Maritime Improvised Explosive Device (M-IED) Threat to Energy Security

By CDR H. Ceyhun TURE

Maritime Improvised Explosive Device (M-IED) Threat to Energy Security

CDR H. Ceyhun TURE (Turkish Navy) is a Subject Matter Expert in Education Training & Exercise Division, NATO Energy Security Centre of Excellence

Introduction

Mitigating strategic vulnerabilities, enhancing Energy Security, investing in stable and reliable energy supply, suppliers, and sources are of significant importance. Together with Maritime Security focused on critical energy infrastructure and trade achieves peace and prosperity for the Alliance and Partners.[1]

Energy Security is a critical component to the common security of NATO. NATO's role in energy security, first defined in 2008 at the Bucharest Summit, has since been emphasized as part of the seven baseline requirements of resiliency for civil preparedness. The NATO Energy Security Centre of Excellence in Vilnius, Lithuania has led NATO's initiatives to assist Allies and Partners awareness and preparedness against hybrid threats to Energy Security since 2012.[2] The readiness of Allies and Partners to successfully execute military operations can be compromised through disruptions of energy supplies. Although the primary responsibility for addressing these concerns lies with individual member states, in accordance with Article 3, NATO members consistently engage collectively in consultations regarding Energy Security.[3] NATO has prioritized its role and efforts into three focus areas; Raising Energy Security Awareness, Supporting the Protection of Critical Energy Infrastructure and Enhancing Energy Efficiency in the Military Operations.[4]

In accordance with the NATO Strategic Concept approved in 2010, NATO's focus on **Maritime Security** was further developed through the Alliance Maritime Strategy document in 2011. The NATO Maritime Security Center of Excellence in Istanbul/Turkiye, actively supports NATO in maritime security matters, aiming to expand the capabilities of NATO and partner nations by providing comprehensive,

[1] NATO Strategic Concept 2022, NATO Website, Accessed 15.05.2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

[2] NATO Energy Security, NATO Website, Accessed 15.05.2023, https://www.nato.int/cps/en/natohq/topics_49208.htm

[3] Countering Terrorism Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 2), 2022, p.161.

[4] Julijus Grubliauskas & Michael Rühle, Energy security: a critical concern for Allies and partners, 2018, p.3.

innovative, and timely expertise in the field of maritime security operations.[5] The Alliance Maritime Strategy document emphasizes the importance of safeguarding the freedom of navigation, sea-based trade routes, critical infrastructure, energy flows, protection of marine resources, and environmental safety as essential components of the security interests of Allies. Additionally, NATO's maritime forces are prepared to contribute to energy security, including the protection of critical energy infrastructure and sea lines of communication.

After defining NATO's approach to Energy Security and Maritime Security, it becomes clear that these two areas are closely interconnected and require a coordinated and comprehensive approach to effectively address shared concerns, specifically focusing on the protection of critical energy infrastructure in the maritime domain. In addition, numbers are incredibly remarkable: water covers 70% of the Earth's surface, approximately 80% of the global population resides within a 100-mile radius of the coastline, and about 90% of global trade is conducted through maritime routes[6] and tankers play a crucial role in transporting more than 50% of the world's oil.[7] As depicted in Figure 1, approximately 33% of the commodities transported globally by sea consist of energy products.[8] Moreover, when considering energy-related products as well, this percentage has the potential to further increase.

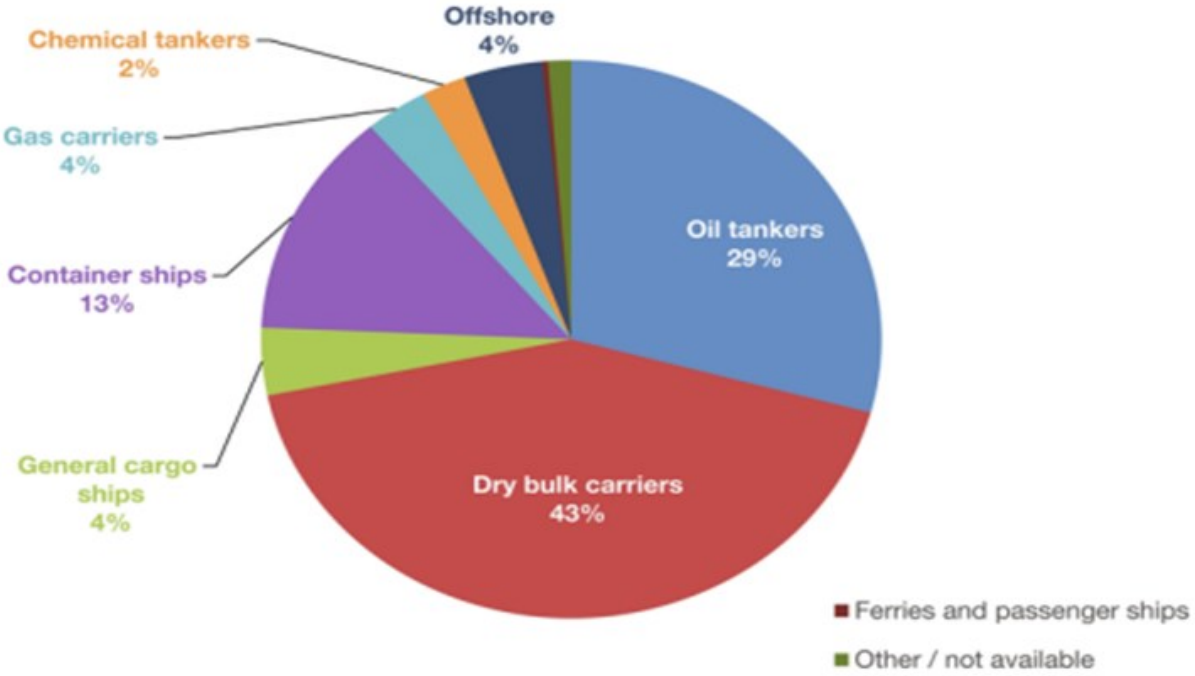

Figure 1. World fleet by principle vessel type in 2018, by share of dead-weight tonnage. Review of Maritime Transport 2018, United Nations 2018

[5] NATO MARSEC COE Website, Accessed 21.05.2023, https://www.marseccoe.org/history/

[6] Alliance Maritime Strategy, Accessed 24.05.2023, NATO Website, https://www.nato.int/cps/en/natohq/official_texts_75615.htm

[7] NATO's maritime activities, Accessed 24.05.2023 NATO Website, https://www.nato.int/cps/en/natohq/topics_70759.htm

[8] Riley EJ Schnurr & Tony R Walker, Marine Transportation and Energy Use, 2019, p.3.

In Addition, maritime energy infrastructure has experienced significant growth and transformation in recent decades. One of the notable developments is the increasing utilization of the sea as a source of energy, with larger wind farms being constructed further offshore.[9] Additionally, the use of underwater pipelines has become the most cost-effective, secure, and efficient method for transporting oil and gas, leading to a global increase in investments in this area.[10] However, maritime energy shipping faces numerous threats[11], including maritime improvised explosive devices (M-IEDs), particularly in chokepoints as illustrated in Figure 2.

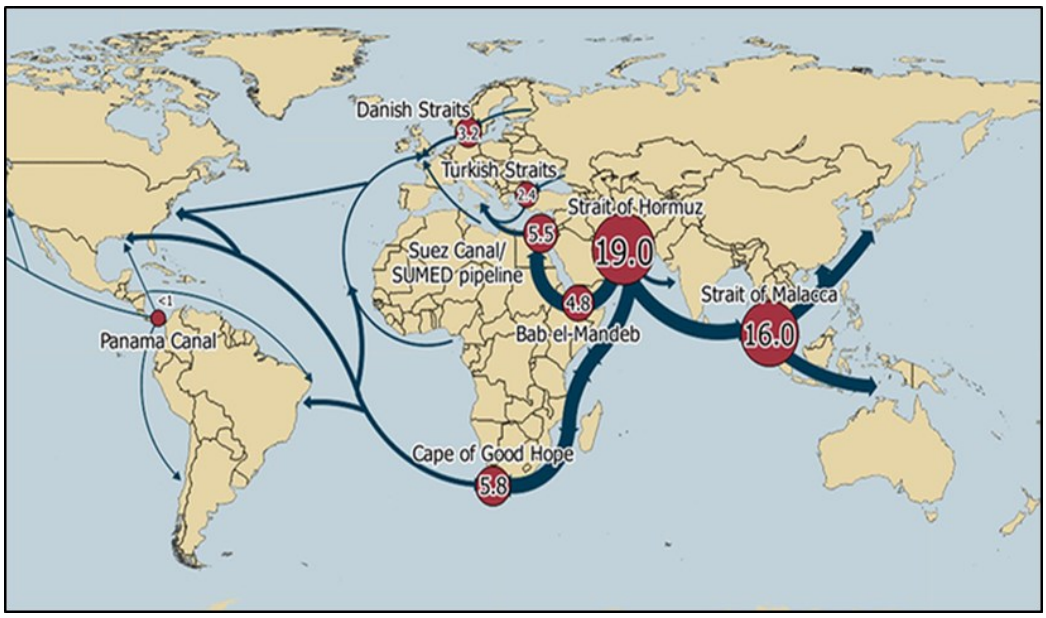

Figure 2. Daily transit volumes through world maritime oil chokepoints. Source: EIA, U.S. Energy Information Administration.

Furthermore, it is important to recognize that critical underwater infrastructures, such as underwater pipelines, offshore windfarms, and electrical cables are increasingly vulnerable targets for terrorists and adversaries. These infrastructures play a vital role in various sectors, including energy production and transmission. Terrorists or adversaries may use M-IEDs to target these underwater assets to disrupt energy supplies, cause economic damage, or gain a strategic advantage.

While addressing the threat of M-IEDs, it is important to conduct a thorough examination of the risks and consequences associated, particularly to emphasize and increase awareness of the M-IED threats and challenges in protecting critical energy infrastructure in the maritime domain. In this regard, this article will focus on the following sections: "Why Terrorists Target Energy Infrastructure", "Improvised Explosive Devices (IEDs)", "Analyzing Maritime Improvised Explosive Devices (M-IEDs)", and finally, "Conclusions."

---

9 UK Board of Trade, A Board of Trade Paper 2022, p.27.

10 Sciencedirect Website, Accessed 19.05.2023, https://www.sciencedirect.com/topics/engineering/submarine-pipeline

11 Oktay Çetin, Mesut Can Köseoğlu, A Study on the Classification of Maritime Security Threat Topics, International Journal of Environment and Geoinformatics (IJEGEO), 2020, p. 369.

Why Terrorists Target Energy Infrastructure

Terrorism directed towards the energy sector is an escalating global phenomenon.[12] Statistics reveal a notable increase in such attacks over the years. In 2003, they accounted for 25% of terrorist incidents, which rose to 35% in 2005. In 2016, there was a 14% surge in terrorist attacks specifically targeting the oil and gas industry, making up nearly 42% of all attacks.[13] Terrorists generally do not display irrational behavior in their actions; instead, they carefully assess vulnerabilities, evaluate potential consequences, and aim to maximize their impact while minimizing costs and risks.[14]

Besides, attacks on maritime critical energy infrastructure or oil tankers could have significant strategic effects. They have the potential to influence global energy prices and even geopolitical dynamics, as seen in the aftermath of incidents such as the Nord Stream pipeline explosions. This factor alone can serve as a major motivation for adversaries or terrorist organizations to target such infrastructures.

Furthermore, the characteristics of energy infrastructures contribute to their attractiveness as targets for terrorists. The restricted mobility and expansive geographic footprint of these infrastructures makes them vulnerable and easier for potential attacks to go undetected and non-attributable. The extensive coverage area, coupled with the difficulties in effectively patrolling and controlling such vast spaces, presents significant challenges for security forces. Moreover, the intricate legal framework in maritime domain, especially in international waters, adds further difficulties.

Threat and vulnerability matrix below presents a risk assessment that highlights the varying degrees to which different types of infrastructure and vessels have been targeted. Certain assets, such as product tankers, VLCCs (Very Large Crude Carrier), offshore vessels, tank farms, and oil and gas processing plants, continue to face threats due to their physical and operational vulnerabilities.[15]

---

[12] Jose R. Valdivia Orbaneja , Subramanian R. Iyer , Betty J. Simkins , Terrorism and oil markets: a cross-sectional evaluation, Finance Research Letters, 2018, p.3.

[13] Countering Terrorism Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 2), 2022, p.166.

[14] Journal of Strategic Security, Accessed 25.05.2023, https://digitalcommons.usf.edu/ cgi/ viewcontent.cgi?article=1258&context=jss.

[15] Ruxandra-Laura Boşilcă, Susana Ferreira, and Barry J. Ryan Routledge Handbook of Maritime Security 2022, p. 209.

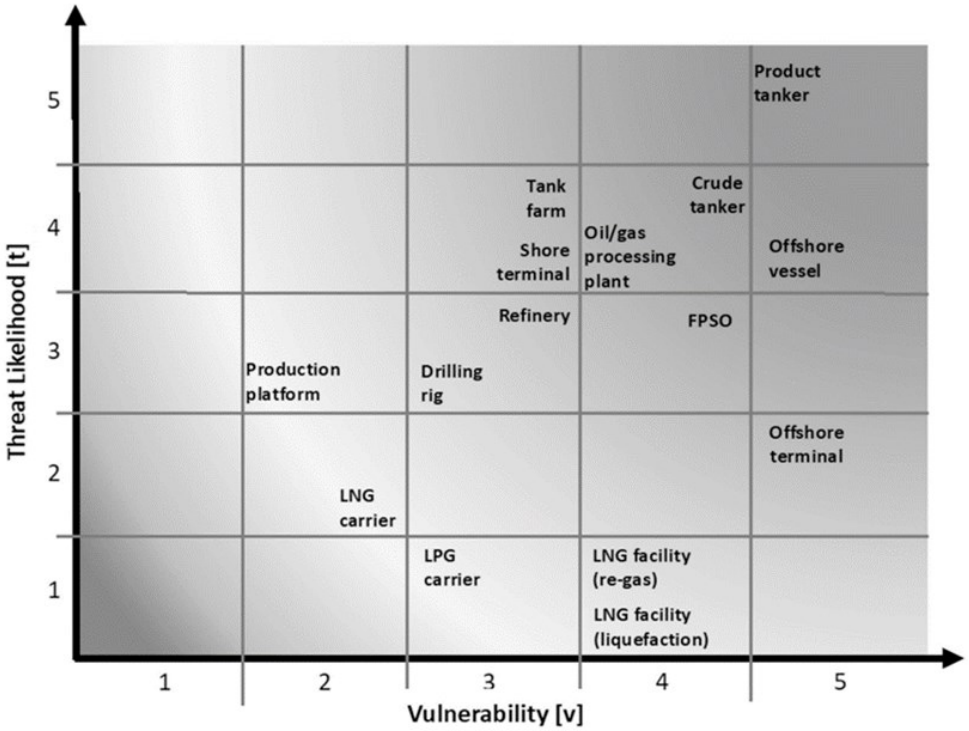

Figure 3. Energy Security at Sea (Vulnerabilities and Threats)

In accordance to Figure 3, tankers and offshore vessels are particularly vulnerable to attacks, during the loading/discharging process, slow speeds in pilotage waters or anchorages, and transiting chokepoints. However, it is important to note that despite these vulnerabilities, oil tankers are not easily destroyed, sunk, or rendered a total loss as evidenced during the 1984–1988 Tanker War.[16] The combination of their structural robustness, double hulls, compartmentalization, and the inherent difficulty in igniting crude oil make it challenging for terrorists or saboteurs to achieve the desired catastrophic effect. While it is not impossible for an attacker with the right weapons or sufficient explosives to destroy a large crude oil tanker, it presents significant difficulties.

Besides the oil sector, the LNG sector is currently experiencing accelerated growth in the number of new tankers and portside liquefaction facilities. These assets are valuable in the processing and delivery of LNG, which is a low-carbon fossil fuel utilized by countries as part of their efforts to move towards net-zero emissions. Currently, this infrastructure is not classified as high risk. As a historical example, during the Iran-Iraq war in October 1984, an LNG cargo vessel took a direct hit from an Exocet anti-ship missile. The ship did not explode, and the crew was able to contain the fire. However, this does not diminish the need for robust security measures for these assets. Instead, it emphasizes the importance of implementing effective preventive security measures.[17]

[16] Strauss Center Website, Accessed 25.05.2023, https://www.strausscenter.org/strait-of-hormuz-oil-tanker-security/

[17] Jessica Resnick-Ault, Who's Afraid of LNG?, Accessed 25.05.2023, http://www.greenfutures.org/projects/LNG/LNG1-4-04.html

Alternatively, a fire in the pipes of a liquefaction facility in Freeport, Texas, USA, in June 2022, brought operations to a standstill for almost a year. Output from the Freeport LNG Facility made up 18% of US LNG exports. This disruption came at a time when Europe was at its most vulnerable, facing a potential shortage of gas in preparations to weather the 2022/23 winter. These types of disruptions to global energy supply and markets are attractive motivations for terrorists and adversaries to exact their demands or objectives. Kinetic destructive methods currently in use and growing are Improvised Explosive Devices (IEDs) used to target critical points within the supply chain of oil, gas, and LNG.

Improvised Explosive Devices (IEDs)

IED is a device placed or fabricated in an improvised manner incorporating explosive material, destructive, lethal, noxious, incendiary, pyrotechnic materials or chemicals designed to destroy, disfigure, distract or harass. They may incorporate military stores but are normally devised from non-military components.[20] We can categorize the main types of IEDs as Victim-Operated IEDs, Command-Operated IEDs, Time-Operated IEDs and it is generally accepted that the main components of an IED include: Switch, Power source, Initiator, Compartment and Explosive (SPICE).[21]

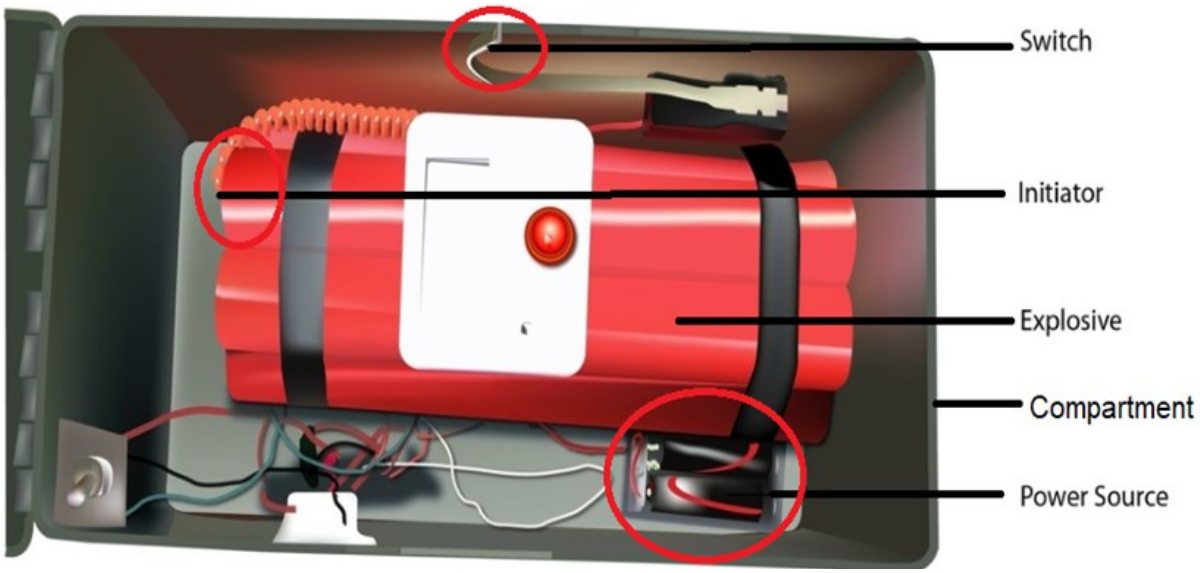

Figure 4. Main Components of an Improvised Explosive Device (IED)

[18] Ruxandra-Laura Boşilcă, Susana Ferreira, and Barry J. Ryan Routledge Handbook of Maritime Security 2022, p. 208.
[19] CNN Business Website, Accessed 20.06.2023, https://edition.cnn.com/2022/06/09/energy/us-lng-plant-explosion/index.html
[20] The United Nations International Ammunition Technical Guidelines, 3rd Edition 2021, p.17.
[21] The United Nations Institute for Disarmament Research (UNIDIR), Accessed 29.05.2023, https://unidir.org/sites/default/files/publication/pdfs//-en-641.pdf

As referred the "the cannon of the 21st century" or "weapon of poor" IEDs have significantly affected operations with their powerful and disproportionate effects. IED threats stems from their low cost and simplicity in production, which gives those who use them an advantage in asymmetric warfare. Their straightforward construction and ability to cause extensive harm present a significant challenge for security forces and civilians alike, requiring increased alertness and countermeasures to reduce the danger.

As it is widely recognized, countering IED attacks demands the imperative of close cooperation among a range of stakeholders, encompassing; diplomatic, military, law enforcement, economic, information, academic, and private sector entities. Figure 6 illustrating the, IED Attack Planning & Phases, shows the necessity for this collaboration.

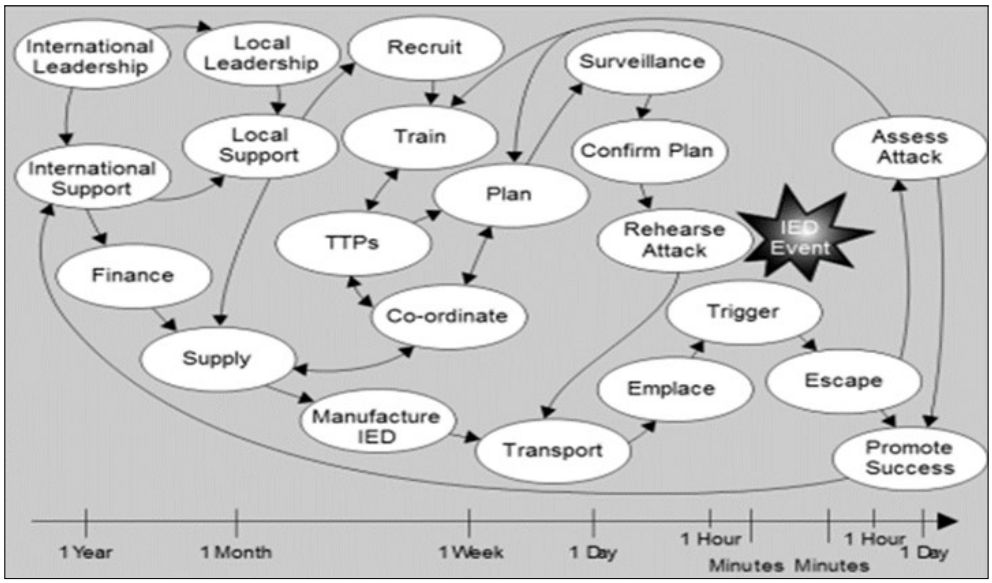

Figure 5. Activities Take Place Before and After IED Attack, *(Source: AJP-3.15)*

In this regard, NATO took measures to coordinate and standardize joint efforts within the coalition, resulting in the establishment of STANAG 2295 (AJP 3 -15), with the objective of fostering mutual comprehension and coordination between nations, this endeavor is referred to as "Counter Improvised Explosive Devices (C-IED)". The purpose is to promote a shared understanding and interoperability among participating countries. In accordance to this publication, C-IED has three main pillars: Attack the Network (Atn), Prepare the Force (PtF) and Defeat the Device (Dtd).

However, the document primarily focuses on land operations because historically the most prominent and observable threat was on land. The emerging threat, which is not addressed, is Maritime Improvised Explosive Devices (M-IEDs). IEDs in the maritime domain pose a growing challenge for governments and industries to address and mitigate their impacts.

Analyzing Maritime Improvised Explosive Devices (M-IEDs)

Historically, the maritime domain accounted for 2% of all IED incidents worldwide since 1969. This relatively low percentage can be attributed to the challenges and limitations that the maritime environment imposes on perpetrators, including planning, logistics, and technical difficulties. As a result, incidents involving IEDs in the maritime environment are less prevalent compared to land-based IED events.[22] However, it should be noted that attacks utilizing IEDs at sea have seen an increase in recent years. Adversaries and various terrorist groups have developed a certain level of maritime capability and new technologies provide terrorists and adversaries with opportunities to explore and develop novel methods.

Notorious Terrorist Abdul Al-Rahim Al-Nashiri, widely recognized as the so called "Prince of the Sea", served as the mastermind behind lots of maritime terrorist operations. Terrorist Al-Nashiri's strategy encompassed four key elements: utilizing a zodiac speed boat laden with explosives to collide with a ship, employing medium sized boats as explosive devices near docks or ports, employing aircraft to target boats through collisions, and incorporating underwater demolition teams.[23]

Below are the six primary categories of M-IEDs, along with explanations, suggestions, and insights derived from past M-IED attacks.

a. Drifting M-IEDs

In the context of drifting IEDs, it is important to note that these explosive devices can be disguised in various forms, such as rafts, life boats, unattended boats, plastic bins, large bags, floating sea mines or other amorphous objects.

Figure 6. Drifting M-IED (Guided by a Suicide Bomber – E. Mediterranean Sea, 17 January 2003)

[22] Hull University Centre for Security Studies IED Project Occasional Paper No. 1, Accessed 29.05.2023, http://www.wbied.com/wbied-articlesresearch/ied-project-occasional-paper-no-1/

[23] Brian Patrick Hill, US Naval Postgraduate School Master Thesis, Maritime Terrorism and the Small Boat Threat to the United States: A Proposed Response, 2009, p. 28.

Drifting IEDs can be detonated either by the perpetrator remotely or through victim-operated mechanisms. The victim-operated aspect means that the IED is designed to explode upon contact with a person or object, often resulting in harm or damage. It is less likely for Drifting IEDs to be time-delayed, the nature of drifting IED situations, where the devices are subject to water currents and movement, makes it tactically rare for time-delayed IEDs to be employed in such scenarios. Drifting IEDs can pose a significant challenge for freedom of navigation and energy shipping.

b. Suicide Borne M-IEDs

The challenges of operating at sea, including distance, water currents, and limited access points, can make it more challenging for terrorists to carry out remote -controlled or timed IED attacks effectively. As a result, terrorists may resort to employing suicide-borne IEDs, where individuals willingly undertake a suicide mission by using small boats or vessels laden with explosives. These individuals aim to approach their target vessel closely and detonate the explosives upon impact, causing significant damage or destruction.[24] These M-IEDs are very similiar with the historical Shinyo suicide boats used by the Japanese Imperial Navy in World War II. These boats had the capacity to carry over 500 pounds of explosives and could reach speeds of nearly 30 miles per hour.[25]

On 6 October 2002, a small boat made of fiberglass, carrying 100 to 200 kg of TNT explosives and guided by two suicide terrorists, deliberately collided with VLCC named MV Limburg, while she was 3 km off the port of Al-Shihr with the assistance of a pilot in order to load its crude oil. At the time of the attack, the MV Limburg was leased to the Malaysian state petroleum company, Petronas, and it was carrying 400,000 barrels of crude oil. As a result of the collision, approximately 90,000 barrels of crude oil spilled into the Gulf of Aden. This event led to a direct increase of $0.48 per barrel in oil prices, due to higher insurance costs for ships visiting Aden.[26]

[24] Meghan Curran, Soft Targets & Black Markets: Terrorist Activities in the Maritime Domain, 2019, p.9.
[25] Bob Hackett and Sander Kingsepp, Shinyo! Battle Histories of Japan's Explosive Moorboats, Accessed 29.05.2023, http://www.combinedfleet.com/ShinyoEMB.htm
[26] The Guardian Website, Accessed 8.06.2023, https://www.theguardian.com/world/2002/oct/17/yemen.france

Figure 7. Aftermath of M/V Limburg Suicide Borne M-IED Attack, 6 October 2002

c. Remotely Controlled M-IEDs

Remotely controlled IEDs provide adversaries with the capability to maintain control over an attack and detonate the explosive device at a specific location and time of their choosing. One option for achieving remote attacks is through the use of Radio Controlled IEDs (RCIEDs). However, conducting an RCIED attack within the maritime domain requires additional considerations.

To carry out an RCIED attack, terrorists generally require a spotter or observer to continuously monitor the target area. Without observing both the IED and the intended victim, they cannot trigger the detonation and achieve their objective. Hence, in maritime settings, terrorists are restricted to areas where they can maintain visual observation, like harbors, piers, shallows, narrow straits, choke points, or facility entrances. However, adversaries may overcome this limitation by utilizing drones or powerful telescopic equipment for observation, enabling them to extend their reach beyond remote distances. Moreover, terrorist organizations or adversaries now have the capability to employ advanced technologies such as remote-controlled, autonomous, or unmanned maritime vehicles.

On 30 January 2017, a frigate was targeted using a remote-controlled small boat. Initially, it was believed to be a Suicide Borne IED attack, but subsequent investigations revealed that the boat had been prepared using advanced technology. It was equipped with various advanced components, such as a remotely operated video camera, an autopilot compass, a GPS system, a throttle controlled by a servomotor, a purpose-built computerized guidance system, and two powerful outboard engines. In essence, the boat was converted into a Remotely Controlled Unmanned

Maritime IED. The attack occurred approximately 30 kilometres away from the Yemeni coast, highlighting the effective utilization of technology to carry out remote assaults from a distant location by terrorists.[27] It should be emphasized that the terrorist's future target could potentially be an oil tanker while it is sailing at a significant distance from the shore.

Figure 8. Video Screenshot, Final Stage of Maritime IED Attack on 30 January

d. M-IEDs at Harbors and Anchorage

When ships are at harbours, anchorage, or approaching these locations, they become more vulnerable to a range of potential IED threats. These threats can be encountered on the surface, underwater, or the airborne domain.[28] These situations can include:

Remote-controlled or suicide boat attacks: Terrorists may employ small boats loaded with explosives to conduct remote-controlled or suicide attacks targeting ships or maritime infrastructures. Drifting IEDs can also pose a potential threat. Therefore, during periods of anchorage or when at harbor if possible, it is crucial to establish a security perimeter with a minimum radius of 100 meters.

IEDs attached to a ship's anchor/hull: Devices that are designed to explode when the ship hoists its anchor pose a potential threat, as they can cause damage or harm to the vessel. Additionally, limpet mines have the capability to be attached to specific sections of a ship's hull. Therefore, in the event of any suspicious situation, it is strongly advised to assign the Navy EOD Team with the task of conducting hull inspections.

---

[27] WBIED, Anatomy of a 'Drone Boat, A water-borne improvised explosive device constructed in Yemen, Frontline Perspective, 2017, p.3.

[28] Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1), 2022, p.32.

IEDs emplaced under or close to piers: Devices that are hidden or placed in proximity to piers, potentially targeting ships during their docking or departing process. Therefore, it is advisable to assign the Navy EOD Team with the responsibility of inspecting the pier before entering the harbour and boarding.

Drone/UAV Attacks Drones can be used to deploy explosive devices onto ships or other targets, and they can also be utilized for direct kamikaze attacks. Therefore, it is crucial for all units, both afloat and ashore, to be equipped with anti-drone electronic warfare devices.

e. Drone/UAV Attacks In Maritime Domain

Due to rapid advancements in Drone/UAV technology, terrorist organizations have increasingly exploited this advantage to engage friendly forces in asymmetric warfare.[29] Maritime assets, whether ashore or afloat, are vulnerable to drone threats. Shore facilities, energy or oil supply facilities, as well as afloat units at harbors, anchorage, or while underway, may confront this threat and suffer casualties or damage from explosives released by drones. The potential threat posed by drones can originate from various directions. Failure to direct radar systems accurately and timely may result in the inability to detect an imminent drone attack.[30] Terrorists or adversaries can utilize drones for various purposes, including:

Engaging by releasing explosives from above: Drones can be weaponized to carry and release explosives, enabling adversaries to engage friendly forces by conducting aerial attacks. This method allows them to target specific locations or personnel with precision.

Figure 9. Drone with ordnance

[29] Zachary Kallenborn and Philipp C. Bleek, Drones of Mass Destruction: Drone Swarms and The Future of Nuclear, Chemical, and Biological Weapons, Accessed 8.06.2023, https://warontherocks.com/2019/02/drones-of-mass-destruction-drone-swarms-and-the-future-of-nuclear-chemical-and-biological-weapons/

[30] Peter Brookes, Reasons It's Tough to Defend Against Drones and Cruise, 2019, p.2.

Engaging through kamikaze attacks: Drones can be used as kamikaze vehicles, where they are deliberately flown into targets to cause damage or inflict casualties. By sacrificing the drone itself, adversaries can conduct suicide attacks without putting their own lives at risk. In addition, swarm kamikaze attacks involves a large number of individual units, which can overwhelm defenses and make it more difficult to track and neutralize each threat. Traditional defense systems may struggle to handle simultaneous attacks from multiple directions. Drone swarming demands advanced capabilities, such as individual drones being able to maintain distance, avoid air collisions, and anticipate the positions of other drones within the swarm at any given moment.[31]

A notable instance occurred off the coast of Oman, on 29 July 2021, when three kamikaze drones launched an assault on the Mercer Street oil tanker. While two of the drones failed to hit the tanker in their initial attack, one managed to successfully fly into the bridge during a subsequent strike. Regrettably, this attack resulted in the loss of life for a security guard and the vessel's captain.[32]

Figure 10. Damage Caused by a Drone Attack on the Oil Tanker (Mercer Street)

Acting as observation tools for planning and executing IED attacks: Drones serve as valuable observation tools, allowing adversaries to monitor the movement of friendly forces and gather intelligence. They can use this information to plan and execute IED attacks at desired locations and times, maximizing the potential impact.

---

[31] Drone swarm technology, Accessed 10 June 2023, https:// www.unmannedsystemstechnology.com /expo/drone-swarm-technology/

[32] The Washington Post Website, Accessed 10 June 2023, https://www.washingtonpost.com/ politics/2021/08/19/ last-month-three-drones-attacked-an-israeli-tanker-heres-why-thats-something-new/

Recording videos for propaganda: Drones equipped with cameras can capture video footage of attacks, which can then be used for propaganda purposes. These videos can be disseminated online or through other channels to amplify the impact of their actions and spread fear or misinformation. In addition, these videos also let terrorist organizations to develop their TTPs and studying the tactics and techniques of Allied forces responding to IED incidents.

f. Underwater IEDs

The specific capability and prevalence of underwater IEDs among terrorist groups is not widely known. However, it is a fact that adversaries have been actively dedicating resources to develop sophisticated underwater military capabilities, which could potentially jeopardize the security interests of member states of NATO and their allies during a crisis situation.[33] NATO issues a warning about adversaries actively surveying and mapping critical energy infrastructure belonging to allied nations, both on land and underwater.[34] Hence, after those critical energy infrastructure mappings, adversaries with the necessary expertise, resources and training could employ divers or remotely operated vehicles to plant and position explosive devices in underwater environments. This method offers several advantages, including the ability to access specific locations, attach devices discreetly, and potentially evade detection.

Additionally, using Underwater IEDs with time-delayed mechanism allow the perpetrators to retreat to a safe distance before the explosive device detonates. The combination of time-delayed underwater IEDs with a remote control (RC) component represents an alarming tactic that adversaries may employ in the maritime domain. This combination allows for greater control over the detonation of the explosive device, enabling perpetrators to remotely trigger the explosion at a desired time and location. The effects of underwater explosions can result in various destructive outcomes, such as harming ships, submarines, critical underwater energy infrastructures, as well as impacting any maritime operations.[35]

Moreover detecting underwater IEDs presents significant challenges due to their concealed nature. Sonar systems, underwater sensors, and advanced surveillance technologies are employed to identify and mitigate these threats. Divers and specialized underwater explosive ordnance disposal (EOD) teams are required for

[33] Lukas Trakimavičius, The Hidden Threat to Baltic Undersea Power Cables, 2021, p.4.
[34] Reuters Website, https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/
[35] H.Ceyhun TÜRE, Examination of Vibration Values Based on Underwater Detonations in Various Depths, Istanbul Okan University Master Thesis, 2015, p.42.

the identification, neutralization, and disposal of underwater IEDs. It is important to highlight that, certain IEDs deployed underwater might specifically aim to target Navy EOD personnel. This observation underscores the added risks faced by these highly trained individuals while carrying out their crucial tasks.

As seen on Nord Stream explosions on 26 September 2022 has brought attention to the susceptibility of undersea energy pipelines and communication cables. As a result, NATO Allies have taken substantial measures to enhance their military presence around maritime underwater critical infrastructure.[36] On 15 February 2023, NATO Secretary General Jens Stoltenberg declared the establishment of a Critical Undersea Infrastructure Coordination Cell at NATO Headquarters. This initiative aims to facilitate improved coordination between essential military and civilian stakeholders, as well as the industry, regarding a matter that is crucial for our security.[37] Besides the collective efforts of NATO, individual nations have also undertaken diverse initiatives, investing in seabed warfare[38] and innovative underwater surveillance technologies.[39] "Saildrone" unmanned surface vessels could be a good example of energy-efficient and innovative seabed surveillance technologies, utilizing wind energy for the vessel and solar energy for the sensors.[40]

Figure 11. Saildrone Explorer in the Persian Gulf on 7 October 2022[41]

[36] NATO Maritime assets play key role in Offshore Critical Infrastructure Security, MARCOM Website, Accessed: 9.06.2023, https://mc.nato.int/media-centre/news/2023/nato-maritime-assets-play-key-role-in-offshore-critical-infrastructure-security

[37] NATO stands up undersea infrastructure coordination, NATO Website, Accessed: 5.06.2023, https://www.nato.int/cps/en/natolive/news_211919.htm

[38] Seabed warfare is a 'real and present threat, Naval Technology Website, Accessed: 5.06.2023, https://www.naval-technology.com/features/seabed-warfare-is-a-real-and-present-threat/

[39] Luca Peruzzi, Seabed Warfare: NATO and EU Member State Responses, Accessed: 5.06.2023, https://euro-sd.com/2023/04/articles/30719/seabed-warfare-nato-and-eu-member-state-responses/

[40] Naval Technologies Website, Saildrone Explorer Unmanned Surface Vessel (USV), Accessed: 11.06.2023, https://www.naval-technology.com/projects/saildrone-explorer-unmanned-surface-vessel-usv-usa/

[41] Elisabeth Gosselin, Saildrone USVs to expand seabed mapping in Atlantic, Pacific, Accessed: 11.06.2023, https://www.c4isrnet.com/newsletters/unmanned-systems/2022/11/09/saildrone-to-expand-its-seabed-mapping-missions-in-atlantic-pacific/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-overmatch

Conclusions

In conclusion, the close interconnection between Energy Security and Maritime Security highlights the importance of a coordinated and comprehensive approach to effectively address shared concerns. The maritime energy infrastructure has witnessed significant growth and transformation in recent decades. However, it is crucial to recognize that alongside maritime energy shipping, critical maritime energy infrastructures such as underwater pipelines, offshore wind farms, and electrical cables are progressively becoming more susceptible to threats from adversaries and terrorists. The use of M-IEDs to target energy shipping & critical underwater energy infrastructures poses significant risks.

Countering the IED threat in the maritime domain necessitates a fluid and comprehensive approach, taking into account the unique characteristics of the maritime environment. This approach requires three-dimensional planning that encompasses not only the surface and air but also the underwater environment. Protecting critical underwater energy infrastructures from challenges like M-IEDs is uniquely difficult due to the vast maritime area and accessibility. It requires specialized equipment, surveillance technologies, research, innovation, intelligence sharing and most importantly coordination among all stakeholders.

At this point, international collaboration among nations is vital to prevent duplication of efforts, maximize resource utilization, effective crisis management and establishing a common legal framework. NATO ENSEC COE's Tabletop Exercises, like Coherent Resilience Baltic-23 "focus on Maritime Critical Energy Infrastructure Protection" provide excellent opportunities for this close cooperation among nations, ministries, private companies (responsible for underwater infrastructure, aerial or underwater surveillance systems, unmanned maritime patrol vessels ext.), military personnel (especially Patrol Vessels & Navy EOD personnel), and academics.

Ensuring a reliable and stable energy supply is of utmost importance, and it is crucial to acknowledge and prioritize the responsibility of protecting critical energy infrastructure. There is no doubt that adversaries and terrorists consistently strive to develop novel methods and technologies to execute attacks on maritime critical energy infrastructures. As the threat of M-IEDs advances in complexity and lethality, collective NATO investments in innovative surveillance solutions and coordination between nations are needed to thwart or minimize the impacts of such attacks.

List of References

1. Bob Hackett and Sander Kingsepp, Shinyo! Battle Histories of Japan's Explosive Moorboats, Accessed 29.05.2023, http://www.combinedfleet.com/ShinyoEMB.html
2. Brian Patrick Hill, Maritime Terrorism and the Small Boat Threat to the United States: A Proposed Response, US Naval Postgraduate School Master Thesis, 2009.
3. CNN Business Website, Accessed 20.06.2023, https://edition.cnn.com/2022/06/09/energy/us-lng-plant-explosion/index.html
4. Countering Terrorism Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 2), 2022.
5. Elisabeth Gosselin, Saildrone USVs to expand seabed mapping in Atlantic, Pacific, Accessed: 11.06.2023, https://www.c4isrnet.com/newsletters/unmanned-systems/2022/11/09/saildrone-to-expand-its-seabed-mapping-missions-in-atlantic-pacific/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-overmatch
6. Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1), 2022.
7. H.Ceyhun TÜRE, Examination of Vibration Values Based on Underwater Detonations in Various Depths, Istanbul Okan University Master Thesis, 2015.
8. Jessica Resnick-Ault, Who's Afraid of LNG?, Accessed 25.05.2023, http://www.greenfutures.org/projects/LNG/LNG1-4-04.html
9. Jose R. Valdivia Orbaneja , Subramanian R. Iyer , Betty J. Simkins , Terrorism and oil markets: a cross-sectional evaluation, Finance Research Letters, 2018.
10. Journal of Strategic Security, Accessed 25.05.2023, https://digitalcommons.usf.edu/ cgi/viewcontent.cgi?article=1258&context=jss.
11. Julijus Grubliauskas & Michael Rühle, Energy security: a critical concern for Allies and partner, 2018.
12. Luca Peruzzi, Seabed Warfare: NATO and EU Member State Responses, Accessed: 5.06.2023, https://euro-sd.com/2023/04/articles/30719/seabed-warfare-nato-and-eu-member-state-responses/
13. Lukas Trakimavičius, The Hidden Threat to Baltic Undersea Power Cables, 2021.
14. Meghan Curran, Soft Targets & Black Markets: Terrorist Activities in the Maritime Domain, 2019.
15. NATO Energy Security, NATO Website, Accessed 15.05.2023, https://www.nato.int/cps/en/natohq/topics_49208.html
16. NATO Strategic Concept 2022, NATO Website, Accessed 15.05.2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

17. NATO's Maritime Activities, NATO Website, Accessed 15.05.2023, https://www.nato.int/cps/en/natohq/topics_70759.html

18. NATO Maritime assets play key role in Offshore Critical Infrastructure Security, MARCOM Website, Accessed: 9.06.2023, https://mc.nato.int/media-centre/news/2023/nato-maritime-assets-play-key-role-in-offshore-critical-infrastructure-security

19. Naval Technologies Website, Saildrone Explorer Unmanned Surface Vessel (USV), Accessed: 11.06.2023, https://www.naval-technology.com/projects/saildrone-explorer-unmanned-surface-vessel-usv-usa/

20. Oktay Çetin, Mesut Can Köseoğlu, A Study on the Classification of Maritime Security Threat Topics, International Journal of Environment and Geoinformatics (IJEGEO), 2020.

21. Peter Brookes, Reasons It's Tough to Defend Against Drones and Cruise, 2019.

22. Reuters Website, https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/

23. Riley EJ Schnurr & Tony R Walker, Marine Transportation and Energy Use.

24. Ruxandra-Laura Boşilcă, Susana Ferreira, and Barry J. Ryan Routledge Handbook of Maritime Security 2022.

25. Sciencedirect Website, Accessed 19.05.2023, https://www.sciencedirect.com/topics/engineering/submarine-pipeline

26. Strauss Center Website, Accessed 25.05.2023, https://www.strausscenter.org/strait-of-hormuz-oil-tanker-security/

27. The United Nations Institute for Disarmament Research (UNIDIR), Accessed 29.05.2023, https://unidir.org/sites/default/files/publication/pdfs//-en-641.pdf

28. The United Nations International Ammunition Technical Guidelines, 3rd Edition 2021.

29. The Guardian Website, Accessed 8.06.2023, https://www.theguardian.com/world/2002/oct/17/yemen.france

30. UK Board of Trade, A Board of Trade Paper March 2022.

31. WBIED, Anatomy of a 'Drone Boat, A water-borne improvised explosive device constructed in Yemen, Frontline Perspective, 2017.

Corresponding address: NATO ENERGY SECURITY CENTRE OF EXCELLENCE, Research and Lessons Learned Division, Šilo str. 5A, LT-10322 Vilnius, Lithuania, NATO Energy Security Centre of Excellence, info@enseccoe.org