Assessment

(U//FOUO) United States-Canada Marine Transportation System: Terrorist Threat Remains Low but Risks Persist

15 April 2011

IA-0270-11

Homeland Security

Office of Intelligence and Analysis

(U//FOUO) United States-Canada Marine Transportation System: Terrorist Threat Remains Low but Risks Persist

15 April 2011

(U) Prepared by the Office of Intelligence and Analysis (I&A), Border Security Division, Northern and Maritime Borders Branch. Coordinated with the Transportation Security Administration (TSA), National Counterterrorism Center (NCTC), U.S. Northern Command, and United States Coast Guard (USCG).

(U) Scope

(//CAN U) This Assessment examines terrorist threats to the Marine Transportation System (MTS) relevant to the U.S. and Canadian maritime borders, and updates unclassified judgments from the 2007 Canadian Integrated Threat Assessment Centre (ITAC) product, "(//CAN U) Terrorist Threat to the Canadian Maritime Sector," and the 2008 USCG Intelligence Coordination Center product, "(U//FOUO) National Maritime Terrorism Threat Assessment." The information is provided in support of the activities of the Department and to assist federal, state, and local government counterterrorism and law enforcement officials in effectively deterring, preventing, preempting, or responding to maritime terrorist attacks against the United States and Canada.

(U//FOUO) This document provides an updated baseline for MTS threats to support the activities of the Department and assist other federal, state, and local government agencies and authorities; the private sector; and other entities, both in implementing joint U.S. and Canadian strategies for northern border security. Moreover, it assists the Department and other federal, state, and local government agencies and authorities; the private sector; and other entities in developing priorities for protective and support measures to address existing or emerging threats to the homeland related to maritime border security.

(U) Key Findings

(U//FOUO) While passenger vessels and terminals will likely remain potentially attractive targets for terrorist attacks, trends in overseas terrorist attacks and the lack of any reporting on maritime terrorist plots against the U.S.-Canada MTS suggests the threat to the majority of the system is low; violent extremists could attack U.S. and Canadian ferries and similar soft maritime targets with little or no warning.

- **(U//FOUO) The capabilities of al-Qa'ida and its sympathizers to conduct small boat waterborne improvised explosive device (WBIED) attacks against the U.S.-Canada MTS probably remain limited.[*] When compared to other tactics, maritime attacks by al-Qa'ida or its affiliates are rare and have only occurred in the Middle East and East Asia.[†] The transferability of this tactic to North America would be problematic given MTS governance and law enforcement that create a less permissive maritime environment.**

- **(U//FOUO) Terrorists probably would be reluctant to use containerized cargo to smuggle weapons of mass destruction (WMDs) into the United States or Canada because the loss of physical control of a valuable weapon would likely pose an unacceptable intervention risk. Nonetheless, this threat remains a low-probability, high impact scenario. We judge that terrorists would seriously consider other maritime means, such as small boats and bulk cargo shipments, to smuggle any available WMD or to conduct related waterside attacks in the United States or Canada if they had the opportunity. This judgment is primarily based on expert opinions from DHS officials, as well as assertions put forth by the Monterey Institute Center for Nonproliferation Studies and other academic or nongovernmental organizations.**

(U//FOUO) Ferries and other passenger vessels remain vulnerable targets for terrorist attack. Although we have no credible reporting that any U.S. or Canadian ferry systems are the target of ongoing terrorist plotting, concerns are elevated because of the focus by al-Qa'ida and its affiliates on attacking soft targets to cause mass casualties, the growth of internationally inspired and homegrown violent extremist (HVE) threats, and the paucity of preoperational indicators for ferry attacks.[‡] Moreover, terrorists might target ferries as a way to compensate for the increasing security measures protecting the aviation sector.

---

[*] (U//FOUO) An improvised explosive device (IED) incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and is designed to destroy, incapacitate, harass, or distract. A WBIED is an IED delivered on or below the water.

[†] (U//FOUO) Al-Qa'ida affiliates are groups that have agreed to partnership with al-Qa'ida, as confirmed by statements from both the affiliates' leader and Usama bin Ladin or Ayman al-Zawahiri. Al-Qa'ida allies are groups that share a common violent ideology or perception of a common enemy with al-Qa'ida, but are not formally recognized by al-Qa'ida as affiliates.

[‡] (U//FOUO) An HVE is a U.S. person who has been radicalized predominantly within the United States and is inspired by one or more foreign terrorist groups to conduct terrorist attacks in the United States. An HVE differs from a domestic terrorist in that the former either follows direction from or is inspired by one or more foreign terrorist groups.

(U//FOUO) Past terrorist successes involving use of toxic industrial chemicals (TICs) in overseas conflicts may encourage attackers to attempt to weaponize large hazardous materials (HAZMAT) shipments moved in the MTS each day. Violent extremists have a limited ability to produce small improvised chemical weapons, but experimentation with these HAZMAT concoctions may eventually result in an evolutionary development of greater attack capabilities.

(U//FOUO) Terrorists and criminals almost certainly will continue their efforts to exploit the MTS to facilitate illegal entry of personnel or other criminal activities. Immigration and mariner document fraud, smuggling, and criminal activities along the waterfront require continuous law enforcement vigilance. Illicit actors may attempt to increase their circumvention of maritime security in North America because of enhanced land border security and air passenger screening.

(U//FOUO) Cyber attacks—regardless of motivation—will continue to represent only a marginal threat to automated ships and port facilities in North America, largely because of the complexity required for a successful attack. A paucity of information regarding such threats remains an enduring intelligence gap. Still, concerns related to maritime supply chain disruption perpetrated by disaffected employees or other insiders—particularly those with system administrator access—are the most frequently voiced by private sector security officials.

(U) MTS Overview and Vulnerabilities

(U//FOUO) The U.S.-Canada MTS consists of ocean, coastal, and inland waterways; ports; intermodal connections; vessels; and commercial, military, and recreational users. The system stretches from the Great Lakes-Saint Lawrence Seaway System—also known as the Great Lakes Marine Transportation System (GLMTS) westward—to the Pacific Ocean along the U.S.-Canada border.

- (U) Over 1.5 million passengers arrive in Canada annually, largely from the United States, and Canada's ports handle a rapidly growing number of cruise ships.

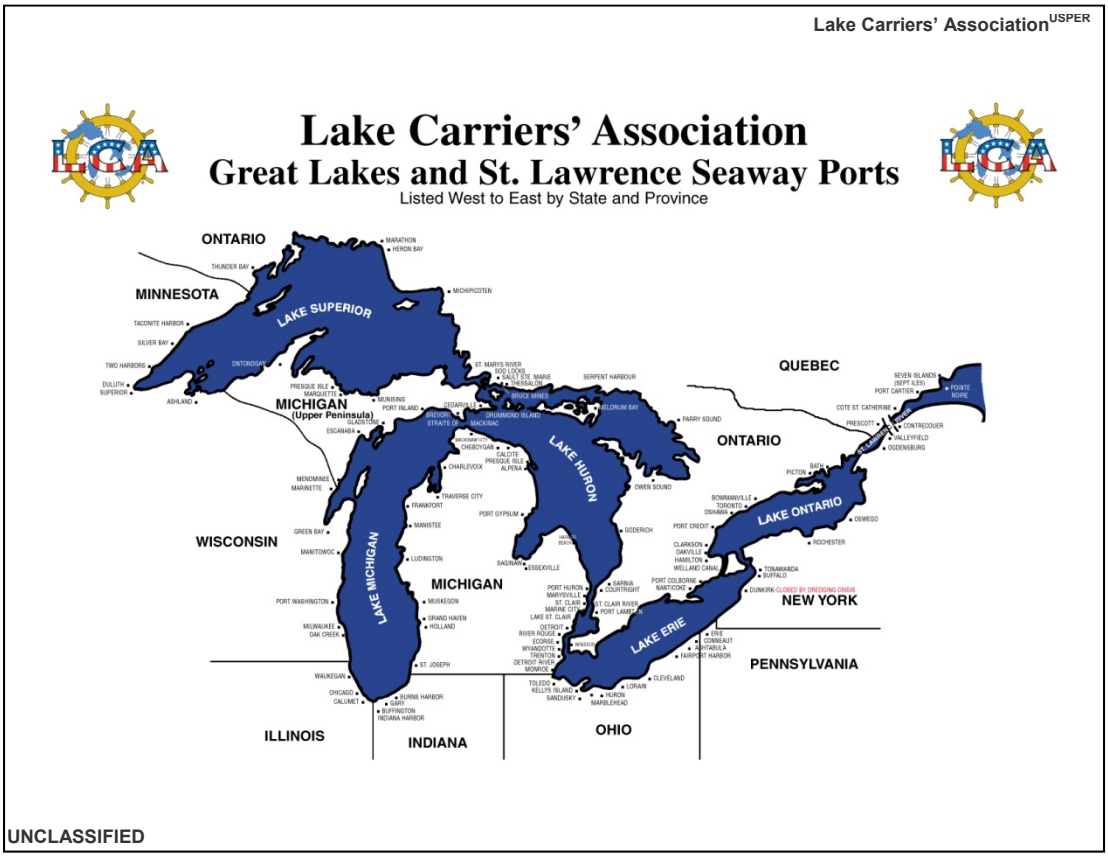
- (U) Besides its ports, Canada also has 10 international ferry terminals, 19 interprovincial terminals, and nearly 300 intraprovincial terminals providing vital links both within and between the provinces. In 2008, Canada's ferries carried more than 48 million passengers and approximately 18.3 million vehicles.[*]

- (U//FOUO) According to TSA, more than 20,000 passenger vessels—including ferries, casinos, and harbor excursion vessels—carry more than 175 million passengers each year in U.S.-Canada waters.

[*] (U) Ferries operate between New Brunswick and Maine, as well as British Columbia and the states of Alaska and Washington. There are also several ferries operating between Ontario and the states of Michigan, New York, and Ohio.

(U//FOUO) The GLMTS is the heart of the U.S.-Canada MTS. The GLMTS is a vital binational waterborne transportation link for moving goods and people. The system encompasses the Saint Lawrence River and the five Great Lakes, and extends over 2,300 miles, encompassing eight states and two provinces with over 32 million citizens. The region produces 50 percent of all U.S. manufacturing output and two-thirds of Canada's. This waterway is expected to increase in importance over this decade as both countries seek ways to ease highway and rail congestion, especially along North America's east and west coasts and the midwest region.

(U) 2010 statistics published by the Saint Lawrence Seaway Management Corporation suggest that the GLMTS is directly and indirectly responsible for 75,000 jobs in Canada and over 150,000 jobs in the United States.



(U) The GLMTS has hundreds of ports, along with myriad cargo handling and intermodal transportation nodes—all of which support a mutually beneficial maritime supply chain.

(U//FOUO) Foreign terrorist plotting indicates that transportation systems remain a target, likely because much of the infrastructure has minimal security or protection and offers the potential for low-risk, high-impact, high-visibility attack results. As tighter security practices change terrorist perceptions of the vulnerability within land and air transportation, maritime transportation could emerge as a likely alternative target. A terrorist attack on even one element of the MTS would have serious local, regional, and far-reaching impacts to domestic and foreign trade-based economies.

(U//FOUO) The MTS has many vulnerable elements including ferries, passenger terminals, cruise ships, commercial vessels, ports, recreational boaters, military support vessels, and industrial facilities. Small arms, bombs, WBIEDs, WMD hidden in cargoes, and weaponized HAZMAT shipments all pose potential threats to the MTS.

- (U) There are more than 250 ports in Canada; three—Vancouver, Montreal, and Halifax—handle the bulk of the containerized cargo, which is more than 3.5 million twenty-foot equivalent units annually.

- (U) Commercial vessels carry roughly 25,000 metric tons, or the equivalent of 870 tractor trailers each year. Oil and chemical carriers and related industrial facilities are potential targets.

- (U) Thousands of recreational boaters in the Great Lakes and other parts of the MTS could provide exploitation opportunities for criminals and terrorists.

- (U) Canada's 10 international ferry terminals, 19 interprovincial terminals, and nearly 300 intraprovincial terminals provide vital links both within and between the provinces and the United States.

- (U) Military or law enforcement vessels could be symbolic targets.

(U) Maritime Terrorism, Targets, and Tactics

(U//FOUO) Ferries and other passenger vessels represent the most likely MTS targets for terrorist attack. Although we have no credible reporting that any U.S. or Canadian ferry systems are the target of ongoing terrorist plotting, concerns are elevated because of the focus by al-Qa'ida and its affiliates on attacking soft targets to cause mass casualties, the growth of internationally inspired and HVE threats, and the paucity of preoperational indicators for ferry attacks. Moreover, terrorists might target ferries as a way to compensate for the increasing security measures protecting the aviation sector.

- (U//FOUO) Since 2008, the ITAC and U.S. and Canadian law enforcement agencies have consistently identified U.S. and Canadian passenger ferries as potential targets for terrorist attacks.

- (U//FOUO) A review of attacks against passenger vessels worldwide suggests that bombs, small arms, or combined attacks would most likely be used to target ferries in U.S. or Canadian waters, as these types of attacks have already occurred in Asia and Europe. These tactics are among the most frequently used by terrorists, are easily transferable to North America, and could be employed in operations that offer little or no warning (see Appendix A for more information on maritime terrorist tactics).*

* (U//FOUO) Appendix A is provided for informational purposes. DHS did not participate in the authoring of this product.

(U//FOUO) **Small Arms and Bombs.** These weapons are probably the most likely weapons of choice in attacking the MTS. The overall terrorist trend overseas toward softer targets—such as mass transit—using small arms and bombs could foreshadow a greater risk of attack to passenger vessels and terminals in the United States or Canada. In particular, the Madrid and London mass transit attacks of 2004 and 2005, respectively, suggest that violent extremists seeking mass casualties and publicity may see maritime transit—ferries, passenger terminals, and cruise ships—in the United States or Canada as attractive, accessible targets (see Appendix B for more detailed information regarding potential indicators of maritime terrorist activity).

(U) International Terrorist Attacks and Plots Against Passenger Vessels, 2009-1982

Date	Group	Passenger Vessel Incident, Attack, or Plot Synopsis
2009	Unknown	12 IEDs were discovered in a second deck trash can on the *M/V Blue Water Princess* ferry in Lucena City, Philippines.
2009	Unknown	Employees of the SuperFerry Ship Company alerted police to an IED that had been placed in the port of Nasipit, Philippines.
2005	Abu Sayyaf Group (ASG)	An IED exploded on the Philippine inter-island ferry *M/V Dona Ramona* just prior to its departure from Basilan Island wounding at least 30 passengers.
2004	ASG	An IED exploded and caused the fire and sinking of the *M/V Superferry-14* off the coast of the Philippines—killing over 100 passengers in the world's deadliest maritime terrorist attack.
1996	Chechen Insurgents	A passenger ferry was hijacked in the Black Sea; 255 passengers were held hostage for four days until surrender to Turkish authorities after pulling into Istanbul.
1992-1994	Al-Gama'a al-Islamiyya	A plot targeted at least four cruise ships on the Nile River in order to undermine Egypt's tourism sector.
1991	ASG	An IED exploded on the *M/V Doulous*, a Christian missionary ship, while port side in Zamboanga City, Philippines, killing two missionaries.
1988	Abu Nidal Organization	A failed VBIED attack at the ferry pier in Piraeus, Greece, followed by a combined arms attack on *M/V City of Poros*, killed 9 and injured 98 passengers near Aegina, Greece.
1985	Palestinian Liberation Front	The cruise ship *M/V Achille Lauro* was hijacked off the Egyptian coast; American passenger Leon Klinghoffer was killed during the voyage.
1982	Moro National Liberation Front	An IED exploded on the second deck of the ferry *M/V Santa Lucia*, killing 2 and wounding 50 passengers at Pagadian, Philippines.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

— (U//FOUO) The September 2010 TSA Office of Intelligence threat assessment for passenger vessels asserts that IEDs would be the most likely weapon to be used for attacks in the United States. This judgment was based on current intelligence reporting and considered current initiatives taken by TSA and other DHS components, including USCG, and Customs and Border Protection (CBP), to protect the U.S. maritime domain.

— (U//FOUO) NCTC analysis of attack trends contained in the Worldwide Incident Tracking System supports the view that terrorists would most likely use bombings or combined-arms attacks to target passenger vessels. Small boat WBIEDs or vehicle-borne IEDs, used by themselves or in conjunction with combined-arms attacks or other tactics, would most likely be used to target other types of moored or slow-moving vessels, particularly those with restricted maneuverability, and fixed coastal facilities.

(U//FOUO) **WBIEDs.** Al-Qa'ida's ability to conduct a small boat WBIED attack against the United States or Canada probably remains limited. Challenging environmental factors, the group's inability to recoup lost maritime terrorism expertise, logistical support demands, and a sensitive and engaged American maritime community all combine to reduce the potential for the operational transferability of small boat WBIEDs to U.S. and Canadian waters.* Still, if a small boat WBIED attack were to occur, analysis of past attacks overseas suggests that a high-speed small boat—30 feet long or less—would be the most likely to be used.

(U) Soft Targets, Small Arms, and the Maritime Domain

(U//FOUO) In the maritime domain, passenger vessels and supporting terminals have both economic and symbolic significance and typically require unfettered access for traveling passengers, making them difficult to secure. We assess that bombings and small arms attacks—the most frequently demonstrated and easily transferable—are the most likely scenarios for these types of targets.

— (U//FOUO) In 2010 the Abdullah Azzam Brigades' (AAB's) unprecedented nighttime WBIED attack on the *M/V M. Star* leaving the Strait of Hormuz suggests that core al-Qa'ida may be relying more on the initiative and maritime expertise of its affiliated groups and violent extremist cohorts for these types of attacks—a judgment based on analysis of Salafi violent extremist-based maritime plots and circumstantial evidence of aspirational intent observed since 2003.

— (U) In 2005, al-Qa'ida plotted a WBIED attack against an Israeli cruise ship in the port of Antalya, Turkey. The plot failed when the bomb-making materials exploded in the terrorists' apartment.

— (U) In 2004, a WBIED attack attempt against a coastal facility occurred in Iraq. Al-Qa'ida's attempted WBIED attack on the al-Basrah Oil Terminal was disrupted by the U.S. Navy and Iraqi security forces.

— (U//FOUO) Non-compliant recreational boaters and differing U.S. and Canadian boating regulations pose significant challenges for U.S. and Canadian law enforcement and harbor security professionals, a situation that may play to the advantage of criminals and terrorists alike.

(U) Summary of WBIED Attacks and Plots Based on Size and Speed of Vessel

WBIED Vessel Size	Type of Approach	Number of Attacks/Plots
< 30 feet long	High speed ingress >30 knots	**10**
	Aggressive 15-30 knots	**2**
	Slow < 15 knots	**1**
	Aggressive 15-30 knots	**1**
30-65 feet long	Slow < 15 knots	**2**

UNCLASSIFIED//FOR OFFICIAL USE ONLY

* (U) Transferability is defined as the likelihood that an operational capability that has been used successfully in one environment can be similarly used by an adversary with equal effect in a different locale.

(U//FOUO) Historical analysis of WBIED attacks and disrupted plots overseas suggests that terrorists are most likely to favor tactics that leverage small vessel speed and maneuverability and the element of surprise. Following the attack against the *USS Cole*, maritime terrorists are less likely to rely heavily upon deceptive tactics—particularly against alerted, potentially armed targets. The July 2010 attack against the *M/V M. Star* was assumed to be a small boat WBIED travelling at 30 knots or greater.

(U) Why Small Boat WBIED Attacks Have Not Occurred in the U.S.-Canada MTS

(U//FOUO) Although small boat WBIEDs have been used by transnational terrorists in past overseas attacks, we assess there are significant impediments to transferring the same level of capability within U.S.-Canada maritime environs, including:

- (U//FOUO) The unsuitability of most homemade explosives in maritime attacks. Chemical instability caused by water contact and the mixture's shock sensitivity encourages attackers to rely upon much harder-to-acquire, tightly controlled commercial- or military-grade explosives.
- (U//FOUO) Foreign terrorists must be sufficiently acclimated to the local maritime environs. Failure to suitably "blend in" or engaging in unusual activities attracts unwanted attention from local recreational boaters, marina and port operators, commercial mariners, and law enforcement personnel plying our waterways. Community-based policing and other efforts, such as the USCG's America's Waterways Watch and the RCMP's Coastal/Airport Watch Program, encourage citizens to report suspicious behaviors to law enforcement authorities—programs that don't exist in areas of past maritime attacks overseas.
- (U//FOUO) The effective governance and rule of law within the U.S.-Canada maritime domain—particularly compared to greater permissiveness in maritime operational environments found overseas where WBIED attacks have been conducted.
- (U//FOUO) The contrasting attractiveness of other more transferable and reliable terrorist tactics, techniques, and procedures against potentially more lucrative targets in non-maritime critical infrastructure and key resource sectors.
- (U//FOUO) The low success rate of maritime attacks vis-a-vis the significant commitment and expenditure of terrorist group and state sponsor resources.
- (U//FOUO) The environmental challenges associated with any maritime activity—regardless of the level of nautical mariner skills within a terrorist cadre.

(U//FOUO) Rampant piracy and maritime lawlessness occurs within sight of land off the coast of Somalia. Yemen's coast, the scene of the two most successful small boat WBIED attacks attributed to al-Qa'ida, also suffers from a paucity of maritime law enforcement or military presence, fostering an operationally-permissive environment for maritime terrorists. Al-Qa'ida's initial WBIED plot against *USS The Sullivans* failed when the overloaded boat sank during launch; however, the lack of effective law enforcement may have allowed Abdul al-Rahim al-Nashiri and his cohorts to retrieve everything for the eventual successful attack against the *USS Cole* 10 months later.

(U) Statistically, seaborne suicide attacks against ships by small boat WBIEDs are the most frequent of all known acts of maritime terrorism, according to Lloyd's Marine Intelligence Unit (MIU). There have been repeated attempts to attack Western—usually U.S.—warships in the Persian Gulf, Arabian Sea, and the Strait of Gibraltar. Only the October 2000 small boat WBIED attack on the *USS Cole* was successful. All other attempts failed due to technical problems or law enforcement disruption. Similar attacks against commercial shipping resulted in the successful attack against a tanker (*M/V Limburg*) in October 2002 and a marginally successful attack against the *M/V M. Star* in July 2010. Other WBIED plots against Iraqi coastal oil facilities and Israeli cruise ships were interdicted or disrupted by military or security forces and law enforcement.

(U//FOUO) Terrorist Groups or Individuals May Threaten the MTS

(U//FOUO) Al-Qa'ida and its affiliates have demonstrated over the last decade both the intent and capability to attack Western maritime interests in the eastern hemisphere and probably pose the greatest threat to the MTS. Al-Qa'ida for years has publicly emphasized attacking Western economic targets, including maritime shipping, and recent intelligence reporting continues this theme. While we have no reporting that these groups WBIED and more advanced maritime capabilities extend to North America, vulnerable elements in the MTS—such as passenger vessels and terminals—could attract the attention of less capable terrorists.*

(U) Al-Qa'ida or Regional Affiliates' Attacks and Plots Against Maritime Targets

WBIED ATTACKS				
Year	**Intended Target**	**Location**	**Terrorist Group**	**Notes**
2010	First nighttime WBIED attack attempt against vessel	*M/V M. Star*	Abdullah Azzam Brigades	Failed WBIED attack against Japanese oil tanker leaving Strait of Hormuz.
2005	Last known WBIED attack plan	Israeli cruise ship	Al-Qa'ida	WBIED plot in port of Antalya, Turkey failed when bomb-making materials exploded in operative's apartment.
2004	Last known WBIED attack attempt against coastal facility	Oil terminals in Iraq	Al-Qa'ida	WBIED attempt on the al-Basrah Oil Terminal and Khawr al Amaya Oil Terminal disrupted by the U.S. Navy and Iraqi Security Forces assets.
2002	Last known successful daylight WBIED attack against vessel	*M/V Limburg*	Al-Qa'ida	WBIED detonated as vessel neared Yemen's Ash Shihr Oil Terminal.
IED & COMBINED ARMS ATTACKS				
Year	**Intended Target**	**Location**	**Terrorist Group**	**Notes**
2006	Last known attempt on a U.S. or Canadian maritime target	Canadian oil refinery in Yemen	Al-Qa'ida in Yemen (now al-Qa'ida in the Arabian Peninsula)	VBIED and armed assault against oil refinery at the Al-Dhaba Port, Yemen. Port security forces destroyed the VBIED as it approached the port.
2005	Last known successful attack on a maritime target	Port of Dellys, Algeria	The Salafist Group for Preaching and Combat (now al-Qa'ida in the Islamic Maghreb)	Two IEDs detonated in the port of Dellys, Algeria: one targeted an Algerian Coast Guard vessel and the second a land route used by emergency responders.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

* (U) More advanced maritime capabilities include small vessels, scuba diving attacks, and attempted non-suicide attacks relying on IEDs.

— (U) The *M/V M. Star*, a Marshall Islands-flagged supertanker owned by Mitsui O.S.K. Lines of Japan, suffered hull damage to the starboard stern area as a result of a probable WBIED attack around midnight local time on 28 July 2010 as the ship was outbound from the Strait of Hormuz. A statement from Yusuf al-Uyayri and the AAB claiming responsibility for the attack was posted on the al-Fallujah Islamic Forums on 3 August. Al-Uyayri stated the attack was an "episode" in their violent jihad to weaken the world order of non-belief that dominates and oppresses Muslims.*

(U//FOUO) Damage from suspected nighttime WBIED attack against *M/V M. Star* in the Strait of Hormuz.

— (U//FOUO) Until the nighttime small boat WBIED attack targeting the *M/V M. Star* in July 2010, there was no evidence suggesting al-Qa'ida or its cohorts had been planning maritime attacks since the thwarted plot by Luai Sakr aka Ekrem Oezer to attack Israeli cruise ships visiting Turkey in 2005.

— (U//FOUO) Al-Nashiri, suspected mastermind behind al-Qa'ida's attacks against the *USS Cole* and *M/V Limburg*, has been in U.S. custody since 2002.

* (U//FOUO) The AAB, which is also known as the Battalion of the Martyr Abdullah Azzam or the al-Qa'ida Organization in the Levant and Egypt, is a Sunni violent extremist group based primarily in Egypt, Jordan, and Syria and is most often associated with Abdullah Azzam, a mentor of Usama bin Ladin and a leader in the modern violent jihadist movement. Attacks perpetrated or claimed by the group usually involve tourist targets in Egypt, relatively sophisticated bombs, meticulous planning, and coordinated attacks. The group is responsible for bombing several Sinai resorts in 2004, resulting in 34 deaths. In July 2005, a series of car bombings in Sharm al-Shaykh was also believed to be the work of the AAB—killing 88 and wounding over 200.

(U//FOUO) **Homegrown Violent Extremists.** The number of HVEs inspired by violent Islamist propaganda is increasing in both the United States and Canada, but we have no indications of plots involving North American maritime targets. Although violent radicalization of certain Muslims within Canada is viewed as a relatively recent phenomenon, the Royal Canadian Mounted Police (RCMP) is concerned about HVEs targeting Canada and its allies. The RCMP assesses, for example, that terrorist supporters in Canada's Muslim, Tamil, and Sikh communities raise funds and spread propaganda for terrorist groups.

(U//FOUO) **Lebanese Hizballah.** This group probably has more advanced maritime attack capabilities than any other terrorist organization, but is unlikely to launch attacks in the United States or Canada. Hizballah remains focused on resistance against Israel, and this group will probably not consider direct attacks on U.S. interests outside the Middle East unless it perceives a direct threat to itself or Iran. Additionally, we have no indication that Hizballah has an adequate logistical support infrastructure to use its maritime capabilities in the United States or Canada.

— (U//FOUO) Hizballah also has extensive experience in maritime smuggling. Since at least 1982, the group has used a variety of vessels and unique delivery means to have weapons shipped covertly from Iran to Lebanon.

(U//FOUO) **Violent Domestic Extremists.** These groups, typically motivated by myriad racial, ethnic, anti-governmental, or socio-economic issues, have demonstrated little interest and capability to attack maritime targets. The focus of their discourse and actions do not suggest increased interest in targeting the maritime sector. The few attacks that have occurred have been broadly spaced in time and by group.*

— (U//FOUO) In January 2011, the violent environmental rights extremist group Earth Liberation Front claimed responsibility for vandalizing at least a dozen commercial fishing boats at a boatyard in Plymouth, Massachusetts.

— (U//FOUO) In 2006, the FBI reported an alleged plot by an alleged member of the Black Hebrew Israelites, a violent black supremacist movement, to sabotage military ships in the Norfolk, Virginia area.

(U//FOUO) According to the nongovernmental organization Southern Poverty Law Center[USPER], an animal rights extremist group claimed responsibility for attempting to sink a 21-foot boat belonging to a targeted bank executive in Sands Point, New York on 24 July 2001. Anonymous mass communiques claimed that several holes were drilled in the executive's yacht before it was set adrift.

* (U//FOUO) For the purposes of this assessment, domestic terrorism refers to U.S. or Canadian citizens associated with violent extremism within their home country and without foreign direction. The legal definition of domestic terrorism as defined in the Homeland Security Act of 2002 states, "Any activity that involves an act committed by a group or individual based and operating entirely within the United States or its territories without direction or inspiration from a foreign terrorist group that is dangerous to human life or potentially destructive of critical infrastructure or key resources, and is in violation of the criminal laws of the United States or of any state or other subdivision of the United States and appears to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion or to affect the conduct of a government by mass destruction, assassination, or kidnapping."

(U//FOUO) **Lone Offenders and Usurped Insiders.** Some American and Canadian employees in the maritime industry use their MTS access for criminal purposes. We share the consensus view of the Intelligence Community and law enforcement community that fringe elements of known violent extremist groups, recently-terminated employees, or even mentally unstable individuals may conduct independent, maritime-related attacks to support their cause or to avenge their grievances. The threat potential is difficult to gauge because very few people, if any, know of the intent and capabilities of these individuals, further complicating law enforcement efforts to detect or interdict their plots.

(U) Other Maritime Border Issues of Concern

(U//FOUO) The MTS faces several other vulnerabilities, including abuse of the crewman visa program, smuggling, cyber threats, and WMD and HAZMAT threats.

(U//FOUO) **Crewman Visa Program.** Issuance of mariner visas continues to pose potential security risks. Once obtained, mariner documents can be used to gain illicit entry into the United States or Canada. Improved fraud detection and information sharing between U.S. and Canadian authorities are needed, according to a series of assessments conducted by the U.S. Human Smuggling and Trafficking Center.

- (U//FOUO) C-1/D visas, issued by the United States to foreign mariners seeking entry to join their ship, can be fraudulently obtained with false letters or contracts from front companies. Since 2006, CBP has identified widespread fraud by Pakistani aliens using mala fide C-1/D crew visas, aided by human smugglers exploiting the overseas visa application process.

(U//FOUO) **Smuggling.** The Great Lakes region is an area of concern for maritime smuggling of drugs, guns, people, and contraband such as cigarettes. The region encompasses more than 1,200 miles of the U.S.-Canada border, with hundreds of isolated islands, ports, and harbors. The United States and Canada have struggled to estimate the scope and scale of smuggling because of limited resources and intelligence gaps. Federal, state, provincial, local, and even tribal agencies with differing jurisdictions, resources, and missions patrol the Great Lakes, complicating enforcement efforts. Regulatory differences, sovereign territory, and privacy laws continue to challenge the collection and dissemination of intelligence among and between U.S. and Canadian law enforcement agencies.

- (U//FOUO) The high volume of commercial and recreational activity on the Great Lakes allows maritime smugglers to conceal themselves amongst legal traffic, making it difficult for law enforcement to identify and interdict them.

- (U//FOUO) The absence of uniform and centrally shared data on small vessel reporting and port arrivals, which currently are based on voluntary, unverified information, makes the magnitude of cross-border traffic difficult to determine.

(U//FOUO) Criminals in small boats can take advantage of the region's extensive and remote tribal shorelines and many islands to smuggle contraband. The Bureau of Indian Affairs (BIA) has specifically identified two federally recognized tribal areas—the Saint Regis Mohawk Reservation along the Saint Lawrence Seaway in New York and the Makah reservation in Washington—as having significant narcotics-smuggling activity, some of which is known to involve small boats.[*]

[*] (U) The BIA 2009 cost estimate for a program to combat drug trafficking on Indian lands along the U.S. northern and southern borders was $3 million annually.

— (U//FOUO) The Saint Regis Mohawk Reservation has a history of exploitation from smugglers on both sides of the border. According to recent U.S. and Canadian open source reporting, maritime smuggling of untaxed cigarettes, high-potency marijuana, and MDMA (ecstasy) continues.

— (U//FOUO) The extent of cross-border contraband-smuggling activity affecting tribal areas is a significant information gap. Although we have medium confidence that the incidence of human smuggling in these areas may have declined significantly since 2001—an estimate largely based on anecdotal law enforcement observations and limited CBP alien apprehension data, such as that involving the Saint Regis Mohawk Reservation dated to the 2000 to 2008 timeframe—the possibility of illegal maritime entry by migrants, criminals, or would-be terrorists cannot be discounted. Historically, these areas have drawn the attention of cross-border smugglers in small boats; however, contraband transfer is the typical modus operandi, according to BIA and I&A analysis of available law enforcement data. Human smuggling across tribal areas along the U.S.-Canada border appears to be much less prevalent, but our assessment is based on extremely limited information.

(U//FOUO) **Cyber Threats.** Cyber threat to North America's port infrastructure probably is low because of the complexity required for mounting a successful attack and the limited effect from disabling any single information technology system in the MTS. Nevertheless, individuals with direct system access still pose the highest non-state cyber threat to port facilities. A co-opted or disgruntled employee—especially one with privileged or administrator system access to sensitive data or process controllers within a coastal facility—may pose a threat to safety or security at a port or other interrelated infrastructure. Additionally, an insider does not necessarily have to damage or disrupt port operations, but can provide useful information to an adversary—wittingly or unwittingly.

— (U//FOUO) No confirmed reporting has altered the judgments made in the 2009 FBI-DHS-USCG joint assessment on the Cyber Threat to U.S. MTS.

(U//FOUO) **WMD and Weaponization of HAZMAT.** Among the greatest potential vulnerabilities to the U.S.-Canada MTS is the introduction of WMD into or through our ports, or via interconnected intermodal means, with the intent to attack the port or targets further inland.[*] Although this remains a high-impact, low-probability scenario, we are increasingly concerned that al-Qa'ida's expressed aspiration to use WMD against the United States may cause the group to pursue an evolutionary strategy of using improvised HAZMAT weapons or TICs against coastal populations or nearby industrial and military facilities.

— (U//FOUO) Should a group acquire a functional WMD, maritime conveyances such as bulk shipments, vessels of trusted shippers, small boats, or commercial or service vessels under 300 gross weight tons may serve as a viable means of transport because maritime conveyances have only limited international oversight and reporting requirements.[†]

[*] (U//FOUO) The greatest observed maritime threat remains smuggling, including special interest aliens with ties to international terrorism and illicit materials.
[†] (U) These vessels are not required to carry automatic identification system equipment in U.S. or Canadian waters.

— (U//FOUO) HAZMAT storage areas are ubiquitous, and shipments occur daily throughout the MTS. Intermodal connectors, modes, and facilities are all prospective terrorist targets. Shipments of TICs, especially highly-combustible fuels and inhalation hazards, present attractive targets for terrorists because they have multiple vulnerability points and their unregulated dispersal could incapacitate, kill, or create widespread panic.*

— (U) Terrorists in Iraq, the Balkans, Chechnya, Sri Lanka, and the Levant have used HAZMAT and TICs—particularly chlorine—against various targets with varying degrees of impact from creating panic to maiming and killing people.

(U//FOUO) Al-Qa'ida has maintained an enduring interest in creating and using improvised biological and chemical weapons on a limited scale for decades, and terrorists have achieved some familiarity with their effects. Concerns about terrorist use of larger quantities of TICs and other HAZMATs are well founded given past attacks overseas.†

— (U) According to a study on toxic warfare, al-Qa'ida has demonstrated interest in toxic warfare over the past two decades. The group has experimented with cyanide gas at its Derunta, Afghanistan facility and plotted to conduct gas attacks in Europe prior to 2002.

(U) Chlorine and Other TICs Remain Attractive to Terrorists and Insurgents

(U//FOUO) Many chemicals produced for industry are inherently dangerous because of one or more of the following characteristics: reactivity, flammability, explosiveness, toxicity, or carcinogenicity. In particular, anhydrous ammonia, hydrogen fluoride, sulfur dioxide, and elementary chlorine can quickly create a toxic gas plume that is capable of inflicting catastrophic loss of life amongst any population in its path.

(U//FOUO) Chlorine is one of the 10 most-produced chemicals and is used by water treatment plants, hospitals, PVC manufacturers, and other industrial users. The chemical was weaponized for use as a choking agent during World War I. In Iraq, insurgents have used bombs rigged to chlorine cylinders, as have other insurgents in the Balkan, Chechen, and Sri Lankan conflicts in an effort to heighten impact. Chlorine and other inhalation-hazard TICs remain attractive to terrorists because they require no additional processing to be employed as a potential mass-casualty weapon, and their use amplifies the media coverage and fear of an attack.

(U) Recent DHS Actions to Mitigate Most Likely Maritime Threats

(U) In addition to the America's Waterways Watch program and ongoing risk mitigation measures by the USCG, TSA's Visible Intermodal Prevention and Response (VIPR) teams have expanded into the ferry and passenger rail transportation systems. VIPR teams have recently been deployed in support of various ferry operations in the United States, especially during periods of seasonably high ridership.

* (U) This includes cargoes such as liquefied natural gas and liquefied petroleum gas, the potential vulnerability of which remains a concern for communities near product processing facilities.
† (U//FOUO) According to I&A and FBI analysis, at least 14 chlorine thefts occurred in the United States between 2003 and 2008.

(U) In 2009, and in cooperation with the USCG, TSA implemented and offered "Ferry Watch" to key stakeholders, encouraging passenger awareness and reporting of concerns to appropriate authorities. The Staten Island, Washington State, and Golden Gate ferry systems already have similar programs. The Cape May, New Jersey–Lewes, Delaware and Galveston, Texas–Bolivar, Texas ferry systems are also implementing this initiative. The Bridgeport, Connecticut–Port Jefferson, New York ferry lines are considering implementation.

(U) Factors to Lessen MTS Vulnerabilities

(U//FOUO) Improved collaboration between U.S. and Canadian officials and law enforcement personnel has the potential to reduce MTS vulnerabilities to terrorism or criminal activity. Such measures might include:

- (U//FOUO) Bringing U.S. and Canadian marine safety, recreational boating, and port security regulations into closer alignment.
- (U//FOUO) Coordinating information between U.S. and Canadian law enforcement agencies concerning the issuance of crew visas to foreign mariners bound for U.S. and Canadian ports. Such information sharing could include improved biometric characteristics of crew visas and fraud detection.
- (U//FOUO) Continued development and deployment of technologies and resources that passively increase the situational awareness of transit riders and employees—particularly the detection and reporting of suspicious activities—as a means to strengthen the security of the passenger vessels.
- (U//FOUO) Expanding the "ship rider" program to improve the effectiveness of maritime law enforcement operations on North American waterways.
- (U//FOUO) Establishing an efficient, jointly U.S. and Canadian accessible, electronic dissemination system for maritime suspicious activity reports.
- (U//FOUO) Coordinating the vetting and sharing of information related to the U.S. Transportation Worker Identification Credential System and parallel Canadian waterfront and marine employee vetting and credentialing processes.
- (U//FOUO) Expanding the sharing of risk-determination data for cargo, vessels, operator, and passenger screening between U.S. and Canadian customs and other maritime law enforcement agencies.
- (U//FOUO) Assessing technologies that will improve situational awareness through Global Maritime Intelligence Integration, particularly those initiatives that apply to the Automatic Identification System "transponder gap" vessels under 300 gross weight.
- (U//FOUO) Expanding the role of tribal law enforcement within the Integrated Border Enforcement Teams and in operations to secure coastlines within Indian Country.

(U) Reporting Notice:

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to the nearest State and Major Urban Area Fusion Center and to the local FBI Joint Terrorism Task Force. State and Major Urban Area Fusion Center contact information can be found online at http://www.dhs.gov/contact-fusion-centers. The FBI regional telephone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm and the DHS National Operations Center (NOC) can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) For comments or questions related to the content or dissemination of this document, please contact the I&A Foreign Disclosure Office at dhsforeigndisclosureoffice@hq.dhs.gov.

(U) I&A would like to invite you to participate in a brief customer feedback survey regarding this product. Your feedback is extremely important to our efforts to improve the quality and impact of our products on your mission. Please click below to access the form and then follow a few simple steps to complete and submit your response. Thank you.

Survey

(U) Tracked by: HSEC-8.1, HSEC-8.4.2, HSEC-8.4.2.17, HSEC-8.4.2.18

Appendix A

JIOCEUR Analysis Center
Intelligence Directorate Counterterrorism/Counterintelligence, IDX

05 January 2009

(U) Terrorist Tactics: Maritime Attacks

(U) This product is derived solely from open source and press reporting and has been approved for release to foreign government officials cooperating with the U.S. in the conduct of official business related to the Global War On Terror (GWOT). Per DoD 5200.1-R (1997). FOUO information should be protected by taking reasonable steps to minimize risk of access (to include posting to the internet) by unauthorized personnel, steps include but are not limited to, storing the information in locked offices, locked drawers, or other equal protection when offices are not manned.

(U//FOUO) Between 2000 and 2005, Islamic Sunni extremists considered, attempted, or executed at least nine different maritime terrorist attacks. Most occurred in the Middle East, with others planned or executed in Europe and Asia.

(U//FOUO) A review of past Islamic extremist maritime terrorist attacks suggests a common operating profile that force protection personnel might use to identify and prevent future attacks. This paper reviews several tactical models terrorists used in maritime attacks or planning.

(U//FOUO) **Attack Models.** Based on data compiled on this report, terrorists prefer using small boats that blend in with the local environment, which are modified to hold significant quantities of explosives to strike static or slow moving targets near ports.

(U//FOUO) Terrorists used or planned to use at least one explosive laden boat in six of the nine cases studied. All of the plans reviewed in this study, whether executed or not, targeted ships or facilities in or near a port, or near the coastline. All of the targets were either stationary or moving slowly. Moreover, while planning generally required several months of preparation, the choice of the final target often appears based on convenience. Further commonalities of these attacks are discussed below. In one of these incidents, simultaneous attacks took place.

(U//FOUO) In two of the nine cases, operatives used improvised explosive devices (IED) either onboard or next to the ship. These two cases suggest operatives carrying IEDs could board commercial vessels in which security is more lax, such as ferries or cruise liners, and conduct an attack, in what would essentially be a maritime version of the train bombings that occurred in Madrid and London.

(U//FOUO) In one of the nine cases, terrorists used stand-off weapons, 107mm rockets, which provided terrorists the ability to operate outside of a security zone established to protect military or civilian vessels or facilities.

(U//FOUO) **Target Selection.** All of the cases involve static or slow moving targets, such as drifting or stationary ships or oil platforms. All of the targets were in a port or coastal area when attacked.

(U//FOUO) **Commonalities of Two Attacks Using Explosive-Laden Boats.** Comparing the successful attacks on USS Cole and M/T Limburg reveals a profile useful for identifying maritime terrorist plots before the attack.

- The attack boats blended into the environment. Witnesses to the Cole and Limburg bombings said they believed the vessels to be fishing boats.
- To offset a heavy load in the front of a small boat, the terrorists added weight to the stern of the boat. The boat used to attack the USS Cole had the hull strengthened was fitted with extra fuel tanks.
- Both attacks took place near major ports. Both target ships were essentially stationary—the USS Cole was moored to a pier and Limburg was drifting towards a mooring buoy.
- Two terrorists piloted the attack boats.

(U) **Case Studies:**

- Singapore Plot—1990s-2001
- Attack on the USS the Sullivans and the USS Cole—2000
- Targeting the Strait of Gibraltar—2001-02
- Attack on the M/T Limburg—Yemen 2002
- Attack on the Superferry 14—Philippines 2004
- Attack on al-Basrah Oil Terminal (ABOT) and Khawr al Amaya Oil Terminal (KAAOT)—Persian Gulf 2004
- Luay Saka and the Antalya Plot—2005
- Attack on the USS Kearsarge and USS Ashland—Jordan 2005
- Attack on Dellys Port, Algeria—2005

UNCLASSIFIED 

(U) Singapore UNCLASSIFIED

(U//FOUO) **Singapore Plot—1990s-2001.** Members of Jemaah Islamiya (JI) in Singapore developed a plan in the 1990s to attack US Navy ships off the coast of Singapore. According to the plot, a small, explosive-laden vessel would attack a US ship traveling eastward from Sembawang Wharf via Pulau Tekong.

UNCLASSIFIED  **(U) Changi Naval Base** UNCLASSIFIED

(U//FOUO) JI identified the narrowest part of the channel and sought to take advantage of topography and geography to conceal the attack vessel from radar and visual detection. However, they shelved the plan due to operational limitations. The plot resurfaced in 2001 when two unidentified Middle Eastern individuals approached JI to learn about US military vessels in Singapore. A JI member conducted reconnaissance of the Changi Naval Base from a ferry that sailed past the base. His conduct on board the ferry attracted the attention of a passenger who reported the operative's behavior and he was later arrested.

UNCLASSIFIED  **(U) Abdul Rahim al-Nashiri and Hassan al-Khamri** UNCLASSIFIED

(U//FOUO) **Attack on the USS The Sullivans and the USS Cole—Yemen, 2000.** As the USS The Sullivans refueled in Aden Harbor on 3 January 2000, a group of men, led by Abdul Rahim al-Nashiri, launched an explosive-laden boat from a nearby beach. Hassan al-Khamri and Taha al-Ahdal were piloting the boat, which sank soon after it got underway. They abandoned the boat, but the next day, Nashiri and others returned to the beach to salvage the boat and the explosives.

(U//FOUO) The cell regrouped and continued planning an attack against a US Navy vessel, including refitting the boat to strengthen the hull and testing the explosives.

(U//FOUO) In the autumn of 2000, the USS Cole was underway to the Persian Gulf for a six-month deployment. En route, she was scheduled to stop in Aden, Yemen for four hours to refuel. The refueling was a routine stop that numerous other ships had made before.

UNCLASSIFIED **(U) Graphic Account of Attack** UNCLASSIFIED

(U//FOUO) The USS Cole reached Aden early on the morning of 12 October 2000 and moored at an offshore refueling pier. A boat approached the USS Cole in a straight line from the shore where a crane had placed it in the water. A sailor standing high up on the destroyer watched the boat approach. Ibrahim al-Thawr and al-Khamri, the two suicide bombers, waved at the sailor and he waved back. The boat pulled alongside the Cole and detonated more than 600 lbs. of explosives. The explosion tore a 40-foot hole in the ship's side, killing 17 sailors and injuring another 42.

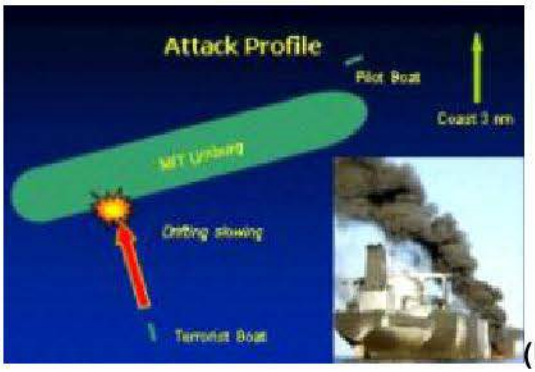
(U//FOUO) **Targeting the Strait of Gibraltar—2001-2002.** Following his success with the USS Cole plot, Nashiri conceived of a maritime terrorist attack in the Strait of Gibraltar (STROG) sometime before 11 September 2001 and initiated the plan in Afghanistan about December 2001. Three Saudi operatives who had trained in al-Qaida camps in Afghanistan traveled to Morocco to plan the attack.

UNCLASSIFIED **(U) Gibraltar** UNCLASSIFIED

(U//FOUO) The three operatives arrived in Morocco in February 2002 to reconnoiter the region. The team's leader, Zuhayr Hilal al-Thabiti, maintained e-mail contact with al-Nashiri from an internet café in Rabat, located east of al-Mukkala. The team traveled around Morocco and to the Spanish enclaves of Ceuta and Melilla along the northern coast of Morocco. The original plan called for a second group of operatives to enter Morocco to carry out the attack from Ceuta or Melilla. It is unknown if the conspirators

traveled to Gibraltar itself; the northern coast of Ceuta is only 12 nautical miles (22 km) from the port of Gibraltar.

(U//FOUO) According to an 18 June 2002 statement from a Moroccan prosecutor, Nashiri's plan involved suicide bombings of US or British Navy ships in the STROG or anchored there.

UNCLASSIFIED 

(U) Illustration of Small Boat Attack UNCLASSIFIED

(U//FOUO) **Attack on the M/T Limburg—Yemen 2002.** The oil tanker M/T Limburg arrived near the Ash Shihr Oil Terminal, off the coast of Yemen, at 1400 on 4 October 2002. The ship was not due at the offshore loading buoy until 6 October, so the captain allowed her to drift in the current to carry her slowly north to the buoy for its scheduled arrival.

(U//FOUO) As the pilot boat approached from the port side, a crewmember reported seeing a second small boat traveling at high speed toward the M/T Limburg's starboard side.

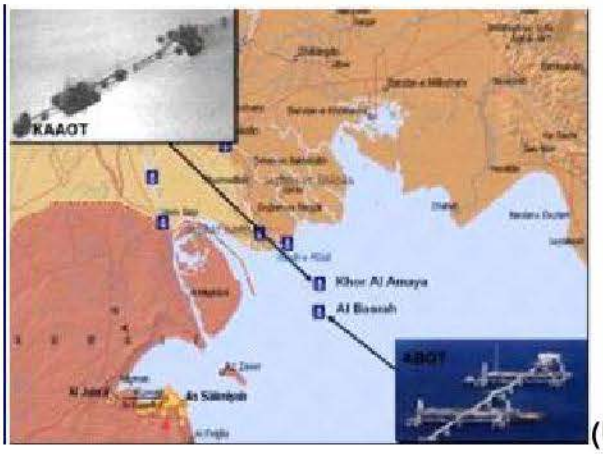
(U//FOUO) When the terrorist boat hit, the explosion blew a hole in the side of Limburg and burning crude oil spilled out into the water. The crew could not extinguish the fire and eventually 12 crewmembers jumped overboard to escape the fire. One drowned.

(U//FOUO) The explosion tore a hole approximately 11 meters high by eight meters wide in the outer hull, tore a hole in the cargo tank, and ignited the crude oil, which burned as it spilled in the water.

UNCLASSIFIED 
(U) Superferry UNCLASSIFIED

(U//FOUO) **Attack on Superferry 14—Philippines 2004.** In the February 2004 attack on Superferry 14 in the Philippines, Redondo Cain Dellosa, an Abu Sayyaf Group (ASG) member, placed an IED on-board the ship and disembarked before the ferry cast off.

(U//FOUO) Between 60 and 90 minutes after the ferry pulled out of Manila, the explosives—eight pounds of TNT packed into a television—detonated and started a fire that engulfed the ship and killed more than 100 passengers and crew. There are indications that the ASG conducted surveillance and reconnaissance prior to the operation. The group's leader said that before they conducted the operation, he personally studied the layout of a similar Superferry, including the placement of an escalator, guards, and a tourist-class room.

UNCLASSIFIED 

(U) ABOT and KAAOT Locations UNCLASSIFIED

(U//FOUO) Attack on al-Basrah Oil Terminal (ABOT) and Khawr al Amaya Oil Terminal (KAAOT)—Persian Gulf 2004. On 24 April 2004, terrorists conducted a maritime attack on the al-Basrah Oil Terminal (ABOT) and the Khawr al Amaya Oil Terminal (KAAOT), just off the coast of Iraq in the Persian Gulf

(U//FOUO) The attack developed late in the day when, at 1700 local time, a dhow approached the two nautical mile exclusion zone around the KAAOT. A US Navy coastal patrol ship in the area, USS Firebolt, launched a boarding team in a RHIB boat. As the boarding team approached the dhow, it exploded. The explosion killed three sailors, two from the US Navy and one US Coast Guardsman.

(U//FOUO) Twenty minutes later, two speedboats entered the two nautical mile exclusion zone established around the ABOT. Iraqi security forces on the terminal opened fire on the boats and both exploded about 50 meters away. At the time of the attack, the Japanese crude oil tanker Takasuzu was alongside fully loaded. Another tanker, the Apollo, was waiting to load.[21] Two other tankers were also present at the terminal. After the attack boats detonated, debris from them was found on the decks of tankers at the ABOT terminal, indicating the boats came very close to successfully hitting the terminal. The explosions damaged living quarters, several electrical generators, and some minor installations.

(U//FOUO) The ABOT and KAAOT facilities closed briefly after the attack. On Monday, 26 April 2004, al-Qaida in Iraq leader Abu Musab al-Zarqawi published on an Islamist web site a signed statement claiming responsibility for the attack.

(U//FOUO) **Luay Saka and the Antalya Plot— Turkey 2005.** On 4 August 2005, an explosion rocked an apartment in Antalya, Turkey, which was rented by al-Qaida operative Luay Saka. A Syrian-born extremist, Saka was wanted in connection with the November 2003 Istanbul bombings. Police arrested him on 6 August 2005 at Diyarbakir Airport attempting to flee Turkey. In addition to the bomb-making material, police found falsified documents for Saka from Syria, Turkey and Tunisia. Police later arrested Hamed Obysi, who was assisting Saka in a plot to attack an Israeli cruise ship due to come into port in Antalya.

UNCLASSIFIED  **(U) Luay Saka** UNCLASSIFIED

(U//FOUO) The explosion occurred while Saka was preparing to build a bomb for use against one or more Israeli cruise ships in the Antalya port or in international waters off the coast of Turkey (Saka's statements have varied). In other statements, Saka claimed that if he were not able to find an Israeli cruise ship, that he would target any nearby NATO vessel. Plans for the bomb appeared to include a peroxide based detonator. Police found 13 pounds of C-4 explosive among Saka's possessions. Saka had purchased a cabin cruiser to use as either his attack vehicle or a platform from which to launch his attack.

UNCLASSIFIED  **(U) Saka's Yacht** UNCLASSIFIED

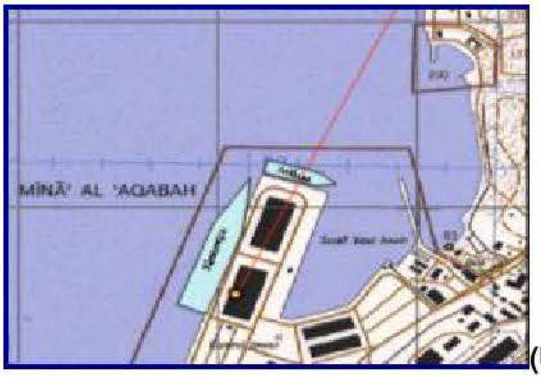
(U//FOUO) After his arrest and during the trial, Saka, who fought in Fallujah with Abu Musab al-Zarqawi, said he volunteered to conduct a strike on Israeli cruise ships in Antalya. This was, in part, because he believed US soldiers used the vessels for rest and relaxation, according to Saka's attorney.

(U//FOUO) Saka claimed that at the time of the fire, he was one to two days from conducting the operation. He said he intended to complete the bomb's construction on board his boat and carry out the attack.

(U//FOUO) **Attack on USS Kearsarge and USS Ashland—Jordan 2005.** On 19 August 2005, extremists fired three Katyusha rockets from the second floor of a

warehouse on a hillside in Aqaba, Jordan overlooking the port. One nearly hit the USS Kearsarge and USS Ashland.

(U//FOUO) According to Jordanian prosecutors, the group initially planned to attack US Embassy in Amman, Jordan, but changed their minds, electing to hit the Israeli port of Eilat. When the two American ships arrived in port on 13 August for a training exercise with the Jordanian navy, the extremists altered their plans.

UNCLASSIFIED 

(U) Approximate Path of Rocket UNCLASSIFIED

(U//FOUO) The group fired three rockets via remote control. One flew over the bow of the Ashland, struck a warehouse and killed a Jordanian soldier. The second landed on the grounds of Eilat Airport in Israel, while the third landed on the grounds of a Jordanian hospital. Investigators reportedly found four other rockets abandoned in the workshop. According to one press account, three Iraqis allegedly involved in the attack had made their way past Jordanian security checkpoints from Aqaba to Amman and eventually crossed the Iraqi border.

UNCLASSIFIED 
(U) Dellys Port, Algeria UNCLASSIFIED

(U//FOUO) Attack on Dellys Port, Algeria—2005. On 23 December 2005, members of the Salfast Group for Preaching and Combat (GSPC) detonated two IEDs in the port of Dellys, killing one and wounding 13. One IED exploded on or next to an Algerian coast guard vessel. The second exploded several minutes later along a land route near the quay, causing injuries to responders. The IEDs were reportedly remotely detonated. The GSPC claimed responsibility for the attack on its website.

POC: NCIS/IDX-CI, DSN 268-1113

Appendix B

ROLL CALL RELEASE

In Collaboration with the ITACG

16 August 2010

(U//FOUO) Indicators of Suspicious Activity in the Maritime Domain

(U//FOUO) Terrorists overseas have conducted maritime operations to support or carry out attacks, using vessels to infiltrate, conduct surveillance, and deliver explosive materials or devices. Similar operations could be conducted in the United States. Personnel working on or along waterways should be vigilant for suspicious activities and report them to local law enforcement, a Joint Terrorism Task Force, or a state and local fusion center.

(U) **Possible Indicators of Suspicious Maritime Activity:** Based on the specific facts or circumstances, the presence of one or more of these indicators may represent suspicious maritime activity:

- (U) Vessels operating outside normal areas, such as fishing boats outside normal fishing grounds.
- (U) Unusual departure or arrival times at berths.
- (U) Attempts to enter or loiter near restricted areas or sites.
- (U) Recreational vessels operating outside normal boating times or locations, or during inclement weather.
- (U) Vessels traveling at night with navigation lights off.
- (U) Vessels which appear to be overloaded, or tarps covering parts of the boat or cargo.
- (U) Unusual activity regularly occurring after normal boating hours at private or public marinas.
- (U) Excessive or unusual equipment on deck, such as fuel barrels, inflatable rafts or communications gear, or lack of proper equipment, such as buoys, transponders, or life-saving equipment.
- (U) Vessels with oversized motors or unusual modifications.
- (U) Vessels carrying excess crew.
- (U) Lack of familiarity with a vessel's standard operations, or failure to obey navigation rules.
- (U) Note-taking or sketching, or use of cameras, video recorders, or binoculars near infrastructure, military bases, bridges, and other potential targets.
- (U) Large cash payments for fuel, slip rental, or other services.
- (U) Continuous presence of operator or crewmembers onboard or nearby.
- (U) Presence and apparent use of makeshift boat ramps.
- (U) Attempts to alter charter routes or destinations.
- (U) Attempts to abandon a vehicle aboard a ferry and walk ashore.
- (U) Consecutive roundtrips aboard a ferry, possibly reflecting surveillance.
- (U) Questions regarding schedules, passenger capacities, onboard safety procedures and equipment, and proximity to critical infrastructure.

(U) **Example of Terrorist Maritime Activity:** In November 2008, terrorists came ashore in Mumbai, India aboard small boats and launched attacks across the city. Authorities missed a number of opportunities to interdict the attackers before they came ashore. The attacks killed 166 and injured 293.

(U) For additional information please see the DHS/USCG Intelligence Coordination Center's National Maritime Threat Assessment, 7 January 2008 and "Potential Maritime Threat Indicators: Law Enforcement," 15 April 2009, or visit ameraicaswaterwaywatch.org.

IA-0415-10

(U) Prepared by the DHS/I&A Homeland Counterterrorism Division, the DHS/I&A Cyber, Infrastructure, and Science Division, the FBI/Directorate of Intelligence, and the Interagency Threat Assessment and Coordination Group. This product is intended to assist federal, state, local, and private sector first responders in developing deterrence, prevention, preemption, or response strategies. Coordinated with the USCG.

CLASSIFICATION: **UNCLASSIFIED//FGI CAN//FOR OFFICIAL USE ONLY**

Office of Intelligence and Analysis

I&A Customer Survey

Product Title: (U//FOUO) United States-Canada Marine Transportation System: Terrorist Threat Remains Low but Risks Persist

1. Please select the partner type that best describes your organization. Select One

2. How did you use this product in support of your mission?

- ☐ Integrated into one of my own organization's finished information or intelligence products
- ☐ Shared contents with federal or DHS component partners
  - If so, which partners?
- ☐ Shared contents with state and local partners
  - If so, which partners?
- ☐ Shared contents with private sector partners
  - If so, which partners?
- ☐ Other (please specify)

3. Please rank this product's relevance to your mission. ***(Please portion mark comments.)***

- ○ Critical
- ○ Very important
- ○ Somewhat important
- ○ Not important
- ○ N/A

4. How could this product or service be improved to increase its value to your mission? ***(Please portion mark comments.)***

5. Was this product provided to you in response to a specific request to DHS I&A? **Yes** **No**

6. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Timeliness of product or support	○	○	○	○	○
Responsiveness to your intelligence needs	○	○	○	○	○
If you answered yes to question 5, please rate your satisfaction with DHS I&A's communication during the processing of your request	○	○	○	○	○

To help us understand more about your organization so we can better tailor future products, please provide:

Your Name and Position

Your Organization

Your Contact Number or Email

Submit Feedback

Notice to DHS I&A Customers

CLASSIFICATION: **UNCLASSIFIED//FGI CAN//FOR OFFICIAL USE ONLY**

Paperwork Reduction Act Compliance Statement

Legal Significance of Office of Management and Budget Control Number: Your response to this feedback request is completely voluntary. The Paperwork Reduction Act requires that the Department of Homeland Security notify respondents that no person is required to respond to the collection of information unless it displays a currently valid OMB control number.

Privacy Act Statement: DHS's Use of Your Information

Principal Purposes: When you provide feedback on an Intelligence and Analysis (I&A) intelligence product, DHS collects your name, position, contact information, and the organization you are representing. We use this information to contact you if we have additional questions about the feedback and to identify trends, if any, in the feedback that you and your organization provide.

Routine Uses and Sharing: In general, DHS will not use this information for any purpose other than the Principal Purposes, and will not share this information within or outside the agency. Aggregate feedback data may be shared within and outside DHS but without including the contact information. In certain circumstances, DHS may share this information on a case-by-case basis as required by law or necessary for a specific purpose, as described in the DHS Mailing and Other Lists System of Records Notice, DHS/ALL-002 (73 FR 71659).

DHS Authority to Collect This Information: DHS requests that you voluntarily submit this information under its following authorities: 5 U.S.C. 301; the Federal Records Act, 44 U.S.C. 3101.

Effects of Not Providing Information: You may opt not to provide the requested information or to provide only some of the information DHS requests. However, if you choose to provide any feedback information, you must provide a classification level as requested on this form. If you opt not to provide some or all of the requested information, DHS will not be able to contact you to fully address your feedback and any additional information needs.

Accessing and Correcting Information: If you need to access or correct the information collected on this form, you should send an email to *ia.feedback@dhs.gov*. You may also direct your request in writing to the appropriate FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under "contacts." Additional instructions are available at that website and in the DHS/ALL-002 System of Records Notice, referenced above.

Return to Form