Backgrounder

Published by The Heritage Foundation

No. 2041
June 11, 2007

Small Boats, Big Worries: Thwarting Terrorist Attacks from the Sea

James Jay Carafano, Ph.D.

Globally, terrorists have shown an increasing interest in using small boats to attack military and commercial shipping and maritime facilities. The tactics and techniques of using commercial or non-commercial vessels (under 500 tons) or swimmers to emplace or deliver improvised explosive devices have proven effective and exportable. Contemporary operational practices by transnational terrorist groups include refining proven attack methods, sharing lessons learned, and encouraging others to adopt effective tactics. Thus, the possibility of such attacks in U.S. waters should not be ignored.

The small-boat threat needs to be addressed, but rather than focusing on this particular terrorist tactic, Congress and the Administration should invest in assets that improve the overall security of the maritime domain. The maritime sector is a large and diverse field with unique and daunting threats. Efforts should be expanded to improve U.S. situational awareness and law enforcement response rather than fixating on specific attack scenarios involving small boats or other terrorist threats.

The Small-Boat Threat

The definition of "small-boat threat" encompasses a variety of possible weapon-delivery vehicles, tactics, and payloads. Vessels include everything from large craft such as small freighters, large privately owned yachts, fishing trawlers, and commercial tugs to dinghies, jet-skies, and submarines, including mini-submarines like those used by the Japanese in the attack on Pearl Harbor.

Talking Points

- Terrorists are always looking for new ways to attack America. Using small boats to deliver a weapon, as in al-Qaeda's October 2000 attack on the USS *Cole*, is one such method.
- Protecting America's ships and ports is important. Over one-third of the U.S. economy depends directly on trade, which is mostly done by sea.
- Dealing with the small-boat threat is a complex challenge, and the solutions chosen will affect not only U.S. security, but also thousands of legitimate small-boat owners and a vast number of American businesses. Imposing more regulations that place significant new burdens on small-boat owners is the wrong answer.
- The right way to address the small-boat threat is to redouble U.S. efforts to improve overall maritime security, modernize the Coast Guard, and improve coordination among federal, state, and local governments and the private sector.

This paper, in its entirety, can be found at:
www.heritage.org/Research/HomelandDefense/bg2041.cfm

Produced by the Douglas and Sarah Allison
Center for Foreign Policy Studies
of the
Kathryn and Shelby Cullom Davis
Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

An attack could involve suicide bombers, as in the case of the attack on the USS *Cole*, or vessels on autopilot or remotely controlled. Improvised explosive devices could be delivered or emplaced by boats or swimmers (assisted or unassisted by breathing devices). This could involve placing a "parasite" on the hull of a craft or deploying tethered (anchored to the sea bottom) or untethered (floating) mines in a sea lane, waterway, or port traffic area.

Besides conventional explosives, the bombers could detonate nuclear, biological, chemical, or radiological devices. Attacks could occur while the targeted ship is docked at shore, approaching a port, sailing in international waters, or in U.S. or Canadian coastal waterways. In addition to ships, attacks could target port facilities; commercial infrastructure (e.g., an entertainment pier, bridge piling, or pipeline); or public events.

How Small-Boat Attacks Are Carried Out

In many respects, small-boat threats resemble other terrorist plots and have a similar signature. They require recruiting, training and planning, surveillance and intelligence collection, operational security, logistical support, rehearsals, information operations, and execution.

On the other hand, these threats have some unique characteristics and considerations. They can require unique attributes and knowledge such as maritime skills (e.g., sailing and scuba diving); familiarity with the target area (such as traffic patterns near a port facility); or explosives training. Unique environmental concerns that can affect the planning and conduct of maritime attacks include weather, tides, and other variables that could affect the dependability and reliability of the strike method. For example, salt, water, and wind can adversely affect weapons delivery and detonation.

Terrorists like predictability. They like to know the obstacles that they will face and the probable results of an attack. Uncertainties in the maritime domain could significantly affect the desirability of employing the small-boat attack method. For example, large public events like a "tall ship" week or a national sporting event might seem inviting targets because of the large crowds of people and the public attention focused on the events. However, large, one-time events are less promising targets because of the additional security and the greater difficulty in predicting the security conditions.

Often, strikes on public venues are more appealing to "lone wolf" attackers who might not weigh the risks and benefits of less well-planned operations as carefully. Likewise, targets such as liquefied natural gas (LNG) tankers or other ships carrying hazardous materials might seem to present tempting opportunities to generate spectacular catastrophic affects. However, from material on the Internet, terrorists already know of the debate over whether or not a small-boat attack could realistically achieve a catastrophic outcome.

On the other hand, normal commercial traffic and port operations bear many of the same characteristics of a desirable terrorist target, including limited responsive security and highly predictable patterns of behavior. For example, high-value ships such as cruise ships and tankers carrying extremely hazardous materials are much more vulnerable when entering or leaving restricted navigable waters along the U.S. coastline, in port areas, or along domestic waterways. During these periods, a large ship typically has a pilot on board, is moving at a low speed, and is following a tight and predictable course because of underwater obstructions and maritime traffic.

Previous al-Qaeda Small-Boat Attacks

The most prominent small-boat attack on a military ship occurred on October 12, 2000, when al-Qaeda operatives detonated a small boat filled with explosives against the hull of the USS *Cole*, which was refueling in the port of Aden, Yemen. The attack killed 17 U.S. sailors and wounded 39 others. It also garnered much publicity for al-Qaeda, which subsequently highlighted the attack in its recruiting videos and other propaganda.

In October 2002, al-Qaeda undertook its first successful attack against a commercial ship using a small boat. Its operatives rammed the French supertanker *Limburg* with a small fishing craft packed with explosives. The attack, which occurred while the *Limburg* was 12 miles off the coast of Yemen, killed one crew member, injured 12 others, and

caused a spill of 50,000 barrels of crude oil along 45 miles of coastline.

Other terrorist groups besides al-Qaeda have attempted to use small boats as weapons-delivery vehicles. On November 7, 2000, a Hamas suicide bomber aboard a fishing boat tried to attack an Israeli patrol craft sailing off the Gaza Strip. Alert crew members detected the threat and sank the boat before the Hamas operative could consummate the attack. The Tamil Tigers have also attempted a number of improvised maritime attacks in Sri Lanka.

In addition to terrorist threats, transnational criminals have used similar tactics to smuggle drugs, weapons, humans, and other contraband. These include everything from building mini-submarines to smuggle drugs across the Gulf of Mexico to trafficking Cuban refugees to Key West. Many of the operational practices employed by transnational criminals are adaptable to terrorist attacks. (Conversely, countermeasures designed to address small-boat threats might also be valuable in combating illicit trafficking by small boats.)

How Serious Is the Threat?

The risks associated with small-boat threats are complex. An assessment of risk combines an evaluation of criticality (or consequences), threat, and vulnerability. Three major risks connected with small-boat threats should be considered.

The Psychological Impact. Research data make a compelling case that "man-made malicious" events create more fear, apprehension, and uncertainty than natural disasters or accidents. Almost every week, the U.S. experiences maritime incidents that are equivalent to a small-scale terrorist attack in terms of endangering life and property. These range from boating episodes involving individuals to commercial industrial accidents that put hundreds of lives and millions of dollars of infrastructure at risk.

The United States has also experienced a number of large-scale maritime disruptions, which have affected thousands to tens of thousands of lives and hundreds of billions of dollars in damage. These include everything from the Texas City (1947) and San Francisco (1944) disasters, which involved large commercial ships carrying extremely hazardous materials, to Hurricane Katrina, which crippled the ports of New Orleans and Mobile. A terrorist attack of similar scale would certainly have a significantly greater impact on the public, particularly because many Americans have only a minimal appreciation of what occurs in the maritime domain. Anxiety is always greater when individuals are less familiar with the situation.

The impact of a terrorist attack might be reflected in many different behaviors and attitudes, from undermining the confidence of Americans in their government to panic buying because of the fear of economic disruption. The scale and duration of psychological damage could vary significantly, depending on the nature of the incident and the character of the response.

Physical Destruction. A small-boat attack is unlikely to cause a large loss of life or property unless it involves a weapon of mass destruction or highly hazardous material that causes a large-scale fire or explosion. Even a large-scale disaster involving thousands of lives and billions of dollars in damage is unlikely to have long-term negative consequences for the U.S. economy.

In many respects, the response required in the event of a small-boat attack would resemble the response to a fire, explosion, or industrial accident. Thus, many of the current safety measures, equipment, drills, and training required for maritime safety would be applicable to reducing the loss of life and property in the event of a small-boat attack. Likewise, any measures to improve overall safety, firefighting assets, all-hazards disaster response capabilities, search and rescue, other emergency services, and salvage and recovery would contribute to reducing damage in the event of a successful attack.

Disruption of Services. Much of the U.S. maritime infrastructure is clustered near urban centers. Thus, attacks might disrupt mass transit, interrupt delivery of goods and services, or require the evacuation of local populations. Some attacks might seek to disable larger vessels to block waterways, bridges, or tunnels. Physical disruptions would likely be highly localized and have little impact on the overall economy or long-term economic growth, even in the case of large-scale disasters.

Near-term economic impact might be more significant and widespread if terrorists conducted multiple attacks at multiple locations or if the attack affected the national supply chain. Government (U.S., Canadian, or Mexican) and/or private-sector responses after a strike (such as closing ports of entry) might be more likely to have a significant economic impact than would the direct results of the physical destruction caused by the attack itself.

On the other hand, individual companies or industries might suffer long-term negative affects, such as the cruise industry if a cruise ship were attacked. This might be reflected in increased insurance rates or loss of customer confidence.

The Scope of the Challenge

The small-boat problem is complicated by the magnitude of areas and activities encompassing small-boat activity; the lack of situational awareness by federal, state, and local authorities; and the limited capacity to interdict active threats.

Policing a Vast Domain. Small boats operate on thousands of miles of U.S. coastline, inland waterways, and lakes. Frequent undeclared entries by small boats occur between the U.S. and Canada and between the U.S. and the Bahamas every day. On any given day, the number of small craft in U.S. waters is vast. Thousands of boats are bought and sold every year, and many small boats are operated with minimal training or licensing requirements. In many areas, small boats operate in proximity to high-value ships and maritime infrastructure without restriction.

Situational Awareness. The requirement for situational awareness in U.S. ports, coastal areas, and waterways evolved primarily in response to the need for aids to navigation and safety. Situational awareness to support physical security and law enforcement activities was not a primary concern.

Post-9/11 situational awareness has been enhanced by adapting existing technologies, such as surface radars in some ports, and by applying new technologies, such as infrared video surveillance and GPS. Few of these capabilities have been or can be applied practically to the monitoring of small-boat activities, although there are some ongoing initiatives. For example, the Coast Guard Research and Development Center has experimented with employing Navy sonobouys to detect small boats in high-density smuggling areas, but implementing such solutions has major technical and cost implications.

Interdiction and Response. Local, state, and federal law enforcement have limited capability to detect threats, and standoff detection is usually restricted to meters at best. For example, the Department of Homeland Security, the Department of Defense, and some local law enforcement authorities have the capability to scan the hulls of boats for parasites. Current detection capabilities are a mix of intrusive and non-intrusive systems. Almost of all of them are time-consuming and costly, and almost all of them present significant "false negatives" and "false positives" problems in attempting to identify threats.

Law enforcement at all levels also has very limited capacity to disable small craft or swimmers and ineffective response times in meeting unanticipated threats. Methods of incapacitation mostly involve the use of potentially lethal force. Rules for the employment of lethal force are not consistent across government agencies. In addition, methods for disabling small boats using non-lethal technologies are neither widely available nor particularly effective.

Only the U.S. Navy has any notable capacity to detect and clear mines and improvised explosive devices at sea or in waterways. No dedicated domestic assets can address waterborne mines. The U.S. navy has conducted some research and has developed some capability to detect and interdict swimmers, but this capacity is not widely available for U.S. ports or waterways. Any application of additional technologies or capabilities for interdiction and response has significant cost and technical implications.

Ensuring Economic Competitiveness. Moving people, goods, and services by sea and waterway is extremely cost-effective. In addition, waterborne traffic, while not without environmental consequences, produces much less air pollution than does moving goods by truck. A significant expansion of domestic maritime traffic for the transportation of goods and people could give the United States a key economic competitive advantage in the

21st century. Smaller craft could play a critical role in this economic expansion. The key challenge to exploiting this potential advantage will be public and private investment in maritime infrastructure.

Currently, the nation as a whole does a poor job of investing in maritime infrastructure. Federal and state laws do not provide adequate incentives and in some cases discourage investment. In regard to security, this provides a dual challenge to policymakers. On the one hand, further excessive regulation and restrictions in the name of enhancing security will only further discourage investment. On the other hand, as the nation increasingly exploits its ability to move by sea, maritime infrastructure will become even more critical to the economy, and concerns over its security will become even more pressing.

The U.S. Response

Post-9/11 security initiatives have only marginally improved the U.S. capacity to deal with the small-boat threat. The recently adopted International Maritime Organization International Ship and Port Facility Security Code and the corresponding requirements in the U.S. Maritime Transportation Security Act address small-boat threats only incidentally by requiring vulnerability assessments, security plans, and security coordinators.

U.S. law requires ships over 500 tons to provide 96 hours notice to the U.S. Coast Guard before entering U.S. waters. This requirement does not address the small-boat threat.

Following the attack on the *Cole*, the U.S. Navy and many of its foreign counterparts substantially improved their force protection procedures. These better military defenses mean that terrorists in the future will more likely choose to attack softer targets such as commercial vessels flagged in the U.S. or friendly countries.

Since 9/11, security has received increased emphasis in U.S. ports and waterways, including more coordination among federal, state, and local entities; greater access control; and added security measures. Some security measures have been introduced specifically to address the small-boat threat. For example, LNG tankers are escorted into port and guarded, although other more vulnerable and volatile hazardous cargo is often not given the same attention. While in port, cruise ships are required to post a picket craft to warn off or interdict small boats.

Some ports have established operational coordination or information sharing centers, such as Operation Seahawk in Charleston, South Carolina. Typically, these centers do not focus on the small-boat threat, although some coordinate reports of suspicious activity or investigations that might uncover such a threat.

While there have also been some efforts to increase and coordinate police, county sheriff, state game and wildlife, and U.S. Coast Guard waterborne patrolling, these programs are modest. In some cases, volunteer groups such as state maritime defense forces have been used to supplement waterborne patrolling.

Development of the national maritime security strategy and the Maritime Operations Threat Response Plan has improved maritime security coordination overall, but it does not address the small-boat threat specifically.

There have been some marginal efforts to coordinate research and development of technologies and techniques and tactics among the Navy, the U.S. Coast Guard, the National Laboratories, federally funded research and development centers (such as RAND and the Homeland Security Institute), and other federal and private-sector entities. However, many disparate pilot projects, experiments, and ongoing initiatives are poorly coordinated and lack a clear plan to operationalize the research results.

In June 2007, the U.S. Coast Guard plans to convene a major conference of maritime stakeholders to propose new measures for dealing with the small-boat threat. The recommendations will likely include a combination of new regulatory requirements and sharing best practices.

Possible Countermeasures

Countermeasures generally fall into one of three categories, and each set of solutions faces significant challenges.

Identification and Accreditation. These measures include proposals for new regulatory regimes requiring additional stipulations for licensing indi-

vidual operators and craft; national standardization of licensing processes and documents (including both the licenses themselves and "breeder" documents such as the documents used to verify identity and legal status); reporting of lost and stolen licenses and craft; and requirements for transponders, which would enable authorities to identify and track small boats.

These proposals raise significant cost and effectiveness issues that need to be addressed, as well as significant issues concerning cost-sharing and responsibility among federal, state, and local entities. Identification and accreditation regimes will also raise privacy concerns similar to those involved in implementing REAL ID. Further regulation of the maritime transport, boating, and recreation industries could have negative economic impacts.

Another challenge is identifying and accrediting the many small boats in U.S. waters that come from outside the United States, particularly from Canada and the Bahamas and/or that are registered overseas and licensed under flags of convenience. One set of proposals would extend the 96-hour notification requirement to all ships (even those under 500 tons) entering U.S. waters.

Yet proposals to extend notification requirements to small boats raise a number of concerns. For example, many small boats can travel to U.S. waters in less than 96 hours (e.g., from Canada, Mexico, and the Bahamas). Small-boat owners are concerned about the cost and inconvenience of complying with such regulations. In addition, such reporting would generate mounds of data, and screening and evaluating those data for useful information poses significant cost and human capital challenges.

Finally, identification and accreditation programs are effective when combined with capabilities to investigate fraud, identify and respond to suspicious activities and persons, and prosecute violators.

Improving Situational Awareness and Detecting Threats. These measures could involve a range of activities from "neighborhood watch" and public awareness programs to technologies that provide wide-area surveillance and standoff detection of explosives and materials used in weapons of mass destruction.

Identifying and monitoring small craft and swimmers poses serious technological challenges. For example, distinguishing small boats and swimmers from waves is often technologically difficult. Detecting suspicious materials at a distance is perhaps the most daunting technical challenge. The costs of establishing and maintaining wide-area surveillance are especially significant.

Finally, situational awareness and threat detection are effective only if they are linked to responsive investigation of suspicious activities and interdiction of threats.

Controlling Access and Interdicting Threats. This approach involves restricting access to sensitive areas, which might include critical infrastructure, extremely hazardous material, national icons, high-value ships such as passenger ships or ferries, or densely populated areas.

Interdiction raises issues concerning the manpower and capabilities available to control access and conduct interdiction. For example, significantly enhancing community policing at sea could be extremely costly. In some cases, restricting or controlling passage is impractical or would significantly disrupt the movement of goods, people, and services.

The most significant technical challenge is developing non-lethal disabling technologies to limit the requirement for employing deadly force. Effective interoperable communications, information sharing, and coordinating joint action among federal, state, and local authorities and the private sector remain significant concerns.

Mitigating the Threat

The maritime domain has a vast number of vulnerabilities, and terrorists have many options and opportunities for determining how, when, and where to attack maritime infrastructure. Fixating on a particular method of attack or trying to protect a particular target set is a self-defeating strategy that not only imposes significant costs on the defender, but also can easily be circumvented by an adaptive enemy.

In that regard, focusing specifically on the small-boat threat is probably not the best way to address

the challenge. Rather, maritime security solutions should focus on:

- **Ensuring resiliency.** Trade accounts for one-third of the U.S. economy, and much of that trade and a significant portion of the nation's transportation and energy infrastructure depends on or is located near maritime infrastructure. The most important national objective in the maritime domain should be to ensure that commerce continues regardless of any natural or man-made disaster.
- **Getting the biggest bang for the buck.** Security investments should be focused on initiatives that provide the most value for improving maritime security overall. Hard choices need to be made. Piecemeal investments in maritime security will add little real security. On the other hand, effective counterterrorism operations that focus broadly on identifying, investigating, and thwarting terrorist activities and plots in the maritime domain offer more value than those that focus narrowly on trying to deny terrorists access to a specific target or delivery means.

What the Government Should Do

To create the most effective public policies to keep the nation safe, free, and prosperous, Congress and the Administration must take a broad and long-term view of the small-boat threat. Any proposed efforts should:

- **Address economic competitiveness, not just security, with solutions that support both objectives.** In particular, the Administration should not impose significant new regulatory restrictions on the operation and licensing of small boats and small-boat operators. Such measures will add little security at significant cost.
- **Insist on programs that best enhance the overall security of the maritime domain and contribute to the resiliency of maritime commerce.** First and foremost, the government should ensure that maritime commerce is not adversely affected in the event of an incident. The Administration should complete, exercise, and refine the plan required by the national maritime security strategy to address issues of business continuity and reconstitution after major disruptions in maritime commerce.
- **Invest more heavily in Coast Guard modernization, particularly in programs that improve situational awareness, law enforcement, and special operations capabilities.** Specifically, priority funding should be given to Coast Guard initiatives that expand the capacity of the service's maritime security teams, develop capabilities for effective non-lethal interdiction of small boats, extend visibility of craft over the horizon by using unmanned aerial vehicles and other technologies, field new state-of-the-art patrol craft, and increase law enforcement investigation and intelligence means.
- **Ensure the right balance of roles, missions, and resources and close cooperation between U.S. Navy and U.S. Coast Guard maritime security missions.** The U.S. Navy should focus on providing intelligence support and mine-clearing expertise and capabilities, as well as sharing research and development in countering small-boat threats with the Coast Guard. The Coast Guard should lead in developing a national maritime domain awareness system, expand its capabilities to investigate and interdict potential threats, and work with state and local governments and the private sector to share information and intelligence effectively.
- **Respect the principles of federalism and exploit the inherent advantages of a free-enterprise approach to providing the most creative, efficient, and effective solutions.** Homeland security grants should be minimal. Instead, the federal government should facilitate the sharing of best practices and allow state and local governments and the private sector the freedom to innovate and adopt measures that are most appropriate for their needs and that would best perform the due diligence necessary to ensure business continuity and disaster recovery.

  Government should also encourage and provide incentives for craft under 500 tons to employ transponder locator and identification technologies. These transponders perform a function similar to what OnStar offers for automobiles. Adopting these technologies would enhance public safety and increase situational awareness, and use of these systems would better enable the

Coast Guard and other rescue services to find craft in need of assistance. The widespread use of transponders would also assist in monitoring maritime traffic.

The Way Ahead

For the United States to develop a comprehensive and multilayered approach to homeland security, it must address the small-boat threat. While the maritime sector is a large and diverse field with unique and daunting threats, the U.S. should develop plans to improve U.S. situational awareness rather than defend against specific threat types. Investing in measures that bolster the U.S. economy and provide the best return for the amount spent are also good approaches for formulating a protection plan against small boats.

In the end, guarding U.S. maritime craft and infrastructure will not only protect the resilience of the U.S. economy and international trade, but also protect a sector that serves as a source of enjoyment and work for millions of American citizens.

—James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation. The author would like to thank Austin Knuppe for his assistance in putting together this paper.