents in the field [to] access criminal, investigation, visa, tax and other point-of-entry decision support tools from remote systems via encrypted wireless links."

New Funding for Port Security

New port security programs require new dollars, and Ridge brought his checkbook along with him to Newark on June 12th last year. There, he announced the release of an additional $170 million in port security grants, in addition to an earlier $180 million already committed "covering recent infrastructure security measures, training, exercises, information sharing and other protective measures." [5] So the total funding for port security grants will total $350 million. "Evaluated and selected by the Transportation Security Administration, the Coast Guard and the Department of Transportation's Maritime Administration," Ridge said, "this latest round of funding has been

awarded to 198 state and local governments as well as private companies... to help improve greater dockside and perimeter protections." Ridge explained that these security dollars "will translate into upgrades such as patrol boats in the harbor, communications tools for better intelligence gathering and coordination, surveillance equipment at roads and bridges, the construction of new command and control facilities and much, much more."

Ridge explained that these new port security measures "are about building on our capabilities—strengthening a vitally important system with additional layers of defense: information sharing, inspections, presence, technology, funding and, of course, vigilance at every turn, at every port, every day."

Wake-up to a Nightmare

9/11 was both a wake-up call to America to be more vigilant along its borders, as well as the sober realization that one of the country's worst nightmares could—and indeed had—come true. In October 2000, former U.S. National Security Advisory Anthony Lake published a book called *Six Nightmares: Real Threats in a Dangerous World and How America Can Meet Them*.[6] In his book, Lake presciently examined half a dozen different nightmare scenarios for American security including a biological WMD attack—and in less than a year, 9/11 took place, proving that nightmares of the sort envisioned by Lake are not science fiction, but sadly a reflection of the new risks and dangers that we face in this increasingly globalizing, interconnected world. As Lake wrote, "We have crossed the threshold to the era of high-tech terror, including the use of weapons of mass destruction." There's no looking back, just ahead to the challenges of this new and dangerous world.

In the months and years since 9/11, America has been working in overdrive trying to solve its newly identified border security challenges. But securing the United States' air, land, and sea borders "is a difficult yet critical task," as Asa Hutchinson explained to Congress when briefing lawmakers on a series of initiatives launched by DHS during the past six months.[7]

Just how difficult? The United States has 5,525 miles of border with Canada—including its winding, mountainous border zone along the Alaska frontier with Canada's Yukon Territory and province of British Columbia, and 1,989 miles with Mexico. But its maritime border is nearly fifteen times longer than its land borders, with 95,000 miles of shoreline, and a 3.4-million square mile exclusive economic zone. And, each year, more than 500 million people cross the borders into the United States, some 330 million of whom are non-citizens, through 317 different ports of entry.

Hutchinson explained the Border and Transportation Security (BTS) Directorate, in partnership with the Coast Guard "watches over our nation's borders and transportation systems," and is responsible for "safeguarding U.S. borders, ports of entry, and transportation systems; facilitating the flow of legitimate commerce; and enforcing U.S. immigration laws." To thwart any attempts to smuggle WMD or other contraband into the United States through U.S. sea ports, Hutchinson said "the Container Security Initiative has established tough new procedures targeting high-risk cargo containers before they embark en-route to U.S. ports," and so far 25 ports, including three in Canada, "through which approximately two-thirds of cargo containers coming to the U.S. will pass—have agreed to participate in the program."

As Hutchinson testified, "Because of the efforts of the dedicated employees of the Border and Transportation Security Directorate—undertaken in partnership with the American people, our federal, state, local, private and international counterparts, and our other colleagues within the Department of Homeland Security—America is becoming safer and more secure every day."

Security Through Multilateralism: U.S. Port & Maritime Border Security After 9/11

The twin terror attacks of 9/11 were a direct assault on our world open borders, free trade, and the expanding zone of global economic integration. Ever since, as the U.S. has sought to tighten up its border security, it has been pulled in two distinct and—on the surface—paradoxically irreconcilable directions: at once withdrawing inward, behind new layers of security protection, surveillance and detection; while at the same time marching outward, into the world and all its dangers, to prevent and pre-empt terror at is very source.

With such long and porous borders, America quickly realized in the aftermath of 9/11 that simply erecting electronic barriers and enhancing its perimeter defenses with the latest generation of biometric sensors, motion detectors and IR scanners, along with biological, chemical, and nuclear detection devices and the like, would still leave the nation vulnerable to a variety of external threats. And by virtue of its continental scale, vast and dispersed infrastructure, long and porous borders, and economic dependence on the free movement of trade goods through its seaports, land border crossings and airports, America remains frustratingly vulnerable to future mass terror attacks, presenting any would-be terrorist with a long list of potential soft targets that are virtually impossible to secure. While that instinct to pull inward and withdraw from the world, like a tortoise under threat which retreats within his shell, is an understandable, indeed a naturally instinctive reaction to the threat of terror, such a withdrawal cannot succeed in securing the American heartland.

At the same time, America has sought to reach outward, into the world, addressing the very source of its security challenges overseas. In so doing, it has effectively improvised its way back toward the very multilateralism critics of American foreign policy say America has abandoned. Granted, America's "coalition of the willing" to oust Saddam, and its earlier enunciated concept of "shifting coalitions" as envisioned by the strategic planners in the Bush Administration to prosecute the war on terror, is a far cry from multilateralism as it is conventionally understood (such as NATO-wide, UN-blessed "multilateral actions" not seen since the air war over Kosovo), the seeds of a truly multilateral response have now been planted by an Administration long-criticized for forsaking multilateralism in favor of unilateral action. Indeed, a look at the evolution of America's maritime and port security efforts since 9/11 shows that America's practical efforts to solve the riddle of post 9/11 border security has compelled it to reach out across the oceans that no longer insulate it from nefarious terror, and address its border security challenges multilaterally through greater security cooperation with its trading partners.

A Layered Approach

According to an overview of Department of Homeland Security's (DHS) port security strategy, "with 95 percent of our nation's international cargo carried by ship, port security is critical to ensuring our nation's homeland and economic security."[8] To successfully shield maritime borders and ports, "DHS is implementing an integrated and collaborative process among international, federal, state, local and private partners to protect our ports and maritime infrastructure by gaining the greatest intelligence about the people, cargo, and vessels operating in our waters and ports." DHS recognizes that protecting America's ports and maritime borders "demands a comprehensive layered defense approach incorporating regulations, inspections, information sharing, vigilance, technology, and presence." Such a "layered" approach extends beyond America's domestic efforts to enhance port and maritime border security to include bolstering security in transit as well as offshore, the latter requiring multilateral cooperation to succeed.

Indeed, on June 21, 2004, Homeland Security Secretary Tom Ridge announced that as part of his department's "Secure Seas, Open Ports" initiative, America would "build upon the layers of security that already in place at the nation's ports" and to "add additional security protections," as "the oceans and ports of the world are vital to the economic livelihood of the U.S. and countries throughout the world."[9] A layered approach to security thus enables DHS to "ensure there are protective measures in place from one end of a sea based journey to the other," and "to protect

the three phases of the journey: overseas, in transit, and on U.S. shores." DHS thus commits to a "joint effort," since "securing our ports and waterways is a team effort," and "everyone, from local governments and private citizens to the international community plays an important role in ensuring that our waterways remain open for business." Further, DHS notes "the U.S. government does not have the resources to secure the ports and waterways alone," and as consequence, "DHS must coordinate its efforts with the nation's trading partners" and at the same time "enlist the expertise of maritime industry and local government agencies, and use the eyes and ears of our citizens, to notice when something is amiss." DHS says the goal is thus "to find the appropriate balance between security and freedom, between inspecting every container and keeping trade moving.'

Multilateralism In Action

The "overseas" layers involve several components, including the Container Security Initiative, the International Ship and Port Facility Security Code, the International Port Security Program, the Customs-Trade Partnership Against Terrorism, the 24-Hour Advanced Manifest Rule, and Operation Safe Commerce:

Container Security Initiative (CSI)

The CSI or Container Security Initiative "incorporates side-by-side teamwork with foreign port authorities" and is "designed to identify, target, and search high-risk cargo." Under CIS, the "screening of containers that pose a risk for terrorism is accomplished by teams of U.S. Customs and Border Protection's (CBP) officials deployed to work in concert with their host nation counterparts," and "potential suspect containers are targeted and identified before being loaded onto vessels."

So far, "nineteen of the top twenty ports have agreed to join CSI and are at various stages of implementation." These include LeHavre, Bremerhaven, Hamburg, Antwerp, Singapore, Yokohama, Tokyo, Hong Kong, Goetborg, Felixstowe, Genoa, La Spezia, Busan, Durban, Vancouver, Montreal, Halifax, and Port Klang—which, combined, account for over two thirds of the containers heading toward the U.S. The next phase of CSI will reach further, enabling DHS "to extend port security protection from 68 percent of container traffic to more than 80 percent - casting the safety net of CSI far and wide," and expanding CSI to include "strategic locations beyond the initial 20 major ports to include areas of the Middle East such as Dubai as well as Turkey and Malaysia."

According to the U.S. Coast Guard, under CSI, CBP has stationed officers in these "major foreign ports, and is working side-by-side with foreign customs authorities to identify and target cargo containers that could present a potential risk for terrorism," and "foreign customs authorities then inspect those containers for possible terrorist weapons before the containers are placed on ships bound for the United States," with CBP officers observing these inspections. "The International Port Security Program will focus on improving the security of the vessels and port facilities that transport, stow, and handle cargo and people, including CSI containers."

International Ship and Port Facility Security Code

The International Ship and Port Facility Security Code is described by DHS to be "the first multilateral ship and port security standard ever created," and thus help "prevent maritime related attacks by making ports around the world more aware of unusual or suspicious activity." It took effect on July 1st, requiring "vessels and port facilities to conduct security assessments, develop security plans, and hire security officers."

International Port Security Program (IPSP)

Under the International Port Security Program, the U.S. Coast Guard and host nations "work jointly to evaluate the countries' overall compliance with the IPSP code," allowing the Coast Guard to "use the information gained from these visits to improves the U.S.' own security practices, and determine if additional security precautions will be required for vessels arriving in the United States from other countries." The U.S. Coast Guard announced the establishment of an International Port Security Program on April 15th to "help the United States and its maritime trading partners better protect the global shipping industry by facilitating the implementation of security improvements in ports around the world," with implementation slated to begin this summer and fall.

It objective is "to engage in bilateral or multilateral discussions with trading nations around the world to exchange information and share best practices to align port security programs through implementation of the ISPS Code and other international maritime security standards," and to promote "information exchange and collaboration with trading nations regarding implementation of established international maritime security standards," the "assignment of International Port Security Program Liaison Officers in three regions (Asia-Pacific, Europe/Africa/Middle East, and Central/South America) for world-wide coverage in order to assist other nations and facilitate the bilateral exchanges," and the "establishment of a Port Security Specialist Team based in Washington, DC, to conduct country/port visits to review and discuss security measures implemented and share 'best practices.'" The Coast Guard pledges to "work bilaterally or multilaterally with countries to schedule visits" and "will work with countries to identify protective measures to help facilitate their compliance with the ISPS Code." The Coast Guard is also "establishing a Port Security Training Program that will incorporate the Inter-American Port Security Training Program (IAPSTP) currently being offered to the Organization of American State member nations."

At the time, Admiral Thomas H. Collins, the commandant of the U.S. Coast Guard, explained that “Shipping is a global industry and the economy of nearly every nation relies on overseas trade," and "by helping other nations evaluate security measures in their ports, we can help to ensure the safety and security of the global maritime transportation system.” As part of its effort, "the Coast Guard and the host nations will work jointly to evaluate the countries’ overall compliance with the International Ship and Port Facility Security Code, an international agreement signed in December 2002" and which came "into full force on July 1." As well, "the Coast Guard will provide assistance with interpretation of the international code, as it has already done through discussions with representatives from over 50 nations."

The Coast Guard plans to work "very closely with Customs and Border Protection to ensure that this program, the Container Security Initiative and other programs are developed and executed in harmony." The International Port Security Program includes a traveling team that will visit approximately 45 countries each year, and International Port Security Liaison Officers that will be stationed around the world to share information on best practices and to provide assistance to the traveling team to "meet with appropriate national authorities to discuss the nation’s maritime security regime and its interpretation and implementation of the international code," "jointly visit representative ports within the country to view implementation," "jointly verify with the host nation the effectiveness of the country’s approval process for port facility and vessel security assessments and plans required under the international code," "provide technical assistance as necessary to assist countries with compliance," and "share information about best practices, both from within the country and around the world."

The Coast Guard says those "vessels that make port calls at countries that are not participants or that are not in compliance with the requirements of the international code could be delayed when attempting to enter a U.S. port as a result of additional enforcement actions," and "enforcement actions could include" such steps as "boarding the vessel at sea prior to entry into port," "controlling the vessel’s movement with armed escorts," "conducting a comprehensive security inspection at the dock or at sea," and "denying entry into U.S. waters." Such measures "will

remain in place until the country demonstrates compliance." As part of its multilateral approach to implementing IPSP, "the Coast Guard invites officials from other nations for reciprocal visits to the United States and select ports to observe the Coast Guard's procedures for implementing the international code." This program is part of efforts within the Department of Homeland Security to develop and enhance international partnerships in order to create a more secure global shipping community, including U.S. Customs and Border Protection's (CBP) Container Security Initiative (CSI).

The 24-Hour Advanced Manifest Rule

The 24-Hour Advanced Manifest Rule, which requires that "all sea carriers with the exception of bulk carriers and approved break bulk carriers" to "provide proper cargo descriptions and valid consignee addresses 24 hours before cargo is loaded at the foreign port" via the "Sea Automated Manifest System." Administered by DHS' Customers & Border Protection (CBP), the 24-Hour Advanced Manifest Rule provides DHS with "greater awareness of what is being loaded onto ships" heading our way.

Customs-Trade Partnership Against Terrorism (C-TPAT)

As well, the Customs-Trade Partnership Against Terrorism (C-TPAT) program ensures that the "thousands of importers, carriers, brokers, forwarders, ports and terminals, and foreign manufacturers have taken the necessary steps to secure their supply chains" and by "providing verifiable security information," enable DHS " to devote more resources to high-risk shipments."

Operation Safe Commerce (OSC)

And lastly, Operation Safe Commerce is a pilot program that "analyzes security in the commercial supply chain and tests solutions to close security gaps," in an effort to identify technologies that "enhance maritime cargo security, protect the global supply chain, and facilitate the flow of commerce."

These overseas initiatives are bound by a common theme: multilateralism. In order to succeed, these efforts require the participation of America's trading partners around the world, and thus can enhance the many new "in transit" activities such as the Smart Box Initiative, the Ship Security Alert System, Automated Targeting System, and 96-Hour Advance Notice Of Arrival, as well as the even more plentiful "onshore" port and maritime border security programs implemented since 9/11, such as the High Interest Vessels Boarding, Operation Port Shield, Automatic Identification System, Port Security Assessment Program, Guarding In-Between the Ports, Operation Drydock, and Americas Waterways Watch; the establishment of a National Targeting Center, Maritime Intelligence Fusion Centers, Area Maritime Security Committees, and Maritime Safety and Security Teams; and the use of Port Security Grants, Non-Intrusive Inspection Technology, and Transportation Workers Identity Cards to enhance the security of our ports and maritime borders.

The Long Journey Toward Secure Port & Maritime Borders

America has been considering the challenges of maritime border and port security since long before 9/11. Indeed, in his July 24, 2001 speech presented before the Senate Committee on Commerce, Science and Transportation on port and maritime security, less than two months before 9/11, Acting Deputy Maritime Administrator Bruce J. Carlton presented the findings of an August 2000 report of the Interagency Commission on Crime and Security in U.S. Seaports, whose "objective was to undertake a comprehensive review of seaport crime, the state of seaport security and the ways in which Government is responding to the problem," and which "identified

threats to seaports and makes recommendations intended to reduce the vulnerability of maritime commerce, national security and the infrastructure that supports them."[10]

In his speech, titled "The Need for Heightened Port Security," Carlton observed that "terrorism is also a concern for seaport security," and that "the threat of such activity and the vulnerability of seaports are the reasons for concern." Noting "U.S. airports and land border crossings have well structured security measures," he explained "our ports do not enjoy the same level of security even though they offer unparalleled intermodal access to our nation's interior." As a result, "addressing port vulnerabilities is key to ensuring that our ports are not targeted for terrorist and criminal activities."

Carlton explained that "MARAD engages in outreach to foreign countries and their port authorities to enhance the efficiencies of global commerce, which in turn benefit our own maritime industry," and recalled MARAD's history serving "as Chair and Secretariat of the Technical Advisory Group (TAG) on Port Security of the Organization of American States (OAS) Inter-American Committee on Ports"—which seeks to "develop solutions and coordinate multilateral approaches to improving port security in the Western Hemisphere" by developing "a hemispheric approach to improving the security of the Inter-American maritime trade corridors," developing "a common port security strategy," devising "basic guidelines and minimum standards of security for ports of member countries of the OAS," and organizing and conducting "annual courses planned under the Inter-American Port Security Training Program, managed by MARAD."

Inter-American Collaboration

Carlton recalled how MARAD "has had an on-going port security program with the Organization of American States (OAS) since the 1980s, including port security outreach," and notes that "since 1995, MARAD has been conducting port security training courses in the Western Hemisphere," and during this period, "over 300 commercial port authority police and security personnel from the 34 member countries of the OAS have been trained." So long before 9/11, America was well aware that "by its very nature, trade is an international business in which U.S. companies rely upon the security and efficiencies of foreign ports." The OAS website recalls that OAS "involvement with port related issues began in the 1950's through what was then known as the Inter-American Port Conference," and "at the time, the Member Countries visualized the creation of an Inter-American organism specialized in port area concerns" to "deal with port sector development issues, analyze the obstacles to such development, and propose possible solutions. At the same time, such an organization would reinforce hemispheric port cooperation." The Inter-American Port Conference was renamed the Inter-American Committee on Ports in 1996.

Continued evidence of America's traditional use of a multilateral approach to port and maritime border security can be found in the post 9/11 era. For instance, consider the approval this past winter of the Strategic Framework for Inter-American Port Security Cooperation by the Organization of American States (OAS) at the Western Hemispheric Port Security Conference, held on February 25-27, 2004.[11] 29 official delegations from the OAS member states attended, for a total of over 400 participants, including high-level port authority reps, security officials from OAS member States, and a variety of experts and executives from companies and NGOs active in the maritime port sector. As an OAS bulletin announced, "Considering that port security is a crucial component in the economic viability of the Americas maritime transportation system and international competitiveness, and that more than four-fifths of the region's trade is carried through these ports, the delegations of the OAS member States to this conference approved a 'Strategic Framework for Inter-American Port Security Cooperation,'" to "help member States in their efforts to combat terrorism and other threats, such as illicit trafficking of drugs, arms, and people, and other forms of organized crime, as well as other offenses affecting the cargo security and maritime traffic."[12]

The framework was developed by the Inter-American Committee on Ports of the OAS to foster an "interdependent network relationship among trade partner ports and associate countries, as well as adherence to a common international standard of security, to protect the flow of international trade and transshipment cargoes, as well as passenger transportation." The framework serves to "guide OAS Member States in developing the institutional readiness and technical capacity to implement necessary port security improvements foster the necessary." It recognizes that "those ports with substandard protective security measures are 'weak links' in the trade network and represent a vulnerability to the international marine transportation system." It aims to "improve and expand the multilateral mechanisms and work with other governments to implement a hemispheric port security framework," and to "strengthen cooperation" among OAS member states in order to "facilitate the flow of hemispheric maritime commerce unimpeded by the direct or indirect consequences of terrorism and transnational criminal activity in any of its variations."

The framework recognizes that "higher security standards" will "necessarily involve a fostering of stronger hemispheric cooperation so that the higher costs involved—improvement of physical and administrative infrastructures, equipment, training and improvement of capabilities, etc.—can be met by all the States as a means to guarantee the homogeneous implementation of new port security standards." It advises member states to "examine existing bilateral and multilateral initiatives that have compatible purposes and structures, and evaluate how they may be used to foster this process." By increasing "the priority and resources devoted to enhancing and maintaining port security in the hemisphere and trade partner seaports," the framework aims to "achieve greater effectiveness and synergy by improving internal and external coordination of national and regional agencies that deal with seaport security and the threats posed by terrorist and organized crime groups, and other malevolent non-state actors."

The Multilateral Imperative

Only by continuing to recognize this international dimension, and working multilaterally with our trading partners the world over, can our ports and maritime borders be protected, and thus prevent a "weak link" from unraveling the efficacy of our multi-layered, and multilateral, approach to port and maritime border security.

Enhanced Border Surveillance for the post 9/11 World

Since 9/11 shook the foundations of the western world—and introduced us to the specter of WMD-terrorism by non-state actors—nation-states have been compelled to enhance their border surveillance with a mix of new and conventional surveillance technologies, enabling them to see further and clearer than ever before. Indeed, there is an emerging doctrine of digital warfare at the U.S. Department of Defense (DoD), which has evolved from Defense Secretary Donald H. Rumsfeld's commitment to the “Transformation” of the U.S. military into a leaner, more technology-driven fighting force—where IT replaces muscle.

A central part of this emerging doctrine is the increased role of surveillance technologies, as tools developed to secure borders leapfrog to the battlefield, transforming the way wars are fought.

Looking beyond one’s borders is an ancient strategic imperative—traditionally achieved through sentry towers, perimeter fences, and reconnaissance patrols of frontier regions. With the advent of long-range electro-optical imaging systems, and aerial and space-based surveillance platforms during and after World War II, border surveillance profoundly extended its reach. During the long cold war, America’s primary strategic threat came from “over the top,” across the vast icy polar sea where Soviet bomber forces, and later land- and sea-based ICBMs, posed a potent threat to the American heartland. The primary means of early warning and detection came from high-altitude aerial surveillance platforms, orbiting space-based surveillance platforms, and a string of ground-based radar sites along the periphery of the Soviet Union, as well as along North

America's northern coast—where the Distant Early Warning Line (DEW Line), a NORAD operated, continental over-the-horizon radar system, passively scanned the skies to provide early detection of a strategic bomber or missile attack.

Each DEW Line site was staffed during the long Cold War years by teams of isolated radar operators, who dutifully monitored their displays 24/7, in an effort to reduce the probability—and frequency—of false alarms and thus prevent an erroneous counter-strike. Though the DEW Line was modernized in the early 1990s, and renamed the North Warning System during the North American Air Defense Modernization (NAADM) program, and is now fully automated and centrally controlled, the primary post 9/11 threat to American security is no longer from strategic bombers or ballistic missiles. (But in the coming years, as North Korea expands the reach of its ballistic missiles and China modernizes its nuclear forces, an external BMD threat may once again resurface as North America's greatest threat.)

Today, the salient threat is from smaller, isolated attacks by terrorist groups and rogue states wielding unconventional weapons such as "dirty" radiological bombs, chemical and biological weapons, and "improvised WMD" such as the commandeered commercial jumbo jets used on 9/11. To provide as much early warning and detection as possible, America is literally looking both "high and low," deploying ground- and sea-based surveillance systems as well as aerial and space-based systems that include both the popular unmanned aerial vehicles (UAVs) as well as orbiting satellite reconnaissance systems.

On these platforms—all the way from the ground up to the skies above—can be found all manner of sensors, capable of providing a wide variety of imaging solutions, each telling us a little more about the external threat environment and—hopefully—providing a more complete and accurate picture of the world beyond our borders. Izhar Dekel, President of Israel's Magal Security Systems Limited, explained that his company's goal is "to provide a total solution—including sensors, software, hardware, and a control unit" to ensure complete perimeter security.[13] And as Eli Yitzhaki, Vice President of Business Development for UAV, Security and Tactical Systems, at Haifa, Israel-based Elbit Systems Ltd., "At the end of the day, you want to make sure the security of a country or site or event has enough layers to protect it."[14]

Short & Medium Range Surveillance Platforms

A standard border security system may include several platforms, providing short-range, medium-range and long-range surveillance. Among the short- and medium-range platforms are:

- *Perimeter fences*—deploy a variety electronic surveillance technologies for intrusion detection and warning. Being ground-based, the strengths of these ground-based systems are primarily short-range, up to around 500 meters.
- *Observation towers*—extend surveillance many tends of kilometers further from a border installation, provide a platform for ground-based medium-range surveillance.
- *Mobile surface observation platforms*—including land vehicles as well as maritime vessels, these surveillance platforms patrol frontier regions and coastal waters, extending the reach of medium-range surveillance sensors through their mobility.
- *Observation aerostats*—these stationary platforms, generally tethered balloons, allow for extended observation over wider areas, extending the reach of surveillance sensors beyond what can be seen from an observation tower.

Dekel said that short-range surveillance and perimeter detection systems are deployed to protect borders as well as sensitive infrastructure installations—Magal has developed systems to secure fiber-optic network junctions in India, and airports, defense and government installations in five countries around the world.

Short- and medium-range platforms integrate a wide variety of sensors - including such systems as taut-wire perimeter detection, vibration intrusion detection, electromagnetic intrusion detection, electrostatic field disturbance, electro-optical observation, and even microwave field disturbance detectors. As well, for high-resolution imaging, motion detection, temperature-differentiation and night-vision, there are a variety of electro-optical (EO) imaging sensors available including optical video detection systems, using arrays of commercially available CCTV cameras well-suited for daytime surveillance; infrared video (IR) detection systems, that can measure changes in thermal energy and provide night-surveillance; and laser illumination systems that can illuminate targets, and enable higher-resolution imaging when combined with other EO sensors. Additional optical components include computer-operated pan/tilt/zoom cameras, visible or near-infrared illuminators for night vision with conventional cameras; and image-intensifiers for long-range night vision with conventional cameras.

Laser illuminated viewing and ranging can enhance long-range surveillance over wide-perimeter areas, and can identify threats over ten miles away. Unlike radar, laser-illumination does not use microwaves, so the reflected signal is easily displayed as a digital video image. Kevin Fairbairn, CEO of Intevac Inc., a developer of laser-illumination surveillance systems, said this technology will enable next-generation surveillance systems to generate real-time, high-resolution imagery for threat identification at much longer ranges than currently possible.

Haim Rousso, a co-managing director of Rehovot, Israel-based El-Op Electro-Optics Industries Ltd., explained that layers of the above-mentioned surveillance platforms can be integrated to enhance border security.[15] He said that surveillance sensors are deployed on ground systems, attached to towers and fences; on ground vehicles and on ships; on stationary aerostats and on automated unmanned aerial vehicles (UAVs)—also known as RPVs or remotely piloted vehicles, which can provide pervasive surveillance of wide areas, and on satellites.

Range v. Resolution

Rousso added that as you go from short-range, ground-based surveillance platforms to aerial and space-based platforms, you face a trade-off with optical scanning sensors. “The trade-off is that long-range usually means lower resolution, and higher resolution usually means shorter-range.”As well, different sensor technologies bring additional trade-offs. For instance, Rousso pointed out that “With electro-optical products you have some limitations of atmospheric conditions, which can’t penetrate very dense smoke or clouds or all that, but in most cases it is still a very reliable solution,” providing high-resolution images in comparison to radar and thermal imaging solutions. However, “Infrared imaging can give you two advantages: night vision—which is needed in most cases IR is used; as well, its thermal characteristics allow you to measure temperature variation as well as to do night-surveillance. It is a good solution if you want for example, to detect people—even if camouflaged and hiding behind various obstacles. They are easy to detect using temperature effects. That is why IR systems are so popular for border surveillance.”

Rousso explained that “a combination of lasers with other imaging systems” can provide “an excellent solution if you want very high resolution images and identification of your target. The combination of laser and other imaging systems gives you many advantages. You illuminate a target with the laser, and see with the CCD camera, and can get a very good sensitivity and a very good resolution, quite a unique solution.”

Long-Range Border Surveillance

Enhancing the above-mentioned short- and medium-ranged observation platforms, there are several long-range platforms briefly mentioned above that operate from the skies above.

Pervasive Aerial Surveillance Platforms, using unmanned aerial vehicles (UAVs), can provide long-range “pervasive surveillance,” essentially “hovering” over a wide-area for an extended period. A well-known UAV is the Predator drone, which became popular during last year’s war in Afghanistan and in the ongoing war on terror. UAVs can taxi, take off and fly autonomously, and can change navigation plans during flight—all whiling sending a stream of observation data to a distant control center.

High-Altitude Mobile Observation Platforms provide long-range mobile surveillance from the sky above—on planes, helicopters, and satellites. Their high-altitude —enables wide-area surveillance.

These long-range platforms employ a similar mix of EO sensors enabling optical and thermal imaging, as well as radarenabling all-weather surveillance, as seen during the sandstorms in the opening days of Operation Iraqi Freedom when satellite and aerial surveillance platforms allowed for all-weather targeting of Iraqi positions.

Just as low-flying UAVs providing pervasive surveillance can provide greater resolution than a higher-altitude surveillance aircraft, low-orbiting satellite platforms can observe an area only during their transit time overheadand higher-altitude geostationary satellites, which over a hovering surveillance platform in high-earth orbit, have reduced imaging resolution. The tradeoff is thus between observation range, and the resolution of the surveillance image. As Rousso explained, “the narrower the angle, the longer the range.” With a high altitude platform, maximizing observational detail requires narrowing the angle of view. “If you’re seeking to get a 60 degree field-of-view, it is very difficult to get a long range. If you have a small angle, just one or two degrees, you can get better ranges.”

Higher resolution images are harder to get with long-range surveillance. Rousso observed, “If you go to space, you have a larger lens, a larger telescope” than you can deploy on a UAV, for instance, “but you can still not see small detail, maybe a resolution of one meter but not better than that. You can see a car from space but it is very, very difficult to see a person from space, even with high resolution satellites today. But if you take a sensor on a tower—and you look 20 km, 40 km, 50 km you can still see people walking, even objects which are smaller than that!” Similarly, Rousso explained, “You get advantages if you are on airplane—you can cover very large areas in a very short time. But if you put it on a car, you get better performance—but then to cover 100 kilometers takes you more time, unless you use many vehicles, scanning or controlling along the line—it's always a tradeoff, of course—it is also a trade off, as in life.”

Space Based Radar (SBR)

In development for the next generation of satellite surveillance is the Space Based Radar (SBR) system. *Federal Computer Week's* Dan Caterinicchia, in *Federal Computer Week* (“Space-Based Radar vendors picked,' March 19, 2003), reported that the US Air Force has selected three vendors to develop and demonstrate a prototype radar payload for the Space-Based Radar (SBR) system to enable the U.S. military to conduct surveillance and reconnaissance missions in dangerous areas at any time, and to further bridge the gap between the defense and intelligence communities.[16] Harris Corp., Northrop Grumman Corp. and Raytheon Co. were each awarded three-year contracts February 21, 2003 for the SBR system. The SBR concept includes on-board processing technology and a large electronically scanned array that will enable each spacecraft to collect and process large amounts of data and imagery in near real-time, Caterinicchia reported. Personnel on the ground then will use the data for tracking mobile targets.

Platform Stabilization

As you climb up what can be thought of as a “platform ladder” from the ground to the sky, a new challenge emerges: that of stabilizing the platform. As Rousso put it, “On most of these platforms you need stabilization technology. You have to stabilize your sensors if you want to get high resolution images. You can’t just put a camera on a ship or airplane or RPV—you have to have very high stabilization, otherwise you lose detail.” On a sentry tower or perimeter fence, “You don’t feel any change or movement, any vibration,” Rousso said. But it gets harder as you increase your mobility as well as your altitude “You can have an excellent camera, but if you vibrate or move it you lose all sorts of information - that is very crucial!” Using gyros and proprietary control technologies, vendors provide stabilization systems that can extend border surveillance from the earth to the sky—and make it possible to gather usable imaging from ocean vessels, helicopters, aircraft and orbiting satellites.

Integration

All of the above-mentioned surveillance platforms can be integrated into a multi-tier surveillance system. To tie all of the data together, the system requires some form of processing, through a security management or a command & control system which can process data streaming in from the array of sensors. Smaller security systems can make do with a desktop security management system—composed of software loaded onto a PC connected to a communication board, but a larger system will require a bona fide control center that monitors, analyzes and responds to the signals relayed to it from the sensors across a wide-area network, using signal analysis algorithms to process and assess the data on a central server—graphically presenting that data on display screens. As Rousso said: “To protect an area—a border, or a site—there’s not just a need to have sensors, you need to have systems—you need to see how you connect all your different sensors.” It’s “not just a connection of this sensor and that sensor, there is still a system level design needed to complete the task.”

Image Processing

The stream of data coming in from surveillance sensors can be hard to interpret. One solution is to use image processing, which Rousso said is “a very useful tool to improve capabilities of varying imaging systems,” and “and in a way that is very fast.” Additionally, image processing can aggregate images gathered from multiple sensors and generate a panoramic, 360 degree image.

A newer technology now emerging is called hyper-spectral imaging (or multi-spectral imaging) which scans and analyzes the spectral signature for different color characteristics. “There are objects that have a characteristic color signature,” Rousso explained, “and if you just look at them when they are part of all the spectra, you will not be able to detect them. But if you just look at that color, it will be very significant.” Rousso added, “This is a very, very powerful tool,” and predicted that “this is going to be very useful in the future, especially from airborne platforms.”

Data Management

To manage all the sensor data, Rousso said there are two approaches that are common: data fusion, and sensor fusion. Data fusion “takes data from radar, acoustic, thermal, and EO imaging” to a “central management software system” which analyzes the data and presents it so “you make your decision.” For instance, this enables you to “fuse radar and EO images—with EO you get a good image of the scenario, with radar you get a bad image but you get excellent information about movement, about changes—so if you put them together, you get a nice image with an emphasis on the things that are changing.”

There is also “sensor fusion,” which enables you to “take the data and fuse them together and compare the images to see the advantages of each of them.” By merging the data from different sensors, you get “get the benefits of IR and other sensors on the same image, and you get better

performance." In most ground stations, you find different displays for the various sensors, Rousso said. "One for visible, one for IR, one for radar," which can be "difficult to watch." But "once you put it on the same display, you get a lot of advantages."

Automated v. Manned Surveillance Systems

Today, there are both manned and automated surveillance systems, but manned systems are much more common and continue to be popular. Manned systems do provide some benefits, particularly when it comes to reducing false alarms, just as they have done since the 1950s on the DEW Line—but manned systems require a recurring human resource cost for the ongoing surveillance effort, and during times of war place the operators in harm's way. However, Rousso said improvements are being made in automated systems, adding that, "No doubt the trend is to be more and more autonomous," leading to further improvements in "your probability of detection and increasing your false alarm probability."

Surveillance Beyond Borders

Historically, border surveillance was conducted from frontier observation posts—sentry towers, perimeter fences, stationary aerostats tethered behind a border installation. But with advancing technology, border surveillance began to climb up the "platform ladder"—from the ground all the way up to the sky above, with each higher rung on that ladder providing wider and more pervasive surveillance.

After 9/11, the ongoing war on terror and the newly articulated military doctrine of strategic pre-emption asserted a pro-active need for "extended surveillance" utilizing advanced technologies on all available platforms, both domestically and globally. Deploying new sensors along an increasingly fortified border is just the beginning. Operation Iraqi Freedom, waged by America to pre-empt—and in theory, reduce future threats of—WMD proliferation, has also contributed to the battlefield "mobilization" of traditional border surveillance technologies, extending them well beyond the frontier. As a result, border surveillance is becoming more active and less passive; more pro-active and less reactive; more tactically offensive than defensive.

This transformation in border surveillance has blurred the traditional boundary between frontier surveillance and battlefield reconnaissance, and the post 9/11 strategic environment is very much a world where the battlefield is everywhere, and the frontline and the homeland are both primary fronts in the war on terror. Indeed, after the Twin Towers fell on 9/11, NATO deployed AWAC radar aircraft to patrol America's skies after it became painfully obvious that America's border surveillance systems were inadequate to provide dynamic, continental early warning in a multi-threat, wartime environment. Consequently, we are witnessing a rapid integration of border surveillance and battlefield reconnaissance technologies with repercussions that will echo long after Operation Iraqi Freedom.

UAVs and Pervasive Surveillance

During the early battles of Operation Enduring Freedom last year, surveillance tools and weapons of war began to merge as surveillance technologies—designed to bring a measure of quiet and early-warning to the frontier—developed teeth, turning state of the art observation platforms into lethal weapons.

Witness the UAV—which began life decades ago as a remotely piloted vehicle (RPV) designed to carry imaging sensors over a border region for wide-area, long-range surveillance. Considered by some to be little more than a toy plane, the UAV's military significance as an offensive weapons-platform did not emerge until Operation Enduring Freedom in Afghanistan. Predators armed with Hellfire missiles were first used by the CIA in Afghanistan, where they were credited with

airstrikes against senior al-Qaida members including Mohammed Atef, the terror network's military chief. A Predator strike in Yemen in November 2002 killed another top al-Qaida operative, and the military used Predators frequently to patrol the no-fly zone over southern Iraq before the current war, and continue to provide “persistent surveillance” over Iraq. Already, in the opening days of Operation Iraqi Freedom, a Predator has been used to destroy an Iraqi anti-aircraft gun outside of Amarah on the Tigris River. The Global Hawk is another unmanned aerial vehicle (UAV) that is providing high resolution intelligence and surveillance imagery to the Air Force and joint battlefield commanders. And the US Navy uses the Neptune Maritime Unmanned Aerial Vehicle (MUAV), which can be launched either from small surface vessels or from land, and was designed for use where developed runways are unavailable, and can be recovered on land or on water.

Yitzhaki explained that UAVs can provide surveillance over “a larger area and can give a solution day or night, with high resolution—and if you need to go lower, because of clouds or angles, they can do so instantly.” In Israel, he said, “We fly over UAVs here all the time,” particularly if there is a need to confirm an intelligence report or respond to an alarm along a border outpost, or to provide wider-area surveillance before sending forces into harm’s way “to make sure there is not somebody waiting for them. This is the perfect and the most cost effective solution I know.”

Another component in America’s military aerial surveillance system is the E-8C Joint Surveillance Target Attack Radar System, known as Joint STARS, a military version of a Boeing 707 jet that has been modified with the latest radar and imaging sensors suspended in a giant pod beneath the aircraft that can direct airstrikes against enemy targets, and provide battlefield reconnaissance of a much wider area, and from a higher altitude, than the elfin UAV.

Toward Netcentric Warfare

USA Today's Byron Acohido reported on the emergence of “netcentric warfare” since the last Gulf War. Now, the US military has a clearer and more continuous picture of the battlefield than ever before - helping to realize the concept of “netcentric warfare” which has been emerging ever since the 1991 Gulf War, linking sensors, communication devices and weapons systems in a seamless digital network.[17]

Acohido observed that netcentric warfare has been made possible during Operation Iraqi Freedom by the integration of data streamed from sensors on space-based and aerial surveillance platforms with sophisticated signal and image processing at the command and control center in Qatar—integrating imaging data from surveillance satellites, U-2 spy planes and Global Hawk UAVs that detect radar and telephone emissions identifying the locations of enemy anti-aircraft systems, government buildings and military facilities. AWACS aircraft circle 30,000 feet above the battlefield, scanning the sky for enemy aircraft and missiles. Joint STARS scan the ground below for moving vehicles, and Predator UAVs circle the battlefield at 15,000 feet ahead of U.S. troops, ready to aim their video cameras on targets that Joint STARS planes identify. All together, this multi-layered system of aerial surveillance—of manned and unmanned aircraft, as well as space-based satellites—send a stream of data from their sensor pods to the coalition’s command and control center in Qatar, providing command staff a more complete picture of the battlefield than ever before experienced.

Since the opening volleys of Operation Iraqi Freedom, when a decapitation strike by precision munitions and satellite-guided cruise missiles sought to assassinate the senior Iraqi leadership, the role of C4ISR—Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance—has been a critical element of coalition war-fighting.

Meanwhile, back on the home front, a variety of new short-range surveillance technologies are emerging—and many are being quickly deployed along America's borders and ports of entry to bolster the country's homeland security capabilities. Such technologies include:

- *Biometrics Scanners*—including facial identification systems, thumb- and fingerprint scanners, iris scanners and voice identification and authentication systems;
- *Nanocrystals*—Nanocrystals and other chip-based sensors such as those being developed at the University at Albany's Public Protection Technology Application Center, which hosts as NanoTech research center that works with local high-tech companies to develop small chemical, biological and surveillance sensors for enhanced border surveillance, intruder detection, and bio/chem weapons detection.[18]
- *Machine Intelligence & Automated Surveillance*—Engineers at the non-profit, San Antonio, Texas-based Southwest Research Institute are working to integrate real-time image-processing and machine perception with traditional video surveillance methods, to provide faster and more accurate analysis of surveillance from multiple video cameras. Using algorithms that incorporate temporal processing and model-based analysis, their system recognizes normal and abnormal motions and can be deployed for perimeter security as well as for under-vehicle surveillance—such as required at airports and defense facilities.[19]

These solutions are just a few of the emerging technologies designed to bolster our surveillance capabilities, so that we can achieve the goal of extended surveillance and better meet the challenges of the post 9/11 world. Like the Manhattan Project a generation ago, the best and the brightest from academia, the military, and industry are applying their skills and their imagination—in thousands of research labs and technology centers all over the world—to this global effort to extend our surveillance capabilities further than ever before, innovating new sensors, platforms, and management systems.

References

1. Homeland Security Secretary Tom Ridge, *Remarks by Secretary Tom Ridge at the Port of Newark, New Jersey*, (Newark, June 12, 2003).

2. Asa Hutchinson, *Testimony before theHouse Select Committee on Homeland Security*, June 25, 2003.

3. Ed Frauenheim, "Accenture Homeland Security win worth up to $10bn," Silicon.com, June 2, 2004.

4. Mark Willoughby, "IT to provide multifaceted security at U.S. borders," Computer World, June 19, 2003.

5. Ridge, op. cit.

6. Anthony Lake, *Six Nightmares: Real Threats in a Dangerous World and How America Can Meet Them* (NY: Little, Brown and Company, 2000.)

7. Hutchinson, op. cit.

8. Department of Homeland Security, *Protecting America's Ports: Maritime Transportation Security Act of 2002* (Washington, D.C., July 1, 2003).

9. Department of Homeland Security, *Secure Seas, Open Ports: Keeping our waters safe, secure and open for business* (Washington, D.C., June 21, 2004).

10. Bruce J. Carlton, Acting Deputy Maritime Administrator, Department of Transportation, Maritime Administration, *The Need for Heightened Port Security,* Statement to the Committee on Commerce, Science and Transportation, United States Senate on Port and Maritime Security, July 24, 2001.

11. *Strategic Framework for Inter-American Port Security Cooperation by the Organization of American States (OAS)*, as approvied at the Western Hemispheric Port Security Conference, February 25-27, 2004.

12. Inter-America Committee on Ports, *Port Newsletter*, no. 2, May 2004

13. Interview with Izhar Dekel, President, Magal Security Systems Limited.

14. Interview with Eli Yitzhaki, Vice President of Business Development for UAV, Security and Tactical Systems, Elbit Systems Ltd.

15. Interview with Haim Rousso, co-managing director, El-Op Electro-Optics Industries Ltd.

16. Dan Caterinicchia, “Space-Based Radar vendors picked," *Federal Computer Week,* March 19, 2003.

17. Byron Acohido, “Warfare enters the digital age,” *USA Today,* March 23, 2003.

18. For more information, visit the website of Albany Nanotech.

19. For more information, visit the website of Southwest Research Institute.