SOFT TARGETS & BLACK MARKETS:

TERRORIST ACTIVITIES IN THE MARITIME DOMAIN

one earth
FUTURE
Peace Through Governance

STABLE SEAS
a program of One Earth Future

SOFT TARGETS
& BLACK MARKETS:
TERRORIST ACTIVITIES
IN THE MARITIME DOMAIN

| Meghan Curran

May 2019

Cover Image: Nigerian separatist militants wheel around their war boat on the Escravos River in Southern Nigeria.
Photo: Dave Clark/AFP/Getty Images.

TABLE OF CONTENTS

INTRODUCTION

December 31, 2014. The Indian Coast Guard, acting on a tip from an internal intelligence agency, intercepts a Pakistani fishing boat in Indian waters, nearing the coastal city of Porbandar. The boat is some 400 nautical miles from Mumbai, where a mere six years earlier, from November 26 to 29, 2008, 10 members of the Pakistan-based terror group Lashkar-e-Taiba (LeT)[1] killed 164 people and wounded an additional 300 in attacks launched from the sea. As the Indian Coast Guard ship, the NS *Rajratan*, moves to intercept the suspicious vessel, it fires several warning shots; however, the vessel speeds toward the Pakistani side of the maritime boundary. Then, according to the NS *Rajratan*'s crew, the vessel's crew sets its own boat on fire, killing all aboard. In the aftermath of the incident, the actions of the Indian Coast Guard are subjected to intense scrutiny. While the Indian Defense Ministry's official position is that the Coast Guard successfully thwarted a Mumbai-style attack against the Indian coast by intercepting suspected terrorists, others within the Indian government believe the response was disproportionate. Even in a country like India, whose defense posture was overhauled in the aftermath of the gruesome November 2008 attacks, a lack of regard for the sea—both its opportunities and its vulnerabilities—is evident. The Mumbai attack is a key example of how violent non-state actors can circumvent onshore regulations and control measures by turning to the maritime space where these measures are often insufficient. The Indo-Pak coast, like many other coastlines across the globe, is a rather permeable environment that has for centuries supported the livelihoods of fishermen and merchants, tolerating transient seacraft. LeT's actions during the attack on Mumbai, and in the months leading up to the attack, illustrate various ways that illicit actors can capitalize on absent or weak systems, capabilities, and infrastructure in the maritime space. The group reconnoitered by sea, trained its assailants on Pakistan's inland waterways, launched its attack from the Karachi seaport, hijacked a fishing vessel, conducted a movement across 50 nautical miles undetected, and amphibiously inserted onto the shores of Mumbai unnoticed except by a handful of local fishermen.[2]

The failure to acknowledge or recognize the importance of the maritime domain to both society and the economy, or sea blindness,[3] simultaneously impacts the marine environment, economic development, and national and human security. Since the early 1990s, consideration of the maritime space from a security perspective has been broadened to incorporate a wider set of issues and activities including "new security" issues such as "terrorism, transnational organized crime or environmental degradation,"[4] which impact a range of actors despite not being directly tied to the wielding of state power at sea. The events of September 11th resulted in a paradigm shift regarding the threat against the international community posed by violent non-state actors and transnational criminals. However, political will and financial and other resources necessary to counter these threats have been disproportionately directed toward land campaigns. Many states provide varying degrees of support to international maritime laws and "demonstrate ostrich-like tendencies when reviewing the relevance of the maritime domain to [their] national security."[5] This results in a collective blind spot regarding complex problems like modern-day piracy, non-state terrorism, and transnational criminality, which propagate at sea.

> *Global counterterrorism strategies must cease to delineate between acts of organized violence on sea and on land. The complexity of global terrorism demands a more comprehensive approach.*

Modern-day maritime terrorism is marginalized by campaigns to engage stateless enemies in land wars. However, effectively combating these enemies requires widening the aperture to consider the litany of ways the maritime space is utilized to promote organized political violence. Global counterterrorism strategies must cease to delineate between acts of organized violence on sea and on land. The complexity of global terrorism demands a more comprehensive approach.

The maritime space offers myriad possibilities for funding onshore violence, including profits from both licit and illicit businesses that traverse the world's oceans, and funds obtained through controlling maritime areas and levying taxes illegally. In addition to utilizing the maritime space to fund onshore campaigns of political violence, illicit actors can also exploit the vast ungovernable space to move personnel, weapons, and other equipment necessary to carry out onshore attacks. Further, nefarious actors can support their operations onshore by illegally obtaining property at sea, such as by stealing finite resources like oil, kidnapping for ransom operations, and committing armed robbery.

The consequences of sea blindness impact not just littoral states but the international community at large. Failing to acknowledge the sea's important role in the endorsement of violence creates a significant hurdle with regards to promoting peace. The world's oceans have a significant, yet under-acknowledged, impact on the United Nations 2030 Agenda for Sustainable Development. In particular, sea blindness directly affects Sustainable Development Goal 16, which is concerned with peace, justice, and strong institutions. Achieving targets like "significantly reducing all forms of violence and related deaths . . . [reducing] illicit financial and arms flows . . . and [reducing] corruption and bribery,"[6] are simply not possible while turning a blind eye to the sea.

This paper aims to reduce sea blindness by elucidating five specific activities violent non-state actors operating in the maritime space engage in. It describes the activities, offers examples from around the world, and explores the group traits and operating environments that favor each of these five activities. By bringing attention to the centrality of maritime activity to the operations of these groups, we hope to demonstrate that governments cannot afford to overlook the sea and the way it shapes conflicts onshore.

We cannot afford to overlook the sea and the way it shapes conflicts onshore.

Photo: NATO Operation Sea Guardian.

SECTION I:
OPERATIONALLY MOTIVATED ACTIVITIES

The first two activities outlined in this paper are operationally motivated activities. The illicit actors/groups who participate in these activities are driven by political motivations, viewing the maritime space as an extension of their theater of operations.

Sailors from U.S. and Nigeria conduct visit, board, search and seizure training at the Joint Maritime Special Operations Training Command as part of Africa Partnership Station West in Lagos, Nigeria. Photo: Petty Officer 1st Class Darryl Wood, U.S. Navy.

ACTIVITY 1
TACTICAL SUPPORT

The movement of goods or personnel by violent non-state actors via maritime routes for the purpose of engaging political or military objectives.

OCCURS IN AREAS WITH:

| Low maritime domain awareness | Inadequate maritime enforcement/response capabilities | Secure land borders | Inadequate port security |

USED BY GROUPS THAT ARE:

Specially trained

Politically motivated

TACTICS INCLUDE:

Raids by sea on land targets

Movement of fighters

Raids by Sea on Land Targets

In 2016, the Israeli Defense Ministry began work on a 37-mile sea barrier to protect against attacks from Gaza by sea. The decision to build the barrier was prompted by a seaborne raid carried out during the 2014 war there. On July 8, 2014, four Hamas naval commandos swam ashore outside Kibbutz Zikim on Israel's southern coast. Carrying automatic weapons, fragmentation grenades, and explosives, Hamas frogmen engaged Israeli forces. The group has also allegedly built underwater tunnels and invested in underwater drones for the purpose of conducting similar seaborne attacks on targets in the Gaza Strip.[7]

In a 1990 incident, members of the Palestine Liberation Front (PLF) boarded a ship in Benghazi, Libya, loaded with 107 mm Katusha rockets, 23 mm cannons, and machine guns. Destined for Tel Aviv, the crew's mission was to launch attacks on the city's beachfront hotels and surrounding residential areas. The attack was thwarted by the Israeli Defense Force, but not before two motorboats successfully made beach landings.

Raids like these, which require moving equipment and personnel great distances over the sea, often demand ample resources and long-term planning. For example, prior to the intended attacks in Tel Aviv, PLF members received intensive naval training from Libyan marine commandos. Similarly, according to the testimony of Ajmal Kasab, the lone terrorist to be captured alive following the seaborne attacks against Mumbai in 2008, Pakistani terror group LeT provided "sea training" to the attackers preceding their mission. As part of this training, recruits were taught how to read maps, measure the depth of the sea, navigate with a GPS along a maritime route, and fish using traditional Indian equipment.[8] However, there are other examples of seaborne attacks against onshore targets that seem to be a bit more opportunistic. For example, in 2009, armed gunmen representing one of many rebel groups hailing from the volatile Niger Delta region came ashore in Equatorial Guinea's island capital of Malabo, intending to attack the presidential palace. The attack came at a time when motorboat raiding parties from the Niger Delta had become increasingly bold, launching raids against banks and other targets in coastal communities throughout the region.[9]
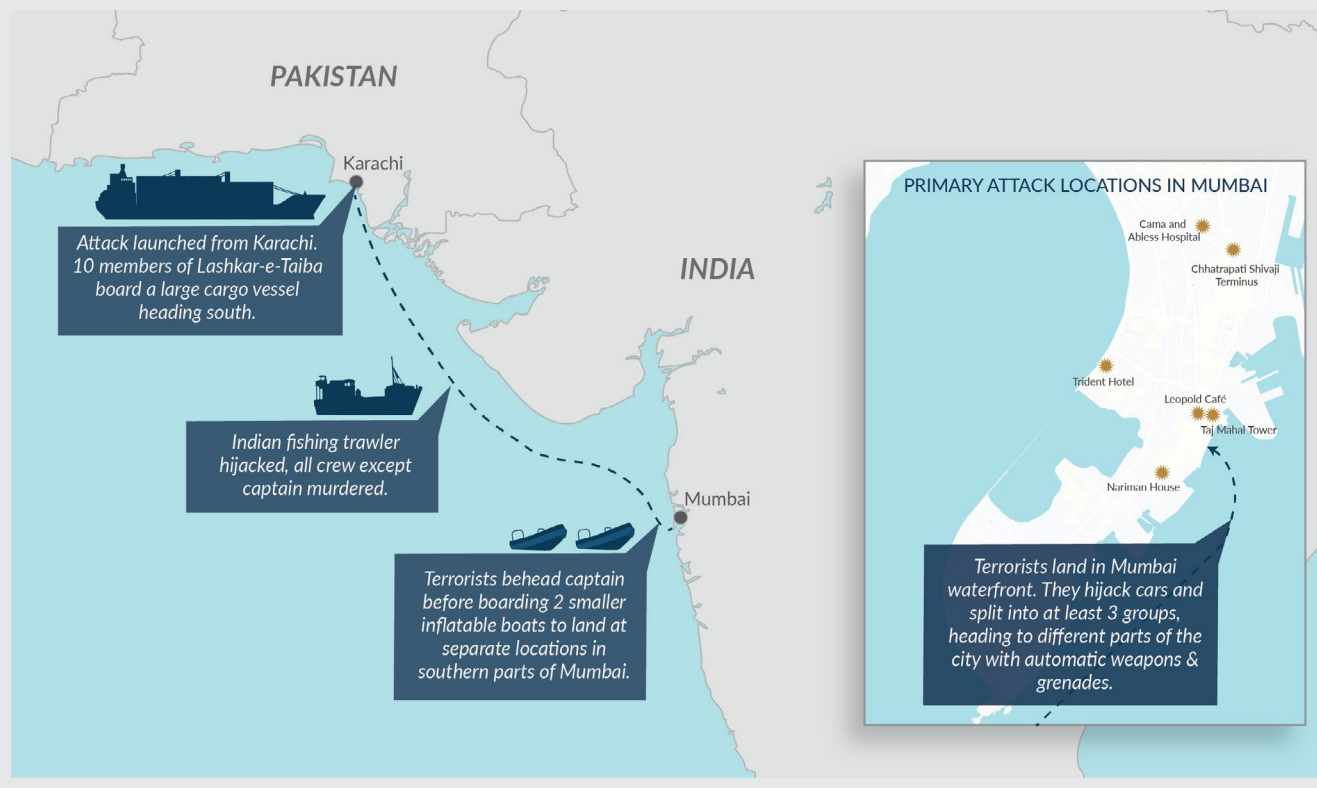
Mumbai Attacks (LeT)

Perhaps one of the most iconic examples of the tactical utilization of the maritime space is the Mumbai terror attack. Likened to the events of September 11th in the United States, the events of November 26, 2008, awoke the collective consciousness of Indian security agencies, triggering a radical overhaul of India's coastal defense architecture. As a result of the incidents, existing plans for a Coastal Security Scheme were expedited, and increased funding was allocated for infrastructure like police and radar stations along India's coastline.[10]

The seaborne attacks, orchestrated by 10 members of Lashkar-e-Taiba, an Islamist terrorist organization based in Pakistan, were well-coordinated and lasted four days. Using the sea to conduct the attacks enabled the terrorists to avoid overland Indian security checkpoints and border crossings. They also utilized an Indian vessel for the attack, allowing them to avoid detection by the Indian Coast Guard.

The attacks were launched from Karachi, Pakistan, where terrorists boarded a large cargo vessel heading south along the Indian coastline with the Arabian Sea. After a day at sea, the terrorists hijacked an Indian fishing trawler and murdered the entire crew except for its captain. Continuing to Mumbai, the group beheaded the captain as they neared their target. They then boarded two smaller inflatable boats, which they landed at separate locations in the southern part of the city. After landing, the terrorists divided themselves into four attack teams armed with AK-47s, IEDs, and grenades, and proceeded to attack six distinct targets throughout the city. The attacks resulted in over 150 deaths.

The Mumbai attacks encouraged a reexamination of India's maritime security posture, leading to a thorough review of the interoperability between the navy, coast guard, and state police, and their collective ability to deal with nontraditional challenges. Since the attack on Mumbai, intelligence reports have indicated that Lashkar-e-Taiba is again preparing for a strike against Indian ships and coastal facilities. As recently as January 2019, other reports have indicated that Pakistani militant commanders continue to train for "samundari jihad" (seaborne jihad) in the Indian seas.[11]

PAKISTAN

Karachi

Attack launched from Karachi. 10 members of Lashkar-e-Taiba board a large cargo vessel heading south.

INDIA

Indian fishing trawler hijacked, all crew except captain murdered.

Mumbai

Terrorists behead captain before boarding 2 smaller inflatable boats to land at separate locations in southern parts of Mumbai.

PRIMARY ATTACK LOCATIONS IN MUMBAI

Cama and Abless Hospital

Chhatrapati Shivaji Terminus

Trident Hotel

Leopold Café

Taj Mahal Tower

Nariman House

Terrorists land in Mumbai waterfront. They hijack cars and split into at least 3 groups, heading to different parts of the city with automatic weapons & grenades.

Movement of Fighters

Current analysis coming out of the Sulu-Celebes Seas region indicates that the Abu Sayyaf Group (ASG), now splintered into several smaller factions, has been using the sea to move foreign fighters into the Philippines. Retaining trained local fighters while recruiting foreigners as suicide operatives allows the group to preserve the capability to carry out an armed assault while simultaneously conducting deadly terror attacks like the January 2019 cathedral attack on Jolo island, which was perpetrated by two Indonesian suicide bombers. Analysts believe that fighters from both Indonesia and Malaysia are transiting the Sulu and Celebes Seas to link up with ASG and its affiliates on the island of Mindanao. One of these sea routes begins in Manado on the island of Sulawesi, Indonesia, and travels northeast toward the Sangihe Islands before landing in General Santos, the Philippines' southernmost city. Another route that also begins in Manado has a stopover in the Talaud islands before heading toward Davao

SEA ROUTES USED BY FIGHTERS TO JOIN ASG

Region in the southern Philippines. Other routes begin in eastern Sabah, Malaysia, and travel east via the Tawi-Tawi islands destined for Zamboanga, where militants travel by boat across the Moro Gulf toward the Cotabato area, just south of Marawi.[12]

Both the movement of fighters via sea routes and targeted onshore raids from the sea capitalize on an environment's low maritime domain awareness, and inadequate port security and maritime enforcement and response capabilities. The decision to carry out such attacks given the high level of reconnaissance necessary to do so reflects a perceived weakness in these areas by the perpetrators, as well as a clear opportunity to circumvent overland control measures.

The Mumbai attack exploited India's inability to identify a credible seaborne threat and respond with appropriate speed and coordination. Prior to the events of November 26, there were multiple intelligence reports warning of an impending attack on Mumbai. Some of these reports even hinted at an attack from the sea; however, Indian authorities deemed the information inactionable,[13] and more pressing security priorities detracted them from effectively addressing the holes in India's pre-attack defense posture. Among other things, the attacks highlighted India's inability to effectively monitor its coastline, a failure that reflected the coast guard's shortage of equipment for coastal surveillance. At the time there were "fewer than 100 boats for more than 5,000 miles of shoreline and minimal aviation assets."[14]

In the lead-up to the successful attack in November, two failed attacks against Mumbai in both September and October even went undetected, further illustrating India's inadequate maritime domain awareness and emboldening the attackers.[15] During the attacks, authorities were slow to respond to reports from fishermen at the landing area, and although local police responded to the event relatively quickly, they lacked the expertise to set up command posts and cordon off the attack sites.[16] National Security Guards, India's elite rapid-reaction force, took nearly 10 hours to reach Mumbai, as they had to be flown in from their headquarters south of Delhi.[17]

Illicit actors who attempt seaborne raids are politically motivated and may face tactical hurdles regarding land-based attacks. Using the sea as an attack route provides new opportunities for these actors, particularly if they can capitalize on the element of surprise, which is exacerbated by weak maritime and law enforcement response apparatuses.
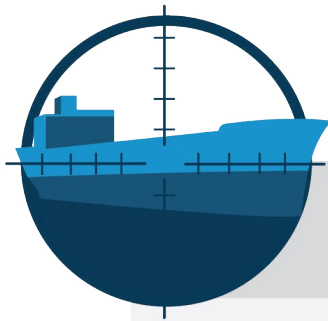
ACTIVITY 2
TARGET

The deliberate, threatened, or actual use of violence by a non-state actor against a maritime target such as a ship, platform, port, wharf, or other maritime infrastructure.

OCCURS IN AREAS WITH:

| Low maritime domain awareness | Inadequate port security | Inadequate maritime enforcement/response capabilities | Target availability |

USED BY GROUPS THAT ARE:

Specially trained

Politically motivated

TACTICS INCLUDE:

Maritime terrorism

Cyber attacks

History of Attacks at Sea

One of the most significant conclusions of the 9/11 Commission Report was that the events of September 11th were not a failure of intelligence, but a failure of imagination.[18] In the years since the attacks, use of the maritime space to carry out attacks has been viewed with renewed interest, citing the lengthy history of attacks at sea. A 1983 RAND Corporation report entitled "A Chronology of Terrorist Attacks and Other Criminal Actions against Maritime Targets" described 111 individual incidents at sea involving "guerillas, terrorists, pirates, [and] ordinary criminals" beginning in 1960. The 35-year-old report highlights a spectrum of activities: "ships hijacked; destroyed by mines and bombs; attacked with bazookas; sunk under mysterious circumstances; cargoes removed; crews taken hostage; extortion plots against ocean liners and offshore platforms; raids on port facilities, attempts to board oil rigs; sabotage shipyards and terminal facilities."[19]

In more recent memory, the 2000 bombing of the USS *Cole* in a Yemeni port by al-Qaeda, the 2004 bombing of SuperFerry 14 by the Philippines' ASG, and Houthi rebels' current use of remote-controlled, explosive-filled vessels to attack Saudi ships and oil tankers, continue to demonstrate the opportunities for illicit actors to utilize the maritime space to conduct devastating attacks. Owing to the sheer size of the maritime space, and the impressive target set it offers (on any given day there are some 50,000 ships carrying more than 90 percent of all international trade),[20] it is well suited as a stage for such attacks.

Beyond terrorist attacks at sea, nefarious actors are increasingly exploiting the technological advances of the cyber age, opening a new venue for maritime attacks that target the international shipping industry and maritime infrastructure like ports.

Maritime Terrorism

The sheer depth of the vulnerable target set at sea, combined with the expansive, ungovernable maritime space, makes the threat of maritime terrorism constant. Seaborne commercial trade is susceptible to terrorist attack due to the "high quantity of cargo involved, its diverse and large international labor force, difficulties of enforcement both in port and at sea, and the poor regulatory environment of international shipping with low levels of accountability."[21] There are ample opportunities to exploit the weaknesses of this system to launch an attack on shipping or port infrastructure that could cause high levels of economic disruption.

Although maritime terrorism has no internationally agreed upon definition, legal scholars have agreed on an operational definition based on Articles 3 and 4 of the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, though the SUA Convention does not reference terrorism specifically.[22] According to the convention, maritime terrorism is defined as "Any attempt or threat to seize control of a ship by force; To damage or destroy a ship or its cargo; To injure or kill a person on board a ship; or To endanger in any way the safe navigation of a ship that moves from the territorial waters."[23]

Maritime terrorism attacks have utilized a diverse set of tactics, including self-guided explosive-laden boats, maritime improvised explosive devices, and fast attack craft.

Maritime terrorist attacks to date have been primarily against passenger ships and ferries. The sinking of SuperFerry 14 in February 2004 near Manila, Philippines, resulted in the largest loss of life in a maritime attack; however, attacks on the USS *Cole* in the Gulf of Aden in October 2000 and on the French tanker *Limburg* off Yemen in October 2002 are more widely cited acts of maritime terrorism because they were initiated by al-Qaeda in the context of 9/11.[24] The maritime terrorist attacks carried out by the "Sea Tigers" of the Liberation Tigers of Tamil Eelam (LTTE) on both merchant ships and Sri Lankan warships are often cited as establishing a precedent for this type of attack. Beginning in 2016, Houthi rebels began conducting attacks against US, Saudi, and Emirati warships, as well as international commercial oil tankers and other civilian ships passing through the Bab el-Mandeb Strait. These attacks have utilized a diverse set of tactics, including self-guided explosive-laden boats, drifting mines, and fast attack craft from which the rebels have fired rocket-propelled grenades.[25]

MARITIME IMPROVISED EXPLOSIVE DEVICES

CAN BE LAUNCHED BY:

OPERATING DEPTHS:
10 ft
200+ ft

FIRING MECHANISMS
remote   magnetic
seismic   pressure

TARGETS INCLUDE:
oil platforms   military vessels   oil tankers & container ships

Maritime Improvised Explosive Devices

Conjuring up a doomsday scenario[26] regarding a maritime terrorist attack is not difficult. A ship could be hijacked and used as a floating bomb, or a shipping container could be used to move weapons and other materials necessary to carry out an attack. While these possibilities exist, maritime targets are often less attractive than land or air targets because they are difficult to attack, and because in general illicit groups tend to lack maritime skills.[27] Nonetheless, violent non-state groups throughout history have used the maritime space in creative ways to inflict terror. One example of this is the utilization of mines and maritime IEDS (MIEDs). These weapons are easy to build and can be launched from several different maritime platforms, including submarines, small commercial vessels, dhows, and fishing vessels. MIEDs can be designed to operate at surf zone (less than 10-foot water depth) to deep water (greater than 200 feet) and can carry a range of payloads. Additionally, they can utilize a variety of firing mechanisms from remote control to magnetic, seismic, or pressure.[28]

The ASG, as well as LTTE, has historically employed MIEDs, targeting oil and gas platforms, shipping containers, and oil tankers. There is evidence as well that al-Qaeda recognized the potential of the maritime space as a stage for similar attacks. To date, al-Qaeda has not demonstrated equivalent emphasis
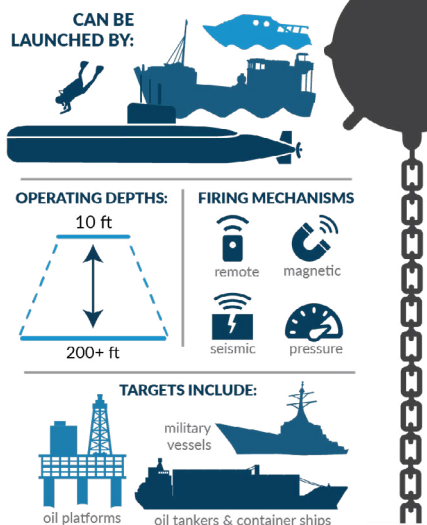
on its maritime terror program as it has in its land-based terror programs; however, from 1998 to 2002, the group's Abd al-Rahim al-Nashiri, also known as the Prince of the Sea, masterminded several waterborne IED attacks, including failed attacks against the USS *The Sullivans* (February 2000) and successful attacks against the USS *Cole* (October 2000) and the MV *Limburg* (October 2001). After he was captured in 2002, it was discovered that al-Nashiri had also been plotting an attack in the Strait of Hormuz, as well as against Dubai's Port Rashid. Additionally, it was determined that his future maritime terrorism plans included "ramming rigid inflatable boats packed with explosives against ships, detonating MIEDs near shipping ports, crashing planes into maritime targets, and developing specially trained diving teams which were to work as underwater demolition teams for the purposes of covertly placing MIEDs."[29]

Small Boat Attacks (Suicide Boats and Drone Boats)

Globally, there are numerous examples of small boat attacks that have been carried out against both military and commercial vessels. Small boats include a variety of possible weapon-delivery vehicles, tactics, and payloads. Vessels can include small freighters, privately owned yachts, trawlers, commercial tugboats, dinghies, Jet Skis, and submarines, to include mini-submarines like those used by the Japanese in the attack on Pearl Harbor.[30]

Attacks involving small boats have often included suicide bombers, who navigate explosive-packed vessels alongside their targets, or purposefully ram them. During WWII, the Japanese pioneered the use of boats on suicide missions. Shinyo, or "sea quake," were one-man motorboats capable of reaching speeds of 35 mph and equipped with two depth charges.[31] The LTTE's Sea Tigers used similar methods on numerous attacks against the Sri Lankan Navy and Sri Lankan oil tankers, setting a dangerous precedent for al-Qaeda's attack on the USS *Cole* in 2000.

In many ways, small boat attacks resemble other terrorist attacks and have a similar signature. They require recruiting and training, as well as high-level planning to include surveillance, intelligence and information operations, and logistical support.[32] However, in other ways, small boat attacks have some unique characteristics. They require maritime knowledge and familiarity with the target area, including maritime traffic patterns, and an understanding of how tides and weather will affect the delivery of the payload.[33] Still, compared to MIEDs, small boat attacks require far less technical expertise and are, therefore, more broadly used.

In January 2017, Houthi rebels employed a first-of-its-kind small boat in an attack against a Saudi naval ship. Three Houthi vessels participated in the attack, surrounding the *Al Madinah* at top speeds.

One of the vessels was able to get close enough to the Saudi ship to ram it, resulting in a large explosion that killed two sailors and injured three others. The attack is thought to be the first ever by a remote-controlled boat. The use of remote-controlled weaponry, which is spreading quickly among even low-tech paramilitary forces such as the Islamic State, has the potential to eliminate many of the resources necessary to conduct these types of attacks in the future.

Attack on the USS *Cole* (al-Qaeda)

The US Navy destroyer *Cole* was attacked on October 12, 2000, 11 months prior to the attacks of September 11th. The *Cole* was attacked during a brief refueling stop in the harbor of Aden, Yemen. The attack involved a motorized rubber dinghy loaded with explosives that joined a group of harbor ships aiding the *Cole* at moor. The dinghy was able to come alongside the *Cole* unabated, and just past noon local time, the explosives on board were detonated. The explosion tore a 40' × 40' hole in the ship's port side, killing 17 sailors and wounding an additional 38.

On October 16, the Yemeni government acknowledged that the bombing had been a terrorist attack, and in December officials arrested two suspects, Fahd al-Quso and Jamal al-Badawi, for their roles in the attacks. In addition, both US and Yemeni officials identified Abd al Rahim al-Nashiri, al-Qaeda's Prince of the Sea, as a key figure in the planning of the bombing. In January 2001, the United States Department of Defense (DoD) released the USS Cole Commission Report, which highlighted the need for a more comprehensive antiterrorism/ force protection (AT/FP) strategy regarding US forces in transit. In a DoD press conference in January of that year, then defense secretary William Cohen remarked that senior defense leadership "needed to engage more vigorously in examination of the range of potential threats [by terrorists]."[34]

Divers

In 2002, the FBI began a nationwide canvassing of shops offering scuba diving instruction. Acting off information gathered from multiple prisoners held at Guantanamo Bay, Cuba, who told authorities that "Scuba dive equipment was something [terrorists] had shown interest in acquiring in efforts to plan future attacks,"[35] the agency moved to compile a list of individuals who had received advanced training. In 2005, a Philippine military report obtained by the Associated Press outlined Indonesia-based group Jemaah Islamiyah's investment in diving and explosive training for the ASG. According to the report, Abu Sayyaf leader Gamal Baharan described how he and other seasoned guerrillas took scuba diving lessons as part of a plot for an attack at sea. Meanwhile, the Indian Coast Guard and Navy have been on high alert since the fall of 2018, due to increasingly frequent intelligence reports that Pakistan-based LeT and Jaish-e-Mohammed (JeM) have been building their sea strike capabilities to include training deep-sea divers.[36]

Numerous Suicide Ship Attacks (Liberation Tigers of Tamil Eelam)

The Liberation Tigers of Tamil Eelam (LTTE) pioneered the use of boats on suicide missions. In the 1990s, their designated sea force, the Sea Tigers, began carrying out attacks using both speedboats and mirage-class fiberglass vessels. While many of these attacks involved swarming a target with several armed small boats, suicide attacks often involved using the same swarming formations with explosive-packed ships designed to ram targets. In June 2000, LTTE suicide boats sank a chartered private ship called the MV *Uhana*. At the time of the attack, the ship was being escorted to Jaffna by the Sri Lankan Navy. Preceding the attack on the USS *Cole* by just four months, it has been suggested that the successful implementation of this activity by the Tigers may have inspired the attack on the *Cole*.

In October 2001, a year after the bombing of the USS *Cole*, the Sea Tigers orchestrated an attack against the MV *Silk Pride*, an oil tanker that was carrying more than 650 tons of diesel and kerosene off the port of Point Pedro on the northern Sri Lankan peninsula of Jaffna. The attack involved at least five boats surrounding the tanker, ramming into it from the side, and starting a fire that quickly engulfed the ship. Three soldiers and four of the bombers, including two women, were killed in the attack.

In a separate incident in January 2007, the Sea Tigers carried out another suicide ship attack, this time against a cargo ship carrying rations to feed civilians on the Jaffna peninsula. The ship was rammed with an explosive-laden boat while it was unloading supplies outside of Sri Lanka's Kankesanthurai port.

A LTTE Sea Tiger fast attack fiberglass boat passing a Sri Lankan freighter sunken by the Sea Tigers just north of the village of Mullaitivu, Sri Lanka. Photo: Isak Berntsen, 2003.

Cyberattacks in the Maritime Space

While illicit actors have long utilized the maritime space to conduct attacks targeting vulnerable vessels, port infrastructure, and coastal communities, the potential for cyberattacks in the maritime domain continues to grow. The 50,000+ ships at sea on any given day have joined a continuously growing list of things that are vulnerable to attack in the cyber domain. This is especially true today, when the international shipping system is highly reliant on technical navigational and logistical systems. In 2013, researchers from the University of Texas using a laptop, a small antenna, and a GPS "spoofing" device, fed a signal to a yacht's navigational system that superseded the genuine one coming from GPS satellites. In doing so, the researchers tricked the ship's computer into believing that it was somewhere it was not, causing it to adjust its heading to stay on course. In 2018, cybersecurity experts with a London-based security company called Pen Test Partners ran a simulation targeting a computer-powered navigation system called the Electronic Chart Display and Information System (ECDIS). This system provides crews an alternative to using paper charts, enhancing navigational safety by assisting with route planning and recording continuous navigational data. The simulation illustrated the ease with which it is possible to hack into an ECDIS and misidentify the location of its GPS receiver.

> *Overall, the maritime industry has been slow to realize the potential for cyberattacks, yet the potential for attacks in the maritime domain continues to grow.*

Overall, the maritime industry has been slow to realize the potential for cyberattacks, and organizations like the International Maritime Organization have also been slow to consider regulations to protect against such attacks at sea. This is in part because cybersecurity in the maritime space is a complex issue that involves many different classes of vessels, carrying a range of outdated operating systems that are highly prone to cyberattacks. Compounding this is the fact that ship crews are highly dynamic, and knowledge and training regarding onboard technical systems is usually low, with maintenance of these systems falling to third-party contractors.[37]

In June 2017, the most devastating cyber attack in history illustrated just how easily the shipping industry could be brought to its knees. Although the industry was not the intended target, its interconnectedness made it vulnerable to attack. Shipping giant Maersk, which owns 76 worldwide ports and over 800 seafaring vessels that carry tens of millions of tons of cargo, found itself dead in the water.[38] For nearly two weeks while the company's IT experts scrambled to rebuild its expansive network, the shipping conglomerate was forced to tape paper shipping documents to containers and book shipments via WhatsApp.

The majority of attention concerning cybersecurity in the maritime domain has focused on the vulnerabilities of the shipping sector; however, maritime ports are also vulnerable to such attacks. As an essential piece of the maritime transportation system, ports play a vital role in global trade, as well as international security, by supporting troop movements and logistics. Like the legacy systems that increase the vulnerability of the shipping industry to cyberattacks, most ports utilize industrial control systems and supervisory control and data acquisition (SCADA) systems, which were designed without consideration of exposure to the internet[39] and can be easily compromised.

Another system that is vulnerable to cyberattacks in the maritime space is the undersea fiber-optic cable network. Comprising over 550,000 miles of cable and responsible for over 97 percent of intercontinental communication, the network can be compromised through illegal data acquisition, or disruption. Hackers can gain access and control data and voice traffic by penetrating terminals in cable landing sites, or by intercepting fiber-optic wavelengths.

UNDESEA FIBER-OPTIC CABLES
ARE RESPONSIBLE FOR TRANSMITTING:

97% INTERCONTINENTAL COMMUNICATION

15 MILLION+ FINANCIAL TRANSACTIONS DAILY, WORTH **$10 TRILLION**

SENSITIVE & NON-SENSITIVE DATA, AND VOICE CALLS BETWEEN CONTINENTS & COUNTRIES

There are 428 known commercial fiber-optic cable routes worldwide,[40] many of which run along heavily trafficked maritime routes and are marked on public maps. Where these cables come ashore, they are especially vulnerable, as there is variability in the level of physical security across countries and cable operators.[41]

The vulnerability of the maritime industry to cyberattack, illustrated through both simulations and real-world episodes, further expands the potential target set for illicit actors. Despite the online presence of the "Islamic State Hacking Division" and the "Cyber Caliphate," there is little evidence that major violent non-state groups currently possess the capabilities to carry out cyberattacks. Nonetheless, these groups' utilization of the information technology space continues to expand, even as their ability to carry out physical attacks and control territory fluctuates. It is not unthinkable that the cyber domain could be a fresh frontier for violent non-state actors. As cybercrime becomes a new breed of transnational organized crime, the established nexus between it and terrorism creates a new stage for such groups to broadcast worldwide terror. As the maritime industry lags behind other industries in its recognition of the real threat in this space, it merely exacerbates these vulnerabilities.

By and large the activities that fit into the "target" category require a very high degree of planning and resourcing, and a special skill set. Operationally motivated attacks that require training divers to employ MIEDs or plotting to bomb a ship at port while accounting for the externalities of the maritime space demand a certain level of expertise, as does plotting a cyberattack on the shipping industry or port infrastructure. Target availability is an important characteristic of environments that encourages activities in this category as they are carried out in close proximity to the shore, often against stationary vessels or port infrastructure, exploiting a lack of maritime domain awareness, and in particular insufficient port security.

The activities that fit into the "target" category require a very high degree of planning and resourcing, and a special skill set.

SECTION II:
FINANCIALLY MOTIVATED ACTIVITIES

The following three activities are financially motivated activities. While political motivations ultimately drive illicit actors/groups to participate in these activities, their short-term motivation is financial gain. Illicit actors who use these activities do so in order to fund their operations and campaigns.

A shipping container at the Port of Salalah. Containerization has revolutionized international trade while also facilitating profitable global illicit trade networks. Photo: Darren Pullen.

ACTIVITY 3
TAKE

To obtain property or persons at sea by wrongful or illegal means.

OCCURS IN AREAS WITH:

Low Maritime Domain Awareness

Inadequate maritime enforcement capabilities

Well developed criminal networks

Geographically advantageous areas, difficult to secure

USED BY GROUPS THAT ARE:

Financially motivated

Politically motivated

Able to control coastal areas

With access to illicit financial networks

TACTICS INCLUDE:

Piracy and armed robbery at sea

Kidnap for ransom

Oil bunkering

Piracy and Armed Robbery at Sea

Piracy, like other forms of organized crime, is an activity that can be easily adopted by violent non-state actors facing financial strain; however, uniquely, these groups must possess a maritime capability. In the post-9/11 era, as regional affiliates of terror groups have proliferated, and state sponsored terrorism has waned, the linkages between crime and terror have been compounded by terror groups' capitalizing on, adopting, and usurping the existing logistical and operational nodes of criminal networks. "While terrorist and criminal organizations . . . have fundamentally dissimilar motives for their crimes, [they] may cooperate by networking or subcontracting on specific tasks when their objectives of interest intersect."[42] As criminal groups and terror groups often share tactics, delineating between those who embrace piracy from a criminal standpoint and those who have more politically motivated incentives can be difficult.

Politically motivated groups adopt piracy tactics for the same reasons that criminal organizations and communities facing dire economic circumstances do: opportunity.

According to the United Nations Convention on the Law of the Sea, piracy is defined as any "illegal [act] of violence or detention, or any depredation, committed for private ends by the crew or the passengers of a private ship . . . on the high seas, against another ship."[43] Conversely, armed robbery at sea occurs in the territorial waters of a coastal state. Both piracy and armed robbery at sea pose significant challenges to a diverse set of stakeholders, undermining security onshore. While neither is a new phenomenon, worldwide attention on piracy has spiked over the last decade, with more notorious attacks earning international headlines, and inspiring Hollywood renditions.

Armed Robbery (Houthis)

On November 18, 2018, Iran-backed Houthi rebels kidnapped 18 fishermen off the coast of the critical port city of Hodeidah on the west coast of Yemen. According to bystanders, the fishermen were taken when they refused to allow Houthis to use their boats to conduct attacks. Days before the kidnappings, the Yemeni minister of fisheries, Fahd Kafayen, accused Iranian ships of harassing, threatening, and kidnapping multiple fishermen in Yemeni waters in the Gulf of Aden and the Red Sea. In addition to using fishing vessels to carry out attacks, it was reported that the Houthis were using the stolen boats to smuggle arms from Iranian ships providing logistical support to the rebels.

A 2008 RAND Corporation study outlined several key factors that have contributed to piracy's reemergence in the contemporary era. Citing an increase in commercial maritime traffic, which has enhanced targets of opportunity because much of the world's sea trade now passes through narrow and congested chokepoints,[44] the report also points to increased investment in land-based homeland security initiatives in the post-9/11 world. Additionally, the report found that the global proliferation of small arms provided pirates and other criminal elements with enhanced means to operate. Other studies that have examined the lure of piracy have focused on the structural and economic drivers that make it appealing in areas where poverty is a persistent challenge. In coastal communities where economic opportunities are bleak, and maritime governing capacity is low, piracy is often viewed as an attractive venture.

Regardless of the motivations behind increased incidences of piracy, there has been much debate regarding its associations with organized political violence. Although virtually all the world's oceans have a long history of maritime piracy that has existed at low, erratic, and opportunistic levels, more frequent and high-profile attacks have generated renewed international interest in the phenomenon, and its nexus with terrorism. While some argue that the conflation of piracy and terrorism is overstated, politically motivated groups adopt piracy tactics for the same reasons that criminal organizations and communities facing dire economic circumstances do: opportunity.

Kidnap for Ransom

Another activity that offers a great deal of opportunity for illicit actors to finance their operations is kidnap for ransom. Kidnap for ransom at sea is an extremely lucrative activity. A 2011 Financial Action Task Force examined 13 piracy for ransom cases in the Gulf of Aden, Indian Ocean, and Arabian Sea, and found that ransom demands ranged from $1.5 million to $35 million.[45] The case studies examined by the FATF also illustrated the global reach of this activity: the hijacked vessels included those owned or operated by Norwegian, Russian, Saudi, Ukrainian, Dutch, Danish, and Belgian entities.[46] The study found that attacking large vessels with high-value cargo, while riskier for the perpetrators, increased the likelihood that the vessel's owners, or insurers, would pay larger ransoms. The high payoffs associated with kidnap-for-ransom activities in the maritime space have made them extremely attractive to illicit actors; therefore, incidences of kidnapping have remained constant, even as worldwide piracy has ebbed and flowed over the past several years.

MARITIME RANSOM DEMANDS RANGE FROM:

$1.5 MILLION

$35 MILLION

Kidnap for Ransom (Abu Sayyaf Group)

In the cultural context of Southeast Asia, defining "piracy" poses a particular challenge, as sea raiding is a historical and deeply rooted characteristic of many coastal societies in the region. Territorial sensitivities complicate the issue further, as piracy is officially defined as occurring on the "high seas" and some states (like Indonesia) in the region possess only territorial and archipelagic waters.

European colonization led to criminalization of piracy-related activities in Southeast Asia, but nonetheless they have remained commonplace. Along the Sulu and Celebes Seas, littoral states often lack the capabilities to secure their territorial waters, and this, coupled with the archipelagic character of the area, which affords numerous safe havens for pirates, makes it ideal for exploitation by organizations like ASG.

EVOLUTION OF ABU SAYYAF GROUP'S TACTICS

TACTICS
Bombings & attacks

FUNDING
external radical Islamist groups

TARGETS
churches, cities - primarily within the Philippines

2000

TACTICS
Onshore kidnapping via maritime routes

FUNDING
Ransoms

TARGETS
Resorts around the Sulu & Celebes Seas

2014 -

TACTICS
Seaborne kidnapping

FUNDING
Ransoms

TARGETS
Seafarers, especially from tugboats

The group, which has split into a number of factions, was founded on an Islamist ideology, but law enforcement and military authorities in the region currently tend to "view the group more as a profit-motivated violent criminal enterprise than a platform-driven political movement."[47] In the 1990s and early 2000s, ASG received significant funding from global Islamist organizations like al-Qaeda and Jemaah Islamiyah; however, changes in ASG leadership coupled with global counterterrorism measures following 9/11 soon began to erode these ties. By the mid-2000s, ASG was growing increasingly dependent on kidnapping and extortion to finance its operations.

Capitalizing on the strong maritime tradition in the area, ASG has carried out several long-range seaborne kidnappings for ransom. Some of the group's most well-known kidnap for ransoms at sea have included the April 2000 attack at a diving resort in Sabah, Malaysia, where militants seized 21 Western tourists and Asian resort workers, before demanding a $16 million ransom payment. In May 2001, a similar attack at a private island resort in the southern Philippines called Dos Palmas resulted in the kidnapping of 20 resort goers and a yearlong hostage crisis, which concluded when a ransom of $330,000 was paid.

In 2013, ASG gunmen raided a Malaysian resort in Pom Pom Island off Semporna, killing a Taiwanese tourist and escaping across the Sulu Sea with another. The next year, in April 2014, the group raided a Malaysian resort in Semporna and utilized the same maritime route to escape with a Chinese and a Filipino hostage. In August 2014, members of Abu Sayyaf abducted a German citizen from his yacht near the island of Palawan. In another high-profile resort attack in September 2015, two Canadians, a Norwegian, and a Filipina woman were taken hostage from the Island Garden City of Samal, Davao del Norte, Philippines. After ransom demands were not initially met, the two Canadian hostages were beheaded. The Norwegian hostage was released after a year in captivity following the payment of a $638,000 ransom.

In 2016, as military offensives began to restrict the group's ability to conduct onshore kidnappings via maritime routes, ASG resorted to abducting foreign tugboat crewmen. In the first six months of that year, the group reportedly earned $7.3 million from ransoms paid by the crew's families and the ship owners of Malaysian, Indonesian, and Vietnamese vessels.[48] In September 2018, two masked men armed with M16 assault rifles boarded the fishing trawler *Sri Dwi* and abducted two Indonesian fishermen off of Sabah. The victims were later transported by speedboat to Talipao on Jolo island, Sulu, and a $1 million ransom was demanded for their release. One victim escaped captivity in December, and the other was released in January 2019. In December 2018, approximately 20 armed ASG members boarded another fishing vessel, this time abducting one Malaysian and two Indonesian fishermen. The second abduction also occurred off Sabah in the vicinity of Lahad Datu.[49] As of April 2019, the fishermen are still in captivity and no additional kidnappings have been reported.

Oil Bunkering

Every year, it is estimated that over $130 billion worth of fuel products are stolen or adulterated from legitimate oil and gas enterprises, and these numbers may be even higher due to high levels of corruption and government involvement.[50] There has been recent international attention regarding these activities, termed "illegal oil bunkering." In the shipping industry, the word bunker refers to fuel and lube oils, which are stored on a ship. Bunkering "could be likened to establishing a floating fuel service station on the high seas or at coastal jetties to supply fuel and provisions of water to ships."[51] Bunkering is practiced primarily in countries with coastal territory, and to an even greater degree in countries with offshore hydrocarbon resources. Bunkering is regarded as a legal activity when the company owning the specialized vessels to sell fuel, oil, and marine diesel possesses the requisite licenses and permits from relevant government agencies to operate a business. The activity is illegal without licensing, or when bunkering products are stolen from pipelines or storage facilities.

There is an established link between hydrocarbon theft and the proliferation of violence worldwide. According to the Atlantic Council's report "Downstream Oil Theft: Global Modalities, Trends, and Remedies," the activity contributes to a multibillion-dollar industry that impacts global security by funding drug cartels, criminal syndicates, and terrorist groups including the Islamic State, Mexican drug cartels, Italian mafia, Eastern European criminal groups, Libyan militias, and Nigerian rebels.

Hydrocarbons account for about one-third of the total worldwide transoceanic trade. According to the United Nations, two-thirds of global daily oil exports are transported by sea, meaning much of the illegal fuel trade is conducted on water. Across the globe, non-state actors offshore have routinely exploited loopholes created by international law and the law of the sea to steal and transfer fuel: crude oil from Libya and Syria has found its way to EU markets, and recently, Russian ships have been found smuggling oil products to North Korea.[52]

Expansive coastlines and limited maritime enforcement capacity create ample opportunities for illicit groups to pilfer and crudely refine valuable bunkering products to fund their operations. The most frequently utilized method of hydrocarbon theft involves the tapping of oil pipelines and well heads, referred to as "hot tapping" or "pressure tapping." This largely undetectable method, usually conducted underwater, involves accessing a high-pressure pipeline and diverting the flow of oil, leaving the pipeline completely functional. Once the product is diverted, it is often pumped onto a waiting vessel and either transported for sale or refined in a crude local refinery.

> *Illicit actors who participate in take activities in the maritime space are usually financially strained, or have weaker financial connections to global terrorism networks.*

Illicit actors who participate in take activities in the maritime space are usually financially strained, or have weaker financial connections to global terrorism networks. Groups like ASG, whose funding from al-Qaeda has been intermittent and inconsistent, might participate in activities in this category in order to continue to exert influence while simultaneously earning the capital necessary to operate. While these activities undoubtedly have political elements to them, their immediate goal is profit. They are likely to be encouraged by environments with low maritime domain awareness, particularly as it pertains to state control over coastal areas. They will also be fostered by well-developed criminal networks, weak transnational counter-piracy strategies, and geography that is advantageous to illicit actors due its difficulty to secure. The 170 miles of the Sulu Archipelago, comprising hundreds of volcanic and coral islands and reefs, and the expansive marshlands of the Niger Delta, which spill into the South Atlantic, are two great examples of environments that create opportunities for politically motivated actors to manipulate existing criminal networks to finance their activities.

Oil Bunkering (Movement for the Emancipation of the Niger Delta)

Conflict in Nigeria's Niger Delta arose in the 1990s stemming from tensions between foreign oil companies and the Delta's minority ethnic groups, who claim the right to self-determination over their traditional lands. In a "frantic bid"[53] to gain attention from both apathetic corporate enterprises and local political elites, many of the Delta's youth have been involved in sabotaging crude oil production in the region.

Geographically, the Niger Delta is advantageous for illicit activities including bunkering. One of the world's largest wetlands, it occupies an area of 70,000 square kilometers, stretching across nine states in southern Nigeria bordering the Gulf of Guinea. Topographically, the area is characterized by swamps, marine water, creeks, canals, and estuaries, and it is dotted with thick forests, making it difficult to secure. Illicit groups have exploited this geography, as well as the ample target set provided by extensive hydrocarbon exploration off the Nigerian coast.

Boats and a barge carrying tanks filled with stolen or 'bunkered' crude oil hide among mangrove trees in the Niger Delta. Photo: Jacob Silberberg/Getty Images.

Competition over oil wealth has fueled violence between local militias and international corporations, as well as between the militias themselves, resulting in a large number of groups complicit in oil bunkering activities. The Movement for the Emancipation of the Niger Delta (MEND) is one of the most prominent groups in the region, dating back to 2005. MEND draws its members from communities across the area, representing Ihaw, Urhoho, Itsekiri, Ikwerreand, and Yoruba tribes, and differs from other groups by "placing its struggle in a social rather than ethnic context."[54]

MEND represents a loose coalition of armed groups responsible for oil bunkering in the Delta region. Using subterranean extraction processes, the group often siphons fuel into waiting speedboats. The products are then sold to international cartels, or on the thriving local black market. In Ore, Ogun State, for example, local manufacturing and construction companies alike prefer the cheap, easily accessible crude product offered by the Delta's youth, to the higher priced legally refined product.[55]

MEND and other groups in the area have also constructed illegal artisan refineries that "cook" the crude material into petroleum products yielding 2 percent petrol, 2 percent kerosene, and 41 percent diesel. Over half of the crude product goes to waste and is dumped into the nearby water, resulting in widespread pollution. These crude refineries typically cost no more than 7 percent of the annual profits they can turn.[56] According to a report commissioned by Shell, bunkering accounted for roughly 15 percent of annual losses for major oil companies in the region, resulting in billions of dollars in profit for criminal networks and illicit groups.[57]
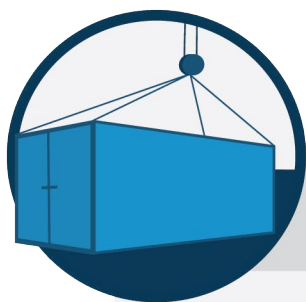
ACTIVITY 4
TRAFFIC & TRADE

The licit or illicit exchange of goods or services at sea to fund onshore campaigns of political violence.

OCCURS IN AREAS WITH:

Low maritime domain awareness	Porous sea borders	Inadequate port security	Well developed criminal networks	Military & law enforcement corruption

USED BY GROUPS THAT ARE:

Financially strained

Connected with established criminal enterprises or illicit financial networks

TACTICS INCLUDE:

Drug trafficking

Mixed maritime migration

Money laundering

Activities that fit into the take category occur outside the bounds of both formal and informal economies. However, a broader range of financially motivated illicit activities in the maritime space is more closely tied to these established systems. Activities that fit into the traffic and trade category often involve illicit actors' establishing a relationship with transnational organized criminal networks or inserting themselves into these networks to earn a profit. Additionally, this category is inclusive of activities surrounding licit businesses in the maritime space. These businesses may produce legitimate goods or services as part of the formal economy, while their profits are used to fund organized political violence.

The Containerized Shipping System and Illicit Trafficking

Today's intermodal universal containerized shipping system comprised of specialized vessels that crisscross the globe on maritime routes, roads, and rail networks is inexpensive and reliable. The system's maritime routes contain over 100,000 merchant vessels, 6,000 commercial ports and harbor facilities, and nearly 50,000 shipping bureaus, uniting 200 coastal nations, territories, and island states. Because so many containers pass through the world's ports every day, only a fraction of these containers can be inspected. In this way, containerization has revolutionized international trade while also facilitating profitable global illicit trade networks. Around the world, traffickers and smugglers are able to evade law enforcement by illegally transporting trafficked commodities into and through this containerized shipping system.

SCOPE OF INTERNATIONAL MARITIME SHIPPING

100,000+ merchant vessels

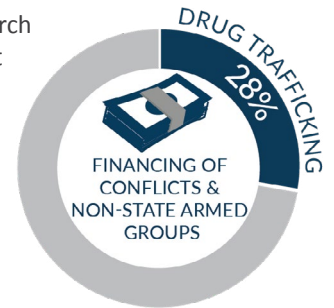**50,000** shipping bureaus

6,000 commercial ports & harbors

In the first comprehensive study on maritime trafficking, a Stockholm International Peace Research Institute report found that many ships involved in illicit transfers of arms, drugs, and equipment were owned by companies based in the world's richest countries. The report showed that the methods used by arms traffickers are similar to those pioneered by drug traffickers. These include "hiding goods in sealed shipping containers, sending the goods on foreign-owned ships engaged in legitimate trade, and using circuitous routes to make the shipments harder for surveillance operations to track."[58]

DRUG TRAFFICKING 28%

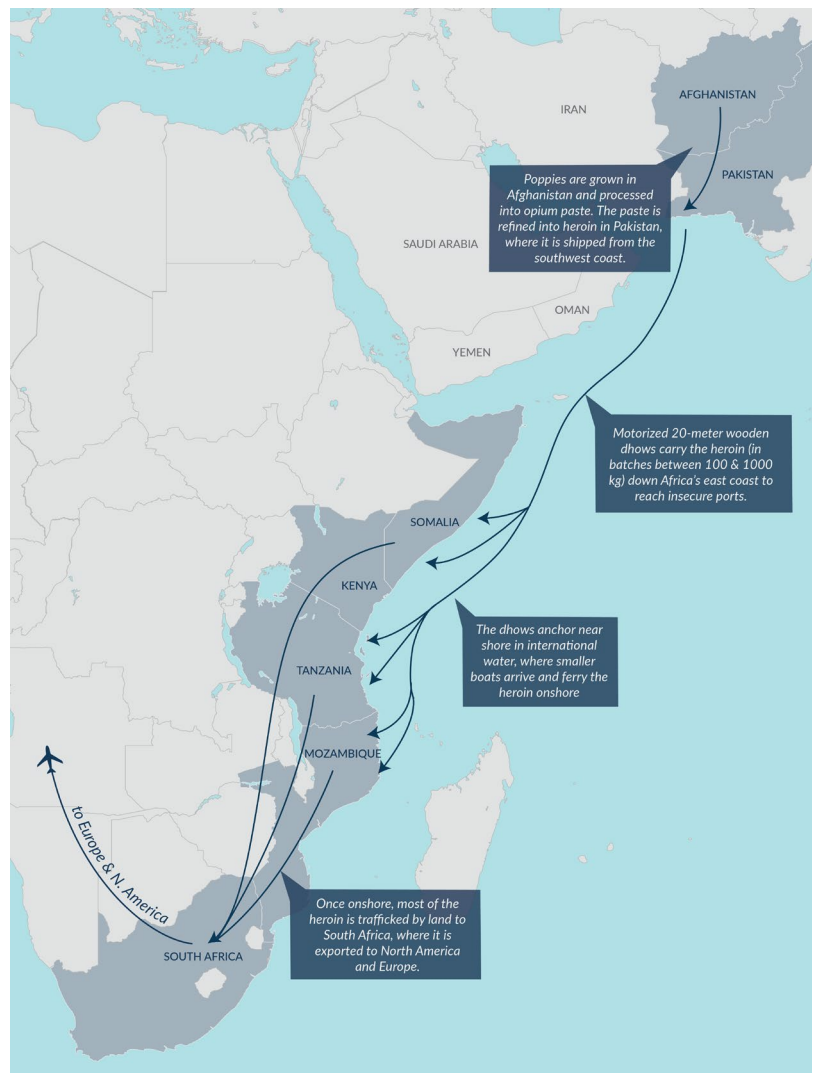FINANCING OF CONFLICTS & NON-STATE ARMED GROUPS

Drug Trafficking

The UN Office on Drugs and Crime's (UNODC's) 2018 World Drug Report predicts that the highest levels of opium and cocaine production ever recorded will lead to increased drug trafficking to meet the demands of new markets. Expanding markets will likely also increase maritime drug trafficking, as many global trafficking routes traverse the world's oceans. A 2018 report on global illicit flows, jointly produced by INTERPOL, RHIPTO, and the Global Initiative against Transnational Crime, found that drug trafficking accounts for 28 percent of the financing of conflicts and of non-state armed groups, including terrorist groups.[59] Maritime drug trafficking, as an extension of trafficking over land, often involves a "marriage of convenience" between politically motivated illicit groups and existing criminal networks. Illicit groups can benefit from the illegal drug trade by securing maritime trafficking routes in exchange for a tax from drug traffickers or producers. The groups can also exploit other actors at sea, including utilizing recreational and fishing vessels to transport drugs.

The international maritime drug trade is highly complex, and its profits fund even landlocked illicit actors. Many of Central Asia's illicit actors are funded by a drug trade that would not reach market without utilizing maritime routes. For example, Afghanistan's notorious heroin trade, which is a critical source of the Taliban's resilience in the country, utilizes a circuitous sea route to reach markets in Europe. The product is transported from Afghanistan to Pakistan's southwest coast, where it then travels by motorized 20-meter wooden dhows along Africa's east coast to reach insecure ports. Off the coast of places like Mozambique, the dhows anchor, awaiting the arrival of smaller boats that ferry the heroin onshore through these ports for distribution.[60]

HEROIN TRAFFICKING ROUTES

Poppies are grown in Afghanistan and processed into opium paste. The paste is refined into heroin in Pakistan, where it is shipped from the southwest coast.

Motorized 20-meter wooden dhows carry the heroin (in batches between 100 & 1000 kg) down Africa's east coast to reach insecure ports.

The dhows anchor near shore in international water, where smaller boats arrive and ferry the heroin onshore

Once onshore, most of the heroin is trafficked by land to South Africa, where it is exported to North America and Europe.

Narco-Submarines (FARC)

In the 1980s, "go-fast boats" became the drug-smuggling vessel of choice in many parts of the world. As radar detection capabilities improved, illicit groups began modifying their vessels to continue their operations. The Revolutionary Armed Forces of Colombia (FARC) illustrated the importance of the sea to the global drug trafficking industry, adapting their maritime transport methods by developing narco-submarines. Originally built to smuggle illicit goods to the United States from South and Central America, narco-submarines are self-propelled maritime vessels with large cargo holds to transport drugs. While early narco-subs were semi-submersible vessels, more recent models are fully submersible, equipped with navigational systems, and capable of traveling long distances.

A boarding team investigates a self-propelled semi-submersible intercepted in international waters off the coast of Central America in 2015. The crew recovered more than 6 tons of cocaine. Photo: Petty Officer 2nd Class LaNola Stone, US Coast Guard.

Evidence of the success of narco-submarines in the illicit drug trade is reflected in a Drug Enforcement Agency estimate that at least 30–40 percent of drugs coming to the United States are transported on narco-subs, with only 5 percent of the vehicles being intercepted by authorities. In 2015, General John Kelly, then commander of the US Department of Defense Southern Command (SOUTHCOM), testified before the Armed Services Committee regarding the threat the illicit drug trade posed to US national security. In his statement, the commander communicated his dissatisfaction with the lack of resources allocated to counter the trade, concluding his statement by cautioning that "terrorist organizations could seek to leverage [the] same smuggling routes to move operatives with intent to cause harm to our citizens or even bring weapons of mass destruction to the United States."[61]

Although FARC was disbanded in mid-2017, narco-submarines continue to be seized in Colombia. By September 2018, the Colombian Navy had captured 14 narco-subs along the country's Pacific coast, more than tripling the seizures of the previous year. According to the US Coast Guard, criminal syndicates in Colombia continue to churn out homemade subs, at an estimated rate of 100 a year. Additionally, other Latin American drug cartels have benefited from the development of the vessels, continuing to use them to transport illicit drugs throughout the region. Today, narco-submarines have been seized in Venezuela, Guyana, Ecuador, and Brazil, and the opportunities for criminal-terrorist cooperation vis-à-vis narco-submarines are many, including the ability to move illicit goods and equipment while remaining largely undetected.

HUMAN SMUGGLING & TRAFFICKING
ACCOUNT FOR ROUGHLY
$150 BILLION ANNUALLY

Maritime Mixed Migration

Maritime mixed migration, which includes migrant smuggling and trafficking, also benefits from utilizing the maritime space. Migrant smuggling involves "a person's entry into a state of which the 'person is not a national or a permanent resident' by crossing borders without complying with national migration law and doing so for financial benefit."[62] Conversely, trafficking involves "the recruitment and transportation of persons, including within one state, by coercive means for purposes of exploitation including sexual exploitation, forced labor

and [slavery]."[63] Combined, human smuggling and trafficking are estimated to be the fourth largest global crime sector today, grossing roughly $150 billion annually. Increases in populations of displaced people worldwide, combined with the interconnectedness of the globalized transportation system, have raised the potential for illicit groups to participate in these activities.[64] A 2018 Financial Action Task Force report on "Financial Flows from Human Trafficking" notes that various terrorist organizations that have controlled or partially controlled territory have used human trafficking to raise funds and support their organizations and activities. These groups include ISIL, Boko Haram, and al-Shabaab.

While both human smuggling and trafficking by sea generally occur as part of wider processes involving land and air movements, detecting these activities at sea often presents greater challenges due to the ungovernable maritime space that allows traffickers to vary their routes. The UNODC estimates that a mere 1 percent of smuggling takes place at sea; however, sea routes are much more perilous and contribute to a much higher human cost, accounting for an estimated 58 percent of overall smuggling fatalities.[65] As issues of human smuggling and human trafficking become more forefront in the public consciousness, stricter border control measures along land routes will undoubtedly push smugglers and traffickers to the sea. The UNODC notes evidence of this between 2009 and 2015, for example, when recorded smuggling activity between Turkey and the European Union shifted from land passages to sea crossings, in response to tightened controls at state borders.[66]

Hundreds of thousands of migrants fleeing Africa's Sahel have tried to reach Europe through Libya. With the removal of Muammar Gaddafi in 2011, and the 2016 EU agreement with Turkey to limit migrant flows through Greece, the human smuggling trade has become a major source of income for cities along Libya's coast. After Gaddafi's fall, terrorist organizations established a presence along both desert smuggling routes and coastal routes. Al-Qaeda extracts revenue from smuggling via its ties to the Libyan black market, and before it was driven out of the coastal city of Sirte, it was reported that ISIS taxed smugglers as they entered port with migrants.[67] In addition to profiting from and facilitating human smuggling and trafficking, illicit groups are increasingly using smuggling networks to enable foreign fighters to move across borders to safe havens.[68]

Licit Business and Money Laundering

Besides profiting from illicit activities at sea, nefarious organizations can also benefit from operating legitimate businesses. These front companies can generate profits and serve as vehicles for money laundering activities. In 2001 the *New York Times* reported that Osama bin Laden owned and operated a string of retail honey shops throughout the Middle East and Pakistan. In addition to generating revenue, the honey was also used to conceal shipments of money and weapons.[69]

There are a few confirmed cases of a legitimate maritime business being used as a front for illicit activities. The first is the case of al-Qaeda in Kenya prior to the 1998 embassy bombings. In August of 1994, Mohammed Saddiq Odeh, a Jordanian member of al-Qaeda who had been trained in the

Maritime Human Smuggling (Tamil Tigers, LTTE)

Sri Lanka's Tamil Tigers were a separatist militant organization fighting for an independent state for Sri Lanka's Tamil minority. Active for several decades between the early 1970s and 2009, the group was highly organized, possessing a political and military wing that included a naval group. The Tamils were supported by an active diaspora population and were rumored to have received training and funding from Indian intelligence services. Besides these external funding sources, the group was actively involved in smuggling human cargoes into Europe and Canada for profit.

In 1986, 155 Tamils were smuggled into Canadian waters from West Germany. Once in Canadian waters, they were taken into custody by authorities. A police station storing the paperwork on the illegal Tamils was firebombed a short time later. Other mass smuggling incidents by sea were carried out in 1986 by the Tamils from West Germany as well as Turkey. Each person paid between $1,700 and $2,900 for their trip from Hamburg to Halifax.[70]

camps in Afghanistan, arrived in Mombasa. That same year, according to court records, another of bin Laden's military commanders, Muhammad Atef, visited Odeh in Mombasa and gave him a fiberglass boat to start a fishing business for al-Qaeda. Under the arrangement, Odeh could take whatever money he needed to live and would give the rest of the profits from the business to al-Qaeda.[71]

The LTTE also operated several legitimate maritime businesses. One was a shipping business that utilized the LTTE fleet to ship timber from Myanmar to Thailand in the late 1980s. This line of business brought the group into contact with the Myanmar military, eventually leading to the establishment of a training base in the town of Twantay in southeastern Myanmar. Another maritime business, Carlton Trading, was an LTTE front company based out of Dhaka, Bangladesh, which was used to move weapons and explosives to operatives in along Sri Lanka's northeast coast.[72]

Unable to access many of its oil and gas installations in the wake of US airstrikes, it was reported in early 2016 that ISIS had begun operating fish farms to fill the void created by its profit losses in the oil industry. Some fish farm owners agreed to cooperate with ISIS, providing a portion of their profits in exchange for protections from the terror group, while other farms left deserted in the fighting were run exclusively by ISIS. Although these specific fish farms were located on inland lakes and waterways, this example shows the potential for similar activities in maritime spaces.

Like take activities, traffic and trade activities in the maritime space are also financially motivated, benefiting from established criminal networks, porous sea borders, and inadequate port security. Relying on relationships and associations with organized criminal enterprises, politically motivated illicit actors finance their activities by utilizing existing logistical and operational nodes integral to these ventures. These activities tend to flourish in environments with high levels of corruption, where public officials turn a blind eye toward the illicit economy, whether out of fear or for personal benefit. In such an environment, delineating between criminal actors and actors with more sinister agendas becomes increasingly difficult.

Traffic and trade activities in the maritime space benefit from established criminal networks, porous sea borders, and inadequate port security, flourishing in environments with high levels of corruption.

ACTIVITY 5
TAX & EXTORT

Obtaining payment outside of sanctioned legal or political frameworks by means of force or intimidation at sea, or by exerting control over a specific maritime area.

OCCURS IN AREAS WITH:

Low Maritime Domain Awareness

Porous sea borders

Inadequate port security

Military & law enforcement corruption

USED BY GROUPS THAT ARE:

Financially strained

Able to control coastal areas

Broad local support for group aims

TACTICS INCLUDE:

Taxation and extortion

Taxation and Extortion in the Maritime Space

According to the Global Initiative's World Atlas of Illicit Financial Flows, illegal taxation is the third largest source of income for non-state armed groups and terrorist groups.[73] As the report notes, these activities are often undertaken by insurgent groups under pressure. As other sources of financing become threatened, armed groups often forcibly collect funds from the communities where they hold influence. Examples of extortion by illicit groups abound, as the Islamic State, al-Shabaab, AQIM, JNIN, FARC, and Boko Haram have all engaged in the activity to generate revenue for their various operations. Illicit groups are able to amass these funds when they control a territory, and either collect them as a show of support from the population (sometimes in the form of Zakat payments) or exert control over territory and impose taxes on communities, business owners, and criminal networks within that territory.[74]

> *Undertaken by political groups under pressure, taxation and extortion make up the 3rd largest source of income for terrorist groups.*

Extortion takes place at sea just as it does on land, with armed groups' exploiting maritime industries like fishing and seaborne shipping. The volume of goods that travel through ports across the globe makes extortion of maritime-centric businesses highly lucrative.

The LTTE benefited greatly from extortion during its lengthy occupation of Sri Lanka's Jaffna Peninsula. During its time reigning over an area in the country's Northern Province, they raised funds by imposing taxes on both licit and illicit goods passing through the region's various ports.

Al-Shabaab operates a comprehensive tax-collection system that has in the past relied heavily on controlling Somali ports. At one point, the group controlled port cities including Kismayo, the commercial capital of Somalia's autonomous Jubaland region. Control over these cities has allowed al-Shabaab to make millions of dollars in profits from charcoal exports.

Before the birth of al-Shabaab in the region, it was reported that al-Qaeda also extorted coastal communities, allegedly seeking refuge in an isolated fishing village called Ras Kamboni on the Kenyan border with Somalia as pressure from AMISOM and US airstrikes mounted. In Ras Kamboni the group built hospitals and training centers with funds from extorting the local fishing trade.[75]

The Houthis have also benefited greatly from extortion activities surrounding ports. Although a cease-fire was declared in the port city of Hodeidah on December 18, 2018, fighting has continued surrounding the port, a lifeline for millions at risk of starvation. Control of Hodeidah is crucial for organizations trying to deliver aid to civilians, as it serves as the entry point for 70 percent of food imports and international aid.[76] But Hodeidah is also critical to the Houthis, who have been taxing commodities and aid coming through the port, helping them to finance their activities and continue to hold territory.

Similarly, the Islamic State in Libya relied heavily on controlling coastal cities and taxing port traffic to fund its operations through collusion with criminal networks. The city of Sabratah, which lies on the Mediterranean coast west of Tripoli, is well known as the migrant capital of Libya. Under ISIS, traffickers paid ISIS a steep tax to send migrants across the sea to Europe, earning millions of dollars a month to continue their activities.

The ability of an illicit group to extort payment by controlling a maritime area requires established political influence. Additionally, extortion activities usually indicate that a group is facing severe financial strain. Extortion activities at sea are usually indicative of inadequate port security, as much of this activity takes place at ports of entry/exit. Additionally, like traffic and trade activities, tax and extort activities often flourish in areas where there is prevalent military and law enforcement corruption.

Illicit Charcoal Trade (al-Shabaab)

In 2012, the United Nations Security Council imposed a ban prohibiting exports of Somali charcoal in an effort to choke off the funding stream to al-Qaeda-linked al-Shabaab. A 2011 UN report detailing how the group benefited from the charcoal trade noted that the group's control of large port cities like Kismayo allowed them to exact taxes on the export of charcoal and to trade charcoal for sugar, which it then smuggled into neighboring Kenya. Shipping companies delivered sugar to Kismayo and collected charcoal for their return journeys, depositing profits into bank accounts in the Gulf States. The money was used to "launder voluntary contributions to al-Shabaab through fraudulent invoicing, overvaluing of import proceeds and undervaluing of exports."[77] This trade cycle was highly dependent on Somali businessmen, lured by al-Shabaab's low tax rates when compared to Somalia's transitional federal government. Additionally, the group offered preferential tax breaks to al-Shabaab-affiliated business.[78]

The six main ports for charcoal exports in southern Somalia were once controlled by al-Shabaab. These included Kismayo, as well as Baraawe, Marka, Buur Gaabo, Eel Ma, and Qudha. Al-Shabaab capitalized on its profits from the charcoal trade by levying taxes against large motor vessel owners (who were taxed per bag of charcoal they transferred), as well as barge owners and porters employed to load and unload charcoal at port.[79]

Despite the UN ban, charcoal exports from Somalia continue to thrive, generating millions of dollars for al-Shabaab each year. The main destination for the illicit trade is Iran, where the product is often labeled as coming from West Africa and then loaded onto Iranian-flagged ships and sent to the Gulf States carrying false certificates of origin. At a UN-sponsored summit in May 2018, Somali officials asked for international cooperation to continue the fight against the illicit trade, noting the connection between the exports and regional insecurity tied to environmental degradation and financial flows to violent armed groups.

Combined Italian and Croatian boarding team approach British Royal Navy vessel during a boarding exercise on Operation Sea Guardian, a standing Maritime Security Operation to deter and counter terrorism and other threats to maritime security in the Mediterranean Sea. Photo: NATO Operation Sea Guardian.

CONCLUSION

The jihadist landscape has evolved a great deal over the course of the last few years. Last year, 2018, saw the Islamic State cede most of its territory in Iraq and Syria, and the deaths of thousands of its leaders have badly damaged the group's command and control infrastructures. Further, the group's revenues and resources have been depleted. A recent United Nations Security Council report states that the Islamic State is "transforming into a terror organization with a flat hierarchy, with cells and affiliates increasingly acting autonomously."[80] Similarly, al-Qaeda's worldwide affiliates are now increasingly identifying locally rather than transnationally. These developments will undoubtedly impact the funding, resourcing, and delivery of acts of political violence.

In the future, local affiliates of organizations like the Islamic State and al-Qaeda will likely be more financially strained, as well as increasingly motivated to conduct attacks to illustrate their relevance as power players on the local and international stage. These organizations going "glocal" means that countering the threats they pose will rely even more heavily on local-level governments, military, and law enforcement professionals working together to comprehensively address factors that encourage and facilitate their activities. As this paper illustrates, these strategies will be incomplete without considering the wide range of activities, both politically and financially motivated, that play out on the world's oceans.

1. As an important first step, stakeholders at all levels should be aware of both historical and current uses of the maritime space and their ties to onshore political violence. **INCREASING MARITIME DOMAIN AWARENESS IS CRITICAL TO ENCOURAGING DIALOGUE AND ENHANCING COLLABORATION AND COORDINATION AMONG BOTH STATE AND REGIONAL PARTIES**, as sea blindness is often a systemic issue. Regional initiatives including the 2017 Jeddah Amendment to the Djibouti Code of Conduct (Western Indian Ocean), the Yaoundé Code of Conduct for the Gulf of Guinea, and the Contact Group for Maritime Crime in the Sulu and Celebes Seas serve as examples of how acknowledging the importance of the maritime space can lead to collaborative regional efforts to combat underlying security issues through facilitating information sharing and lessons learned.

2. Second, **IT IS CRITICAL THAT STAKEHOLDERS WORK TO IDENTIFY SPECIFIC ENVIRONMENTAL RISK FACTORS THAT ENCOURAGE ILLICIT MARITIME ACTIVITIES.** This includes characterizing and addressing weak or under-resourced systems like maritime enforcement and response capacity, and maritime infrastructure like ports. As well, acknowledging socioeconomic and political conditions that invite illicit activities and promote an illicit economy is crucial, as terror groups will usurp existing systems to facilitate and fund their operations.

3. Third, **STAKEHOLDERS SHOULD UNDERSTAND UNDER WHAT CONDITIONS ILLICIT GROUPS ARE LIKELY TO PARTICIPATE IN CERTAIN ACTIVITIES.** As the range of activities described in this paper illustrates, the maritime space can be used for both financial and political gain. Therefore, understanding the financial, tactical, and operational needs of these groups is key to neutralizing these activities. Further, it is imperative that stakeholders are cognizant of how curbing a particular activity might influence a group's adoption of another. There are numerous examples of how onshore operations to curtail illicit activities have led to these activities playing out at sea. As the international community works to address the maritime drivers of organized political violence, it is important to recognize that one maritime activity might easily supersede another, particularly if a group possesses a maritime capability.

4. Finally, **THE INTERNATIONAL COMMUNITY MUST ACKNOWLEDGE THAT VIOLENCE DOES NOT START AND END AT THE SHORE.** The longer the world's vast, ungovernable maritime spaces are ignored and deprioritized in the fight against global crime and terror, the more dire the consequences.

ENDNOTES

1 There are variations of the spelling of the long form of LeT. These include Lashkar-e-Taiba and Lashkar-e-Tayyiba.

2 Alan Cummings, "The Mumbai Attack: Terrorism from the Sea," Center for International Maritime Security, July 29, 2014, cimsec.org.

3 Dave Mugridge, "Malaise or Farce: The International Failure of Maritime Security," Canadian Naval Review 4, no. 4 (2009): 21.

4 Christian Bueger and Timothy Edmunds, "Beyond Seablindness: A New Agenda for Maritime Security Studies," International Affairs 93, no. 6 (November 2017): 1296.

5 Mugridge, "Malaise or Farce," 22.

6 "Sustainable Development Goal 16, Targets and Indicators" United Nations, Sustainable Development Knowledge Platform, https://sustainabledevelopment.un.org/sdg16.

7 Judah Ari Gross, "IDF Says It Targeted 'Advanced' Hamas Naval Capabilities in Gaza Airstrikes," Times of Israel, May 30, 2018, https://www.timesofisrael.com/idf-says-it-targeted-hamas-submarine-drones-in-gaza-airstrikes/.

8 "Prior to Deadly 26/11 Mumbai Terror Attacks, Ajmal Kasab Was Given Exhaustive 'Sea Training,'" India Times, November 25, 2018.

9 "Gunmen in Boats Attack Presidential Palace in Equatorial Guinea," New York Times, November 7, 2009.

10 Abhijit Singh, "India's Coastal Security: An Assessment," Observer Research Foundation, November 23, 2018, https://www.orfonline.org/expert-speak/indias-coastal-security-an-assessment-45692/.

11 "Pakistan Based Terror Groups Training Cadre for 'Samundari Jihad': Government," Economic Times, January 2, 2019, https://economictimes.indiatimes.com/news/defence/pakistan-based-terror-groups-training-cadre-for-samundari-jihad-government/articleshow/67347936.cms.

12 Sam Yusa, "Malaysia and Indonesia Foreign Fighter Transit Route to Philippines Identified," Defense Post, November 20, 2018.

13 Paul Staniland, "Improving India's Counterterrorism Policy after Mumbai," CTC Sentinel 2, no. 4 (April 2009).

14 Robert D. Blackwill, Peter Chalk, Kim Cragin, C. Christine Fair, Brian A. Jackson, Brian Michael Jenkins, Seth G. Jones, Angel Rabasa, Nathaniel Shestak, and Ashley J. Tellis, "The Lessons of Mumbai" (occasional paper, RAND Corporation, Santa Monica, CA, 2009), 9.

15 Ibid.

16 Ibid., 10.

17 Ibid.

18 James Stavridis, "Terrorists Have Been All Too Effective by Air and Land. What If They Hit by Sea?" Time, June 29, 2017.

19 Brian Michael Jenkins, Bonnie Cordes, Karen Gardela, Geraldine Petty, "A Chronology of Terrorist Attacks and Other Criminal Actions against Maritime Targets (RAND Paper Series, Rand Corporation, Santa Monica, CA, September 1983),6.

20 "Shipping and World Trade: Overview," International Chamber of Shipping, http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade.

21 "Security in Maritime Transport: Risk Factors and Economic Impact," Maritime Transport Committee, Organization for Economic Cooperation and Development, 2003, http://www.oecd.org/newsroom/4375896.pdf.

22 Lydelle Joubert, "The Extent of Maritime Terrorism and Piracy: A Comparative Analysis," Scientia Militaria: South African Journal of Military Studies 41, no. 1 (2013): 113.

23 Derek Johnson, Erika Pladdet, and Mark Valencia, "Introduction: Research on Southeast Asian Piracy," in Derek Johnson and Mark Valencia, eds., Piracy in Southeast Asia: Status, Issues, and Responses (Singapore: Institute of Southeast Asian Studies, 2005).

24 Sam Bateman, "Assessing the Threat of Maritime Terrorism: Issues for the Asia-Pacific Region," Security Challenges 2, no. 2 (2006), https://www.regionalsecurity.org.au/Resources/Files/vol2no3Bateman.pdf.

25 Michael Knights and Farzini Nadimi, "Curbing Houthi Attacks on Civilian Ships in the Bab al-Mandab," Policywatch 2998, Washington Institute, July 27, 2018, https://www.washingtoninstitute.org.

26 Ibid.

27 Jonathan Lee Mocker, "Maritime Improvised Explosive Devices: A Threat Based Technology Study" (master's thesis, US Army Command and General Staff College, 2015), https://apps.dtic.mil/dtic/tr/fulltext/u2/a624055.pdf.

28 Ibid.

29 Marco D. Tomasi, "Water-Borne IED Threats and the Strait of Hormuz," JIEDDO J2 Global Information Research Center, n.d., https://info.publicintelligence.net/JIEDDO-Hormuz.pdf.

30 James Carafano, "Small Boats, Big Worries: Thwarting Terrorist Attacks from the Sea," Heritage Foundation, 2007, https://www.heritage.org.

31 Ibid.

32 Ibid.

33 Ibid.

34 Gerry J. Gilmore, "Cohen Absolves USS Cole Skipper, Crew," DoD News, January 22, 2001, http://archive.defense.gov/news/newsarticle.aspx?id=45123.

35 Karen Brandon, "FBI Puts Scuba Dive Shops, Schools on Terrorism Alert," Chicago Tribune, June 6, 2002.

36 Shishir Gupta, "India on Alert against Possible Lashkar, Jaish Attacks from the Sea," Hindustan Times, October 12, 2018.

37 Oana Maria Dinu and Anamaria Ilie, "Maritime Vessel Obsolescence, Life Cycle Cost and Design Service LIfe," IOP Conference Series: Materials Science and Engineering 95, no. 1 (2015), http://iopscience.iop.org/article/10.1088/1757899X/95/1/012067/pdf.

38 Andy Greenberg, "The Untold Story of Notpetya, the Most Devastating Cyber Attack in History," Wired Magazine, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

39 Saed Abu-Nimeh, Ernest Foo, Igor Nai Fovino, Manimaran Govindarasu, and Thomas Morris, "Cyber Security of Networked Critical Infrastructures," IEEE Network 27, no. 1 (2013): 3–4, DOI: 10.1109/MNET.2013.6423184.

40 Louise Matsakis, "What Would Really Happen if Russia Attacked Undersea Internet Cables," Wired Magazine, January 5, 2018.

41 John Filitz, "Threats from Below: Undersea Fiber-Optic Cable Criticality," One Earth Future Foundation, March 27, 2019, 3, https://stableseas.org/publications/threats-below-undersea-fiber-optic-cable-criticality.

42 Stanojoska Angelina, "The Connections between Terrorism and Organized Crime: Narcoterrorism and Other Hybrids" (paper, Faculty of Security, Skopje, Republic of Macedonia, n.d.), 1, https://wb-iisg.com/wp-content/uploads/bp-attachments/4745/Angelina-Stanojoska_The_Connection_between_Terrorism_and_Org.pdf.

43 "Legal Framework for the Repression of Piracy under UNCLOS," United Nations, http://www.un.org/Depts/los/piracy/piracy_legal_framework.htm.

44 "Increase in Piracy and Terrorism at Sea: Little Evidence Supports Fear That the Two Crimes Are Merging" (press release, RAND Corporation, Santa Monica, CA, June 2008), https://www.rand.org/news/press/2008/06/05.html.

45 "Organized Maritime Piracy and Related Kidnapping for Ransom," Financial Action Task Force, July 2011, http://www.fatfgafi.org/media/fatf/documents/reports/organised%20maritime%20piracy%20and%20related%20kidnapping%20for%20ransom.pdf.

46 Ibid.

47 Alexandra Amling, Curtis Bell, Asyura Salleh, Jay Benson, and Sean Duncan, "Stable Seas: Sulu and Celebes Seas," One Earth Future Foundation, February 19, 2019, 26, https://stableseas.org/publications/sulu-celebes-seas.

48 Jim Gomez, "AP NewsBreak: Abu Sayyaf Hot $7.3 Million from Kidnappings," Associated Press, October 27, 2016.

49 "Two Piracy Incidents Reported to ReCAAP ISC Last Week," SAFETY4SEA, November 12, 2018, https://safety4sea.com/two-piracy-incidents-reported-to-recaap-isc-last-week-2/.

50 Jeff Desjardins, "Fuel Theft Is a Big Problem," Business Insider, May 7, 2017.

51 Oriji Alurechi Boniface and Odagme Baridor Samuel, "Oil Bunkering Activities in the Niger Delta 'The Way Forward,'" American Journal of Engineering Research 5, no. 4 (2016): 169–173, http://www.ajer.org/papers/v5(04)/U050401690173.pdfhttps://www.researchgate.net/publication/311486000_Oil_Bunkering_Activities_in_the_Niger_Delta_The_Way_Forward.

52 Peri-Khan Aqrawi-Whitcomb, Morgan D. Bazilian, and Cyril Widdershoven, "The World's Most Dangerous Black Markets," YaleGlobal Online, October 9, 2018, https://yaleglobal.yale.edu/content/worlds-most-dangerous-black-markets.

53 Paul Ugor, "The Niger Delta Wetland, Illegal Oil Bunkering and Youth Identity Politics in Nigeria," Postcolonial Text 8, no. 3 (2013), https://www.postcolonial.org/index.php/pct/article/view/1725/1606.

54 "Movement for the Emancipation of the Niger Delta (MEND)," Global Security, https://www.globalsecurity.org/military/world/para/mend.htm.

55 Ugor, "Niger Delta Wetland," 8.

56 Ibid.

57 Ibid., 7.

58 Richard Norton-Taylor, "Sea Trafficking Report Reveals How Ships Move Guns and Drugs," The Guardian, January 29, 2012, https://www.theguardian.com/world/2012/jan/30/sea-trafficking-report-guns-drugs.

59 Global Initiative, "World Atlas of Financial Flows," 2018, https://globalinitiative.net/wp-content/uploads/2018/09/Atlas-Illicit-Flows-FINAL-WEB-VERSION-copia-compressed.pdf.

60 "How WhatsApp Has Helped Heroin Become Mozambique's Second Biggest Export," BBC, July 9, 2018.

61 Byron Ramirez, "The Criminal and Terrorist Threat of Narco Submarine Technology," Geopolitical Monitor, June 7, 2016, https://www.geopoliticalmonitor.com/the-criminal-and-terrorist-threat-of-narco-submarine-technology/.

62 "Protocol against the Smuggling of Migrants by Land, Sea and Air, Supplementing the United Nations Convention against Transnational Organized Crime," United Nations, November 2000, https://www.ohchr.org/EN/ProfessionalInterest/Pages/TransnationalOrganizedCrime.aspx.

63 Ibid.

64 "Financial Flows from Human Trafficking," Financial Action Task Force, July 2018, https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf.

65 "Global Study on Smuggling of Migrants," United Nations Office on Drugs and Crime, 2018, https://www.unodc.org/documents/data-and-analysis/glosom/GLOSOM_2018_web_small.pdf.

66 Ibid.

67 Alexander Farley, "The New Slave Trade: Migration, Trafficking, and Terrorists in Libya," Environmental Change and Security Program, Wilson Center, 2018, https://www.newsecuritybeat.org/2018/08/slave-trade-migration-trafficking-terrorists-libya/.

68 Global Initiative, "World Atlas of Financial Flows."

69 Eben Kaplan, "Tracking Down Terrorist Financing," Council on Foreign Relations, April 2006, https://www.cfr.org/backgrounder/tracking-down-terrorist-financing.

70 "Funding Terror: The Liberation Tigers of Tamil Eelam and Their Criminal Activities in Canada and the Western World," Mackenzie Institute, 1995, http://mackenzieinstitute.com/funding-terror-the-liberation-tigers-of-tamil-eelam-and-their-criminal-activities-in-canada-and-the-western-world/.

71 Marc Lacey and Benjamin Weiser, "After Attack, Kenya Traces Qaeda's Trail in East Africa," New York Times, December 1, 2002, https://www.nytimes.com/2002/12/01/world/after-attack-kenya-traces-qaeda-s-trail-in-east-africa.html.

72 Peter Chalk, "Liberation Tigers of Tamil Eelam's (LTTE) International Organization and Operation: A Preliminary Analysis" (Commentary no. 77, Canadian Security Intelligence Service, March 17, 2000).

73 Global Initiative, "World Atlas of Financial Flows."

74 Yuliya Zabyelina, "Extortion as a Method of Terrorism Financing," Strategic Hub for Organized Crime Research, November 1, 2018, https://shoc.rusi.org/informer/extortion-method-terrorism-financing.

75 Ibid.

76 Ahmed Al-Haj and Maggie Michael, "Key Battle for Strategic Port Risks Tipping Yemen into Famine," Navy Times, October 4, 2018.

77 Mark Leon Goldberg, "How the Charcoal Trade Fuels Terrorism," UN Dispatch, February 22, 2012, https://www.undispatch.com/how-the-charcoal-trade-fuels-terrorism/.

78 Ibid.

79 Ibid.

80 "Twenty-First Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and Associated Individuals and Entities," United Nations, January 26, 2018, https://www.un.org/en/ga/search/view_doc.asp?symbol=S/2018/14.

ONE EARTH FUTURE

oneearthfuture.org

One Earth Future (OEF) is a self-funded, private operating foundation seeking to create a more peaceful world through collaborative, data-driven initiatives. OEF focuses on enhancing maritime cooperation, creating sustainable jobs in fragile economies, and research which actively contributes to thought leadership on global issues. As an operating foundation, OEF provides strategic, financial, and administrative support allowing its programs to focus deeply on complex problems and to create constructive alternatives to violent conflict.

STABLE SEAS

stableseas.org

Stable Seas, a program of One Earth Future, engages the international security community with novel research on illicit maritime activities such as piracy and armed robbery, trafficking and smuggling in persons, IUU (illegal/unregulated/unreported) fishing, and illicit trades in weapons, drugs, and other contraband. These activities perpetuate organized political violence and reinforce each other to threaten economic development and the welfare of coastal populations.

CONTACT US

📞 303.533.1715   ✉ info@oneearthfuture.org   📍 525 Zang St. Broomfield, CO 80021

STABLE SEAS

a program of One Earth Future

one earth
FUTURE
Peace Through Governance