



Calhoun: The NPS Institutional Archive
DSpace Repository

Faculty and Researchers

Faculty and Researchers Collection

2005-02-01

**An Interagency Approach to U.S. Port
Security; Strategic Insights, v. 6, issue 2
(February 2005)**

Henrikson, Andrew C.

Monterey, California. Naval Postgraduate School

Strategic Insights, v.6, issue 2 (February 2005)

<http://hdl.handle.net/10945/11202>

Downloaded from NPS Archive: Calhoun



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



An Interagency Approach to U.S. Port Security

Strategic Insights, Volume IV, Issue 2 (February 2005)

by [Andrew C. Henrikson](#)

Strategic Insights is a monthly electronic journal produced by the [Center for Contemporary Conflict](#) at the [Naval Postgraduate School](#) in Monterey, California. The views expressed here are those of the author(s) and do not necessarily represent the views of NPS, the Department of Defense, or the U.S. Government.

For a PDF version of this article, click [here](#).

Introduction

The terrorist attacks of September 11, 2001 illustrated in graphic terms the vulnerability of the United States to asymmetrical attack. The relative ease with which the nineteen Al Qaeda terrorists hijacked four airplanes and used them as deadly ballistic missiles was inconceivable to the citizens of the world's only remaining superpower. In an instant, it became painfully clear that despite its nuclear missiles, tanks and aircraft carriers, America was absurdly vulnerable to attacks coming from "below the radar." Al Qaeda proved terrorist attacks could come from unexpected directions, using more imagination than conventional power. This new sense of insecurity has defined the post-11 September world for the U.S.

In the wake of the terrorist attacks, the federal government immediately began assessing its vulnerability to asymmetric threats across a broad spectrum. Numerous public and private sector facilities were classified as "critical infrastructure," and as such, worthy of protection. Even more concerning was the realization that the instant effects of an asymmetric attack on U.S. critical infrastructure had the potential for far-reaching, extremely damaging impact on the U.S. economy. This economic "ripple affect" was most clearly illustrated by the near collapse of the U.S. commercial aviation sector in the months following the 11 September attacks. Al Qaeda showed the world (and probably itself) that asymmetric terror attacks have the potential to be "strategic" in consequence. One of the most vulnerable sectors of the U.S. economy identified during these post-11 September assessments was the maritime transportation system (MTS), specifically U.S. seaports.

Despite the now recognized strategic threat posed by terrorism in the post-11 September world, the Department of Homeland Security (DHS) has yet to engage in a comprehensive, coordinated process of developing strategy at operational levels. Establishing the broad outline for a DHS interagency operating strategy for U.S. port security is the goal of this essay. An interagency approach would leverage limited homeland security resources, allowing dollars spent to return a higher security yield. Such a strategy would serve not only to close the gaps in port security, but it would also seek to overlap coverage where gaps previously existed. Such overlapping operations will create security zones where agencies can support mutual objectives, not security gaps where there is an absence of responsibility.

Accomplishing this specific goal, however, requires a brief examination of two more general areas: First, the importance of U.S. port security as both an economic target and as a conduit for terrorist activity. Second, the more general aspects of homeland security strategy, for port security strategy is merely a sub-set of that larger strategy.

The Importance Of U.S. Port Security

America is a maritime nation, and its participation in the global economy is a direct function of the free flow of seaborne trade. As noted by retired U.S. Coast Guard (USCG) Commandant and current Deputy DHS Secretary James Loy:

“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... 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... or illegal weapons.”^[1]

While not immediately recognizable to most Americans, the MTS drives the U.S. economy. By logical extension, the MTS also serves as an engine for the global economy.

Seaports have not only been identified as terrorist targets, but also as potential low-tech gateways for the introduction of weapons of mass destruction (WMD) into the U.S. homeland. In his 2000 *Foreign Affairs* article, retired USCG Commander Steven Flynn mapped out a nightmare scenario:

“...why should a rogue state or terrorist organization invest in ballistic missile technologies when a weapon of mass destruction could be loaded into a container and sent anywhere in the world? Osama bin Laden could have a front company in Karachi, Pakistan, load a biological agent into a container ultimately destined for Newark, New Jersey, with virtually no risk that it would be intercepted. He could use a Pakistani exporter with an established record of trade in the United States. The container would then be sent via Singapore or Hong Kong to mingle with the half million containers that are handled by each of these ports every month. It could arrive in Long Beach or Los Angeles...”^[2]

Luft and Korin presented the same concern in a more concrete form in a recent 2004 *Foreign Affairs* article, where they noted:

“Intelligence agencies estimate that al Qaeda and its affiliates now own dozens of phantom ships-hijacked vessels that have been repainted and renamed and operate under false documentation, manned by crews with fake passports and forged competency certificates. Security experts have long warned that terrorists might try to ram a ship loaded with explosive cargo, perhaps even a weapon of mass destruction, into a major port or terminal. Such an attack could bring international trade to a halt, inflicting multi-billion-dollar damage on the world economy.”^[3]

It would be easy to dismiss these scenarios if large-scale drug smuggling did not already set the precedent of U.S. port vulnerability.

In light of the potential losses in terms of both lives and economic costs, it is strange that the terrorist threat to U.S. seaports has not been met with a comprehensive “interagency” federal (i.e. DHS) security strategy. Federal efforts to protect U.S. ports remain scattered amongst a handful of agencies. The USCG has developed operational and regulatory strategies for vessels, ports and waterways; customs and immigration efforts have focused on increased foreign and domestic cargo control and increased immigrant screening. The Transportation Security Administration

(TSA) has announced its jurisdictional primacy without fielding much in the way of resources, and Congress has established only lengthy regulatory priorities. The federal government has engaged in a great deal of *activity*, but it has not made a similar effort at *coordinated activity*.

The Unique Problem of Homeland Security Strategy

In the days after 11 September, the concept of “homeland security”^[4] went from something completely unknown to most Americans to a guiding principal of American life and U.S. defensive strategy. Terror attacks on U.S. interests overseas did not drive the idea of homeland security to the top of the domestic agenda. Despite the notable exceptions of the first World Trade Center attack and the Oklahoma City bombing, terrorist attacks on American targets seemed a foreign policy problem—a problem of “over there,” not “here.” It took Al Qaeda, nineteen hijackers and four commercial jets to make homeland security an American household term.

Despite its common usage, “homeland security” is a term more often used than explained. Homeland security strategy is a purely defensive strategy. It is a civil law enforcement, intelligence and quasi-military^[5] strategy aimed at deterring and preventing attacks within the domestic territory of the U.S. A central tenant of homeland security strategy is the reduction of vulnerability. Because asymmetric groups are difficult to track and their attacks are difficult to predict, the U.S. does not have the luxury of controlling the variables of conflict by taking the offensive inside the U.S. homeland.

A brief discussion of vulnerability is useful to illustrate the importance of the defensive nature of homeland security strategy. A framework for threat analysis used at the National Defense University refers to the “threat equation”. The threat equation pseudo-mathematically defines the threat of attack (T) as the product of a defender’s vulnerability (V) and an opponent’s capability (C) and intent (I). More simply stated: $T = V \times C \times I$.^[6] The character of T as a product of multiplication has important implications for strategy. If one or more of the variables in the equation increases, T increases. Similarly, if any one of the variables V , C or I approach 0 ($? 0$), then the rules of multiplication dictate that T will also approach 0.

If one combines the quasi-mathematical nature of the threat equation with the uncertainty in predicting asymmetric attacks, it is clear that in terms of homeland security strategy, the U.S. realistically only has the potential to directly affect V . The reduction of the value of V is the logical goal of prevention. The mathematical effects of a reduced V (or $V? 0$) on I and C are the logical goals of deterrence. Therefore, if one accepts the premise of the threat equation, the importance of the reduction or mitigation of vulnerability (V) on homeland security strategy becomes clear. The mathematics of the threat equation demonstrates that defensive strategy is strongest when it seeks to minimize the single variable within the defender’s actual control - V .

As previously stated, the goal of this essay is to suggest broad strategic principals for instituting an interagency operations concept for America’s maritime ports within DHS. It is centered on the idea that defensive strategy should increase security coverage across existing security gaps, creating zones of shared responsibility. This suggested approach for overlapping security coverage, accompanied by a corresponding reduction in V , will serve the mutually related strategic goals of prevention and deterrence.

Review of Existing Sources of Strategies

Despite the volume of federal homeland security strategies issued by the U.S. government in the wake of September 11th, a review of those documents did not identify any clear joint or interagency operating concepts. These policy documents provide general guidance regarding the goals of homeland security and the need to share information and coordinate effort, but none recommend the formulation of a joint operations concept within DHS. In many ways, this is

amazing considering the general public perception that DHS was created in order to “consolidate” federal homeland security efforts.

The *National Strategy for Homeland Security*[\[7\]](#) established the three goals of homeland security: the prevention of terrorist attacks, the reduction of U.S vulnerability to terrorism and the minimization of damage from attacks that occur. Nowhere in this policy document was there a strategic objective of coordinating the efforts of federal agencies to mutually support each other’s assigned functions, i.e., to “close gaps” or leverage resources. There was emphasis on the interaction between the federal, state and local levels, but no such interagency emphasis federally. Similarly, the *National Strategy for Combating Terrorism*[\[8\]](#) neglected any strategic objective for closely coordinating government actions to improve defense. The strategy was more or less a focused statement of the objectives of the Global War on Terror. Like the *National Strategy for Homeland Security*, the *National Strategy for Protecting Critical Infrastructure and Key Assets*[\[9\]](#) also stressed coordinated action between the federal, state and local levels; however, there was no similar statement regarding the lateral coordination of federal agencies to ensure critical infrastructure is protected. This strategy reflected much of the same political rhetoric as the previous strategies, but it did not suggest any concrete actions for ensuring coherent federal interagency effort.

Two remaining strategic statements specific to DHS also failed to recommend or require interagency action. *Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan*[\[10\]](#) and the more focused *Maritime Strategy for Homeland Security*[\[11\]](#) both seemed to favor the continuation of single federal agency responsibility and function. Both defy the apparent logic of creating DHS.

Congressional intent in this area was similarly short on “joint” vision. The *Homeland Security Act* (HLSA)[\[12\]](#) and the *Maritime Transportation Security Act* (MTSA)[\[13\]](#) were both exacting in their detail regarding “organizing for homeland security”, but neither sought to coordinate operational efforts within DHS. The HLSA “combined” agencies into a new cabinet department, but it made only passing reference to establishing homeland security task forces similar to the existing Joint Interagency Task Forces combating narcotics[\[14\]](#). The HLSA made such task forces discretionary and provided no funding for them. MTSA was primarily regulatory, and clearly illustrated congressional intent regarding port security—increased security regulation for the private sector. If Congress saw value in the strategic pursuit of port security, it passed two major pieces of legislation pass without focusing available federal resources on the problem.

A review of non-governmental literature did, however, identify a useful 2003 *Proceedings* article by USCG Reserve Lieutenant Paul Fawcett focusing on joint operations between the U.S. Navy and USCG in foreign littoral environs[\[15\]](#). The purpose of this paper was limited, but the joint operations solutions offered apply equally well to the problem presented in this essay. Fawcett’s suggestions are incorporated into this strategy: joint training, exchange programs, command courses and joint exercises.

A Joint Operating Concept for U.S. Port Security

While heralded to the public for combining numerous agencies under a single cabinet department, the creation of DHS did not increase the overall coherence of U.S. homeland security strategy in terms of port security. Historically, the various agencies within the federal bureaucracy, to include DHS, do not “play well” together; there have been only rare compelling reasons for cooperation. They possess different corporate cultures, and they measure their successes and failures by different metrics. Too often, bureaucracy “A” does not truly understand bureaucracy “B”, and it is only in times of crisis that they attempt to truly coordinate operations with each other. The results are frequently *ad hoc* and inefficient. The learning curve for this non-strategic approach is steep, and it discourages calm, coordinated action.

The Primary Federal Actors

At this juncture, federal port security responsibilities are spread between a few of “primary jurisdiction” DHS agencies. The USCG, an independent agency under the DHS Secretary, is the lead agency with overall oversight of the port environment. The USCG has security responsibility for vessels, waterways and port facilities. These security responsibilities are distributed throughout the USCG, through the various Captains of the Port, the Marine Security Offices and Law Enforcement operations. The USCG differs from all other agencies involved in port security in that it is a uniform, military organization. It has a military culture, more akin to the U.S. Navy than the other DHS port security elements.

The military nature of the USCG grants the agency the prime leadership role in interagency port security operations. The USCG has almost twenty years of joint experience with the traditional military services, and it has developed an institutional appreciation for joint operations, planning and exercises. The USCG has assigned personnel to joint commands, and as an institution, it understands the benefits of such commitment. The USCG also serves as a natural liaison to the U.S. Navy in terms of broader homeland defense issues during times of actual national security crisis. As such, joint homeland security operations in the maritime environment should continue to be lead by the USCG.

Having established the USCG as the “prime mover” for DHS port security efforts, it is important to realize that it is not the only actor. The creation of DHS was accompanied by the organization of two new agencies, both with important port security roles. The creation of U.S. Customs and Border Protection (CBP) consolidated the federal inspection responsibilities related to both the inspection of international cargo and the examination of persons arriving at U.S. maritime ports. CBP, a component of the DHS Directorate for Border and Transportation Security (BTS), is focused on intercepting WMD bearing shipping containers and/or Al Qaeda members carrying falsified passports. CBP maintains Container Security Initiative (CSI) liaison offices in major overseas seaports, all in an attempt to identify high-risk cargo before it reaches the U.S.

The role of CBP in port security is important, but like the USCG its resources are limited. As noted above, the actual percentage of cargo inspected is extremely low. CBP relies on risk-based “targeting” to identify those containers and ships that present the greatest threat to the U.S. homeland. Those high-risk entities are then the focus of CBP inspection efforts, but this process requires high quality intelligence to complete the risk analysis.

The creation of DHS was also accompanied by the creation of a new investigative/enforcement agency, U.S. Immigration and Customs Enforcement (ICE), another BTS component. ICE is charged with investigating and enforcing the customs and immigration laws at U.S. seaports, but it was assigned no broader security role. As such, the agency participates in many activities that generate homeland security intelligence, but that information is primarily applied to ICE investigations, not in support of defensive port security strategy.

BTS is also the home of the last major DHS component with port security responsibilities, the Transportation Security Administration (TSA). Created to address the very security lapses that allowed the 11 September hijackings, TSA has focused most of its efforts on airport security, but it is also tasked with broader transportation security responsibilities. Maritime security is one of the TSA’s stated areas of responsibilities, but so far, TSA has contributed little more than grant funding to the port security problem.

To integrate and maximize the efforts of these DHS components, this essay suggests the following strategic concepts be adopted and embraced. What follows is neither unique nor original. Rather, it is the application of doctrine that exists unevenly inside and outside of DHS and applying it to a specific problem in a coordinated, coherent manner.

A Suggested Paradigm Shift

The first pillar of the proposed strategy is a paradigm shift within DHS. This change in thinking must encompass two main ideas: viewing the MTS as a “system” and appreciating security vs. law enforcement. These notions are not completely foreign to those involved in port security, but neither are they accepted as guiding strategic principles.

The federal government has long organized agencies by functional responsibility. For example, CBP “inspects” cargo, but the USCG and TSA have responsibility for securing the port facilities where cargo is unloaded. The reality of the MTS, however, is that U.S. seaports are a mosaic of functional areas; they are an integrated system of maritime transportation, cargo processing, cargo storage, and intermodal transportation. Ports are holistic entities, comprised of federal agencies, state and local authorities, port authorities, private companies and transportation systems.

If one accepts this suggested paradigm, then it is clear that dividing the federal responsibilities for port security through limited functional assignments is illogical. Rather, all federal responsibilities related to port security should be evaluated, prioritized and refocused. The easiest way to create a systemic approach to port security is not to re-organize the existing bureaucracy; rather, it is to expand the functions and responsibilities of the various actors to create a more comprehensive approach. An interagency operations strategy is the best way to acknowledge the shared strategic goal of protecting U.S. ports and expanding overall security coverage.

The second required paradigm shift is a change in the functional application of existing authority, specifically regarding CBP and ICE. These agencies (and their predecessors) traditionally evaluate their successes by statistically capturing enforcement results—numbers of arrests and seizures. Such metrics require positive (i.e., offensive) action. However, security has a different set of metrics. Successful security does not involve arrests or seizures (although it could); it involves a lack of asymmetrical attacks. Thus, agencies must accept that their actions in support of port security may not yield the traditional measures of success

Both of these paradigms must be driven home by clear and unambiguous policy guidance from the President, the DHS Secretary and Congress. Failure to do so will lead to the very situation noted by Congressman Ike Skelton in considering one of the major pitfalls inherent to joint operations, “doing what one knows, rather than what should be done”^[16]. If existing paradigms were sufficient, doing more of the same would naturally reduce V. Nothing in the literature reviewed for this essay suggests this is a satisfactory strategic approach.

Joint Education

After the necessary paradigm shift, the single most important strategic concept advanced by this essay is that of joint education. DHS was created hastily, and it combined agencies that were familiar, but not intimately familiar, with each other. By creating the equivalent of the military’s staff and command colleges, DHS managers from USCG, CBP, ICE and TSA could study not only each other’s agencies, but also how their agencies fit within the broader DHS framework and the broader framework of homeland security strategy. Such education would also allow for a common understanding of the asymmetrical threats facing the U.S., for many DHS employees receive their information from media outlets like CNN, not DHS itself.

This interagency education concept would be familiar to the USCG, as professional education is a general requirement for advancement. This emphasis on education is not similarly strong in CBP or ICE (TSA is too new to comment on). In these agencies, professional education is limited to technical matters and rarely involves studying outside entities, practices, procedures or strategies. If employees of the agencies noted gathered to study both technical problems and strategic

issues, it is likely they would begin to develop a true “DHS perspective” (and corresponding doctrine) for port security. DHS officers and managers would then take their rightful place in developing the operational strategies needed to achieve true interagency operations in the maritime environment.

USCG officers Ross and Coleman developed this notion in detail in a 2003 *Homeland Security Journal* article^[17], wherein they stressed the importance of drawing on the precedents of joint military education. The authors suggested the establishment of a National Homeland Security University along the lines of the National Defense University. The author’s concluded their essay by asking a simple yet relevant question, “Can we wait... until after an abject failure, to begin a methodical effort to break down agency stovepipes and erase cultural barriers?”

Joint Training

Joint training should also be an important concept of any interagency operations strategy. Wherever and whenever possible, the DHS agencies should participate in appropriate joint technical training (differentiated from “education” as described above). Such training could include, for example, multi-agency law enforcement training. USCG could teach CBP and ICE about enforcement in the maritime environment, and CBP and ICE could teach USCG enforcement personnel about core federal enforcement functions (search and seizure, interviews and interrogations, etc.). These DHS entities could jointly create and run a port security training program U.S.C.G. an operational level course directed at personnel assigned to port security billets.

Such training, aimed at “workers” as opposed to officers or “managers,” would encourage cohesion at lower operational levels. It would familiarize port security entities with each other and develop a framework of shared interests and objectives. It would also stress cooperation at the level where critical port security work is actually carried out.

Exchange Programs

Interagency training and education should be accompanied by appropriate interagency assignments. Again, this would be a familiar concept to USCG, yet less familiar to ICE and CBP (TSA has few personnel outside of airports to exchange). ICE and CBP liaison positions could be created on the appropriate USCG staffs that manage the greater share of port security matters—the Captain of the Port and district law enforcement staffs. USCG personnel could be assigned to ICE and CBP management staffs as maritime liaison personnel. At lower levels, USCG Investigative Service (CGIS) agents and Law Enforcement Detachment (LEDET) personnel could serve tours in ICE port security/investigations squads, and ICE agents and CBP officers could serve CGIS or Field Intelligence Support Team (FIST) tours. These types of joint assignments should become a prerequisite for advancement in all DHS port security agencies.

Such exchange tours would serve the invaluable function of dispersing operational knowledge throughout DHS port security agencies and they would break down the barriers of individual corporate cultures. An infusion of intimate familiarity would allow DHS entities to avoid the critical mistakes of insular operations, such as making faulty assumptions about what other agencies can or will do in a given situation. Familiarity will also slowly develop a shared understanding of what types of information are valuable (from a security standpoint) to other DHS entities.

Joint Exercises

Lastly, the DHS entities involved in port security should test their interagency education, training and operations through tough, real world exercises. This author has participated in homeland security exercises that were little more than “open book tests,” which allow participants to

maximize their “notional” preparation and response. Such exercises do not strain existing security plans to identify weaknesses, instead they allow for DHS entities to cheat the system and “pass” the test.

Real life asymmetrical attacks will not favor those who have failed to test their security and coordination plans. The American public and Congress would be rightly indignant if during a critical port security event, it learned that ICE agents conducting a surveillance of a threatened port facility could not communicate with a USCG patrol boat that was following a suspect small boat. The fact is that joint exercises are needed to resolve critical operational issues.

Interagency Operations

As a final product of the strategic concepts described above, the DHS agencies involved in port security should begin to design a comprehensive DHS port security strategy, involving sustained interagency operations. These interagency operations should be logical and productive for all involved. In no case should they be reduced to one agency “doing the work” of another. Rather, interagency port security operations should be designed to be mutually supportive, ensuring that overall DHS resources are leveraged to achieve synergistic levels of security.

The potential scenarios for ongoing joint operations are numerous, but a few illustrations are helpful:

- ICE and CBP personnel could provide a landside security and enforcement component when the USCG deploys its Maritime Safety and Security Teams (MSST—waterborne special operations-type security teams) to U.S. seaports during high risk operations, such as high risk military out-loads.
- ICE and CBP personnel could augment USCG FIST teams when deployed in response to high-threat security operations, providing a higher degree of domain awareness.
- CBP, ICE and USCG could develop interagency response plans for periods of elevated Homeland Security Advisory System threat levels.

These suggestions represent only the “tip of the iceberg” where interagency port security operations are involved. The application of interagency resources would allow for participating agencies to maximize their effectiveness by using each other as “force multipliers.”

The USCG, ICE and CBP (and TSA to the degree it has resources to deploy) should coordinate their efforts in the MTS domain, because each owns a “piece of the puzzle.” As suggested, the MTS is really a holistic transportation system, and attempts to break it down into limited bureaucratic responsibilities will ultimately reduce security. Security will only be increased and V reduced when DHS begins to view the MTS as a system in need of a systemic approach to security. DHS must develop a strategic plan that views its own agencies as part of a coherent security system that matches form to function in the maritime environment.

There should never be a “line” where the responsibility and authority one DHS agency stops and another takes over. Rather, there should be a “zone” of shared responsibility and authority where problems are coordinated and assets are shared to achieve a common strategic objective: the defense of U.S. seaports. Artificially dividing ports into functional bureaucratic areas is a tactic of the pre-11 September world, and it should be discarded in favor of a more coherent pursuit of port security.

About the Author

Andrew C. Henrikson is a Senior Special Agent with U.S. Immigration and Customs Enforcement (ICE), Department of Homeland Security (DHS), and he is currently assigned to the International Terrorism section of the Joint Terrorism Task Force in Seattle, WA. He was a founding member of the U.S. Coast Guard's Area Maritime Security Committee for the Puget Sound area, and he has served in ICE port security/investigations assignments at the Port of Tacoma, WA. Prior to the creation of DHS, he served as a Special Agent with both the U.S. Customs Service and the U.S. Secret Service. He has served as an active duty Naval Intelligence Officer assigned to Joint Task Force FOUR, a joint counter-narcotics intelligence/operations command in Key West, FL, and subsequent assignments in reserve intelligence units at NAS Alameda, CA, and NAS Whidbey Island, WA. He holds a Bachelor's degree in Anthropology from the University of California at Berkeley, and he is currently a Masters student in the National Security Studies program at American Military University.

For more insights into contemporary international security issues, see our [Strategic Insights](#) home page.

To have new issues of *Strategic Insights* delivered to your Inbox at the beginning of each month, email ccc@nps.edu with subject line "Subscribe." There is no charge, and your address will be used for no other purpose.

References

1. Loy, James M. and Robert G. Ross, "[Global Trade: America's Achilles' Heel](#)," *Homeland Security Journal* (February 2002).
2. Flynn, Stephen E., "[Beyond Border Control](#)," *Foreign Affairs* 79, no. 6 (November/December 2000): 57-68. Accession number 3668249, page 4.
3. Luft, Gal and Anne Korin, "Terrorism Goes to Sea," *Foreign Affairs* 83, no. 6 (November/December 2004).
4. For the purposes of this essay, the term "homeland security" is differentiated from "homeland defense," the role of the military in defending the US from asymmetric threats.
5. Despite the USCG role in military operations, its role in terms of homeland security is primarily civil law enforcement related; therefore, its participation is termed "quasi-military" for the purposes of this essay.
6. Larsen, Randall J. and Ruth A. David, "[Homeland Security: Assumptions First, Strategy Second](#)," *Homeland Security Journal* (October 2000).
7. [National Strategy for Homeland Security](#), 2002.
8. [National Strategy for Combating Terrorism](#), 2003.
9. [National Strategy for the Physical Protection of Critical Infrastructures and Key Assets](#), 2003.
10. [Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan](#), 2004.
11. [Maritime Strategy for Homeland Security](#), 2002.

12. [Homeland Security Act of 2002](#), 107th Congress, 2nd Session, H.R. 5005 (introduced June 24, 2002).

13. [Maritime Transportation and Security Act of 2002](#) (Public Law 107-295).

14. Subtitle H, Section 885 of the HLSA authorizes the DHS Secretary to create Joint Interagency Homeland Security Task Forces similar to the counter-narcotics Joint Interagency Task Forces already established at Key West, FL, and Alameda, CA. Creation of such task forces was left both discretionary and unfunded.

15. Fawcett, Paul, "Jointness is the Key to Success in Coastal Warfare," *Proceedings of the United States Naval Institute* 129, Issue 8 (August 2003). Accession number 10494780.

16. Skelton, Ike, "Joint and Combined Operations," *American Defense Policy*, edited by Peter L. Hayes, Brenda J. Vallance and Alan R Van Tassel (Baltimore and London: Johns Hopkins University Press, 1997).

17. Ross, Robert G. and Peyton M. Coleman, "[The Way Forward: Education and Jointness in Homeland Security – Learning from the Department of Defense](#)," *Homeland Security Journal* (May 2003).