

EXPLORING LETHAL AUTONOMOUS WEAPON SYSTEMS AND MARITIME TERRORISM: IMPLICATIONS FOR PAKISTAN'S MARITIME SECURITY

Mubashar Hassan Shahid¹

ABSTRACT

Technology miniaturization, enhanced computing power and rapid advancements in AI and precision-guided munitions suggest that uncrewed systems are likely to evolve into Lethal Autonomous Weapon Systems (LAWS). The rise of LAWS, coupled with the increasing influence of violent non-state actors (VNSAs), private military contractors (PMCs) and state-sponsored proxies (SSPs), presents a dangerous proposition in the maritime domain. However, research in this domain is limited, especially in countries like Pakistan. This paper addresses two central questions, i.e., how LAWS may supplement efforts of Maritime terrorists and what implications it poses for Pakistan's maritime and national security. Employing qualitative analysis, the study draws on primary data retrieved from (but not limited to) policy/ doctrines and semi-structured interviews with maritime security experts, whereas secondary data has been sourced through open-source intelligence, scholarly books, journal articles and case studies of maritime incidents. The data is analysed using the choice theoretic model for terrorism studies, complemented by the critical maritime infrastructure model proposed by Beuger and Liebetrau. Findings reveal that anti-state actors, despite having limitations of resources, have been able to evolve and adapt to technology far more quickly than conventional forces. Balancing plausible deniability and visibility, these actors threaten not just Pakistan's maritime security but also undermine regional security.

KEYWORDS: Lethal Autonomous Weapon Systems (LAWS), Autonomous Uncrewed Systems, Geography, Technology, Maritime Terrorism.

INTRODUCTION

Operation Spider Web was one of the most sophisticated operations undertaken by Ukrainian Security forces against Russian Strategic assets. From the smuggling of drone components to explosives to evacuating Ukrainian operatives from Russian territory before the attack, it required meticulous planning and the use of technology. The most integral component of the whole operation was the hybrid approach, where drones were operated with a human in the loop and autonomously (Kateryna Bondar 2025). The autonomous operation may not have been fully autonomous but it presents us with the future of warfare. The Israeli Harpy UAV, introduced in 1989, can fly into enemy territory and exhibits a high level of autonomous capability (Israel Aerospace Industries Mini HARPY n.d.). Its purpose is to detect, identify and target an enemy radar emitting device all on its own once launched.

¹ PhD Scholar, Department of International Relations, University of Karachi. He can be reached at mushi437@gmail.com.

In the absence of any radar signal, it is programmed to loiter and strike any target of opportunity. But with increased computing capability and satellite pictures making the battlefield more transparent, the development of Kargu-2, a Turkish-made autonomous drone, is no surprise. It was reportedly the first Unmanned Combat Aerial Vehicle that autonomously decided to kill human beings in conflict-ridden Libya. (United Nations Security Council 2021). UCAVs with autonomous capability to decide on engaging a target in a combat situation are a new revolution in military combat, albeit with consequences. The use of such autonomous systems with lethal firepower has started a debate over the legal responsibility. Machines cannot be held responsible for any violation of law, hence the growing debate over autonomous weapon systems. And coupling this predicament with the role of violent non-state actors, state-sponsored proxies and private military contractors, it creates a complex web of uncertainty, immorality, volatility and lethality.

The Israel-Palestine conflict (Post Oct 7, 2023, attacks) saw the use of AI-based targeting by Israeli forces. The Houthis in support of the Palestinian cause, targeted Israel-bound shipping using various weapons that include ballistic missiles, drones/ UAVs and remotely controlled suicide boats. The impact was not only on increased operational costs but such actions may multiply in the future with the availability of Commercial off-the-Shelf (COTS) technology in 'anonymous decision making' just as it did with drones and UAVs. Extensive research is being conducted on LAWS but its impact on maritime domain, especially maritime terrorism, with particular focus on Pakistan's maritime security, has yet to be thoroughly assessed. This paper addresses two central questions, i.e., how LAWS may be utilized by anti-state actors in the maritime domain and what implications this poses for Pakistan's maritime and national security.

The paper discusses various definitional viewpoints of multiple states in order to bring clarity to the subject while also discussing the intricacies and complexities linked to maritime security. The impact of the availability of autonomous weapon systems to anti-state actors and its impact on Pakistan's maritime security will be investigated through this study while proffering policy options to enhance efforts to counter the threat. This study adopts a qualitative research design guided by interpretivist thinking to develop an understanding of the use of Lethal Autonomous Weapon Systems (LAWS) by anti-state actors in the maritime domain and identify the threats posed to Pakistan's maritime security. Primary data is drawn from doctrinal/ policy documents and semi-structured interviews with maritime security experts, whereas secondary data is compiled through open-source intelligence (OSINT), public reports on LAWS, and case studies of maritime asymmetric incidents. The evidence is analysed using the choice-theoretic model for terrorism studies to develop an understanding of the motivations/ working and decision-making of anti-state actors/ terrorist groups. This is coupled with identifying vulnerabilities in Pakistan's critical MIS as per the model proposed by Beuger and Liebetrau in order to identify threats posed by LAWS and anti-state actors and propose a way forward.

DEFINITIONAL STANDPOINT

There is considerable ambiguity with regard to the definition of LAWS. Various states and organizations have offered different definitions as per their own understanding. It is pertinent to mention that various states use the terminology 'Autonomous Weapon

Systems’ and do not use the word lethal on the pretext that lethality is only the system's capability to apply lethal force. Various states have also applied different approaches to define LAWS or equivalent systems. With the passage of time, various states have redefined LAWS, albeit with minor differences. A case in point is the US Department of Defence (DoD) definition which no longer uses the word ‘lethal’ as part of the terminology and has also removed the ‘human’ from supervision and replaced it with ‘operator’.

The current US DoD definition states it as a “weapon system that, once activated, can select and engage targets without further intervention by an operator. This includes, but is not limited to, operator-supervised autonomous weapon systems that are designed to allow operators to override the operation of the weapon system, but can select and engage targets without further operator input after activation” (US Department of Defence Directive 3000.09 - Autonomy in Weapon Systems n.d.). The Chinese, on the other hand, have approached the system differently. They have classified LAWS into ‘Unacceptable’ and ‘Acceptable’ autonomous weapon systems. They have described five qualities within a system that would make it acceptable for use in war and conflict or otherwise. These five qualities are lethality, autonomy, impossibility of termination, indiscriminate killing and evolution. They have hence defined ‘acceptable autonomous weapon system’ as one that has a “high degree of autonomy, but is always under human control. They can be used in a secure, credible, reliable and manageable manner, can be suspended by human beings at any time and comply with basic principles of international humanitarian law in military operations, such as distinction, proportionality and precaution” (Working Paper of the People’s Republic of China on Lethal Autonomous Weapons Systems 2022).

India has also been a supporter of emerging technologies and has voted for responsible research and development of such systems under the ambit of international law. India has maintained its stance that the Group of Governmental Experts (GGE) under the ambit of the Convention on Prohibitions or Restrictions on the use of Certain Conventional Weapons is the right forum for developing a global consensus on LAWS but it has recently abstained from UNGA resolution on LAWS in 2024, where previously it had voted negatively in 2023. It now believes that any blanket disapproval of these technologies is counterproductive and has stressed the need for understanding the positive effects of developing such technologies. This opinion has also been stressed by the United Nations Institute for Disarmament Research in its study, which has described Command and Control, Information Management, logistics and training as four key aspects where AI can be involved in key military tasks other than its lethal use (Grand-Clément 2023).

Pakistan has also participated in the global debate over LAWS and has put forward its own understanding of LAWS. Pakistan has voiced opinions based on responsibility and accountability with the operationalization of such weapon systems and has proposed that accountability of any such system must be ensured. Pakistan in 2023 submitted its definition of LAWS as “LAWS are not one or two types of weapons. Instead, they are a capability category, i.e., a weapon system incorporating autonomy in its critical functions, specifically in target selection and engagement. The challenges associated with these weapon systems stem from this capability, which lends itself to layers of unpredictability and cascading impacts” (United Nations 2023). For the purpose of this paper, the definition proposed by Pakistan will be taken as a reference.

MARITIME TERRORISM – AN APPRAISAL

A consensus on the definition of Maritime Terrorism (abbreviated as MT for this paper) does not exist, just like there is no internationally accepted definition of terrorism. The Council for Security Cooperation in the Asia Pacific (CSCAP) Working Group has offered an expansive definition for the types of events that comprise maritime terrorism and shall be used as a reference for this paper:

“the undertaking of terrorist acts and activities (1) within the maritime environment, (2) using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, (3) against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities” (Greenberg 2010).

Although the definition provided for ‘Terrorism’ in Pakistan’s Anti-Terrorism Act 1997 is all-encompassing, there is no specific mention of the maritime domain or sea in the Act. The act aptly covers all the actions undertaken by a person, but with the availability of commercial off-the-shelf technology to various actors, the designation of responsibility has become cumbersome and difficult. The most noticeable incident was the USS Cole bombing in 2002, while berthed at Aden, which was targeted by an explosive-laden boat commandeered by suicide bombers (US Department of Defence 2001). The attack took place in Yemen, but the Americans forced the Sudanese government to pay compensation to the aggrieved families (USS Cole bombing: Sudan agrees to compensate families 2020). Similarly, despite multiple investigations, no blame could be ascertained for the attacks in September 2022 on undersea gas pipelines taking gas from Russia to European countries in the Baltic Sea (Paul Kirby 2025). The recent use of explosive-laden UAVs to target a ship attempting to bring aid to besieged Gaza in the waters of Malta is another classic example where the identity of the attacker remains anonymous, despite all indicators pointing towards Israel or Israeli state-sponsored proxies. With satellite communications, along with optical gadgets commercially available, it has become relatively easier for VNSAs, PMCs and state-sponsored proxies to operate out at sea and present a potent threat in order to further their cause. Nothing can be ascertained, but the fact remains that technology is firmly in the driving seat.

THEORETICAL FRAMEWORK

Terrorists all over the world work on a strategic logic (one or a combination) as explained by Kydd and Walter in their paper ‘The Strategies of Terrorism’ (Kydd and Walter 2006), as given in the table below. The five principal strategic logics have also remained the same since being identified in 2006. The political interests are regime change, territorial change, status quo maintenance, social control, or policy change (Kydd and Walter 2006). The choice theoretic model often associated with Rational Choice theory has been extensively applied for terrorism studies which hypothesizes that terrorists operate as rational actors having political, religious, or ideological objectives. The theory stipulates that terrorists carefully weigh every option before selecting a target, finding the right way to execute the plan and also how to gain maximum coverage out of it.

The cost-benefit ratio applies to them as it applies to any state organization. Hence, for such organizations, finding suicide bombers would always be difficult but it is easier to use technology to achieve the same effect. Similarly, launching a cyber- attack on a state asset can produce a similar effect. Using technology such as LAWS or other uncrewed systems also allows them to cover their tracks, as the operator (in the case of uncrewed systems) may be sitting far away from the actual crime scene. More importantly, they can attack the hard targets, ones that are well defended physically and create a visible impact. Terrorists seek recognition and anonymity is neither their desire nor attractive to them. Hence, it can be concluded that technology, for anti-state actors/ terrorist organizations, is but a tool to gain the maximum visibility. The decentralized structure of terrorist organizations allows them the operational freedom to exploit technology to the fullest. All these actors have also utilized social media networks to great effect with the use of video and image editing software, as well as providing live coverage of their terrorist acts.

LAWS TECHNICAL REQUIREMENTS

LAWS is a complex technological system. Any uncrewed system requires, in principle, a propulsion system, a detection system, weapons and a data processing system. In the case of LAWS, the technological requirements increase exponentially. The following are the requirements for LAWS to function effectively.

Technical Requirements	Remarks
Sensors	• Optical/ thermal imaging cameras, RADARs, SONARs • Detecting the target
AI & Machine Learning/High-performance Computing	• Data availability, Filtering/ Processing the data • Distinguishing/ identifying the target
Communication System	• Reliable system from the platform to the operating base • Also serves as a link from the ground station, where the human can disengage the platform from an attack
Navigation and Autonomous Systems	• System's ability to navigate not just itself but the weapon (if being launched from the platform) • Understanding the topography and geography of the environment • Ability to perform in a GPS-denied environment

WHY DO LAWS ATTRACT TERRORISTS IN THE MARITIME DOMAIN?

Imagine a scenario where a single USV is loitering out at sea with a specific direction to target an eastbound vessel with a length of more than 200 metres and a specific design (like LNG-carrying ships). This USV is fed with a database of pictures of various merchant ships out at sea and is also linked to the data acquired from the Automatic Identification System

(AIS) of the merchant ships and has an image recognition software to better identify the merchant ship from its colours and contours. The USV decides on its own when and where to attack the merchant ship. This fear has been raised by various academics and practitioners. Dr Alexander Blanchard and Jonathan Hall have argued in their paper that LAWS appeal to terrorists not because of anonymity but because of a lack of defensive mechanisms and the factor of multiplication (Dr Alexander Blanchard and Jonathan Hall 2023). Armin Krishnan's book 'Killer Robots' has raised the same fears on the "availability of such sophisticated technology to rogue states, private organizations and even malevolent individuals" (Krishnan 2010).

Terrorists, whether they operate on land or at sea, have the same objectives, which do not change. The smugglers trafficking illicit cargo, including drugs, would not want their supply chain disturbed and will resort to any measure to ensure their supply lines remain intact. Hence, their objective of maintaining the status quo in order to achieve financial gain out of trafficking illicit cargo holds good. It would ensure that any security infrastructure brought up to curb his illegal business is dealt with and what better way than seeking a VNSA for hire. Tehrik e Taliban Pakistan (TTP), a proscribed terrorist organization currently operating from Afghanistan, is alleged to be an Indian funded terrorist organization having its roots within the Taliban ideology. It has been reported that TTP has used commercially produced quadcopters to drop a bottle filled with 400-700 grams of explosives, nails and ball bearings, along with a grenade as a catalyst (Iftikhar Firdous 2024).

This locally developed 'quadcopter dropped explosive' entrapment is indicative of the use of commercially available technology by terrorists. In addition, various terrorist organizations operating in Baluchistan province are also funded by the Indian govt in addition to political and material support to the leadership of these proscribed organizations (Ambassador Munir Akram 2021). These terrorist organizations have repeatedly targeted rail and road infrastructure, as seen by the Jaffar Express attack, challenged government writ by stopping traffic on roads and attacking public buildings during nighttime, while also launching attacks on Chinese and Chinese interests, such as the Gwadar Port Project, a critical element of CPEC (Abdullah Khan 2025). When it comes to Port areas, even SOP violations can lead to explosions and considerable damage/ loss of lives as in the case of Beirut Port, Lebanon, in August 2022 and Bandar Abbas, Iran, in April 2025 (El Sayed 2022). LAWS offers a host of options to the terrorist groups, something that other means did not offer to them in the past. A case in point is the recent attack on a Pakistan Coast Guard boat near the coastal town of Jiwani (3 Pakistan Coast Guard Personnel Killed After Militants Open Fire On Patrol Boat In Arabian Sea 2026). The terrorists used a manned boat to target the PCG boat, thus increasing the risk of retaliation and killing/ injuring/ capturing of its personnel. However, had this been an attack by an uncrewed boat operating autonomously, it would have achieved the same objective without risking the lives or identity of its operatives.

UNDERSTANDING THE THREAT TO CRITICAL MIS

The maritime domain is vast and encompasses a multifaceted list of infrastructure, stationary and dynamic, onshore and offshore, above water and underwater. To develop a

better understanding of what all target sets are available to maritime terrorists, it is important to identify critical MIS, especially in the case of Pakistan. Bueger and Liebetrau have presented a model to categorise critical Maritime Infrastructure (MIS) within five broad fields, i.e., transport, fishery, energy, communication and ecosystems (Bueger and Liebetrau 2023). The model, as depicted below, clearly indicates the wide variety of elements within MIS that need protection from contemporary threats.

	On the Sea	In the Sea	On Land
Transport	Ships, shipping lanes	Emissions	Ports
Energy	Platforms	Platforms, electricity cables, pipelines	Ports, landing stations, repair facilities
Communication	Repair Ships	Data Cables	Landing stations, repair facilities
Fishery	Ships, fishing zones	Fishing gear, aquaculture	Ports, aquaculture
Eco-systems	Biodiversity	Biodiversity, carbon sink, carbon storage	Coastal areas, beaches

Figure 1 - Bueger & Liebetrau Model of Critical MIS

In the case of Pakistan's critical MIS, Karachi Port Complex and Port Qasim become the top priority. They handle almost 97% of Pakistan's sea trade and all oil and gas imports are handled at these two co-located ports. Gwadar Port has yet to be fully operational. In addition, Pakistan relies heavily on international shipping for exports and imports and only a small fleet of the Pakistan National Shipping Corporation handles some of the oil and bulk imports. In addition, a large percentage of the population living on the coast is directly or indirectly employed in fishing, especially in the coastal villages. Furthermore, Pakistan is connected to the world through submarine cables which mostly land at Karachi. Although redundancies to the cables are available, the heavy data traffic and damage to cables, whether caused by accident or malintent, cause significant loss to the economy (Rabia Khan and Yushma Umar 2025). A detailed analysis of the critical MIS is as follows:

➤ LACK OF DIVERSITY IN MIS

The lack of diversity in Pakistan's MIS can be seen from the location of Pakistan's MIS. Its two major ports, Karachi Port and Port Qasim, LNG terminals, almost all submarine cables and landing stations, the only shipyard and the main fish harbours (Karachi Fish Harbour handles 90% of fish catch and 95% of fish exports) are all co-located at Karachi. Pakistan is not connected through underwater electricity cables to any country; no underwater oil or gas pipeline is laid for oil/ gas imports and neither are any wind farms located in Pakistan's waters. This lack of diversity in MIS allows terrorists to consolidate their efforts into a single area with maximum effect. It also increases the dependency of a state on a single focal point. Any terrorist attack on Karachi Port would have far-reaching consequences that would linger for a considerable time.

➤ **FISHERY SECTOR**

Most of the job opportunities in the maritime sector are linked to the fishery sector. Despite having a long coastline and an Exclusive Economic Zone (EEZ) of 240,000 sq km, the sector is marred by poor safety and hygiene standards, subpar freezing facilities onboard that ultimately block exports of high-quality fish products. This results in reduced exports, which are evident from the average unit price of less than 2.5 US\$ per kg from 2018-21 as compared to 5-8 US\$ per kg of the regional countries (Aamir Shafaat Khan 2021). Reduced catch leads to reduced income, non-availability of state support in terms of zero/ low interest loans, lack of education facilities and a dilapidated health sector, ultimately leading people to be misdirected and indoctrinated by terrorist organizations (Shahid and Zeb 2024). Another major issue is related to the registration of boats with the Sindh and Baluchistan governments and the installation of vessel tracking systems (Balochistan Sustainable Fisheries and Aquaculture Policy 2025-2035, 2025).

➤ **SHIP RECYCLING & STEEL INDUSTRY**

Pakistan has one of the world's largest ship-breaking sites in Baluchistan (Gadani). At one time, the ship recycling business was the backbone of the maritime economy and handled as many as 30000 personnel in its workforce in the 80s. It has been marred by poor health, safety and environment (HSE) standards for the past 2-3 decades. The Hong Kong Convention (HKC), which came into force on 26 June 2025, is expected to further aggravate the situation for ship recycling businesses. The business community is ill-prepared to follow HKC guidelines and thus will lose out on precious business. The ship recycling industry also feeds into the steel industry as a raw material and helps Pakistan save precious foreign exchange as well as provide jobs in the steel sector. The downfall of this ship recycling business would lead to a higher cost of raw materials for the steel industry, higher production costs for steel, which would ultimately result in job losses and/or closure of businesses (Shahid and Shahid 2024). These job losses would lead to poverty and poverty is a critical factor exploited by terrorist organizations during recruitment and as a motivational driver.

➤ **PORT SECURITY**

The security of Pakistan's largest port, KPT, is undertaken from the land side by the Port Security Force established under a Presidential Ordinance of 2002 (Port Security Force Ordinance 2002 2002). The Port Security Force is generally designed to cater to traditional security threats. The seaward security is provided by the Pakistan Navy (PN), which operates multiple platforms under an elaborate security scheme to ensure round-the-clock security. The security of Port Qasim is also augmented through PN resources. Similarly, seaward security of Gwadar Port is also ensured by PN, whereas external landward threats to Gwadar Port Area of Responsibility are catered to by the Pakistan Army. However, the ability to tackle lethal autonomous weapon systems for securing port infrastructure remains a challenge at KPT, PQA and Gwadar Port. This threat is further augmented with unplanned and unchecked development, especially in the case of the Karachi Port area. Most of the POL facilities are located close to ports or inside port facilities. Port areas are generally very densely packed together with multiple storage areas of various items located close to each other. The results would be catastrophic if such storage facilities were targeted by terrorists with LAWS and could lead to damage as seen

in the case of the Beirut Port blast. It gives the terrorist organizations suitable visibility while achieving the effect of challenging the state's writ.

➤ **SUBMARINE CABLES**

Pakistan is presently connected with 7 submarine cables, with all of them landing at Karachi. Another two cables are due for connectivity by 2027 and they are also planned to be landed at Karachi. With no cable repair or cable-laying ship facility available, Pakistan relies solely on foreign ships for the repair or laying of cables. With almost 100% dependency on submarine cables, it is imperative for Pakistan to ensure security around these cables and landing stations. Fishing vessels have accidentally damaged submarine cables while trawling their nets and the same can be undertaken by VNSAs. Autonomous ship control technology has been installed on various ships and barges; however, integration of such technology by terrorist groups in the maritime domain is unlikely in the near future, as it can act as a fishing boat trawling its nets with the intention to damage submarine cables. Nevertheless, causing damage to a landing station through LAWS remains a viable possibility.

Nevertheless, a critical factor that is not adequately covered by the Beuger and Liebetrau model is the spread of population along the coastal regions. Pakistan has a growing population but the coastal population is primarily centred in and around Karachi (around 20.3 million). In comparison, the Gwadar district in Baluchistan, with a coastline of almost 600 km, has a population of around 300,000 (Population Census 2023 n.d.). Hence, Pakistan's total coastal population constitutes only a limited proportion of its national population, with a vast majority in Karachi. Drawing a comparison, the Chinese population is divided along the imaginary Heihe-Tengchong line. To the east of this line, lives 94% of the Chinese population (43 % of the Chinese land mass), whereas the remaining 6% lives to the west of this line (57% of the land mass). Although various topographical and environmental reasons have impacted this Chinese divide, there is no doubt that Pakistan's coastal population spread is uneven, presenting Karachi as a critical strategic necessity with no redundancy.

PAKISTAN AND MARITIME TERRORISM

A threat in the maritime domain has serious repercussions not just for the coastal nation but for the global maritime community. This is especially a worry when two neighbouring nuclear-armed states with a history of territorial disputes, allegations of cross-border terrorism and strained diplomatic relations are confronted by multiple VNSAs/ PMCs/ SSPs in the region (Shahid and Zeb 2024). Pakistan has suffered from the scourge of terrorism for the past two and a half decades. The first reported incident of maritime terrorism in Pakistan's history is the attempted hijacking of a Greek freighter at Karachi (Jenkins and Janera Johnson 1975).

To accomplish this, the Pakistan Navy in 2013 established the Joint Maritime Information Coordination Centre (JMICC) at the national level to integrate multiple domestic organizations, including intelligence agencies, to collect and filter information in order to augment efforts to enhance maritime security. It acts as a hub for regional cooperation with its linkages with multiple international organizations that have security interests in the

greater IOR. The Joint Maritime Information Organization bill has been pending passage through the parliament since 2018. Nevertheless, capacity enhancement of Pakistan Maritime Security Agency (PMSA) and Pakistan Coast Guard (PCG) and the optimum operationalization of Local and Regional Security Stations (LSS/ RSS) is being undertaken to enhance coastal surveillance and improve response times against any threat in the littorals. Pakistan Navy has been undertaking Maritime Security Operations (MSOs) independently under the flag of Regional Maritime Security Patrol (RMSP) and with international partners under the flag of Coalition Maritime Forces (CMF).

MARITIME INCIDENT - ATTACK ON KSA FRIGATE AL-MADINAH IN 2017

The attack on the Saudi Frigate Al Madinah in January 2017 tells us how maritime terrorism has evolved over the period of time. The Saudi frigate was operating in Red Sea close to Yemen's Hodeidah Port when it was targeted by an uncrewed remotely operated suicide boat (LaGrone 2017). The boat allegedly controlled by the Houthis targeted the Saudi Frigate which resulted in the deaths of two Saudi naval personnel and the injury of others. American Vice Admiral Kevin M. Donegan believes that terrorists no longer wish to use suicide bombers as the primary weapon and are more intent on using suicide remote control boats for the same purpose without the use of human beings. (Tyler Rogoway 2017). The Admiral's statement provides us with two important conclusions. Firstly, the use of USVs is a real threat and secondly, NSAs have evolved and are looking for alternative ways and means to undertake such attacks. And hence the use of technology to circumvent the need for suicide bombers. Considering that this attack took place in 2017, it can be hypothesized that remote operation, either through satellite or Very High Frequency (VHF) tele-communication, was available to the alleged perpetrators. More so, the fact that such an attack was successful in 2017 implies that even better technology would now be available to terrorist groups. In view of the above, the following is pertinent about Pakistan's maritime security:

1. Sir Creek Issue and a disputed maritime boundary present India, a regional competitor, with an opportunity through SSPs/VNSAs to utilize such uncrewed systems (whether autonomous or human in the loop) and threaten Pakistan's maritime security.
2. The availability of commercial off-the-shelf technology to utilize satellite imagery to detect, track, identify and target high-value targets is another major concern. This indicates that threats can be posed not just in littoral waters but also at far distances where regular ISR patrols are not being undertaken. Use of mother boats to launch smaller armed skiffs/boats/UAVs operating autonomously to target merchant ships is also a major concern.
3. EW spectrum is critically important for maritime security operations to deter any threat from LAWS in maritime domain. All LAWS require some sort of communication network, which is essentially required to communicate with the data system that feeds it. It requires a continuous update of its position and hence, the EW spectrum, including the communication spectrum, is to be dominated by the state.

WAY FORWARD

The extensive use of technology by terrorists to accrue maximum benefits is a major concern but the state has the resources to use the same technology to its benefit with a far greater impact. But to generate those effects, it is paramount for Pakistan to address the root cause of terrorism, especially in the maritime domain. With MIS a critical asset, it requires a multi-pronged approach to address the issues of amalgamation of technology with terrorist outfits and creating a significant impact on the most economically downtrodden coastal community. The following is recommended in this regard:

a. POLICY LEVEL

- i. Pakistan may go for formulation of local regulations to cater for LAWS and may amend the Anti-Terrorist Act 1997 suitably to cater for the definition of LAWS and their use by terrorists till the time an international consensus is achieved.
- ii. Publication of Maritime Policy/ Strategy and passage of JMIO bill at the earliest is considered a necessity to streamline responsibilities and ensure necessary legal cover.
- iii. Development of uncrewed vehicles (UxVs) and counter systems, including but not limited to UAVs, USVs and UUVs in the public and private sector needs to be encouraged at multiple levels, including tax breaks, access to firing ranges and regulated availability of desired explosive material. This would allow for the development of technology to cater to the projected threats. Moreover, rules and regulations for import of technology linked to autonomous systems need to be stringently regulated to raise the cost for terrorist groups. A licensing mechanism on the lines of small arms may also be considered.

b. IMPROVING SECURITY INFRASTRUCTURE

- i. MIS, especially the facilities located at Karachi, need to be protected against UxVs threat. The protection levels have to be raised and brought to standards attained at airports or military bases. Since these facilities are operational round the clock, technology and AI have to take a front seat to ensure any challenges posed by LAWS are addressed by technological solutions. This includes optical and infrared devices, drone communication scanners, drone detection radars to detect incoming threats connected with AI platforms, and non-kinetic threat elimination systems like directional jamming systems. Security around cable landing stations also needs to be brought at par with Port areas.
- ii. All threats emanate from the land. Hence, for the threat not to proceed to sea from Pakistani territory, cooperation between PCG, PMSA, ANF, Police, Customs, Intelligence agencies and other domestic organizations involved is essentially required. The provincial governments must enforce the rules with regard to boat registration and vessel monitoring systems. Any autonomous weapon system that can develop as a threat at sea has to be transported out through a boat and the best way to stop it is before its embarkation onto a boat.

c. ELIMINATING THE ROOT CAUSE

i. Diversification of Port infrastructure requires Gwadar Port Project to become a success. But it requires sustained political will and infrastructure development through public and private investments. The success of Gwadar also lies in gaining public support as well as population management. This also entails protection of local populace from exploitation while affording them opportunities to compete for the jobs being offered at Gwadar. Also, Gwadar Port will not succeed without its connectivity to hinterland through western CPEC corridor.

ii. Two sectors of Blue Economy, i.e., fisheries and ship recycling, need a plan to be developed on modern lines and as per international standards. Both sectors are labour-intensive and can provide multiple employment opportunities. The ship recycling sector needs to be brought in line with HKC standards and that requires legislation at provincial and federal levels. The provincial authorities must ensure promulgation of health, safety and environmental standards and same should apply to the fisheries sector.

CONCLUSION

Technology has been a driving force in changing the character of warfare, but its adaptation by terrorist organizations has transformed the way security is perceived by the state. Proliferation of LAWS into terrorist organizations, especially those operating against critical MIS, demands an urgent and multi-faceted response. Enhancement of Maritime Domain Awareness would only be beneficial if the state mechanisms cooperate and can respond to a threat quickly. This can be enhanced through indigenously developed AI-powered security systems, hardening security around critical MIS and ensuring stringent import controls on AWS technology. Terrorists would continue to seek visibility and to create fear amongst the masses. LAWS offers terrorists visibility and opportunity to create fear amongst the masses, but the state has the resources to cater to this challenge and provide security not just to its masses but also to improve overall maritime security.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author.

REFERENCES

- 3 Pakistan Coast Guard Personnel Killed After Militants Open Fire On Patrol Boat In Arabian Sea. 2026. <https://www.marineinsight.com/3-pakistan-coast-guard-personnel-killed-after-militants-open-fire-on-patrol-boat-in-arabian-sea/>.
- Aamir Shafaat Khan. 2021. 'Chinese Ban on Nine Firms Hits Pakistan's Fish Exports'. <https://www.dawn.com/news/1636776>.
- Abdullah Khan. 2025. 'BLA's Shifting Claims: A Timeline of the Jaffar Express Hijacking'. <https://www.picss.net/articles/blas-shifting-claims-a-timeline-of-the-jaffar-express-hijacking/>.
- Ambassador Munir Akram. 2021. "Statement on Agenda Item 111: "Measures to Eliminate International Terrorism"". United Nations.

- Balochistan Sustainable Fisheries and Aquaculture Policy 2025-2035. 2025. Quetta, Pakistan. <https://balochistancode.gob.pk/lawdir/3f877f8d-9c7e-427a-ab37-e04b81d69b32.pdf>.
- Bueger, Christian, and Tobias Liebetrau. 2023. 'Critical Maritime Infrastructure Protection: What's the Trouble?' *Marine Policy* 155:105772. doi:10.1016/j.marpol.2023.105772.
- Dr Alexander Blanchard, and Jonathan Hall. 2023. 'Terrorism and Autonomous Weapon Systems: Future Threat or Science Fiction?' <https://cetas.turing.ac.uk/publications/terrorism-and-autonomous-weapon-systems-future-threat-or-science-fiction>.
- El Sayed, Mazen J. 2022. 'Beirut Ammonium Nitrate Explosion: A Man-Made Disaster in Times of the COVID-19 Pandemic'. *Disaster Medicine and Public Health Preparedness* 16(3):1203–7. doi:10.1017/dmp.2020.451.
- Grand-Clément, Sarah. 2023. *Artificial Intelligence Beyond Weapons - Application and Impact of AI in the Military Domain*. Geneva: UNIDIR. https://unidir.org/wp-content/uploads/2023/10/UNIDIR_AI_Beyond_Weapons_Application_Impact_AI_in_the_Military_Domain.pdf.
- Greenberg, Michael D., ed. 2010. *Maritime Terrorism: Risk and Liability*. RAND Corporation Monograph Series. Santa Monica, CA: RAND Center for Terrorism Risk Management Policy.
- Iftikhar Firdous. 2024. 'Pakistani Officials Believe Pakistani Taliban Has Developed "Nascent" Drone Technology'. <https://www.thekhorasandiary.com/en/2024/09/25/tkd-exclusive-pakistani-officials-believe-pakistani-taliban-has-developed-%27nascent%27-drone-technology>.
- Israel Aerospace Industries Mini HARPY. n.d. Retrieved 30 April 2026. <https://automatedresearch.org/weapon/israel-aerospace-industries-mini-harpy/>.
- Jenkins, Brian M., and Janera Johnson. 1975. *International Terrorism: A Chronology, 1968-1974*. R-1597-DOS/ ARPA. Santa Monica: RAND Corporation. <https://www.ojp.gov/pdffiles1/Digitization/28210NCJRS.pdf>.
- Joint Maritime Information Coordination Centre. n.d. Karachi. Retrieved 29 April 2026. <https://www.jmicc.gov.pk/aboutus.aspx>.
- Kateryna Bondar. 2025. 'How Ukraine's Operation "Spider's Web" Redefines Asymmetric Warfare'. <https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare>.
- Krishnan, Armin. 2010. *Killer Robots: Legality and Ethicality of Autonomous Weapons*. Repr. Farnham: Ashgate.
- Kydd, Andrew H., and Barbara F. Walter. 2006. 'The Strategies of Terrorism'. *International Security* 31(1):49–80.
- LaGrone, Sam. 2017. 'Navy: Saudi Frigate Attacked by Unmanned Bomb Boat, Likely Iranian'. *United States Naval Institute News*, February 20.
- Paul Kirby. 2025. 'Ukrainian Held in Italy over Blast Mystery of Nord Stream Gas Pipelines'. <https://www.bbc.com/news/articles/crkz1jl5j06o>.
- Population Census 2023. n.d. Retrieved 29 April 2026. <https://census23.pbos.gov.pk/>.
- Port Security Force Ordinance 2002.

- Rabia Khan, and Yushma Umar. 2025. 'Pakistan's Digital Dilemma – The True Cost of Internet Shutdowns'. <https://mhrc.lums.edu.pk/pakistans-digital-dilemma-true-cost-internet-shutdowns>.
- Shahid, Mubashar Hassan, and Rizwan Zeb. 2024. 'Treading Turbulent Waters: Pakistan's Readiness to the Looming Threat of Maritime Terrorism'. *Margalla Papers* 28(1):211–25. doi:10.54690/margallapapers.28.1.249.
- Shahid, Sanaa Mubashar, and Mubashar Hassan Shahid. 2024. 'Triangle of Progress - China Pakistan Economic Corridor, Ship Recycling and Steel Industry'. *Polaris – Journal of Maritime Research* VI(1):48–62. doi:10.53968/pjmr.2024.001.6.
- Tyler Rogoway. 2017. 'Attack on Saudi Frigate off Yemen Was Made by Drone Boat'. <https://www.twz.com/7769/attack-on-saudi-frigate-off-yemen-was-made-by-drone-boat>.
- United Nations. 2023. *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*. CCW/GGE.1/2023/CRP.1. Geneva. [https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_\(2023\)/CCW_GGE1_2023_CRP.1_0.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf).
- United Nations Security Council. 2021. *Final Report of the Panel of Experts on Libya Established Pursuant to Security Council Resolution 1973 (2011)*. S/2021/229. New York. <https://docs.un.org/en/S/2021/229>.
- US Department of Defence. 2001. *DoD USS COLE Commission Report*.
- US Department of Defence Directive 3000.09 - Autonomy in Weapon Systems. n.d.
- USS Cole bombing: Sudan agrees to compensate families. 2020. *BBC News*, February 13.
- Working Paper of the People's Republic of China on Lethal Autonomous Weapons Systems. 2022.