
INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

**MARITIME SECURITY THREATS AND LEGAL RESPONSES:
NATIONAL AND INTERNATIONAL PERSPECTIVES**

- Akhila JS¹ & Sandra S Nair²

ABSTRACT

Maritime security is an essential component of international trade, national security and the protection of human life, yet the openness and transnational character of the maritime domain create significant opportunities for organized criminal and terrorist activities. This paper examines the major contemporary maritime security threats associated with human smuggling, human trafficking, illicit arms trafficking, maritime terrorism and other unlawful acts against the safety of maritime navigation. It analyses the international and national legal frameworks developed to prevent, suppress and prosecute such activities, with particular emphasis on the International Ship and Port Facility Security (ISPS) Code under SOLAS Chapter XI-2, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention) and its 2005 Protocol, the United Nations Convention against Transnational Organized Crime (UNTOC) and its relevant Protocols, the UN Firearms Protocol, the Arms Trade Treaty and the STCW Convention. The study also examines the Indian maritime security framework and the roles of the Indian Coast Guard, Indian Navy, Directorate General of Shipping, Customs, Immigration, Police, intelligence agencies and port authorities in prevention, interception, investigation and prosecution of maritime security offences. Relevant judicial decisions are considered to demonstrate issues of jurisdiction, vessel inspection, seizure, evidence collection and inter-agency investigation. The study finds that maritime security threats are interconnected and frequently involve transnational criminal networks, jurisdictional complexities, corruption, technological vulnerabilities and humanitarian concerns. It argues that effective maritime security cannot depend upon a single convention, agency or technological mechanism. A comprehensive approach combining risk assessment, maritime domain awareness, intelligence sharing,

¹ Legal Practitioner, LLM Candidate

² Legal Practitioner, LLM Candidate

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

effective port and vessel security, trained personnel, strong national implementation, international cooperation, victim protection and respect for human rights is necessary to strengthen the security of ships, ports, maritime infrastructure and international shipping.

INTRODUCTION

The movement of people, products, energy and strategic commodities around the world is largely dependent on maritime transit which is the foundation of international trade. The marine domain which includes ships, ports, coastal regions, territorial seas, international shipping routes, offshore installations and maritime infrastructure is more than just a mode of transportation. Opportunities for various forms of transnational crime and security threats are created by the sea's openness and international character, the massive volume of cargo transported the challenge of continuously monitoring large maritime spaces and the jurisdictional complexities associated with ships operating across multiple states. The protection of ships, ports, maritime infrastructure, seafarers, passengers, cargo and maritime transportation systems against deliberate illegal acts, criminal activity and other hazards is sometimes referred to as maritime security. Piracy, armed robbery, terrorism, illegal ship seizures, human smuggling, human trafficking, illicit arms trafficking, drug trafficking, stowaways, sabotage and other organized marine crime are all current maritime security threats. These dangers may arise separately, but they are also related. For example, the same criminal networks may be involved in the transportation of weapons, the financing of terrorist activities, the trafficking of people and the smuggling of migrants. As a result, the international community has created a thorough institutional and legal structure to handle maritime security. The International Ship and Port Facility Security (ISPS) Code which is enforced by Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS), 1974 is one of the most significant tools. An obligatory security regime for international shipping is established by the ISPS Code which went into effect on July 1, 2004. A significant international criminal-law framework against illegal activities against ships is also provided by the 1988 Convention for the Suppression of Unlawful activities against the Safety of Maritime Navigation (SUA Convention) and its 2005 Protocol. Deliberate acts or criminal activity that jeopardize the safety and security of ships, ports, people, cargo, maritime infrastructure or the larger marine environment are considered maritime security threats. Threats to maritime security typically include deliberate behaviour in contrast to

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

typical marine safety concerns which might result from mishaps, technical malfunctions, bad weather or human mistake. There are specific vulnerabilities in the maritime area. Large amounts of expensive goods or dangerous materials may be carried by ships, ports have vital infrastructure and vast transportation networks and ships operate in an environment where quick aid may not be accessible. The Flag states, coastal states and port states have different marine jurisdiction. Investigation, interception, prosecution and evidence gathering may become especially challenging as a result. The collaboration between flag states, coastal states, port states, shipping firms, coast guards, navies, customs authorities, immigration authorities, police agencies and international organizations is necessary for modern maritime security.

HUMAN SMUGGLING BY SEA

Human smuggling, specifically known as "smuggling of migrants" in international law is the act of assisting someone to enter a state illegally for financial or other material gain. This concept is established in Article 3 of the United Nations Convention against Transnational Organized Crime (UNTOC) addendum, the Protocol against the Smuggling of Migrants by Land, Sea and Air. The primary goal of migrant smuggling is typically to earn material or financial gain by enabling unauthorized cross-border travel. The migrant may agree to the transportation at first but there may be significant risks involved in the trip. Because they can evade traditional border-control stations, maritime routes are especially appealing to smugglers. Migrants may be transported via small boats, fishing boats, cargo ships and other craft. A smuggling operation may become a major marine safety and humanitarian emergency if unseaworthy vessels are used.³ Because human smuggling includes the illicit movement of people over international borders using marine routes, frequently employing risky and covert means, it raises a variety of major maritime security issues. The usage of dangerous and inappropriate vessels is one of the main issues. Overcrowded boats, fishing vessels, small craft or vessels that aren't built to carry a lot of people are often used by smuggling networks. These ships might not have the necessary safety precautions, life-saving appliances or navigational equipment. Migrants may therefore be at a significant risk of capsizing,

³Anne T Gallagher and Fiona David, *The International Law of Migrant Smuggling* (Cambridge University Press 2014) 403–489 (ch 6, 'Migrant Smuggling by Sea: Interdiction and Rescue').

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

colliding, sinking and drowning, resulting in a humanitarian and maritime security situation.⁴ Identity fraud and forgeries are significant security risks. Forged or fraudulently obtained passports, visas, identification documents and other travel documents may be used by criminal networks engaged in migrant smuggling to assist the transit of migrants. Immigration, customs, port and maritime authorities may find it challenging to identify people and ascertain their true nationality or reason for travel if they present false documentation. It might make it possible for people engaged in other illegal activities to travel across international borders covertly. There is often a connection between organized transnational criminal networks and human smuggling. Personnel or groups operating across multiple nations may be involved in smuggling operations; distinct personnel are in charge of recruitment, transportation, documentation, lodging, cash collecting and transfer across various sea routes. These networks operate in several jurisdictions, making investigation and prosecution challenging. Legitimate companies, ships and commercial transportation systems may also be used by criminal groups to hide their operations, making it more difficult for maritime law enforcement to identify them. Another major marine security issue linked to migrant smuggling is corruption. Criminal groups may try to bribe or otherwise influence maritime workers, immigration officials, customs officers, port employees or anybody else with authorized access to ports and vessels. Unauthorized individuals may be able to obtain counterfeit documents, evade inspection, enter restricted locations or access ships and cargo facilities as a result of this corruption. Therefore, avoiding corruption and upholding the integrity of port workers are crucial components of a successful marine security system. Stowaways may also be a result of human smuggling on commercial ships. Cargo containers, engine rooms, storage sections, and other restricted areas of a ship might serve as hiding places for migrants who want to enter another nation. The crew and passengers may have major safety and security issues if there are unauthorized individuals on board a ship. Additionally, it can present administrative and legal challenges for the shipowner, master, port authorities, and immigration officials, especially if the stowaway's identity and country cannot be determined right away. The development of maritime humanitarian crises is another significant issue. Maritime authorities may have to deal with criminal investigations and their duties to protect human life at sea at the same time when they find or intercept a vessel transporting undocumented migrants. Search and rescue efforts may be necessary right

⁴James Kraska and Raul A Pedrozo, *International Maritime Security Law* (Martinus Nijhoff Publishers 2013) 657–689 (ch 19, 'Migrant Smuggling at Sea').

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

away for overcrowded or unseaworthy vessels. Effective law enforcement and border control measures must be balanced with the duty to protect vulnerable people and assist those in need by maritime authorities. In addition, there may be a direct connection between human smuggling and other significant organized crime. After using smugglers to cross a border, people may fall prey to human trafficking, forced labor, sexual exploitation, kidnapping, extortion or other types of maltreatment. Migrants may occasionally be misled about the terms of transportation or the nature of the arrangements leading them to become reliant on criminal networks. This illustrates how, despite their legal significance, the lines separating human trafficking from migrant smuggling may become ambiguous in real life. Human smuggling is a multifaceted maritime security problem that involves maritime safety, organized crime, corruption, document fraud, unauthorized access to ships and ports, humanitarian emergencies and possible human trafficking. It is not just an immigration or border control issue. Cooperation between coastal states, flag states, port authorities, coast guards, customs, immigration officials, law enforcement, shipping corporations and international organizations is necessary for an efficient response. UNODC has acknowledged that human trafficking, assault, kidnapping, extortion and other serious crimes may overlap with migrant-smuggling operations at sea which may involve intricate linkages between law enforcement and rescue missions. It is essential to distinguish between trafficking and smuggling.⁵ The illegal movement or entry of a person into another state for monetary or material gain is the main focus of human smuggling. In contrast, the goal of human trafficking is exploitation. It is possible for someone to consent to being smuggled at first and then fall victim to human trafficking.

*United States v. Moe*⁶,

This is an important maritime human-smuggling case arising from the voyage of the vessel M/V Golden Venture which was used to transport Chinese nationals towards the United States. The vessel was part of an organized smuggling operation in which migrants paid substantial amounts to smugglers for transportation. The case demonstrates how maritime smuggling operations can involve multiple organizers, recruiters, crew members and financial arrangements. The case is significant because it illustrates the organized and transnational

⁵ Protocol against the Smuggling of Migrants by Land, Sea and Air 2000, art 3; Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children 2000, art 3.

⁶*United States v Moe*, 65 F 3d 245 (2d Cir 1995) (Golden Venture).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

character of maritime migrant smuggling. The vessel itself became an instrument of the criminal enterprise, while the organizers operated through different jurisdictions. It is therefore useful when explaining why maritime migrant-smuggling investigations require cooperation between immigration authorities, coast guards, police, customs and prosecutors.

Principle: Maritime migrant smuggling can constitute a complex transnational criminal enterprise involving the vessel, crew, organizers, recruiters and financial beneficiaries.

*Hirsi Jamaa and Others v. Italy, Application*⁷

This is one of the most important international maritime-migration cases. The case concerned Somali and Eritrean migrants who had left Libya aboard vessels bound for Italy. Italian authorities intercepted them on the high seas and transferred them back to Libya. The European Court of Human Rights held that the migrants came within Italy's jurisdiction because Italian authorities exercised control and authority over them, even though the interception occurred outside Italian territorial waters. The Court found violations concerning non-refoulement, protection against inhuman or degrading treatment and the prohibition of collective expulsion. It emphasized that maritime interception and the fight against irregular migration do not release States from their obligations under international human-rights and refugee law.

Importance for maritime security: It demonstrates that enforcement against maritime smuggling must be balanced with search-and-rescue obligations, human rights and protection of vulnerable migrants.

HUMAN TRAFFICING BY SEA

One of the most serious types of organized international crime is human trafficking often known as trafficking in persons. The UN Trafficking in Persons Protocol's Article 3(a) defines trafficking as the recruitment, transit, transfer, harboring or receiving of individuals for the purpose of exploitation using specific coercive, deceitful or abusive tactics.⁸ Sexual exploitation, forced labor or services, slavery or behaviors akin to slavery, servitude and organ removal are all considered forms of exploitation. Different phases of human trafficking

⁷*Hirsi Jamaa and Others v Italy*, App no 27765/09 (ECtHR, Grand Chamber, 23 February 2012), paras 74–82.

⁸ Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing UNTOC 2000, 2237 UNTS 319, art 3(a).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

may involve the use of maritime transportation. Small boats, passenger ships, cargo ships and fishing vessels may be used to convey victims. In certain situations, the marine sector itself may turn into a site of exploitation and forced labour.

IMPLICATIONS OF MARITIME SECURITY

Because human trafficking combines organized crime, unlawful transportation, exploitation and occasionally corruption, it poses a serious threat to marine security.⁹

Traffickers may exploit:

- isolated maritime routes;
- inadequate inspection of vessels;
- weak port controls;
- fraudulent documentation;
- corrupt officials;
- inadequate crew monitoring;
- subcontracting and complex ownership structures;
- fishing vessels operating far from shore; and
- vulnerabilities of migrant and seafarer populations.

People who are trafficked may experience physical brutality, psychological abuse, forced labour, sexual exploitation and lack of liberty. Victims should not be treated like immigration offenders by marine security enforcement.¹⁰ A successful reaction must include victim identification and protection. In order to move victims away from law enforcement officials, human traffickers may take advantage of remote marine channels. Traffickers may have more opportunity to hide the movement and exploitation of people on vessels that operate in isolated or less-monitored locations. These routes are especially susceptible to criminal activity due to the size of the maritime realm and the challenge of constantly

⁹James Kraska and Raul A Pedrozo, *International Maritime Security Law* (Martinus Nijhoff Publishers 2013) 657–689; Anne T Gallagher and Fiona David, *The International Law of Migrant Smuggling* (Cambridge University Press 2014) 403–489.

¹⁰Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children 2000, arts 6–8.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

monitoring all vessels. Inadequate vessel inspection is another opportunity for traffickers to profit. Traffickers may hide victims in restricted areas of the ship such as cargo areas or accommodations if vessels are not thoroughly examined. Inadequate inspection protocols may enable trafficking activities to go unnoticed especially in cases when authorities lack sufficient resources, qualified staff or trustworthy information about the ship and its crew. Trafficking can be made easier by lax port regulations. Ports serve as important entry and exit points for both people and goods. Inadequate access-control systems, inadequate surveillance, or insufficient screening of individuals may enable victims or traffickers to enter and exit port facilities without being properly detected. These vulnerabilities may be exacerbated by a lack of coordination among port authorities, immigration officials, customs authorities and law enforcement. Fraudulent documentation is another tactic utilized by traffickers. To hide victims' identities and movements traffickers may use fictitious passports, visas, employment documents, identity papers, crew records or other paperwork. Authorities may find it challenging to identify victims, determine their true identity and spot unusual movements as a result of these documents. Trafficking can also be facilitated by corruption among officials or other individuals with access to maritime facilities. Criminal networks may try to influence or bribe security workers, immigration officers, customs officers, port officials or other people. Traffickers may be able to avoid inspections, obtain private information, enter restricted areas without authorization or transfer victims covertly thanks to corruption. Inadequate personnel surveillance can also be exploited by traffickers. Traffickers may take advantage of vulnerable labour or hide trafficking activities aboard vessels if shipping companies or vessel operators lack efficient methods for tracking recruiting, working conditions, crew identity and movement. This is especially important for industries where employees could be at sea for extended periods of time and have no access to outside help. Subcontracting and intricate ownership and management arrangements might make it more difficult to assign blame and uncover human trafficking. Shipowners, operators, managers, hiring firms, contractors and subcontractors from various jurisdictions may be involved in maritime operations. These intricate structures may be used by criminal actors to hide their actions and impede accountability and investigation. Because they may stay at sea for long stretches of time and operate in isolated locations where routine inspections are challenging, fishing vessels that operate far from shore may be especially vulnerable. In addition to potentially being subjected to forced labour, exploitation, violence or other forms of abuse, workers on

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

such vessels may have restricted connection with authorities. Detection and rescue may become far more challenging because to the distance from shore.

Finally, traffickers may take advantage of sailors' and migrants' weaknesses. People who are economically underprivileged unfamiliar with the legal system, reliant on employers or recruiters or have poor communication skills may be more susceptible to exploitation and fraud. Forced labour, sexual exploitation, debt bondage and other forms of coercion may occur after migrants are promised safe transit or genuine employment. Similar to this, when abusive employers or middlemen control their working circumstances, seafarers may be exploited. Traffickers may have several options to hide their actions in the maritime environment. Human trafficking at sea must be prevented and detected by bolstering vessel inspections, port controls, documentation verification, crew monitoring, anti-corruption systems, oversight of recruiting and subcontracting and protection of vulnerable migrants and seafarers.

LEGAL RESPONSE

The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, which supplements UNTOC is the main international framework. States must make trafficking illegal, work with other countries, stop trafficking and safeguard victims. Border control and victim identification should be combined by maritime authorities. Because victims may be unable or reluctant to identify themselves as victims of human trafficking, training for port staff, coast guards, immigration officials, seafarers and law enforcement agents is crucial.

*People of the Philippines v. Hadja Jarma Lalli y Purih, Ronnie Aringoy y Masion*¹¹,

This is a particularly useful maritime human-trafficking case. The case concerned the trafficking of a woman who was transported from the Philippines to Malaysia aboard the ship M/V Mary Joy. One accused argued that he could not be convicted because he was not part of the group that physically transported the victim aboard the ship. The Supreme Court considered the statutory concept of trafficking and the participation of persons involved in the transportation process. The case demonstrates that maritime trafficking should not be examined merely by asking who physically operated the vessel. The recruitment,

¹¹*People of the Philippines v Hadja Jarma Lalli y Purih and Ronnie Aringoy y Masion*, GR No 195419 (Supreme Court of the Philippines, 12 October 2011), 675 Phil 126.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

transportation, transfer and exploitation of the victim and the participation of different members of the trafficking network must be examined.

Principle: Transportation of a trafficking victim by sea can form an important part of the trafficking offence, and liability may extend beyond the person who physically controls the vessel.

Manila Regional Trial Court, Philippines¹²

This is another directly maritime trafficking case. Four young girls were recruited for sexual exploitation and transported aboard a vessel from Iloilo towards Manila. Philippine Coast Guard personnel involved in anti-trafficking operations identified the girls on board, separated them from the accused and facilitated their rescue. The court found that the transportation had been completed for purposes of the trafficking offence even though the victims were intercepted before reaching their final destination. The case therefore illustrates an important principle: the criminal character of trafficking does not necessarily disappear merely because law-enforcement authorities intercept the vessel before the intended destination is reached. It is particularly useful for explaining the role of coast guard and maritime police in identifying trafficking victims during vessel inspections.

Principle: Maritime transportation of victims can constitute part of trafficking even where the victims are intercepted before reaching the intended place of exploitation.

TRAFFICKING OF ILLICIT ARMS BY SEA

Unauthorized transnational movement or transfer of firearms, their parts and components and ammunition is known as illicit arms trafficking. In addition to making illegal manufacturing and trafficking illegal, the UN Firearms Protocol mandates that states implement licensing, marking, record-keeping, tracing and other control mechanisms.¹³ Because ships and ports are components of international supply chains, the maritime industry is especially significant. Criminal organizations may try to smuggle illegal weapons into legal cargo, take advantage of containerized trade, or transport weapons over international boundaries using ships and transshipment routes.

¹²*People of the Philippines v M^a Christina Magante y Tabadilla*, Criminal Case No 11-283640 (Regional Trial Court, Manila, 25 November 2013).

¹³Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing UNTOC 2001, 2326 UNTS 208, arts 3–5, 7–8.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

WHY MARITIME ROUTES ARE ATTRACTIVE FOR ARM TRAFFICKERS

Individuals and organized crime networks engaged in illegal arms trafficking might take advantage of a number of opportunities presented by maritime shipping. The massive amount of legal cargo that is moved through international ports on a daily basis is one of the main causes. It is very impossible for authorities to physically inspect every shipment because millions of containers and cargo consignments travel through the worldwide maritime supply chain. As a result, criminal networks can try to hide illegal firearms amid legitimate trade goods. Arms smugglers find marine channels appealing because of the vast global transportation networks. Ships may visit multiple ports in a single journey and frequently transit between various nations. Authorities may find it challenging to spot suspicious shipments and track down the source, transit path and ultimate destination of illegal weapons due to this transnational mobility. The intricacy of international marine trade may be used by criminal organizations to hide the transportation of illegal items. The presence of numerous transshipment locations is another significant concern. Before arriving at its destination, cargo may be carried via multiple ports or shifted from one vessel to another. The movement of illegal weapons may become increasingly challenging to track with each new transfer. Determining where the illicit activity started and which authorities should be in charge of the inquiry can also be challenging due to the participation of many ports and transportation businesses. The detection of arms trafficking may be made more difficult by the intricate ownership and logistics structures connected to international shipping. A shipowner, charterer, freight forwarder, cargo owner, shipping agent, terminal operator and multiple international subcontractors may all be involved in a single shipment. These intricate arrangements can be used by criminal organizations to hide the true source, ownership or destination of illegal weapons and to complicate investigations. Another important problem is the challenge of physically examining each container. Ports have to keep international trade flowing smoothly while also guarding against security risks. A thorough physical examination of every container would result in significant delays and financial expenses. In order to identify suspect shipments, authorities typically rely on risk-based inspections, intelligence, documentation checks, scanning technologies and other techniques. Vulnerabilities may also arise from variations in country export-control and customs systems. Standards for licensing, documentation, inspection, arms control and customs procedures

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

may vary by state. Criminal networks may try to route goods through jurisdictions where regulations are less effective in order to take advantage of disparities or vulnerabilities between national systems. Therefore, stopping illegal arms trafficking requires effective international collaboration and protocol harmonization. The nature of an armaments shipment may also be concealed by using fraudulent or false documents. Weapons may come with counterfeit permits, invoices, certifications or other documentation or they may be mislabeled as genuine business items. Customs and port authorities may find it more challenging to discover illicit consignments through ordinary document analysis as a result of such tactics.

Finally, insider threats and corruption pose serious risks to the maritime supply chain. By supplying information, getting around security measures or enabling the unlawful transportation of cargo, people having authorized access to ports, terminals, cargo data or security systems may aid criminal organizations. As a result, in addition to physical security measures, effective port security also necessitates personnel screening, anti-corruption measures and insider threat monitoring. Before arriving at its destination, a single consignment of illicit weapons may travel through multiple jurisdictions. This may lead to inquiries about the location of the offense, which state has jurisdiction, which authority should look into the shipment and which state should bring charges against the perpetrators. This jurisdictional intricacy highlights the importance of international collaboration, information exchange, reciprocal legal aid and efficient customs coordination in the battle against marine arms trafficking.¹⁴

CONSEQUENCES OF ILLICIT ARMS TRAFFICKING

International peace, national security, public safety and marine security are all severely impacted by illegal arms trafficking. Its ability to fuel armed conflicts by supplying weapons to parties engaged in civil wars, insurgencies and other violent conflicts is one of its most important effects. Continuous access to weapons obtained illegally can raise casualties, prolong confrontations and make peaceful resolution more challenging. By giving terrorist groups access to firearms, ammo and other weaponry needed to carry out violent acts, illicit arms trafficking can help bolster these groups. Weapons may be obtained by terrorist groups via illegal international supply chains or criminal networks. As a result, the maritime

¹⁴ James Kraska and Raul A Pedrozo, *International Maritime Security Law* (Martinus Nijhoff Publishers 2013) 411–466 (chs 13–14, port, port-facility and ship security); Michael McNicholas, *Maritime Security: An Introduction*, 2nd edn (Butterworth-Heinemann 2016) 137–168.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

transportation system may play a significant role in the transfer of weapons meant for terrorist purposes. The growth of organized crime is another effect. Illegal weapons can be used by criminal groups to carry out violent crimes, intimidate witnesses, maintain territorial control and safeguard their operations. Significant revenues from the trafficking of weapons may also be used to fund other types of organized crime. Armed robberies and piracy at sea can also be facilitated by illicit weaponry. Criminal organizations that operate in coastal or maritime regions may get firearms illegally and use them to assault fishing vessels, commercial ships and other maritime targets. Thus, the degree of violence connected to marine criminal activity may rise due to the availability of illegal firearms. There might be a link between people trafficking and illegal weaponry trafficking. Weapons may be used by criminal groups engaged in human trafficking to intimidate, control, threaten, or punish victims. In a similar vein, the same criminal networks may engage in many types of smuggling and trafficking, such as the transportation of drugs, weapons and people. Violence in coastal areas may also rise as a result of the availability of illegal firearms. Armed criminal groups may target communities near ports, maritime boundaries and trafficking routes. Increased availability to illicit firearms may exacerbate local communities' feelings of insecurity, intimidation, and violent crime. Fragile states may become even more unstable as a result of illegal arms trafficking. Armed groups and criminal organizations can be strengthened by the unchecked circulation of firearms in areas with weak governmental structures, law enforcement agencies, and border control systems. This can weaken the state's authority, fuel political unrest, and make it more challenging to restore efficient governance.

Lastly, various types of transnational criminal activity may be made easier by illegal arms trafficking. Weapons can be traded for cash, drugs, or other illegal goods, resulting in linked criminal markets. This proves that trafficking in maritime weapons cannot be viewed as a singular crime. It is a component of a larger network of international organized crime that includes corruption, smuggling, drug and people trafficking, terrorism, and piracy. Therefore, the trafficking of illegal weapons via maritime routes poses a multifaceted danger to maritime security. Criminal organizations can take advantage of the massive amount of marine trade, intricate international shipping networks, numerous transshipment locations, jurisdictional disparities, and weaknesses in port infrastructure. Strong export and customs regulations, intelligence-led inspections, safe port infrastructure, trustworthy documentation systems,

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

anti-corruption initiatives, and tight international collaboration are consequently necessary for effective prevention. The interconnectedness of today's maritime security concerns is demonstrated by UNODC's emphasis on the link between illegal firearms trafficking and terrorism, organized crime, and other types of trafficking.

INTERNATIONAL LEGAL FRAMEWORK

UNTOC is complemented by the UN Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition. In addition to providing systems for licensing, marking, record-keeping, tracing, seizure and international cooperation, it mandates that states create offenses related to illicit manufacturing and trafficking. Conventional arms transfers are likewise regulated internationally by the Arms Trade Treaty (ATT).¹⁵ Effective port security within the ISPS framework can help prevent unwanted access, identify suspicious activity and improve control over people, cargo and port infrastructure at the maritime level.

*State of Tamil Nadu v. Capt. Dr. L. Mariya Anton Vijay & Ors.*¹⁶

This is one of the most important Indian maritime case. The case arose from the interception of M.V. Seaman Guard Ohio, a Sierra Leone-registered vessel, by the Indian Coast Guard in Indian territorial waters. The vessel was found carrying 35 firearms, 5,682 rounds of ammunition and 102 magazines, without the required authorization and documentation. A joint interrogation team involving the Indian Coast Guard, Customs and other agencies inspected the vessel. The vessel was subsequently handed over to the Coastal Security Group and the matter was investigated by the Q Branch-CID.

The Supreme Court examined, among other matters, the application of the Arms Act, 1959, the possession of firearms aboard a sea-going vessel and the statutory exemption concerning ordinary armament or equipment of a vessel. The Court emphasized that where an accused seeks to rely on the exemption, the firearms must actually form part of the vessel's ordinary armament or equipment. The mere fact that weapons are found aboard a ship does not automatically make them lawful. This case is exceptionally useful for your maritime-security topic because it demonstrates the entire chain:

¹⁵Arms Trade Treaty 2013, 3013 UNTS 269, arts 6–11.

¹⁶*The State Rep by Inspector of Police, Q Branch CID, Tirunelveli Range, Tamil Nadu v Mariya Anton Vijay*, Criminal Appeal No 836 of 2015, decided 1 July 2015, (2015) 9 SCC 294; [2015] 7 SCR 581; 2015 INSC 463, paras 104–114.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

Coast Guard interception - boarding - vessel inspection - seizure of arms - FIR - transfer of investigation - forensic examination - prosecution under the Arms Act.

Principle: Possession of large quantities of firearms and ammunition aboard a vessel without lawful authorization can attract the Arms Act, and the maritime location of the vessel is important in determining jurisdiction.

*Dudnik Valentyn v. Inspector of Police*¹⁷

This case arose from the same M.V. Seaman Guard Ohio episode and provides useful details concerning the maritime investigation and prosecution. The investigation found 35 firearms, 5,682 rounds of ammunition and 102 magazines aboard the vessel. The weapons were seized after physical verification, and the accused were arrested after failing to produce appropriate licences or authorizations. The case is particularly valuable for your section on investigation by maritime agencies because it records the role of the Coast Guard, Customs, Marine Police and Q Branch-CID. It also demonstrates the importance of the vessel's location, the deck log, documents concerning the weapons, and the circumstances in which the vessel entered Indian waters.

Principle: Investigation of maritime arms offences requires examination of the vessel's location, documentation, crew, weapons, licences, logbooks and the circumstances of possession.

MARITIME TERRORISM

Terrorist acts against ships, ports, marine installations, passengers, crews or other maritime infrastructure are referred to as maritime terrorism as is the use of maritime transportation to carry out terrorist acts.¹⁸ Terrorist groups are drawn to the maritime area because ships may transport dangerous materials, lucrative cargo and large numbers of passengers. Because a big port's disruption can have an impact on both domestic and international trade, ports are also strategically significant.

Examples of maritime terrorist threats include:

¹⁷*Dudnik Valentyn v Inspector of Police*, CrI A (MD) Nos 41, 43 & 44 of 2016 (Madras High Court, 27 November 2017), reported as [2018] 1 MLJ (CrI) 173.

¹⁸Natalie Klein, *Maritime Security and the Law of the Sea* (Oxford University Press 2011) 147–210 (ch 4, 'Terrorism and Proliferation of Weapons of Mass Destruction').

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

- hijacking of ships;
- hostage-taking;
- attacks against passenger vessels;
- bombing or sabotage of ships;
- attacks against ports;
- use of vessels to transport terrorists or weapons;
- attacks against offshore installations;
- deliberate collision or grounding of ships; and
- use of ships or hazardous cargo to cause mass casualties or economic disruption.

The IMO identifies terrorism as a significant maritime security concern and developed enhanced security measures following the attacks of 11 September 2001.

MARITIME TERRORISM AND STRATEGIC SHIPPING ROUTES

Narrow straits, canals, large ports and frequently frequented sea routes are areas where the hazard is most severe. Attacks against strategically significant tankers or ships transporting hazardous materials can have far-reaching effects. A huge vessel being purposefully grounded or obstructed in a narrow navigation channel, for instance, might impede maritime commerce, harm the environment and have serious economic repercussions. Situations involving the intentional grounding or abuse of tankers have been identified by the IMO as security risks.

*Mohammed Ajmal Amir Kasab v. State of Maharashtra*¹⁹

The 26/11 Mumbai terrorist attackers used the maritime route to enter India. They hijacked the fishing vessel M.V. Kuber, killed its navigator and subsequently proceeded towards Mumbai carrying firearms, ammunition and explosives. The Supreme Court's judgment provides detailed evidence concerning the maritime journey, the vessel, the weapons and the terrorist conspiracy. The case demonstrates how maritime transportation can be exploited for terrorist infiltration of coastal territory. It also illustrates the importance of coastal

¹⁹*Mohammed Ajmal Mohammad Amir Kasab v State of Maharashtra*, Criminal Appeals Nos 1899–1900 of 2011, decided 29 August 2012, (2012) 9 SCC 1; AIR 2012 SC 3565; 2012 INSC 357, paras 316–321.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

surveillance, intelligence sharing, vessel identification, interception and investigation. For your BNS-related discussion, this case can be connected with Section 113 BNS, which now deals with terrorist acts, while the factual and legal issues may also attract the UAPA and other special laws depending upon the circumstances.

Principle: Maritime routes and vessels can be used as instruments of terrorist infiltration and attack, making maritime security an essential component of national security.

*Massimiliano Latorre & Salvatore Girone v. Union of India*²⁰

The *Enrica Lexie* litigation is another major maritime-security case. The incident involved the Italian-flagged commercial vessel *Enrica Lexie* and an Indian fishing vessel, *St. Antony*. Two Italian Marines aboard *Enrica Lexie* fired upon the fishing vessel, resulting in the deaths of two Indian fishermen. The incident generated extensive litigation concerning maritime jurisdiction, coastal-State powers, flag-State jurisdiction and the application of the SUA Act. The Kerala High Court considered the applicability of India's Suppression of Unlawful Acts against the Safety of Maritime Navigation and Fixed Platforms on Continental Shelf Act, 2002 (SUA Act). The Court held that both the commercial vessel and fishing vessel came within the statutory definition of "ship" and examined the territorial application of the SUA Act to India's maritime zones.²¹ The dispute subsequently reached the international level, making *Enrica Lexie* a major authority on the interaction between maritime criminal jurisdiction and international law.

Principle: Maritime security incidents involving violence against persons aboard vessels require careful determination of the applicable maritime zone, flag-State jurisdiction, coastal-State jurisdiction and relevant international conventions.

UNLAWFUL ACTS AGAINST THE SAFETY OF MARITIME NAVIGATION

SUA CONVENTION, 1988

The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988, commonly known as the SUA Convention, was adopted in Rome on 10

²⁰*Enrica Lexie*

²¹*Republic of Italy through Ambassador v Union of India*, (2013) 4 SCC 721; *Massimiliano Latorre and Salvatore Girone v Union of India*, SLP (C) No 20370 of 2012, orders in the *Enrica Lexie* proceedings.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

March 1988 and entered into force on 1 March 1992. It was subsequently strengthened through the 2005 Protocol. The Convention was developed in response to growing concern about serious unlawful acts against ships, including hijacking, violence against passengers and crews, sabotage and other conduct threatening maritime navigation.

Article 3 covers important offences such as:

- seizure of a ship by force or threat;
- acts of violence against persons aboard a ship;
- destruction or damage to a ship;
- placing destructive devices or substances aboard a ship;
- certain acts interfering with safe navigation; and
- other conduct threatening maritime safety.

The central purpose is to ensure that persons committing such unlawful acts do not escape accountability merely because the offence has an international or maritime character.²²

2005 PROTOCOL

The SUA system was further enhanced by the 2005 Protocol. It increased the penalties for, among other things, using explosives, radioactive or biological, chemical or nuclear material and several hazardous compounds with the intention of intimidating a populace or coercing a government or international organization. The SUA framework links international criminal cooperation and counterterrorism with maritime law. One of the most significant clauses addressing crimes against the security and safety of ships is found in Article 3 of the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988 (SUA Convention). Article 3's main goal is to identify and penalize serious unlawful behavior that endangers the security of boats, the safety of maritime navigation and the lives of people on board. In order to recognize major maritime offenses as crimes and prevent criminals from readily avoiding prosecution by using variations in country legal systems or the global nature of maritime transportation, the provision creates a common worldwide legal framework. According to Article 3, it is illegal for someone to unlawfully and knowingly take

²² Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation 1988, 1678 UNTS 221., SUA Convention 1988, art 3(1)(b)–(c).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

control of a ship by using force, threats of force, or other forms of intimidation. This clause addresses actions that are frequently connected to maritime hijacking. Article 3 may apply, for instance, if an individual or organized group violently seizes control of a commercial vessel and stops the crew and master from carrying out their legal duties. Because the unlawful seizure of a vessel might put everyone on board in risk, interfere with international navigation, and even give criminals or terrorists control over the ship and its cargo, the offense is especially serious. Acts of violence against individuals on board a ship that are likely to jeopardize the vessel's safe navigation are also included under Article 3. Serious physical assaults on the ship's master, crew, passengers, or other individuals are included in this. Because it may make it more difficult for the master and crew to manage the ship properly, violence on a vessel can have repercussions that extend beyond the immediate victim. An assault on the master or bridge staff for instance, could make it impossible to operate the ship safely and increase the chance of a collision, grounding, or other nautical mishap. Destroying a ship or damaging a ship or its cargo in a way that could jeopardize the ship's ability to navigate safely is another significant category. The safety of a ship and everyone on board might be gravely jeopardized by purposeful damage to its hull, propulsion system, steering gear, navigation equipment, or other vital parts. Such behavior may also have negative effects on the environment and the economy, especially if the ship is transporting chemicals, oil, or other dangerous materials. As a result, the clause acknowledges that intentional damage to a ship that endangers marine navigation is more than just a property offense. Article 3 further makes it illegal to put or cause to be placed aboard a ship any equipment or material that could threaten the ship's safe navigation by destroying or damaging the ship or its cargo. In light of terrorist acts and sabotage, this clause is very crucial. An explosion, fire, structural damage, or loss of propulsion could result from the covert placement of an explosive device, hazardous material, or other damaging item on a ship. The clause is meant to stop anyone from using ships as targets for sabotage or as tools for major maritime catastrophes. Certain behaviours that obstruct a ship's safe operation or navigation are also covered by the Convention. When behaviour interferes with a ship's operation and puts the ship or its occupants in danger, it may be considered a serious international maritime offense. The bridge, communications, steering, propulsion, and other critical systems must all operate properly for navigation. Therefore, a seemingly localized criminal act might become a major threat to maritime safety through deliberate manipulation

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

with these systems. Article 3 also includes certain communications of false information when such information is likely to jeopardize the safe navigation of the ship. False information about navigation and security of the vessel will make the captain and crew members to take dangerous steps or unnecessary deviation of the vessel. In the modern era, ships are dependent on navigational and operational information. The significance of article 3 is not only because of identification of offenses but also because of its provision of an international base for criminal cooperation. Ships travel among various countries and even within one journey a ship passes through the territorial waters of various countries. In some cases, the nationality of the ship, nationality of the offender, place of committing the crime and destination of the ship may affect a case. Without international legislation, it may be possible for criminals to exploit the difference in the legislation of the two countries.

SUA Convention works under the assumption that serious acts of offense against maritime navigation should not get away unpunished simply because it is an international maritime environment. States Parties to the SUA Convention are supposed to provide appropriate jurisdiction over the acts described in the Convention. Also, it becomes essential to take measures to deal with such offenses under the process of law. The SUA Convention thus enhances the principle of “extradite or prosecute” according to which no state party should provide sanctuary to any person accused of the serious SUA offenses. Article 3 is of particular importance with respect to maritime terrorism. Even though the SUA Convention does not limit itself to only terrorism, still various acts specified in the article 3 are done for terrorist purposes. For example, hijacking, violent attacks against passengers or crew, sabotage and destruction of the ship may be done with the intention of terrorism. SUA Convention is therefore a significant tool for combating terrorism against the ships and maritime transportations. Article 3 also plays a role in the protection of international maritime commerce. Global trade today depends a lot on the safe passage of ships. Any malicious act against the ship will result in loss of human lives, loss of cargo, environmental pollution, disruption of shipping schedule, closure of port and substantial economic loss. It is therefore clear that maritime navigation safety is directly related to international trade. Further expansion of the international legal framework in the field of combating unlawful acts that threaten maritime security was made in 2005 through the Protocol to the SUA Convention, which dealt with serious acts, among others, some uses of explosive, radioactive, biological, chemical or nuclear materials and also any other conduct involving ships or persons which

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

may seriously threaten maritime security. Thus, the SUA regime developed its position to deal with the emerging threats of terrorism and maritime security. So, Article 3 can be regarded as an important article of the international legal framework on unlawful acts concerning maritime navigation. According to it, conduct includes the following actions: unlawful seizure of ships, serious violence against persons on board ships, destruction or damage to ships, placing of destructive devices or substances on board ships, and any other act that may endanger the safe navigation. In general, its purpose is to make sure that maritime offenders cannot take advantage of the international nature of shipping and lack of coordination between different national jurisdictions.

Extradite or Prosecution

One of the key principles provided for in the SUA Convention is the obligation of the Contracting Governments to take the appropriate measures regarding the offenders, including prosecution or extradition.²³ Such principle helps to prevent exploitation of jurisdictional gaps between States by maritime criminals.

*Institute of Cetacean Research v. Sea Shepherd Conservation Society*²⁴

It is an important international maritime case dealing with the conduct that may affect the safety of navigation. The lawsuit dealt with actions against Japanese whaling vessels made by Sea Shepherd. The US court examined the meaning of piracy and took into account the prohibition of unlawful and intentional acts under the SUA Convention that endangered the safe navigation of a ship. The court described actions like violence against persons on board a ship, damage to ships or cargo and placing devices or substances on board ships, causing damage. It is also worth mentioning the significance of the SUA regime in regard to serious unlawful acts affecting maritime navigation.

Principle: International maritime law makes a distinction between ordinary protest or interference and unlawful conduct that threatens the safety of maritime navigation; serious acts affecting ships may be included in the international framework, such as SUA.

²³SUA Convention 1988, arts 6–10.

²⁴725 F.3d 940 (9th Cir. 2013)

INTERNATIONAL SHIP AND PORT FACILITY SECURITY (ISPS) CODE

International Ship and Port Facility Security (ISPS) Code is one of the key international instruments regulating maritime security. This instrument creates an integrated security regime applicable to ships and port facilities involved in international maritime shipping. The main goal of the Code is to protect ships and ports from any intentional threats to their security, such as terrorism, hijacking, sabotage, unauthorised access, smuggling and other activities which might have an adverse impact on safety and security of maritime transport. ISPS Code is a response to fundamental changes in the international security environment, which occurred after terrorist attacks on 11 September 2001 in the United States. Until this time, international regulations for the maritime industry were focused mainly on the aspects of maritime safety, such as accident prevention, seaworthiness, safety of lives at sea and navigation regulation. Terrorist attacks of 9/11 showed that the transportation infrastructure can be used for terrorist purposes. Therefore, there was a need in creating an integrated system dealing with maritime security issues. According to IMO, ISPS Code has been developed as a response to the threats faced by ships and port facilities after the attacks of 9/11. The International Maritime Organization (IMO) reacted very quickly to the changes in the security environment. The diplomatic conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 (SOLAS) took place in London in December 2002.²⁵ This conference adopted SOLAS amendments and established a new Chapter XI-2 entitled "Special Measures to Enhance Maritime Security". Regulation XI-2/3 of this chapter included ISPS Code into the SOLAS regime. The amendments and the Code entered into force on 1 July 2004. In other words, the ISPS Code is not only the set of recommendations provided by the IMO. The Code operates under SOLAS Chapter XI-2 and the mandatory provisions of the Code become legally binding for SOLAS Contracting Governments and ships and port facilities covered by the Code. IMO considers ISPS Code as the core of its regulatory framework for maritime security.

RELATIONSHIP BETWEEN SOLAS CHAPTER XI-2 AND THE ISPS CODE

²⁵International Maritime Organization, *International Ship and Port Facility Security (ISPS) Code*, 2003 edn, IMO Publication K116E (IMO, London 2003), Introduction; International Convention for the Safety of Life at Sea 1974, ch XI-2.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

To assess the legal significance of the ISPS Code, it is necessary to consider its relationship with SOLAS. SOLAS 1974 is one of the major international maritime conventions addressing safety issues of ships and persons at sea. As a result of the amendments of 2002, a new Chapter XI-2 “Special Measures to Enhance Maritime Security” was created.

This chapter serves as the basis for the ISPS Code. Thus:

SOLAS 1974 - Chapter XI-2 - ISPS Code - Security requirements for ships and port facilities

Regulation XI-2/3 makes the ISPS Code the relevant international maritime security regime. There are many other requirements set by Chapter XI-2, among which those concerning the following aspects: security levels, ship security alert system, port facility security and the role of the ship’s master in relation to security matters. Such a relationship is essential for the following reason: the ISPS Code becomes a part of the international treaty-based regulatory system rather than being separate from it.

SCOPE AND APPLICATION OF THE ISPS CODE

The ISPS Code is mostly applied to ships and port facilities involved in international maritime transport within the scope of SOLAS Chapter XI-2. The relevant SOLAS security regime, among others, applies to passenger ships and cargo ships with the gross tonnage of 500 or higher, including high-speed craft, mobile offshore drilling units and the port facilities servicing such ships when they are involved in international voyages. Thus, the ISPS Code imposes certain obligations for the participants in the maritime transportation process. It does not apply only to the vessel. Security is seen as a ship-port interface issue, which means that the security of the ship and port facilities where the ship is sailing have to be addressed together. For instance, if there is a well-developed security system on board a vessel, it cannot be safe, if it is sailing into the port with the very weak access control system. On the contrary, even if there is a very secure port, it can be jeopardized by vessels with the poor security system coming into it.

MAIN OBJECTIVES OF THE ISPS CODE

The principal purpose of the ISPS Code is to develop an internationally harmonized mechanism for identifying, evaluating and dealing with threats to maritime security. One of such objectives is to establish cooperation between Contracting Governments, governmental bodies, local authorities, shipping companies and port industry. Maritime security cannot be

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

ensured by one authority because the threats can be originated from outside the ship or port. Therefore, the information and responsibilities must be shared among different authorities. Another objective is to define the roles and responsibilities of different parties involved in ensuring maritime security. ISPS Code specifies the responsibilities at governmental, company, ship and port-facility levels. Such an approach will help to eliminate confusion about who should act in case of a security threat. In addition, ISPS Code attempts to encourage the early information gathering and exchange. If information about the terrorist threat, suspicious person, vessel or cargo is received by one authority and is not communicated to other authorities responsible for the security, the effectiveness of the whole system will be seriously undermined. Another objective of the ISPS Code is to develop a systematic approach to performing Ship Security Assessment and Port Facility Security Assessment which will be used as the base for developing security plans. And finally, the ISPS Code aims to ensure that the security measures are proportionate to the level of threat. The system does not require each ship and port facility to have permanent high security measures, but provides the possibility to vary the security measures according to changing situation and threat level.

RISK-BASED APPROACH OF THE ISPS CODE

One of the main peculiarities of the ISPS Code is its risk management approach. It means that not all ships and port facilities have the same threats. The vessel sailing through low-risk areas may have different security risks compared with the vessel arriving into the port which is situated in a high-risk terrorist zone. Thus, the security measures should be based on:

Threat - Vulnerability - Risk Assessment - Appropriate Security Measures

Such an approach involves authorities in the process of identifying possible threats, estimating vulnerabilities and introducing appropriate measures in accordance with a level of the risk. Thus, if the intelligence service has some information concerning a higher probability of a terrorist attack on a certain port, then some additional access controls, surveillance, screening and security forces may be applied. In case when the level of the threat falls, it may be possible to go back to the normal level of security measures. According

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

to the definition of the IMO, the ISPS Code is the risk management activity, when security measures are established through risk assessment and security levels.

STRUCTURE OF THE ISPS CODE

The ISPS Code includes two main parts: Part A and Part B.

Part A – Mandatory Provisions

In this part, there are mandatory requirements. These requirements concern the specific security measures and obligations that must be observed by the relevant governments, port facilities, shipping companies and ships covered by the code.

Mandatory requirements include the following items:

- security assessments;
- security plans;
- security officers;
- security levels;
- access control;
- monitoring of restricted areas;
- cargo security;
- ship security;
- port-facility security;
- security communications;
- verification and certification; and
- procedures for responding to security incidents.

Part A requirements being incorporated into the SOLAS security framework are legally binding requirements for the States and entities concerned. As it is stated by IMO, Part A contains detailed mandatory maritime and port-security requirements.

Part B – Recommendatory Guidance

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Part B provides guidance on how mandatory provisions contained in Part A can be implemented. Therefore, in legal terms, Part B differs from Part A.

In this part, there are recommendations, explanations and examples that can help Governments, companies, ships and port facilities in observing Part A requirements effectively.

Thus, in case when Part A establishes that security assessment must be performed, Part B provides recommendations concerning the factors that can be considered during such an assessment and ways of finding out vulnerabilities.

Therefore, we can say that Part B serves as an implementation guide for Part A.

Main difference is the following:

Part A defines mandatory security requirements that must be met, but Part B shows how these requirements can be met.

SHIP SECURITY ASSESSMENT (SSA)

A Ship Security Assessment (SSA) is a systematic examination of the security threats and vulnerabilities associated with a particular ship. The assessment considers matters such as the possibility of unauthorized persons boarding the vessel, unauthorized access to restricted areas, sabotage, terrorist attacks, suspicious cargo, stowaways and other activities that could threaten the security of the ship. The purpose is not simply to identify threats but to determine the weak points of the vessel's security system.

For example, an assessment may reveal that:

- a particular access point is insufficiently monitored;
- identification procedures are weak;
- restricted areas are inadequately protected;
- cargo documentation is insufficiently verified; or
- communication procedures during a security incident are inadequate.

The findings of the Ship Security Assessment form the basis for preparing the Ship Security Plan (SSP).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

SHIP SECURITY PLAN (SSP)

The Ship Security Plan is the operational security document developed for the individual ship. It establishes the procedures and measures that must be followed to protect the ship from identified security threats.

The plan may address matters such as:

Access control: determining who may board the ship and under what conditions.

Restricted areas: identifying areas where access must be controlled.

Monitoring: establishing procedures for surveillance and observation.

Cargo security: preventing unauthorized interference with cargo.

Personnel security: verifying the identity and authorization of persons working on or visiting the ship.

Security communications: establishing procedures for reporting and responding to security incidents.

Emergency response: establishing procedures for dealing with security threats.

The Ship Security Plan is therefore the practical mechanism through which the findings of the Ship Security Assessment are converted into operational security measures.

PORT FACILITY SECURITY ASSESSMENT (PFSA)

Security under the ISPS Code does not stop at the ship. Port facilities must also undergo security assessment. A Port Facility Security Assessment (PFSA) identifies vulnerabilities within the port facility and determines the potential consequences of different security threats.

The assessment may examine:

- port entrances and exits;
- fencing and perimeter security;
- access points;
- cargo-handling areas;

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

- passenger areas;
- restricted zones;
- security equipment;
- surveillance systems;
- communication systems;
- personnel security;
- vehicle access; and
- the ship-port interface.

The objective is to identify areas where a terrorist, criminal or other unauthorized person could gain access or cause harm. The findings are then used to prepare a Port Facility Security Plan (PFSP). SOLAS Chapter XI-2 requires Contracting Governments to ensure that port-facility security assessments are carried out and that security plans are developed, implemented and reviewed in accordance with the ISPS Code.

PORT FACILITY SECURITY PLAN (PFSP)

The Port Facility Security Plan establishes the measures that a particular port facility must implement to address the vulnerabilities identified through its security assessment.

It may include measures concerning:

- access control;
- identification of port personnel;
- screening of persons;
- monitoring of restricted areas;
- surveillance;
- vehicle control;
- cargo security;
- protection of critical infrastructure;

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

- security communications;
- emergency procedures;
- coordination with law-enforcement agencies; and
- procedures applicable at different security levels.

The PFSP therefore provides the operational security framework for the port facility.

THE ISPS CODE FOR THE SECURITY OFFICERS

There are certain security obligations created under the ISPS Code.

- Company Security Officer – CSO

The Company Security Officer is responsible for security related issues within the company. The CSO will help ensure that the company's ships are in compliance with the applicable security requirements and also assist in developing, implementing and maintaining ship security arrangements.

- Ship Security Officer – SSO

The Ship Security Officer is responsible for security issues on board the ship. The SSO will play an essential part in implementing the Ship Security Plan and carrying out security inspections on board the ship.

- Port Facility Security Officer – PFSO

The Port Facility Security Officer is responsible for security issues within the port facility. The PFSO will play an essential part in implementing the Port Facility Security Plan.

The IMO has identified the CSO, SSO and PFSO as important security personnel that can assess threat and prepare and implement security plans.

THE THREE SECURITY LEVELS

One of the key features of the ISPS Code is the three security levels.

Security Level 1 – Normal

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Security Level 1 is the normal operating level. Minimum appropriate protective security measures are maintained continuously at this level.

For instance, routine procedures for controlling access, verification of identities, monitoring and security patrols may be maintained.

Security Level 2 – Heightened

Security Level 2 comes into effect when there is an increased risk of a security incident.

This level will require additional security measures for as long as the increased risk remains. It includes measures such as increased surveillance, additional control of access, extensive screening and cooperation between security authorities.

Security Level 3 – Exceptional

Security Level 3 comes into effect when there is a probable or imminent risk of a security incident.

This involves further specific protective measures for a limited period. This level aims at addressing serious and immediate security threats. Most importantly, Security Level 3 is an exceptional level and can only be implemented when there is credible information about probable or imminent security incident.

SHIP SECURITY ALERT SYSTEM (SSAS)

Another significant measure adopted through SOLAS Chapter XI-2 is the Ship Security Alert System (SSAS). The system enables a ship to transmit a security alert to the designated authority in case of a serious security incident. It is especially important in cases of hijacking, terrorist attack or any other kind of serious security interference. According to SOLAS Chapter XI-2, ships operating under the relevant regime shall be provided with a ship security alert system.

THE ROLE OF THE MASTER

It is essential to note that the ISPS Code acknowledges the special authority of the Master of the ship in terms of security. The SOLAS Chapter XI-2 also clearly states that the Master has professional responsibilities and discretion in making decisions which are necessary for the maintenance of security on board. The Master is not supposed to be influenced by the

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

company, the charterer or any other person when making his decision concerning the security of the vessel. This is crucial since security incidents can develop very quickly at sea. The Master has to take quick decisions in order to ensure the safety of the crew, passengers, the vessel and its cargo.

THE IMPORTANCE OF THE ISPS CODE IN MARITIME SECURITY

The main significance of the ISPS Code consists in the fact that it changed the maritime security from an issue of individual countries to an issue of international security system. It provides common criteria for ships and ports all over the world. It is especially significant since international ships are constantly moving from one jurisdiction to another. For instance, the vessel may be registered in India, owned by a company in some other country, managed in some other jurisdiction and visiting ports in many continents. In the absence of international security standards the vessel can encounter absolutely different security requirements in each port.

ISPS CODE AND PREVENTION OF MARITIME SECURITY THREATS

The ISPS code has particular relevance to the discussion on maritime security threats in your topic. As for the issue of human smuggling and trafficking, proper access control, identification system, monitoring and port security measures will make it harder for any unauthorized persons to get aboard vessels or restricted port areas. Concerning illicit arms trafficking, cargo security, access control, documentation and surveillance will help prevent any movement of dangerous or prohibited cargo. Regarding the issue of maritime terrorism, security assessment, security plan, restricted areas, surveillance, security levels and ship security alert systems can be used as preventive measures to counter terrorist threat. In the case of unlawful acts against ships, the ISPS code will help strengthen preventive measures through reduction of possible vulnerabilities that can be used to commit such acts. Thus, the ISPS code serves mostly as a prevention instrument whereas other international documents, for instance, SUA convention, deal with the criminalization and suppression of unlawful acts.

PORT FACILITY SECURITY ASSESSMENT AND PLAN

Ports are especially vulnerable due to the fact that they link the sea transportation with land one, as well as represent large concentration of people, cargo and infrastructure. The Port Facility Security Assessment (PFSA) helps identify all existing vulnerabilities within the port

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

facility. Consequently, the Port Facility Security Plan (PFSP) will serve to establish measures that help eliminate these vulnerabilities.

Port security measures may include:

- perimeter protection;
- access control;
- identification systems;
- surveillance;
- screening of persons;
- monitoring of cargo;
- restricted areas;
- vehicle control;
- security patrols;
- communications;
- emergency response;
- coordination with police and coast guard authorities; and
- protection of critical infrastructure.

The SOLAS Chapter XI-2 requires port facilities to conduct security assessments and develop, implement and review security plans in compliance with the ISPS Code.

DECLARATION OF SECURITY

Declaration of Security (DoS) is an important tool for establishing security responsibilities between a ship and port facility, or ships in some cases. Declaration of Security identifies the respective security responsibilities of each party and ensures that it is clearly understood who is responsible for certain security measure. This is especially useful when a vessel enters a port in which the security situation, operational circumstances, or activities require additional coordination.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

SHIP SECURITY ALERT SYSTEM

The SOLAS Chapter XI-2 requires that vessels in the relevant regime be fitted with a Ship Security Alert System (SSAS). This system allows a ship to send a security alert to a designated authority in such a way as not to raise an alarm on board that may compromise the safety of the crew.

This issue is especially pertinent to the following types of scenarios:

- Hijacking;
- Terrorist attacks;
- Illegal boarding;
- Armed attacks; and
- Other security emergencies.

SECURITY OF INTERNATIONAL PORTS

Port security cannot be dissociated from national security as the ports are entry points through which people, cargo, and potentially dangerous materials enter or leave the state. Thus, the successful security regime for ports should entail the cooperation of the following parties:

Port authorities + Customs + Immigration + Police + Coast Guard + Navy + Intelligence agencies + Shipping companies + Terminal operators + Other relevant regulatory bodies.

Security efforts should commence prior to the arrival of the vessel at the port through the exchange of information and the pre-arrival security information and should extend throughout the vessel's stay at the port and departure from it.

MARITIME SECURITY AND CARGO SECURITY

Cargo security is critical because the legal cargo can be used to smuggle:

- Illicit arms;
- Drugs;
- Explosives;
- Trafficked persons;

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

- Stowaways;
- Contraband; and
- Others.

Due to the enormous volume of cargo handled in modern ports, physical inspection of every piece of cargo is practically impossible. As a result, risk-based inspection, analysis of the intelligence data, documentation verification, container security and cooperation between customs and port security are imperative. The approach taken under the ISPS is fundamentally risk-based: the security measures taken should correspond to the threat.

MARITIME SECURITY AND STOWAWAYS

Stowaways present another problem related to both maritime security and migration. People may attempt to hide themselves aboard the vessel without any permission, especially in cargo areas or in port facilities.

The stowaway issue brings about:

- security threats;
- safety threats;
- problems with immigration;
- humanitarian issues;
- financial losses to the shipowner; and
- links with the migrant smuggling or trafficking.

There is specific guidance adopted by the IMO relating to the prevention of unauthorized access to the ships from stowaways and the distribution of responsibility in relation to handling stowaway cases. There are several maritime security, safety, legal and humanitarian issues associated with the presence of stowaways on ships. A stowaway is any person that accesses the ship without the authorization or the consent of the ship owner, ship master or appropriate authorities. This happens when a person accesses a ship while the ship is docked in the port and hides in cargo compartments, containers, engine compartments, passenger compartments or any other part of the ship. The presence of stowaways on ships poses certain

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

maritime security, safety, immigration and legal challenges to the master, crew members, ship owner, port authorities and any other maritime security organizations. Stowaways pose potential unauthorized access threats since their access to a ship occurs in a manner which bypasses the existing access control and identification mechanisms. Stowaways pose potential security gaps in relation to the port security, access control mechanisms to vessels and cargo handling processes of vessels. Even though stowaways are not necessarily security threats or criminals, the authorities need to identify the reasons behind their access and intentions. It gets particularly problematic in situations whereby there is uncertainty as to whether the person in question is an illegal immigrant, a victim of human trafficking or any other person involved in criminal activities. Stowaways also cause maritime safety problems. Stowaways may hide in places such as cargo compartments, containers, machinery compartments and places containing dangerous goods. Such people may lack adequate provisions such as food and water supply, ventilation and proper medical care during their voyage. Stowaways hiding in dangerous places pose risks to the masters and crew members who may be required to remove them from dangerous locations. In some instances, stowaways may be exposed to dangerous conditions such as extreme temperatures, toxic fumes, machinery movement and other dangerous situations. Thus, the master has to protect the safety of the stowaways as well as the safety of the crew members. The presence of stowaways causes immigration and jurisdictional complications. Once a stowaway is discovered, the authorities need to determine the stowaway's identity, nationality, immigration status and the destination of the person. The individual may not possess valid travel documents or may refuse or be unable to disclose his or her identity. Questions may then arise regarding which State is responsible for accepting the person, whether the person should be returned to the State of origin or another appropriate State, and what procedures should be followed before the vessel is permitted to continue its voyage. Because a ship may operate under the flag of one State, depart from a port in another State and discover a stowaway after reaching a third State, several jurisdictions may become involved. There are also significant humanitarian concerns. A stowaway may be a vulnerable person who has fled poverty, persecution, conflict or other difficult circumstances. Some stowaways may have been deceived or forced by criminal networks and may actually be victims of human trafficking. Therefore, authorities should not automatically treat every stowaway simply as an immigration offender. Their physical condition, safety, nationality, circumstances of travel

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

and possible victim status should be properly assessed. Where there are indications of trafficking or other exploitation, appropriate victim-protection mechanisms should be activated. The presence of stowaways can also result in considerable financial and operational costs for shipowners. Once a stowaway is discovered, the vessel may experience delays, additional administrative requirements, security arrangements, medical expenses, legal costs, deviation of the voyage or expenses associated with repatriation. The shipowner may also have to cooperate with immigration authorities, port officials and other governmental agencies. Consequently, preventing unauthorized access and discovering stowaways at the earliest possible stage can reduce both security risks and financial losses. Stowaways may also have potential links with migrant smuggling and human trafficking. A person may have paid a smuggling network to gain unauthorized access to a vessel and travel to another country. In more serious situations, a person may have been recruited, transported or concealed as part of a trafficking operation. A migrant who initially consented to irregular transportation may subsequently become subject to coercion, exploitation, forced labour or other forms of abuse. For this reason, authorities must distinguish carefully between ordinary stowaway cases, migrant-smuggling situations and human-trafficking cases.

The IMO has provided guidance on stowaways, especially regarding prevention of unauthorized access to ships and the allocation of responsibilities among the different stakeholders whenever there is a discovery of stowaways. The main emphasis in the IMO framework is on collaboration between the shipowner, master, port authorities, Government and others to prevent boarding and solve cases of stowaways in an effective and humane manner. Some of the preventive measures include enhancing controls at ports and ships, securing sensitive areas, monitoring people accessing vessels, conducting proper security procedures and establishing proper communication between ships and ports. The issue of allocation of responsibilities is very critical since stowaway cases involve many stakeholders. The shipowner and the master have the responsibility of ensuring the security of the vessel and wellbeing of the people who board it. The port authorities and Government have the responsibilities of ensuring the security of the port, controlling immigration and the identification and handling of people accessing ships without proper permission. Collaboration between these different authorities will help in arriving at the proper solution such as documentation, disembarkation and other legal requirements. Therefore, stowaways are not simply immigration problems; they may present maritime security, safety and

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

economic risks, immigration and jurisdiction challenges, costs to shipowners, humanitarian issues and even migrant smuggling or human trafficking. Effective implementation of the ISPS code, access control measures, port surveillance, crew vigilance, reporting and collaboration between the maritime and immigration authorities are critical for avoiding unauthorized access and solving stowaway problems.

ROLE OF MARITIME DOMAIN AWARENESS

Maritime Domain Awareness (MDA) is an integral part of modern day maritime security and is defined broadly as effective understanding of activities, events and circumstances within the maritime domain that could impact the security, safety, economy or environment of a State. Through MDA, the authorities are able to get information on what is taking place at sea, where it takes place, who is involved and whether the activity poses a security threat. MDA is very critical because of the vast nature of the maritime domain, its dynamic nature and difficulty of monitoring it continuously. Vessel Tracking and Identification is an essential task in MDA. It is vital for authorities to know what ships are working in particular maritime area, their whereabouts, destinations and their movements. Information about vessels' movement can be used for detection of unusual behavior such as entry into unexpected area, deviating substantially from the announced route, stopping for some unknown reasons or approaching some restricted maritime facility. Vessel tracking information does not necessarily mean that the ship is doing something illegal but at the same time it may become an indicator that requires further investigation or monitoring. Thus, continuous tracking is a powerful tool for detection of vessels that need additional attention of maritime security authorities. Another technological instrument of MDA is the Automatic Identification System (AIS). The system makes it possible for adequately equipped ships to transmit information about its identity, whereabouts, course and speed, as well as other navigation data. The information may be used by authorities for monitoring of maritime traffic and analysis of vessels' movements. Comparing the information with others, authorities can find discrepancies that require additional investigation. Nevertheless, the AIS cannot be considered as only one source of information on maritime security because the information might be either inaccurate, absent or incomplete. Thus, effective MDA involves both the use of AIS and other instruments such as radar, satellite, intelligence and other surveillance systems. Another important aspect of MDA is Radar Surveillance. It includes both coastal and maritime radar systems. These systems detect and track vessels within their operational

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

areas. The radar is especially helpful when vessels operate in the coastal waters and approach the port. In addition, the radar can be helpful in cases when vessels do not provide any reliable identification information. Using both radar information and AIS data, authorities can compare the vessel detected by radar with the identity and whereabouts provided by AIS. Thus, their combination gives a more accurate picture of the maritime situation. Satellite monitoring greatly expands the possibility of states to observe maritime operations in large geographical areas. Satellites give information about the vessels operating far from the coast and it is especially valuable in those areas where the coastal radar coverage is limited. Observation using satellites may be of assistance in watching shipping routes for ships operating in restricted or sensitive areas and abnormal maritime activities. Satellite observation may be of great significance in cases where the jurisdictional area for maritime observation is very big and surveillance equipment used conventionally may not be sufficient for continuous monitoring of the whole area. Coastal surveillance also constitutes an essential component of MDA. Coast States may make use of radars, patrol boats, aircrafts, unmanned vehicles, observation points, among other technologies for monitoring activities that take place in their coastal and territorial waters. Coastal surveillance is particularly significant in relation to the detection of activities such as illegal entry, smuggling, trafficking, illegal fishing, suspicious movement of vessels and other forms of maritime crime. Coastal surveillance also facilitates search and rescue missions and allows for a swift response when there is any danger associated with a particular vessel. Effective MDA requires extensive intelligence sharing since there may be certain information available with different government departments regarding suspects, terrorist groups, trafficking operations, suspicious vessels and persons. For instance, there may be certain information concerning suspecting cargo in the possession of customs, information concerning irregular migrants with immigration authorities, information about organized criminal groups in the possession of police agencies and unusual movements of vessels with maritime authorities. Unless such agencies exchange the relevant information, individual pieces of information may not add up to give the overall picture of the security threat that exists. Sharing of intelligence makes it easier to have a fuller understanding of the security risks in the maritime environment. Port information systems are also important in MDA because of the crucial role that ports play in the interaction between ships and the terrestrial transportation network. Port authorities may have information relating to vessels, cargo, crew members, passengers, arrival and departure

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

times, berth assignments and other related operations. Combining this information with security and law enforcement information can help to detect any suspicious ships, persons or cargo prior to its arrival at the port which will enhance maritime security measures including those provided for by the ISPS Code. Ship reporting system also offers another source of information. Ships are supposed to report their identity, position, route, cargo, among other information under national or international agreements. In this way, reporting helps to keep track of vessels sailing in particular regions. By using such technologies as tracking systems and intelligence, reporting about ships could help authorities identify those vessels which do not report or the reports of which contain false information.

It should also be noted that information provided by shipping companies, ship owners, masters and other parties involved in maritime business could be useful for MDA as well. For example, shipping companies may have information about unusual arrangements regarding carrying of cargo on board, suspicious people who may be on board, changes in plans of voyages or any other situation that might be concealed from authorities. In this case the cooperation between maritime industry and government authorities would result in improvement of general picture of maritime security. This cooperation is especially important in ISPS scheme when security obligations are divided between Governments, companies, ships and port facilities. One of the most important features of Maritime Domain Awareness is cooperation between international and interagency bodies. Maritime threats seldom occur within jurisdiction of one State only. Ships carrying out smuggling, trafficking and other criminal activity may cross jurisdictions of many States visiting many ports before reaching final destination. In this regard the information about vessel or criminal network may be dispersed among different States. Cooperation between neighboring coastal States, regional and international organizations, coast guard services, navy, customs and police agencies and other institutions would help exchange information and identify threats. The importance of Maritime Domain Awareness is especially high in combating human smuggling and human trafficking. Information about movement of the vessels, their unusual routings, repeated visits to remote areas, suspicious ownerships and other criteria could help to detect suspicious vessels. If the information is analyzed in conjunction with migration and law-enforcement intelligence data, it will enable authorities to detect the existence of networks engaged in trafficking or smuggling prior to moving victims. Thus, MDA makes contribution both to maritime security and to protection of vulnerable persons. The third sphere where MDA may

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

be effectively used for prevention purposes is the issue of arms trafficking and other kinds of maritime smuggling. It is possible to analyze movement data of a vessel in connection with cargo information, port information and intelligence reports. Any unexplained deviation from a route, stop at a distant location or any inconsistencies between declared cargo of a vessel and available intelligence should be considered by authorities as a reason for further investigation. MDA itself does not prove commission of any crime; it simply provides authorities with information which is useful for conducting risk assessment and taking necessary actions. With respect to maritime terrorism, MDA provides authorities with the tool for identifying potential threats on the early stages. Monitoring of vessel movements, port activity and intelligence information can help to detect suspicious activities that require increased security measures. In case of a credible threat, authorities can increase monitoring, raise a security level, cooperate with security agencies and take preventive measures. MDA becomes an integral part of preventive security measures provided for in the ISPS Code. MDA is also very much connected with the issues of maritime safety and search-and-rescue operations. Even though Maritime Domain Awareness has primarily security connotations, the same information can be used to detect distressed vessel, identify vessels capable of giving assistance and organize a rescue operation. Information about vessel position, route and speed can be helpful for determining the appropriate response in case of a search-and-rescue operation. Therefore, MDA has contributions to maritime security, maritime safety and humanitarian assistance. Another important aspect of MDA is that it enables authorities to act prophylactically. Under traditional law-enforcement measures authorities usually act after a crime has been committed. Thanks to MDA authorities get the opportunity to detect unusual activities and potential threats on the early stages of their development. For example, the unusual movement of a vessel and intelligence information regarding a criminal organization can be an early sign of some smuggling or trafficking activity. Authorities can increase monitoring or take appropriate investigative measures. However, MDA presents certain difficulties. Maritime information is gathered from an enormous number of sources, and States could be faced with huge amounts of information. However, the question is not only about collecting the information but about its quality and relevance. False information, technical problems, gaps in AIS communications, difficulties in communication and discrepancies in databases can significantly undermine MDA process. There are also problems connected with the issues of cybersecurity, data protection and safe exchange of

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

intelligence information. Therefore, States require a proper technology, trained personnel and specific procedure for analyzing and protecting maritime information. MDA effectiveness is based on the integration rather than independent surveillance system. Only AIS does not give full maritime information, the same way as the radar, satellite imagery or intelligence information do. The main value is given when the information collected from different sources is analyzed jointly. Such analysis gives an overall picture, which allows distinguishing normal maritime activity from the suspicious one. Thus, Maritime Domain Awareness could be called the information and intelligence base of maritime security. MDA allows States and maritime authorities to monitor vessels and maritime activity, to identify possible threats, exchange information, estimate risks and react to them. With the help of the integration of AIS, radar, satellite monitoring, coastal surveillance, port information, ship reporting, intelligence and cooperation with other countries, MDA allows authorities to transfer from purely reactive to proactive and preventive maritime-security system. Regarding the issues of human smuggling, human trafficking, illicit arms trafficking, maritime terrorism and other unlawful activities, the successful MDA could give authorities the information for detecting suspicious activities and preventing them from turning into dangerous threats for ships, ports, people and international maritime trade.

INTERNATIONAL COOPERATION

As the maritime crime often involves cross border issues, international cooperation is absolutely necessary.

States should cooperate:

1. by sharing information
2. through mutual legal assistance
3. by extraditions
4. through joint investigations
5. by maritime patrol cooperation
6. by exchanging intelligence
7. through capacity-building

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

8. through training
9. by port State control
10. by customs cooperation
11. through Interpol and other law-enforcement cooperation
12. by regional maritime-security mechanisms

The SUA Convention itself emphasizes the necessity of international cooperation, requiring States to undertake appropriate actions regarding offenders, such as prosecution or extradition.

MARITIME SECURITY IN INDIA

Due to India's geographical position, maritime security becomes crucial for the country. India has a long coastline, significant commercial ports, offshore operations, as well as strong dependence on sea transportation. India adopts the international maritime-security regime using its legal and administrative institutions. One of the significant developments is Merchant Shipping (Ships and Port Facility Security) Rules, 2024. These Rules have been adopted by the Government of India on 19 June 2024 in accordance with Part IX-B of the Merchant Shipping Act, 1958 and have appointed the Director General of Shipping as the Designated Authority under the ISPS-related framework.

Therefore, the maritime-security regime in India includes interaction between:

- Merchant Shipping legislation;
- ISPS provisions;
- SOLAS provisions;
- port facility security authorities;
- Directorate General of Shipping;
- Indian Coast Guard;
- Indian Navy;
- customs administration;

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

- immigration authorities;
- police;
- intelligence agencies; and
- port authorities.

Such an inter-agency approach is necessary as no one agency has a full control over the maritime area.

CHALLENGES IN MARITIME SECURITY ENFORCEMENT

Despite creation of numerous international conventions, codes, protocols and national regulations concerning maritime security, the implementation of these measures is a serious issue. Maritime security problems become more and more transnational, technologically complex and intertwined. Smuggling, human trafficking, illegal transfer of weapons, terrorism, piracy, ship hijacking, etc. may involve several countries, criminal syndicates and several transportation modes. Effective maritime security, therefore, presupposes not only adoption of international rules, but also their proper implementation through surveillance, investigation, prosecution, international cooperation and protection of vulnerable individuals.

VAST MARITIME AREAS

One of the most important problems in enforcing maritime security regime is the immense geographical scope of the maritime area. Oceans, territorial seas, exclusive economic zones, and international shipping routes comprise enormous areas which cannot be physically observed constantly by any enforcement agency. The coast State might have long coastline and vast maritime zones which should be controlled, while the vessels could navigate hundreds and even thousands of nautical miles from any port or enforcing agency. Constant maritime surveillance is also costly. Effective monitoring involves the use of patrol ships, aircraft, helicopters, satellites, radar equipment, automatic identification systems, communications and human resources. Many Developing States and smaller coastal States lack sufficient resources to provide for complete surveillance systems. Criminal groups can take advantage of areas which have limited or no surveillance. Risk-based surveillance,

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

maritime domain awareness and intelligence sharing become critical tools used to enhance maritime security rather than attempting to physically monitor all parts of the oceans.

JURISDICTIONAL PROBLEMS

The issue of jurisdiction is one of the most complicated issues in the enforcement of maritime security because of the complexity of maritime crimes. A ship can be flagged under one State, owned by a company incorporated in another State, operated by a company in yet another State, transport cargo belonging to people from various countries, and even attacked and intercepted in the waters of yet another State. The perpetrator then flees to another state. The result is that questions may emerge as to which State is the flag State, the coastal State, the port State, State of nationality of the offender, State of nationality of the victim, etc. Such jurisdictional complexities may lead to difficulties in investigating, collecting evidence, making arrests, extradition and prosecution of offenders. Criminal organizations take advantage of such jurisdictional problems by moving from one State to another and using international waters to hinder enforcement of law. The SUA Convention, UNTOC and Protocols seek to minimize jurisdictional gaps through the creation of offences, jurisdictional provisions and procedures for international cooperation. Yet, enforcement of these rules ultimately depends upon the legislative and enforcement abilities of individual States.

IDENTIFICATION OF CRIMINAL NETWORKS

Contemporary maritime crimes involve the use of transnational criminal networks to commit crimes rather than isolated individuals. Human trafficking, migrant smuggling, arms trafficking and other maritime crimes may involve various types of criminals including recruiters, financiers, vessel owners, intermediaries, transporters, corrupt officials and persons responsible for receiving the illegal goods or victims in their destination points. Organized criminal entities may intentionally keep themselves anonymous through use of shell companies, front businesses, false documentation, intermediaries and complex ownership structures. In such a case, a vessel might appear to be owned by a legal entity while in reality, its actual beneficial owner may be hidden behind several corporate structures. Additionally, cargo might be accompanied with legitimate documentation in spite of having a totally different nature. This makes investigation of the crime difficult since authorities have to trace not only the offender but also the whole network behind the offense. For this reason, effective enforcement demands financial investigation, intelligence,

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

examination of business structures, document checking, international information exchange and collaboration between maritime and land law-enforcement agencies.

TECHNOLOGICAL CHALLENGES

Technologies have emerged as a security tool as well as a weakness in the maritime sector. Nowadays shipping relies much on digital tools for navigation, communication, handling of cargo, management of ports, vessel tracking and logistics. While all this has helped to enhance the efficiency and safety of shipping processes, weaknesses in the technologies may be exploited by criminal entities or terrorist organizations. Cybersecurity threat may affect port management systems, databases for cargo, communication networks, navigation systems and other maritime infrastructure. Criminal organizations may take advantage of weaknesses in vessel tracking, documentation and electronic communication systems. On the other hand, authorities may experience problems in maintaining security technologies up to date due to their expensive nature and need for specialized personnel. What is important, solution lies not in introduction of new technologies but rather in proper maintenance, integration and updating of them.

INSIDER THREATS

Insider threat is a situation when an individual with legitimate access to a ship, port, cargo handling facilities or security system intentionally or negligently assists in commissioning of unlawful activity. Potential insiders might be any of the following persons: port staff, shipping company personnel, contractors, security personnel, cargo handlers, maintenance staff and other people with legitimate access to maritime infrastructure. An insider might assist in facilitating criminal activity through providing information about security procedures, allowing unauthorized access to restricted areas, facilitating shipment of banned cargo and helping criminals evade inspection. Because insiders have legitimate access, it becomes more difficult to discover their criminal activities than an offense conducted by an external agent. Maritime security measures need to address this challenge as well.

CORRUPTION

Corruption may undermine even advanced maritime-security systems. The groups engaged in smuggling, trafficking and illegal transport of weapons may try to bribe various government officials such as port authorities, customs, immigration officials or any person capable of

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

assisting illegal activity. Such officials will be able to provide information, grant access, alter documentation, fail to notice suspicious actions or obstruct inspection of cargoes. Thus, physical security will become useless if the persons responsible for enforcing it will be corrupt. Therefore, anti-corruption strategies need to include strict regulations, transparency of procedures, personnel screening, discipline, financial control and independent investigations of corruption. The problem of corruption should become an integral part of national maritime security policy, rather than an additional one.

HUMAN RIGHTS AND HUMANITARIAN CONCERNS

Enforcement of maritime-security policy should take into account human rights and humanitarian considerations. It is especially relevant in case of migrants, refugees, people in distress at sea and victims of human trafficking. For instance, if a ship carries irregular migrants, some of them may actually be victims of trafficking and in danger because of unseaworthiness of the vessel. In such a situation, maritime authorities will have to conduct a search-and-rescue operation and deal with immigration and criminal issues simultaneously. Security measures must not cause any unnecessary harm to people who are vulnerable. Victims of trafficking should not be treated as offenders just because they have entered the state territory in an irregular way or used some illegal means of transportation. It shows that the implementation of maritime security should take place within the framework of international law on human rights, refugee protection and maritime law.

UNEQUAL IMPLEMENTATION OF INTERNATIONAL STANDARDS

Another significant problem is uneven implementation of international standards by different states and ports. International conventions may set up equal obligations for States, but there are large differences between States in terms of financial capacity, technologies, institutional capacity, trained personnel and enforcement capacity. Some major international ports may have advanced security systems, biometrics, scanning of containers, cyber security and specially trained security personnel. Other ports may lack such capacity. Criminal organizations will exploit such differences by choosing routes with weaker security controls. Technical assistance, training and cooperation are needed to reduce such differences. International standards will be effective only when States will have practical capabilities to implement them.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

MEASURES TO STRENGTHEN MARITIME SECURITY

STRENGTHENING ISPS CODE COMPLIANCE

First and foremost, it is necessary to ensure proper implementation of the International Ship and Port Facility Security (ISPS) Code. Compliance should not be confined to creating security documents to comply with regulations. Governments, shipping companies and port facilities should carry out regular security assessment, inspection, audit, exercise and drill. The Ship Security Plan and the Port Facility Security Plan should be reviewed and updated periodically. Security personnel should know their roles and duties and be able to deal effectively with security incidents. Moreover, security levels should be determined taking into account the real threat environment. Hence, proper implementation of the ISPS Code implies constant monitoring.

BETTER INTELLIGENCE SHARING

Sharing intelligence is very important as information on a particular maritime threat can be spread over different authorities or even different countries. Customs authority will have some information on suspicious cargo, immigration authority will have information on irregular migrants, police agency will have information on criminal network, and maritime authority will notice some unusual vessel movements. In case if these authorities work separately, the linkages may go unnoticed. Therefore, developing intelligent information-sharing system and communication procedures can help in detecting threats in time. International cooperation is also very important as criminal networks operate transnational.

USE OF ADVANCED TECHNOLOGY

Advanced technology can greatly enhance the work of maritime security enforcement. The satellite monitoring, AIS, radar, coastal surveillance systems, unmanned systems, biometric identification, container-scanning systems, CCTV, vessel monitoring systems and integrated port information systems will give a better understanding of maritime situation. Technology can help in identifying unusual vessel movements, monitoring restricted zones, identifying unauthorized persons and examining suspicious cargo. Nevertheless, technological systems should be accompanied by adequate cybersecurity measures as digital vulnerabilities can turn into security threat themselves.

TRAINING AND CAPACITY BUILDING

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Training plays an important role in achieving effective maritime security. The seafarers, port officials, customs officers, immigration officials, police officers, coast guards, navy officers and security officials should be given proper training related to the types of threats that they may face. Proper training in the identification of suspicious behavior, trafficking patterns, migrant-smuggling patterns, cargo security, document inspection, emergency response, cybersecurity and ISPS code is important. Moreover, officials should be trained on how to protect the victims of human trafficking and other vulnerable persons. Exercises and simulations are important in this regard as they will help in testing the security plans in case of emergencies.

PROTECTION AND IDENTIFICATION OF VICTIMS

Enforcement of maritime security should have a good focus on the victim protection process. The persons who have been intercepted at sea or during port inspections may be victims of human trafficking and not criminals participating in illegal activities. Thus, there should be procedures established to detect trafficking indicators, separate victims from traffickers, provide medical help and give them protection and legal assistance. The victims should not automatically be assumed to be immigration offenders. It is very important because the victims might not want to share information about themselves due to fear, intimidation, trauma or language problems.

STRENGTHENING ARMS-CONTROL MEASURES

The illicit arms trafficking can be reduced through stronger measures of marking, licensing, records, tracing, customs inspections, exports and international cooperation. The firearms and other weapons should be properly marked to track their origins and movements. The controls should be tightened for the manufacturing, imports, exports, transfer and storage of firearms and ammunition. Risk-based intelligence should also be used by the customs and port officials to detect suspicious shipments of firearms. International cooperation is necessary because the arms shipment could have passed through several countries before reaching its final destination.

STRENGTHENING PORT PERIMETERS AND ACCESS CONTROL

Effective security in ports requires a reliable perimeter protection and access control system. The port administration should define areas where only authorized individuals have access

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

rights. Identification cards, biometric control, surveillance cameras, security services, control and screening systems can limit unauthorized access. Access control should be introduced also on ships. Boarding procedures for ships and controlling visitors can prevent boarding by stowaways, trafficking and other types of security threat. Testing of the security systems on a regular basis is necessary as physical protection system can become ineffective due to damage, aging or insufficient maintenance of equipment.

INTERNATIONAL LEGAL COOPERATION

Without international legal cooperation it is not possible to deal effectively with maritime security threat. States are obliged to implement efficiently the international instruments, such as the SUA Convention and its Protocols, UNTOC and its Protocols, SOLAS Chapter XI-2 and ISPS Code, together with other relevant international instruments concerning maritime security and criminal law. Cooperation may include, inter alia, extradition, mutual legal assistance, joint investigations, exchange of information and evidence, coordination of maritime operations and cooperation of law enforcement agencies. It decreases the probability of using discrepancies of legal systems by criminals.

WHOLE-OF-GOVERNMENT APPROACH

Maritime security must not be considered as the competence of the navy or the coast guard only. Contemporary maritime security challenges are multidimensional and thus cooperation among civilian and military authorities is required. Port administrations, customs, immigration services, police, intelligence agencies, coast guards, navies, shipowners and maritime administrations are obliged to work through mechanisms of coordination. Each of the agencies has some specific information, powers and capacities. Combining them increases the effectiveness of the system for maritime security. It is thus important to use the whole-of-government approach and multi-agency cooperation.

IMPORTANT INTERNATIONAL LEGAL INSTRUMENTS

The international legal framework for maritime security is constituted by several conventions, protocols and codes. No international instrument covers all the maritime security threats. On the contrary, different instruments cover different aspects of security, criminality, shipping safety, organized crime, trafficking and arms control. SOLAS 1974 – CHAPTER XI-2. The International Convention for the Safety of Life at Sea, 1974 (SOLAS) is one of the key

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

international maritime conventions. While SOLAS focuses on the safety of ships and persons at sea, its Chapter XI-2, "Special Measures to Enhance Maritime Security," addresses the issue of maritime security. Chapter XI-2 sets out the legal basis for the ISPS Code. It provides for special security measures applicable to ships and port facilities falling within its scope and includes requirements concerning security levels, ship security alert systems and governmental duties. The incorporation of maritime security into SOLAS shows how close the issues of safety and security are in contemporary shipping.

INTERNATIONAL SHIP AND PORT FACILITY SECURITY (ISPS) CODE

The ISPS Code is the key international instrument concerning security of ships and port facilities. It was adopted in 2002 and came into force on 1 July 2004 under the SOLAS Chapter XI-2 framework. The Code provides for a risk-based security system encompassing Ship Security Assessment, Ship Security Plan, Port Facility Security Assessment, Port Facility Security Plan and security officers. It also sets out three security levels: normal, heightened and exceptional. Part A of the Code contains mandatory provisions, while Part B provides guidance for its implementation. The ISPS Code is primarily preventive in nature and seeks to identify vulnerabilities and introduce measures before any security incidents take place.

*Essar Bulk Terminal Ltd. v. ArcelorMittal Nippon Steel India Ltd*²⁶

This is the most relevant Indian case on the issue of ISPS port security. In this case the AMNS Jetties were ISPS-certified by the Directorate General of Shipping. Under the Port Facility Security Plan the access to the ISPS area had to be controlled. Petitioner complained that some unauthorized persons were allowed to enter the port facility. The court examined the relationship between ISPS compliance, port security, statutory duties and national security. The case is important as it demonstrated that ISPS compliance entails statutory security obligations, rather than an ordinary commercial contract between the parties. The Port Facility Security Plan was considered security sensitive due to its connection to port and national security.

Principle: ISPS compliance and control of access to ISPS area have statutory and national-security dimension.

²⁶Gujarat High Court, 18 October 2021

*Vardhman Shipping Inc. v. Mercantile Marine Department*²⁷,

In this case there were foreign flagged vessels and the decision taken by the Directorate General of Shipping, Mercantile Marine Department and Port State Control. Reference was made to the SOLAS and the ISPS Code as well as the procedures of Port State Control. A decision was taken to expel the vessels based on security considerations. This case shows how Port State Control, maritime safety and security, DG Shipping and regulatory action can be taken against vessels. It will be very helpful for showing that maritime security law enforcement does not only involve criminal prosecutions but administrative and regulatory actions including inspection, detention and expulsion may be taken when there is a problem with the vessel.

Principle: Port State Control and maritime administrations may take regulatory action against vessels based on security and compliance issues.

*Vizhinjam Steamer Agents Association v. Union of India, Kerala High Court*²⁸

This is a very useful recent authority on maritime security in Kerala. In this case the issue was about crew change and bunkering activities at Vizhinjam port and infrastructure that must exist at the port as per ISPS Code. The record showed that until the relevant certification in June 2023, the port lacked the necessary infrastructure or facilities under ISPS Code. It also addressed the security risks of allowing crew changes from unscheduled vessels at outer anchorage. The case can be linked with risks of unauthorized entry into ships, immigration violations, trafficking and smuggling and lack of port security controls.

Principle: ISPS infrastructure and crew change procedure are important aspects of maritime and port security.

SUA CONVENTION 1988

Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988 is often known as SUA Convention. It is one of the important international criminal law instruments for dealing with unlawful acts against ships. It provides provisions on very

²⁷Kerala High Court, 11 November 2020

²⁸19 May 2025

serious offences like unlawful seizure of ships, violence to any person on board the ship, acts of destruction or damage to the ships or placing of destructive devices or substances aboard ships which pose a risk to safety of maritime navigation. The Convention is important in this context because it attempts to ensure that no serious offender goes scot free by changing jurisdictions.

2005 SUA PROTOCOL

The 2005 Protocol to the SUA Convention enhanced the original SUA Convention by broadening the scope of conduct that could be an international maritime offence. This protocol also tackles more serious threats, which include, but are not limited to, certain uses of explosives, radioactive, biological, chemical, and nuclear materials and acts associated with terrorism. The 2005 SUA Protocol has been crafted in recognition of evolving maritime security threats since the adoption of the original SUA Convention. The protocol, thus, enhances the international legal regime on maritime security threats including terrorism and unlawful acts involving ships.

UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME (UNTOC), 2000

The United Nations Convention against Transnational Organized Crime (UNTOC) establishes an international framework for combating organized criminal activities across international borders. The convention promotes international cooperation in extradition, mutual legal assistance, law-enforcement cooperation and the criminalization of participation in organized criminal groups. The importance of UNTOC in maritime security is due to the fact that many maritime threats including human smuggling, trafficking and arms trafficking involve transnational organized criminal networks. In this regard, UNTOC lays down a criminal-law framework which complements the specialized maritime security instruments.

TRAFFICKING IN PERSONS PROTOCOL, 2000

The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children, supplementing UNTOC is the key international instrument dealing with human trafficking. It establishes a comprehensive international framework for the prevention, prosecution and protection of victims of human trafficking. Human trafficking is recognized under this protocol as an act that involves the recruitment, transportation, transfer, harbouring

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

or reception of persons through specified coercive, deceptive or abusive means for the purpose of exploitation. This protocol is highly relevant to maritime security due to the fact that trafficking networks can use shipping services, ports and fishing vessels to traffic victims.

SMUGGLING OF MIGRANTS PROTOCOL, 2000

The Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing UNTOC sets up an international framework for the prevention and combating of the smuggling of migrants. This protocol is highly relevant to maritime security due to the fact that the protocol specifically addresses the issue of maritime migrant smuggling.

UN FIREARMS PROTOCOL, 2001

The Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition, supplementing UNTOC, outlines an international framework for combating illicit firearms trafficking. Measures such as criminalization, licensing, marking, record keeping and tracing have been promoted. Such measures are especially significant for maritime transport since the illicit firearms could be hidden in cargo and moved from one port to another. Thus, the Protocol assists maritime port-security measures by tackling the criminal supply chain in the context of illicit weapons trafficking.

ARMS TRADE TREATY, 2013

The Arms Trade Treaty (ATT) sets out common international standards for the international transfer of conventional arms. The general purpose of the ATT is to decrease the probability that international arms transfer will pose a threat, cause the risk of illicit trafficking or result in international insecurity. While the ATT is not strictly speaking a maritime instrument, it is of relevance to maritime security, since a considerable amount of international arms trade may be conducted via maritime transport and ports. The implementation of proper export controls and international arms-transfer procedures helps prevent weapons' diversion to illicit channels.

STCW CONVENTION

The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978 (STCW Convention) sets international standards with regard to the training,

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

certification and watchkeeping of seafarers. The STCW Convention and its requirements are of relevance to maritime security, as well-trained seafarers are better prepared to recognize security threats. Security training enables the crew members to know the procedures related to unauthorized access, suspicious activities, emergency situations and other maritime security threats.

RELATIONSHIP AMONG THE MAJOR INSTRUMENTS

These international instruments should not be considered as separate or competing legal regimes. Rather, they should be regarded as complementary components of the maritime security regime. The relationship may be described in the following way:

- SOLAS Chapter XI-2 forms the treaty-based maritime security framework.
- ISPS Code sets out detailed preventive security measures for ships and port facilities.
- SUA Convention sets out an international framework for criminal law in respect of acts of unlawful interference with maritime navigation.
- 2005 SUA Protocol extends the SUA framework to cover other serious acts of terrorism and security-related conduct.
- UNTOC provides the general framework for countering transnational organized crime.
- Trafficking in Persons Protocol specifically addresses human trafficking.

Smuggling of Migrants Protocol specifically addresses migrant smuggling, including sea-based migrant smuggling.

- UN Firearms Protocol addresses illicit manufacturing and trafficking of firearms.

Arms Trade Treaty regulates the international trade in conventional arms.

- STCW Convention provides the international standards for training and qualifications of seafarers, including security training.

Combined, these instruments establish a multi-layered system of maritime security, where prevention, criminalization, investigation, prosecution, international cooperation, training and victim protection are interlinked.

CONCLUSION

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Although there is an elaborate international legal framework of maritime security, there are still challenges in enforcing it. Large oceanic spaces, complicated jurisdiction, high levels of sophistication of transnational criminal groups, technological vulnerability, insider threat, corruption, humanitarian considerations, as well as uneven implementation of international standards may hamper the success of maritime security efforts. There is a need for a holistic approach to maritime security. Improving compliance with ISPS Code, maritime domain awareness, intelligence sharing, technology surveillance, personnel training, victim protection, arms control measures, port security and cooperation in international law is required. In addition, a whole-of-government approach to maritime security is also required, where naval, coast guard, customs, immigration, police, intelligence, port and maritime administration officials will have to cooperate. International legal framework provides the basis for such approach. SOLAS Chapter XI-2 and the ISPS Code mostly provide preventive measures concerning ships and port facilities, SUA Convention and its 2005 Protocol provide means for suppressing acts of unlawful interference with maritime navigation. UNTOC and its Protocols deal with transnational organized crime, human trafficking, migrant smuggling and illicit firearms trafficking, while the Arms Trade Treaty and STCW Convention help with arms control and maritime personnel competence.

In conclusion, an effective system of maritime security will be impossible to create based only on one particular convention, institution, or technology. It will require permanent risk assessment, implementation of international laws, strong national institutions, technological capacities, well-trained personal, international collaboration, and respect for human rights. The main goal is to create a situation in the maritime area where ships and ports will be protected and secure and international trade will be able to continue without any terrorist, trafficker, smuggler or any other organized criminal activity. International Ship and Port Facility Security Code is an essential development in the area of maritime law and maritime security. Adopted in December 2002 following post-9/11 security concerns and brought into force on 1 July 2004, it created an effective and mandatory security regime via SOLAS Chapter XI-2. One of its key features is the separation between Part A and Part B. Part A includes mandatory provisions, and Part B – guidance on implementation of the provisions included in Part A. International Ship and Port Facility Security Code is based on a risk management approach, requiring threat assessment before implementing corresponding protective measures. It determines the responsibilities of the Government, shipping company,

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

ship and port facility and introduces such important mechanisms as Ship Security Assessment, Ship Security Plan, Port Facility Security Assessment, Port Facility Security Plan, Company Security Officer, Ship Security Officer, Port Facility Security Officer and three security levels. So, International Ship and Port Facility Security Code can be called the main international preventive tool for protecting ships and port facilities from maritime security threats. It doesn't replace the criminal law tools such as SUA Convention, it complements them trying to prevent security incidents. Maritime security has come a long way since it was confined to such issues as piracy and armed attacks. Today it is a highly multi-faceted area covering terrorism, human smuggling, human trafficking, illicit arms trafficking, unlawful taking of ships, sabotage, stowaways, organized crime etc. Human smuggling poses a threat to the security of borders and maritime transportation, human trafficking is a grave violation of human dignity accompanied by exploitation and organized crime. Illicit arms trafficking strengthens organized crime and terrorism and leads to destabilization of situation. Maritime terrorism and other unlawful acts pose threats to human lives, to ships and infrastructure, to the international trade, to environment and economy. All these problems have been addressed by means of the combination of maritime law, international criminal law, port security standards and law enforcement cooperation. The ISPS code, implemented via SOLAS Chapter XI-2, is a basic preventive security code regulating international ships and port facilities. It provides for risk assessment, security plans, designated security officers, information exchange, and different security levels. SUA Convention and its Protocol of 2005 supplement the above-mentioned preventive measures by creating the international legal framework for suppression and prosecution of serious unlawful acts against ships. Thus, to ensure maritime security, it is not enough to provide only physical security of ships and ports. It is necessary to assess risks, apply intelligence-led enforcement, possess technology, competent people, adequate national legislation, cooperate internationally and respect human rights. Since maritime threats today are inter-connected and transnational, States need to adopt an integrated maritime security strategy able to combat crime, terrorism, trafficking and unlawful acts and at the same time preserve the safety and security of international shipping. Thus, maritime security aims at protecting not ships and ports but the whole system of maritime transport and maritime law. This means that both the Indian and international regimes governing maritime security can be viewed as having a hierarchical approach. At the international level, UNCLOS provides the general law

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

of the sea regime; SOLAS Chapter XI-2 and the ISPS Code provide the preventive regime for ship and port security; SUA Convention provides the regime covering any unlawful act against maritime navigation; UNTOC and its Protocols provide the regime dealing with organized crime, trafficking, migrant smuggling and firearms trafficking; and other international instruments govern specific aspects of maritime security and safety. At the national level, all these obligations have been domesticated in the Merchant Shipping Act, 2025, Coast Guard Act, Arms Act, UAPA, Anti-Hijacking Act, maritime unlawful acts regime, Maritime Anti-Piracy Act, immigration and customs regimes as well as other relevant criminal statutes. The Merchant Shipping Act, 2025 is especially important because it is the current Merchant Shipping Act of India and has an explicit safety and security regime. Clearly, this does not only involve arresting a suspect or seizing the offending ship. An investigation into a maritime security incident is more than that. Such an investigation should identify the offense, the perpetrators of the offense, the offending vessel, the offending cargo, the criminal network involved, the financial beneficiaries, the jurisdictional basis of the offense and any international connections.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>