FROM POLICY TO PRACTICE: ADDRESSING IMPLEMENTATION CHALLENGES IN THE ISPS CODE TO ADVANCE SDG 8

Mutiat M. Abdulsalam*

Abstract

The International Ship and Port Facility Security (ISPS) Code, adopted under the auspices of the International Maritime Organization, represents a critical framework for safeguarding maritime facilities and operations from security threats. Beyond its security mandate, the effective operationalisation of the ISPS Code holds significant potential for advancing Sustainable Development Goal 8 (SDG 8) promoting sustained, inclusive, and sustainable economic growth, full and productive employment, and decent work for all. This paper critically examines the extent to which Nigeria has operationalised the ISPS Code and identifies persistent implementation gaps undermining its efficacy. Drawing on legal analysis, policy review, and empirical findings from relevant maritime stakeholders, the study interrogates structural, institutional, and capacity-related challenges, including inadequate funding, limited technical expertise, weak enforcement mechanisms, and inter-agency coordination deficits. The analysis further explores the socio-economic implications of these shortcomings for the maritime workforce and broader economic productivity. The paper argues that closing these implementation gaps is imperative not only for enhancing maritime security but also for creating a safe, enabling, and productive work environment within the maritime sector. In conclusion, it offers policy recommendations for strengthening regulatory frameworks, capacity building, and stakeholder collaboration to align Nigeria's ISPS Code implementation with the objectives of SDG 8.

Keywords: ISPS Code, maritime security, implementation gaps, SDG 8, decent work, economic growth.

1. Introduction

Maritime security has emerged as a cornerstone of global economic stability and sustainable development. In recognition of the growing threats to international shipping and port operations, the International Maritime Organization (IMO) introduced the International Ship and Port Facility Security (ISPS) Code in 2004 as part of the amendments to the Safety of Life at Sea (SOLAS) Convention.

[1] The Code provides a comprehensive framework for preventing and responding to security risks that could disrupt maritime trade and endanger lives, property, and the marine environment. This was necessitated in the wake of the terrorist attack on the United States of America (USA) on September 11, 2001 and the possibility of similar attacks in the maritime domain.

The Code promotes cooperation between government agencies, shipping companies, and port administration in identifying security threats and preventing security incidents that may affect ships or port facilities. It introduces effective preventive and deterrence measures against terrorism, within the maritime domain, in all its forms and plays a significant role in enhancing maritime and ensuring the efficiency of international maritime transport.[2] The ISPS Code creates a unified legal instrument under the auspices of the IMO, to facilitate cooperation between the SOLAS contracting port states and the shipping industry to address the problem of port security as a sub-set of maritime security. The measures in the Code require security adjustments to be made by the parties and this could go a long way to enhance international trade. The ISPS Code applies to ships on international trips (including passenger ships, cargo ships of 500 gross tons or more, and mobile offshore drilling rigs), as well as port facilities that serve such ships.[3]

---

*Ph.D. Department of International Law, Obafemi Awolowo University. mmabdulsalam@oauife.edu.ng

[1] International Maritime Organization (IMO), International Ship and Port Facility Security (ISPS) Code, adopted 12 December 2002, entered into force 1 July 2004, IMO Doc. SOLAS/CONF.5/34.

[2] TA Mensah, 'The Place of the ISPS Code in the Legal International Regime for the Security of International Shipping' [2004] (3) *World Maritime University Journal of Maritime Affairs* 17.

[3] ISPS Regulation, para. A/3.1.

Beyond its security-oriented purpose, the ISPS Code also plays a crucial role in fostering economic resilience and productivity, particularly in maritime-dependent economies such as Nigeria.[4] Nigeria's maritime sector, which contributes significantly to national revenue through international trade and port operations, remains central to the realisation of Sustainable Development in the country. Ensuring that the maritime sector is run as a decent work environment, with the aim of realising SDG 8, is also connected to the promotion of sustained and inclusive economic growth.[5] Yet, the effectiveness of the ISPS Code's implementation in Nigeria has been met by several constraint.[6]

This paper therefore interrogates the extent of Nigeria's compliance with and operationalisation of the ISPS Code. It situates the discussion within the broader context of maritime governance and sustainable development, examining how lapses in implementation impede economic efficiency, employment generation, and decent working conditions in the maritime industry. Through a critical analysis of legal and policy frameworks, stakeholder engagement, and empirical observations, the study highlights the nexus between maritime security and economic growth. Ultimately, it argues that bridging these implementation gaps is vital not only for strengthening maritime security but also for advancing SDG 8 and achieving Nigeria's long-term development objectives.

2. Examination of the Extent of Implementation of the ISPS Regulation Code

Since the Passage of the ISPS Code Implementation Regulations in 2014, Nigeria has continued to take steps towards the implementation of the ISPS Code, to enhance the state of the ship and port security which directly influences the decent maritime work environment. NIMASA was designated as the DA for implementing the ISPS Code in 2013, replacing and taking over the responsibilities of the Presidential Implementation Committee on Maritime Safety & Security (PICOMSS). NIMASA guided the drafting of

---

[4] International Maritime Organization, SOLAS Consolidated Edition 2020 (IMO Publishing 2020).
[5] United Nations, *Transforming our World: The 2030 Agenda for Sustainable Development* (UNGA Res 70/1, 25 September 2015) Goal 8.
[6] Nigerian Maritime Administration and Safety Agency (NIMASA), *ISPS Code Implementation Guidelines in Nigeria* (NIMASA, 2021).

the ISPS Regulation with the assistance of the Ministry of Transport and the Ministry of Justice. A substantial part of the Regulation is implemented through physical inspection. As a result, the appointment of the Lead RSO and other RSOs was a necessary step needed to fill the capacity gap in the physical assessment of port facilities. Actions like the Verification Inspection Exercise (VIE), and inspection of certification documents became possible under the authority of the DA. Based on the power granted in the Regulation, as far back as 2018, NIMASA sealed off erring jetties for failure to comply with the provisions of the ISPS Regulation, which affected Heyden Petroleum Jetty, Index Petroleum Oil Jetty, Waziri Jetty operated by Hemsmor Nigeria Limited, NIPCO in Lagos, while the Pinnacle Oil and Gas Petroleum, Warri.[7] In 2018, the United States Coast Guard (USCG) expressed satisfaction bout the extent of implementation of the ISPS Code at the Nigerian ports, as the nation was said to have achieved 90% compliance. Unfortunately, in 2019, there was a relapse, as a result of which the country was sanctioned, including the imposition of conditions to be met before port entry can be granted to ships that have visited some port terminals in Nigeria in the course of their last five port calls.[8] It was presumed that the Nigerian ports were not in compliance with port security measures as a result the measures were aimed at protecting the US ports from security risks that may be posed by ships from Nigeria, including the risk of port terrorism.

So far, it has been nine years since the enactment and implementation of the ISPS Code Regulation in Nigeria, yet safety and security issues are persistent. In an interview with The President of the Maritime Security Providers Association of Nigeria (MASPAN), Emmanuel Maiguwa, he identified some major challenges undermining the efficiency of the ISPS Code Regulation. According to him, several ports are at security level one, this being the lowest level of security creates an avenue for the perpetration of maritime crimes including the trafficking of hard drugs routed through Brazil, which also creates an avenue for the problem of stowaways. Another major security challenge is the inflow

---

[7] 'NIMASA seals off erring jetties over non-implementation of ISPS code' *Blue Print* (Lagos, 27 July 2018) https://blueprint.ng/nimasa-seals-off-erring-jetties-non-implementation-isps-code/
[8] 'ISPS Code implementation and US sanctions on Nigeria' *Ships & Ports*, (Lagos 15th April 2019) https://shipsandports.com.ng/isps-code-implementation-and-us-sanctions-on-nigeria/

of dangerous drugs often discovered during Customs examinations. This speaks to the inadequacy of the system of cargo checks which may also be traced to the inadequate implementation of the International Cargo Tracking Note (ICTN). Other challenges that were identified include the smuggling of narcotics and fake products, trafficking of firearms, and dumping of contraband. [9]

Earlier in the year 2024, the United States Coast Guard (USCG) evaluated the level of implementation of the ISPS Code and reached an agreement with NIMASA. They decided to work on a three-year plan that would involve a bi-annual assessment of the level of compliance with the implementation of the ISPS Code at Nigerian ports, under the supervision of NIMASA. The agency has collaborated with relevant stakeholders over the years to achieve its mandate, and the United States Coast Guard has provided the necessary support and assistance to achieve safer and more secure waterways in Nigeria and the Gulf of Guinea.[10]

3. The State of Ship and Port Security in Nigeria Today

The ISPS Code supports major improvements to the operation of ship and port security. The Code though not expressly mandatory, and without the actual specification of security-related offenses and punishment thereof. However, it set out measures for preventing and responding to maritime security issues at the ports and its adoption is mandatory for state parties to the SOLAS convention. Thus, the ISPS Code leaves much to be done by the state parties in the course of domestication and implementation. An analysis of the ISPS Code shows that the implementation of the security measures prescribed therein would be sufficient to guard against common security threats. Unfortunately, Nigerian ports are still confronted with numerous security incidents, including stowaway problems, smuggling of drugs and weapons, and illegal migration, all pointing to inadequate implementation of the provisions of the code.

---

[9] Adaku Onyenucheya, 'Nine years after ISPS domestication, maritime insecurity persists' *The Guardian* (Lagos, 27 September 2023) https://guardian.ng/business-services/maritime/nine-years-after-isps-domestication-maritime-insecurity-persists/
[10] Amaka Anagor-Ewuzie, 'US moves to remove condition of entry on American-bound vessels from Nigeria *Businessday* (Lagos, 10 February 2024).

Since Nigeria domesticated the ISPS Code in 2014, Ship and port security incidents have been through an undulating curve, from the period of high occurrence during which the Nigerian waters were considered a hot spot for maritime insecurity, through a steep reduction in attacks and the current reemergence of various security threats at the port and onboard vessels within the Nigerian maritime domain. By 2018, the frequency of security breaches at the Nigerian ports led stakeholders to point an accusing finger of indifference towards port security, at the Nigerian Ports Authority (NPA). This followed a series of attacks on several ships at the port including MV Pamyat; MV Asia Ruby, MV Aquata, MT Sichem New York, MV Kiana, and MV Dino. Bandits mounted and attacked MV Pamyat on the 2nd of March 2018, while the ship was berthed at berth 14 of the Lagos Port Complex (LPC) Apapa. The attackers were armed robbers who simply stole 11 buckets of paint from the ship. The attack on MV Ruby occurred on the 24th of April, at berth 8 of the LPC, while the ship was discharging cargoes. The robbers carted away several of the goods from the ship, without being cautioned by security operatives. Similarly, on the 3rd of March 2018, at the Tin Can Island Port Complex (TCIPC), also in Lagos, MV Aquata and MT Sichem New York were attacked at berths 2 and 1 of the port, while discharging cargo. The robbers approached the waterfront, in an outboard engine boat, three of them gained access onboard and severely injured the armed watchman onboard in the course of making their escape. Sea robbers also attacked MV Kiana on the 22nd of March 2018, while the ship was discharging its cargo of bulk sugar belonging to the Bua Refinery. [11]

This disturbing pattern continued in 2019, in that year, the IMB reported that Nigeria recorded the highest incidents of port security attacks across the country, with about 11 reported cases of actual armed robbery by the third quarter of that year. On the 24th of March 2019, an anchored oil tanker secured at the anchorage in the Lagos Port was boarded by two armed robbers who succeeded in stealing oil cargo from the ship using hose pipes. Also, on the 25th of July 2019, 10 armed robbers attacked and stole the ship's store of a berthed ship from the pain locker, while cargo operation was ongoing. At Onne,

---

[11] Shulammite Foyeku, 'Security breaches rock Nigerian ports; stakeholders accuse NPA of indifference' (*Ships & Ports* (Lagos, May 8, 2018) https://shipsandports.com.ng/security-breaches-rock-nigerian-ports-stakeholders-accuse-npa-indifference/

on the 14th of August 2019, a berthed offshore supply vessel was attacked by two armed robbers who carted away properties from the ship's pump room.[12] In 2020, there was a slight reduction in the incidents of armed robbery within the Nigerian ports as the country recorded 46 cases by the third quarter of the year. There was a further reduction in 2021 as the country recorded 27 incidents of armed robbery against vessels at port anchorages.[13] Although this is said to be a drastic reduction compared to the previous years, the aim of enhancing the security of the maritime work environment is far from being achieved.

In March 2022, members of the Maritime Workers Union of Nigeria (MWUN) protested against the escalating security threats at the ports and on private jetties across the country, traced to the inadequacy of ship and port security, which made the maritime space porous and opened to large shipment of illicit drugs, arms, and ammunition.[14] Likewise, there is a report of a rise in insecurity within the GoG in 2023 and this extended to incidents of armed robbery at the Nigerian ports. According to the IMB, there has been a series of incidents of armed robbery at various ports in West Africa, including Nigeria. The first nine months of 2023 recorded 21 cases, compared to 14 cases recorded within the same duration in 2022. Out of those 21 incidents of attacks, 17 were armed robberies and only four were piracy.[15] One such incident is the illegal boarding of a Liberia-flagged cargo ship MSC Wave F, on the 28th of April 2023. The ship was illegally boarded by 8 armed robbers while being berthed at the Tin Can Island Terminal, but when the security crew were alerted, the robbers took to their heels.[16]

---

[12] Caroline Tokulah-Oshoma, 'Piracy, armed robbery in Gulf of Guinea and other Maritime Offences Act 2019' *The Guardian* (Lagos, 18th February 2020) https://guardian.ng/features/piracy-armed-robbery-in-gulf-of-guinea-and-other-maritime-offences-act-2019/

[13] 'Nigeria marks 27 attacks on ships at port anchorage' (Safety4sea editorial team, December 21, 2021) https://safety4sea.com/nigeria-marks-27-attacks-on-ships-at-port-anchorage/

[14] Victor Ahiuma-Young,' Workers raise alarm over security threats at nation's ports' *Vanguard* (Lagos31 March 2022) https://www.vanguardngr.com/2022/03/workers-raise-alarm-over-security-threats-at-nations-ports/

[15] 'IMB confirms rise in Gulf of Guinea piracy' *Ships&Ports*, (Lagos, October 12 2023) https://shipsandports.com.ng/imb-confirms-rise-in-gulf-of-guinea-piracy/

[16] 'Maritime Threats in the Gulf of Guinea – An Update' (ARETE 2nd June 2023) https://areteafrica.com/2023/06/02/maritime-threats-in-the-gulf-of-guinea-an-update/

4. Efforts Made to Enforce the ISPS Regulation

Since the domestication of the ISPS Code in 2018, certain further efforts have been made to implement the provisions of the ISPS Code regulation in Nigeria. These efforts are however interconnected with maritime safety and security initiatives, since ship and port security are indeed aspects of maritime security. The efforts will be discussed below.

4.1 Nigerian Ports, Port Infrastructure and ISPS Implementation

As of 2023, Nigeria has six major seaports, including the Tin Can, Lekki Deep Sea Port, and Apapa Quays in Lagos, Onne and Port Harcourt ports in Rivers state, Warri Port, and Calabar Port. The Apapa Quays, established in 1913, has since been the major seaport in Nigeria. The port is accessible to all for use for all forms transportation and is often utilised for heavy cargo conveyances. The Tin Can Port, located 7km Northwest of Apapa Quays, is a derivate of the merger of Roro and Tin Can Island Port, it is the second largest port in Nigeria, engaged in facilitating international shipping. The Lekki Deep Sea Port was recently concluded in 2022 for facilitating shipping in the Lekki Free Trade Zone. The Lekki Deep Sea Port is however the largest seaport in Nigeria and one of the largest in Africa, with a depth that doubles that of the Apapa Port and the capacity to take 2.5 million TEUs. The Onne Port is an oil and gas-free zone, one of the largest of such across the globe, built to facilitate production and operations in Nigeria's oil sector. The Port Harcourt Port is another port built to facilitate Nigeria's oil business. The port, with a quay length of 1259 meters, is sighted in the Niger Delta, and built with 16 mass storage, with a capacity of 3,048 tonnes. The port is known for serving pilotage and towage services. The Calabar Port Complex was built nine years after Nigeria gained independence, as a trade center to service the Eastern and Northern regions of the country as well as facilitate international trade, as a transshipment port for oil products from Calabar and Akwa Ibom. The Warri Port was specifically built to aid the shipment of cargo to Anambra, Imo, Edo, Delta, and any other part of the country. It supports swift cargo and documentation clearance. A general assessment of the ports shows that the Tin

Can Island Port and Apapa Port jointly handle 70% of imports in the country, while the Onne Port handles 80% of crude oil exports in the country.[17]

As far as the implement the ISPS Code is concerned, the government has continued to make efforts by putting in place both soft and hard infrastructure. Some of these include the passage into law of the Suppression of Piracy and Other Maritime Offences (SPOMO) Act 2019 for the punishment of piracy, armed robbery, and other maritime crimes, the launching of the Integrated National Security and Waterways Protection Infrastructure, otherwise called the Deep Blue Project (DBP), and the erection of a concrete fence and the installation of an automated access control gate at the Tin Can Island ports.[18] Another such development is the introduction of Electronic Cargo Tracking Notes across all the Ports, this will make information about the cargo and their content easily accessible.[19] It will enhance the flow of inbound outbound vessel flow and create space for docking and equipment unloading. The various efforts made have driven some results as reports have shown a drop in the cases of armed robbery at the Nigerian ports. For instance, Nigeria recorded 31 cases of piracy and armed robbery in 2018 and 21 cases in 2019, out of which were 17 cases of armed robbery and 4 cases of piracy.[20] However, there is still a lot to be done to see to the full implementation of the ISPS Code, to have the desired state of security necessary to create a decent port work environment.

In terms of security equipment, in May 2022, the Nigerian Navy (NN) took delivery of a new landing ship transportation called NNS KADA, which is 100 meters in length. It is a tool for non-kinetic operation and for delivering humanitarian services, peace enforcement and carrying military hardware to neighboring states. Furthermore, the NN has facilitated the construction of offshore patrol vessels, fast attack crafts, and steward

---

[17] Ovuokeroye Edih *et al,* 'The effect of optimal port operations on global maritime transportation: a study of selected ports in Nigeria'[2022] (2) (2) *Journal of Money and Business* 172-186.

[18] Anozie Egole, 'NPA boosts TinCan ports security' *Punch Newspaper* (Lagos, 9th March 2023) https://punchng.com/npa-boosts-tincan-ports-security/

[19] Anozie Egole, 'Truckers divided over NPA's electronic call-up system' *Punch Newspaper*, (Lagos, 26 October 2023). https://punchng.com/truckers-divided-over-npas-electronic-call-up-system/?utm_source=auto-read-also&utm_medium=web

[20] Kunle Sanni, 'Nigeria records drop in sea robberies, piracy attacks – Report' *Premium Times* (Nigeria, 21 July, 2022) https://www.premiumtimesng.com/news/top-news/544222-nigeria-records-drop-in-sea-robberies-piracy-attacks-report.html?tztc=1

boats to promote maritime security. Some of these vessels have already been received. A Respondent interviewed at the Nigerian Navy disclosed that in March 2023 that two High-Endurance Offshore Patrol Vessels (HE-OPV) have been received from Dearsan Shipyard, Turkey, to boost maritime security. This is in line with the objective of fleet renewal policy aimed at developing a system capable of sustaining effective and round-the-clock presence in the exclusive economic zones. He noted that the naval shipyard was also constructing 20 houseboats for operations in the brown water.

The NN has also recently acquired new combat helicopters and strategic military drones under its short, medium, and long-term fleet renewal plans. In February, the navy received two helicopters (document number 1), and several other platforms, including two 38m fast patrol craft, another 409m fast patrol boat, and three 46m fast patrol boats, are currently under construction or expected to launch soon. The long-term plan includes the delivery of the high endurance offshore patrol of 76m and 20 houseboats under construction by the Naval Shipyard Limited. Additionally, the Navy War College's curriculum is being improved to keep up with the evolving maritime environment. The Naval Warfare Course 8 has 24 participants, including 17 naval officers and two officers each from the air force and army.[21] Maritime domain awareness activities like the Falcon Eye have been useful in detecting illegal activities. For instance, the detection of vessels loading LNG without necessary documentation and approvals from relevant authorities. Eg The arrest of Very Large Crude Carrier (VLCC), MT Heroic Idun 26 Indian, Pilipino, Sri Lankan and Polish nationals in August 2022. Though some of these vessels were later released.[22]

4.2   Enactment of the Suppression of Piracy and Other Maritime Offences (SPOMO) Act. 2019

To combat piracy and other maritime crimes, Nigeria passed into law the Suppression of Piracy and Other Maritime Offences Act, 2019 (POMO Act). The law aims to tackle

[21] 'Naval War College Graduates 30 In Course 9 In Calabar' (TVC News, 12th September, 2025) https://www.tvcnews.tv/naval-war-college-graduates-30-in-course-9-in-cal/ accessed 30th September 2025.
[22] Tola Adenubi, 'Nigerian Navy releases Norwegian vessel convicted of oil theft' (Tribune Online, 1st June, 2023) https://tribuneonlineng.com/nigerian-navy-releases-norwegian-vessel-convicted-of-oil-theft/

piracy, armed robbery, and all forms of illegal activities against ships and maritime infrastructure including fixed and floating platforms. The Act also gives legal effect to UNCLOS and SUA Convention. It expressly recognizes that illegal activities can be committed against ships, aircraft, fixed or floating platforms, persons, or cargo onboard. This by implication spread to the scope of the ISPS Code.[23] Interestingly, SPOMO like the ISPS Code designates NIMASA as the agency of government responsible for coordinating other law enforcement agencies towards realizing its implementation.[24] To avoid the hindrance that may be caused by the lack of access to funding, the act set aside the Piracy and Maritime Offences Fund" (the "Fund") to be used for financing its implementation.[25]

Whereas the SPOMO is a welcomed development, it does have certain limitations capable of inhibiting its effectiveness. These limitations include the failure to coordinate anti-piracy efforts in the regional arena and the omission of giving a detailed prescription of how to apply proceeds of piracy in a manner that will enhance the realization of deterrence. It also fails to take cognizance of sociological and environmental factors that engender maritime crimes.[26] However, on the other hand, its implementation will facilitate the efforts to address some of the maritime threats that the ISPS Code hopes to address.

4.3 The Deep Blue Project, and the Launching of Operation Calm Water and Operation Sanga Sung

The duo of Operation Calm Water and Operation Sanga were launched by NIMASA, in collaboration with the NN, to check the extent to which the security operatives are ready to respond to security threats. In addition, the administration of former President Muhammadu Buhari launched the Integrated National Security and Waterways Protection Infrastructure, commonly referred to as the Deep Blue Project (DBP) in 2021.

---

[23] Section 4 of SPMOA; This section itemises a total of 18 acts that constitutes maritime offences within SPMOA
[24] Section 17 (2) of the SPMOA.
[25] Ibid Section 19.
[26] Maurice Ogbonnaya, 'Nigeria's anti-piracy law misses the mark' (*Institute for Security Studies'* https://issafrica.org/iss-today/nigerias-anti-piracy-law-misses-the-mark (7th May 2020).

The DBP is a $195 million investment in vessels, maritime domain awareness platforms, and land and sea assets, obtained with the sole aim of helping the country to have a better grasp of the security of her maritime domain, by combating piracy, armed robbery and other security threats within the Nigerian internal waters and in the GoG. The Deep Blue Project is a joint initiative of the Federal Ministry of Transportation and Federal Ministry of Defence, being implemented by NIMASA, with personnel drawn from various security agencies including the Nigerian Air Force, Nigerian Navy, Nigerian Army, Nigeria Police, and the Department of State Services. The project aims to prevent illegal activities within Nigeria's Exclusive Economic Zone (EEZ), enforce maritime regulations, enhance the safety of lives at sea, and prevent illegal activities in the inland waterways.[27] To effectively tackle maritime security issues in Nigerian waters up to the Gulf of Guinea, the project has deployed land, sea, and air assets. DBP operates through a comprehensive maritime security infrastructure, comprising both civilian and military personnel. Its key operational components include the Command, Control, Communication, Computer, and Intelligence (C4i) Centre, as well as marine, air, and land assets. The C4i Centre functions as the operational hub of the DB project and operates around the clock. Its personnel are on constant surveillance of the security systems, namely the C4i and Intelligence systems, to identify and coordinate responses to maritime security threats and other suspicious activities within the Nigerian maritime domain.[28]

To facilitate the implementation of the DBP, several security facilities were put in place, including the Command, Control, Computer, Communication, and Intelligence (C4i) Centre for Domain Awareness and Intelligence gathering, to aid in gathering intelligence information that could aid early detection of impending security attacks and prevention of such attacks. Security equipment was also acquired, including 16 armored vehicles meant to be used for coastal patrol, and a 600-strong Maritime Security Unit having specific

---

[27] NIMASA, 2020, 'Deep Blue Project: Facing Maritime Security Head-On' (The Voyage, (8) (4) Available Online: https://nimasa.gov.ng/deep-blue-project-facing-maritime-security-head-on/ Accessed 21 November 2021.
[28] Guy Martin, 'NIMASA Getting Ready for Major Deep Blue Deliveries' *Defence Web*, (Nigeria, August 3, 2020) https://www.defenceweb.co.za/featured/nimasa-getting-ready-for-major-deep-blue-deliveries/

training for interdiction. Besides the equipment to be used on land, other equipment was also acquired for use in the air space, these are two Special Mission Aircraft (SMA) for EEZ surveillance, three Special Mission Helicopters (SMHs) which can be used for conducting search and rescue missions, and four Unmanned Aerial Vehicles (UAVs). Some sea assets were also acquired, these comprise two Special Mission Vessels (SMVs) and 17 Fast Interceptor Boats (FIBs).[29]

The DBP is targeted at achieving effective implementation of relevant maritime instruments including IMO Resolutions A. 584(14) and A. 584 (13) which implore state parties to address threats to the safety and security of ships, and persons onboard in case of the former and the latter focusing on the need for efforts to address piracy and armed robbery in adjacent waters.[30] Resolution A.584(14), adopted 20th November 1985, spelt out, "measures to prevent unlawful acts which threaten the safety of ships and security of their passengers and crew", and particularly, resolution A. 545(13) of 17th November 1983, which "urges Governments to take, as a matter of highest priority, all measures to prevent and suppress acts of piracy and armed robbery against ships in or adjacent to their waters, including strengthening of security measures" (IMO, 2019). The DBP also works as a tool for the implementation of maritime safety and security provisions of international law instruments like UNCLOS, the 1988 SUA Convention, its 2005 amendment and its Protocol, the SOLAS Convention, and the ISPS Code. [31]

4.4 Establishment of the Nigerian Government and Industry Joint Working Group (NIWG)

Established in May 2020, the NIMASA/Industry Working Group (NIWG) is the first coordinated effort between industry and the Nigerian Government (represented by

---

[29] Philip Kyanet, 'President Buhari: Deep Blue Project Offers Robust Infrastructure to Secure our Waters' (NIMASA 10 June 2021) https://nimasa.gov.ng/president-buhari-deep-blue-project-offers-robust-infrastructure-to-secure-our-waters/

[30] Curtis Bell *et al,* 'A Report on Pirates of the Gulf of Guinea: A Cost Analysis for Coastal States' *Stable Seas* (West Africa, November 2021) https://www.unodc.org/documents/Maritime_crime/UNODC_Pirates_GoG_A_Cost_Analysis_for_Coastal_States.pdf

[31] Peter Udochukwu Ohagwa, 'Analysis of Nigeria's Deep Blue Project: a new paradigm for maritime security in the Gulf of Guinea' (Masters Dissertation, World Maritime University, 2022) https://commons.wmu.se/cgi/viewcontent.cgi?article=3099&context=all_dissertations

NIMASA, Ministry of Transport, Nigerian Navy, Interpol, Marine Police, Customs and Nigerian Ports Authority) to address the issues of maritime security. The NIWG is comprised of several agencies of government and stakeholders in the Nigerian maritime industry. These are NIMASA, the Ministry of Transport, Nigerian Navy, Nigeria Ports Authority, Marine Police Interpol, representatives of the Nigerian oil industry (OCIMF), and representatives of the shipping industry ICS, BIMCO, INTERCARGO, INTERTANKO, and the Nigerian Shipowners' Association). The formation of the NIWG is the first collaboration between government agencies and industry stakeholders to address maritime security issues. This has helped to carry along other security agencies like Interpol, Marine Police, Customs, and Nigerian Ports Authority (NPA) to enable them to make their input to address the maritime security problem facing the country.[32] The main goal of creating the NIWG is to speed up efforts to address maritime security threats by facilitating stakeholder interaction, pursuing projects through mutual collaboration, and improving transparency between government and industry in addressing the shared goal of achieving the region-wide permanent prevention of piracy and armed robbery. Therefore, Nigeria and other coastal states in the Eastern Gulf of Guinea will be able to realize the full potential of their Blue Economies if maritime operations and seafarers are kept safe in the area. Another significant advancement made under the auspices of the NIWG is NIMASA's ability to collaborate directly with the IMO in the efforts to implement a National Maritime Security Strategy. As a result, the Maritime Industry's Best Management Practices West Africa Guidelines were approved.[33]

4.5 Ship Documentation Compliance and Security Levels

Since the domestication of the ISPS Code, NIMASA has been collaborating with other security operatives to see to its implementation. This includes measures adopted to

---

[32] 'NIMASA and Industry Working Group claim progress on maritime security efforts' *Safety4Sea* (London, 12 October 2020) https://safety4sea.com/nimasa-and-industry-working-group-claim-progress-on-maritime-security-efforts/

[33] 'Nigerian Government and Industry Joint Working Group (NIWG) statement on maritime security collaboration' (OCIMF, 9th October 2020) https://www.ocimf.org/news-and-events/news/bulletins/nigerian-government-and-industry-joint-working-group-niwg-statement-on-maritime-security-collaboration.

prevent or respond timorously to any security threat within the Nigerian maritime domain. These include the requirement that ship Captains submit Security-Related Pre-Arrival (SRPA) information to the Designated Authority (DA) at least 48 hours before the ship arrives at the port. Also, the Captain of the ship must submit a DOS to the PFSO within 72 hours preceding the arrival of the ship at the port and such shall be sent to the DA not later than 48 hours before the arrival of the ship. Every ship shall a 24-hour surveillance to detect any movement or threat that may not be spotted via the radar. A pre-departure search shall be conducted on every vessel before leaving the port, the ship shall ensure that the Automatic Identification System is turned on, to ease communication and response from the NN or any other NN or other Regional Maritime Rescue Coordination Centre (RMRCC). [34]

5.   Challenges Undermining Effective Implementation of the ISPS Regulation Code in Nigeria

Certain limitations are inherent in the wording and provisions of the ISPS Code, which are capable of undermining the effectiveness of the Code in addressing modern security threats. While there are other limitations relating to the provisions made for its implementation at the national level. These limitations will be examined as follows:

5.1 Inherent Limitations in the Provisions of the ISPS Code

One of the inherent limitations of the ISPS Code is the inability to identify and capture emerging ship and port security threats and make adequate provisions to address them. At the time of enacting the ISPS Code in 2004, the possibility of a cyber security attack in the shipping industry was not immediate. However, the extent of development of modern technology today makes cyber security attacks a major potential threat to the shipping industry. Today, cargo ships have increased capacity and they are interconnected due to the monitoring software used by companies often employed for online monitoring of those ships. Furthermore, international business transactions are largely conducted online and this implies further interconnectedness, through which the shipping industry may be

---

[34] Osagie Edward, 'NIMASA Issues Advisory to Forestall Maritime Threats, Stowaways' *NIMASA Report* (Nigeria, 4th November 2021) https://nimasa.gov.ng/nimasa-issues-advisory-to-forestall-maritime-threats-stowaways/

exposed to cyber-attacks. For example, in 2017, Maersk, a global shipping company lost over $300 million (three hundred million US Dollars) to the NotPetya attack, in the aftermath of cyber warfare between Ukraine and Russia. Considering that Maersk is a shipping giant calling at over 76 ports across the globe and accounting for over 800 cargo ships which is about one-fifth of the global trade volume, the cyber threat could have gone out of hand.[35]

The downside is the avenue for security attacks in cyberspace to spread easily thereby causing large havoc. It is therefore necessary for the ISPS Code to contain provisions capable of preventing cyber security attacks and in the event of such an attack, curtailing its spill-over effects. In this age of digital technology and digital transactions, it is inadequate for ship and port security regulations to omit provisions capturing cyber security threats.

Another inherent limitation of the ISPS Code is the provision relating to the security assessment of cargo at the ports. PSA is to be conducted to identify dangerous goods meant to be security targets or to be used for launching security attacks. This includes explosive and dangerous materials that may be stored in a port. It is therefore crucial to implement security measures to prevent threats to and from dangerous materials. However, while ports and contracting governments are responsible for ensuring adequate implementation of these measures, it would require that security measures and risks be assessed constantly. It may however not be feasible to reassess holistic port security every time new cargo arrives. Therefore, the security assessment of transiting cargo mainly accounts for stationary risks rather than transitory and adaptive threats.

It is also an observable limitation of the ISPS Code is the restricted applicability to SOLAS ships, and the deliberate exclusion of government ships, warships, fishing vessels, and vessels weighing less than 500 tons. Meanwhile, the vessels expressly excluded are found everywhere within the maritime domain, thereby compromising the security operations of the port states and those vessels to which the Code applies.

---

[35] Jill Leovy, 'Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks' *Los Angeles Times* (USA 17 August 2017). https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

Although the IMO considered the adoption of procedures for the safe operation of non-SOLAS ships, however, because the ISPS Code does not prescribe mandatory guidelines or minimum standards, regulation of the activities of such ships was resolved to be at the discretion of the contracting government.[36] In the case of Nigeria, the ISPS Code regulation is silent on the fate of non-SOLAS ships, this leaves a lacuna that is capable of constituting implementation challenges as well as exposing the country's maritime space to security threats in the future.

Another obvious limitation of the ISPS Code is that the measures prescribed therein are strictly preventive and less responsive to attacks. Although there are skirmishes of reference to access control, the ISPS Code lacks substantial provisions on how to respond to security attacks.

The ISPS Code does not mention the aftermath of security incidents.

5.2 Lack of Centralized System of Communication of Adopted Security Level

One of the fundamental provisions of the ISPS Code is the obligation imposed on contracting governments to decide the security level to apply to the ship and port facility, which may be security levels 1, 2, and 3. Directly connected to this is the requirement that a ship shall only dock at a port with the same security level as the ship and this must be promptly communicated through the DOS, before entering the port territory. A ship having a lower security level must increase its security level to be granted access to the port. The process of increasing security level is costly, time-consuming, and may not be immediately achievable at the point of entering a port. However, the process of communication of security level becomes cumbersome in the absence of a database, duly updated to enable shipping companies to take necessary steps to upgrade ship security as the need may rise or designate ships to ports at commensurate security level. This is capable of hindering all the parties involved from preparing and implementing proper

---

[36] Rupert Herbert-Burns, Sam Bateman and Peter Lehr, 'Lloyd's MIU Handbook of Maritime Security' (2008)   (CRC Press, Illustrated).

security measures on visiting vessels.[37] The ISPS Code only requires that information about the security levels be provided when a vessel approaches the port, which limits its effectiveness in achieving its core objective of facilitating early and efficient exchange of maritime security-related information at national, regional, and international levels.

More recently, NIMASA introduced a system for checking illegal port activities which requires that the captain of every ship present their DOS to the PFSO of the point of call within a maximum of 72 hours before arrival and such shall be further conveyed to the DA within 48 hours. Furthermore, the SSO must ensure that 24-hour surveillance is maintained on the ship to detect any illegal movements by persons, small boats, or skiffs that the radar may be unable to capture.[38] Although these are important developments, however, where there is a disparity between the security level of the ship and the port being approached, 72 hours may not be sufficient to beef up security if needed by the port or the ship, thus causing a hindrance to the transaction.

Moreover, regardless of a vessel's level of preparedness in terms of security measures, maritime security threats such as armed robbery can occur at any time in the course of navigation or at anchorage. Thus, the effectiveness of the ISPS Code may be dependent on available information through statistics on the status of the vessel during an attack. When information about security incidents in a particular country is not available, analyzing statistics on attacks that occur while ships are at berth or anchor can be a useful way to evaluate the effectiveness of the ISPS Code.

5.3   Inadequate Skilled Manpower

Implementation of the ISPS Code regulation, at a level that will enhance the state of port security requires specialized training. One of the major issues capable of hindering the adequate implementation of the ISPS Regulation in Nigeria is the lack of the requisite technical know-how among the security and port officers. However, efforts are being

---

[37] Ersi C. Likmeta, 'ISPS CODE: The Effectiveness, Its Drawbacks and Potential Improvements' (United Nations, January 20, 2022) https://nomikospalmos.wordpress.com/2022/01/20/isps-code-the-effectiveness-its-drawbacks-and-potential-improvements/

[38] Osagie Edward, 'NIMASA Issues Advisory to Forestall Maritime Threats, Stowaways' (NIMASA, November 2021) https://nimasa.gov.ng/nimasa-issues-advisory-to-forestall-maritime-threats-stowaways/

made to address this issue, the efforts include the establishment of a Port Training Institute at Apapa Dockyard, under the auspices of the NPA, through which a marine harbor situation center was commissioned for the training of NPA staff. This training is expected to enhance the capacity of operation personnel, pilots, marine officers, tug masters, and radio signal operators, to improve their ability to carry out port security operations. It also includes the adoption of stimulators to verify the capacity and suitability of berths available to shipping lines and their operation.[39]

Furthermore, there was a series of training organized under the auspices of the West and Central Africa Port Security Project (WeCAPS). WeCAPS is an initiative adopted to reduce vulnerabilities and reinforce the capacity to respond to maritime accidents and security attacks to enhance safety and security at sea. Assessment of the Lagos ports was conducted, particularly the Lagos port complex (Apapa) and Tin Can Island port complex, to ascertain the readiness of the ports to detect security threats and respond to such threats. The assessment produced a long list of security training that is required, including training of officials to aid compliance with the obligations under the ISPS Code. These include mandatory training of port staff prescribed in the ISPS Code, particularly provisions of articles 18.1 and 18.2. The former is the training of the PFSOs. There is a need to train Senior Security Staff on the conduct of security inspection, cyber security situation analysis, and responses to cyber threats. Other training that is required are basic pilot training for patrol crews, training on the conduct of evaluation of security situations and risks, surveillance monitoring, and procedures for response to port security threats, ship security threats, and security threats in the waterway. In the event of a suspected threat, procedure for control of access to restricted areas, management, and use of Integrated Security Management Systems The exhaustive list of areas where training is lacking shows the lack of readiness for adequate implementation of the ISPS Regulation and points to the lack of political will.[40]

---

[39] 'NPA Port Training Institute Commissions Marine and Harbour Simulation Centre' (Maritime News Roundup, June 2019) (Dreging & Drill Haull), https://www.ddhmag.com/nigerian-maritime-news-roundup/
[40] 'Technical support to port security in the port Lagos, Nigeria - West and Central Africa port security project (M/W)' (Département Paix, stabilité, sécurité - P2S > Pôle Menaces globales et criminalité

The problem of inadequate skilled manpower was related to inadequate intelligence and hinted on by the Chief of Naval Staff, when he said that the vast area of the NMD poses a challenge for effective policing of the area. Therefore, intelligence plays a crucial role in ensuring maritime security. Due to limited resources and the need to meet operational mandates while saving costs on logistics, the Navy relies on both human and technologically-driven intelligence.[41]

5.4   Lack of Adequate Funding

The purchase of maritime security equipment is capital-intensive and requires deliberate acts by the government, however, lack of adequate funding makes it difficult to meet the requirement. Meanwhile, the ISPS Code has specific requirements that shall be met by installing and purchasing security equipment, these equipment are expensive but failure to acquire them may hinder ports in developing states in their efforts to implement the provisions of the Code. Some of the Port Facility Security equipment includes Fencing, gates, vehicle barriers and lighting, Closed-circuit television (CCTV), Communications and x-ray equipment, Archway and hand-held metal detectors, Perimeter/intruder detection systems, Automated access control equipment (e.g. identification readers or keypads), Information and computer protection systems, Explosive trace and vapor detection equipment. [42]Also, the Code specifies three security levels 1, 2, and 3 with the requirement that the ship be berthed at a port having the same security level. In most of the Nigerian ports, there is a need to increase the security level, in the wake of the recurring armed robber and other attacks at the ports. However, increasing the level of security will come at a huge cost, requiring deliberate investment and requisite political will. Most developing countries including Nigeria have found it difficult to pump money into increasing their security level as this will affect the profit obtainable from the ports. On the other hand, the failure to enhance port security increases port vulnerability and makes the ports less attractive to investors and ships calling at the port.

organisée, (24/06/2022) https://expertise-france.gestmax.fr/8037/1/technical-support-to-port-security-in-the-port-lagos-h-f

[41] Chief of Naval Staff, Vice Admiral Emmanuel Ogalla (March 15th 2023)

[42] 'Port Facility security' (Seably) https://www.seably.com/courses/port-facility-security-personnel-awareness/lessons/0/steps/2 3rd September 2020.

5.5   Lack of Adequate Port Security Equipment and Maintenance Deficit

The full implementation of the ISPS Code places a huge responsibility on the government in terms of the security equipment required to be put in place. Whereas the Nigerian Government has been proactive in its efforts to implement the requirements of the Code, as a result of which significant progress has been made, there is a lot that is yet to be done. Similarly, in 2020 some maritime security equipment was donated by the United States to the NN to provide support to enhance the capacity of the NN to secure the Nigerian coastline. These equipment includes best-in-class sensors and radars, communications and networking equipment, thermal-imaging cameras, and software that can be harnessed to enhance the capacity to counter imminent threats.[43]   However, Nigeria has seven ports and several port terminals and facilities that require adequate security as a result, there is a need to purchase other security equipment to aid the full implementation of the ISPS Code.

Recently, the European Union (EU) called out the Nigerian government regarding the security equipment that ought to be put in place to aid the full implementation of the ISPS Code and enhance port security. These include the installation of CCTV cameras at different parts of the ports to enhance the much-required 24-hour surveillance, the erection of perimeter fencing of the port, and putting on ground access badges to monitor and prevent illegal access to the port premises.[44]

5.6   The Challenge of managing Vessels outside the Scope of the ISPS Code

The ISPS Code expressly excludes some vessels, to which its provisions will not be applicable, these are commercial vessels and barges having less than 500gt weight, warships, manual fishing boats, and old fishing boats that are used for non-commercial purposes. The knowledge of these types of vessels that constitute exceptions in the Code may be used to the advantage of attackers who may use such boats and vessels to

[43] Soonest Nathaniel, 'U.S Boosts Nigeria's Maritime Security With New Surveillance Equipment' (Channels News, 11 December 2022) https://www.channelstv.com/2020/12/11/u-s-boosts-nigerias-maritime-security-with-new-surveillance-equipment/

[44] Adedapo Adesanya, 'EU Tasks Nigeria on Seaport Security' *Business Post* (Lagos, 3rd May, 2023) https://businesspost.ng/general/eu-tasks-nigeria-on-seaport-security/

perpetrate attacks. This leaves the contracting state with the option to cover such boats in the domesticated version of the Code. However, Nigerian ISPS regulation did not capture those vessels. As a result, attacks may be launched using those vessels thereby making it difficult to have full implementation.

To summarize, the ISPS Code does not apply to several types of vessels that are susceptible to terrorist attacks or exploitation. These vessels comprise fishing vessels, container ships built before July 2001, vessels not involved in international voyages, and cargo ships with tonnage of less than 500.[45] It's important to note that the ISPS Code does not cover yachts and marinas. This is because yachts are typically less than 500 tons, and marinas are not equipped to handle ISPS vessels. However, small vessels and ports can threaten security as they fall outside the scope of the ISPS Code. Even without domestic legislation or law enforcement, it's still necessary to address the potential threats posed by non-SOLAS vessels. To this end, the IMO has provided non-mandatory guidelines to help mitigate these risks.[46]

6. Conclusion

The ISPS Code remains a pivotal instrument for ensuring maritime safety and security, yet its broader developmental relevance often goes underappreciated. In the Nigerian context, the Code's implementation has revealed deep-seated structural, institutional, and capacity-related deficiencies that hinder both maritime security and economic progress. The persistence of these challenges has significant implications for the realization of SDG 8 in the maritime sector, as insecure and inefficient port environments deter investment, disrupt trade, and limit decent employment opportunities for maritime workers.

Bridging these gaps requires a deliberate shift from policy rhetoric to actionable practice. Strengthening regulatory oversight, enhancing inter-agency coordination, and investing in

---

[45] McNaught, Fiona, 'Effectiveness of the International Ship and Port Facility Security (ISPS) code' in addressing the maritime security threat (*Geddes Papers* 200 (2005)) 89-100.
[46] Damir, Z. E. C., Vlado FRANČIĆ, and Marija ŠIMIĆ HLAČA, 'Ports Security Organization and Functionality–Implementation of the ISPS Code in Medium and Small Countries' [2010] (28) *Human Systems Integration to Enhance Maritime Domain Awareness for Port/Harbour Security* 41.

technical and human capacity development are essential steps. Moreover, integrating the ISPS Code into Nigeria's broader economic and labour policies can create a synergistic framework that promotes security, productivity, and sustainable employment.

In conclusion, operationalising the ISPS Code effectively is not merely a maritime security imperative, it is also a developmental necessity. By aligning implementation strategies with the goals of SDG 8, Nigeria can transform its maritime sector into a secure, inclusive, and economically vibrant space that supports national growth and global competitiveness. Although efforts to implement the ISPS Code has been continuous, including the area of intelligence gathering where the NN is using area surveillance to inspect the region and identify vessels that are illegally positioned for this purpose. However, more efforts must be put-in to reaslise SDG 8, by creating secured work space needed to enhance the productivity of the sector and aid economic growth and development.