MRC MARITIME RESEARCH CENTER
FOUNDATION FOR UNDERWATER DOMAIN AWARENESS

New Frontiers of India’s Underwater Security

Need for CMF in UDA through iCET

Short Report

By

Commodore (Dr.) Somen Banerjee (Retd.)

14 June 2023

New Frontiers of India’s Underwater Security
Need for CMF in UDA through iCET

Commodore (Dr.) Somen Banerjee, (Retd.)

Introduction

One of the goals of India's 'Atmanirbhar Bharat' launched by Hon'ble Raksha Mantri in September 2022 is Civil-Military Fusion (CMF). The concerted effort by the Ministry of Defence (MoD) has not just increased the indigenous components of defence acquisition, but India's defence exports have reached an all-time high of ₹15,920 crore in FY 2022-23. Indian Navy’s consistent endeavour has been appreciated by Hon’ble Prime Minister during the recent ‘Swavlamban’ Seminar. However, changes in the nature and character of warfare have forced all countries to revisit their maritime defence strategies. Sabotage, grey-zone conflict, and asymmetric warfare are altering the **balance of threat**, even when the **balance of power** between countries remains relatively unchanged. Routine underwater commercial activities are being targeted and weaponised, increasing vulnerabilities to critical national infrastructure. Against this backdrop, the importance of Underwater Domain Awareness (UDA) need not be overstated. However, the mere absorption of advanced underwater technologies would be inadequate for optimal defence for critical underwater national assets, constituting an effective deterrence, or conducting an offensive/covert action against an adversary. There will be a need to synthesise the existing Organisations, Innovations, and Logistics, or the OIL of CMF for enhancing the UDA.

This paper seeks to examine the application of CMF in UDA. It studies the scope of increasingly vulnerable maritime infrastructure like oil and gas pipelines, electricity grids, and underwater communication networks that have emerged as the new frontlines of potential conflict. In addition, it identifies the possible vulnerabilities of adversaries in the immediate neighbourhood. The paper further explores the increased weaponisation of liminal technologies that could morph UDA from the benign realms of Science and Technology (S&T) to geopolitical and strategic contestation for monopoly in the years ahead. Therefore, the National Security Council will also have to identify new technologies requiring collaboration under the India-US Initiative on Critical and Emerging Technologies (iCET) in UDA domain. Finally, the paper suggests for enhancing India’s maritime security, minor structural changes that would be necessary by synthesising Organisations, such as International Fusion Centre – Indian Ocean Region (IFC-IOR), The Coast Guard, National Institute of Ocean Technology (NIOT), Ministry of Petroleum and Natural Gas (MoPNG), Ministry of Communications (MoC), and Ministry of Electronics & Information Technology (MoEIT).

New Frontiers of Warfare – Commercial Offshore Infrastructure Systems

On 26 September 2022, three unexpected gas leaks were observed a few kilometres apart in the Danish and Swedish Exclusive Economic Zones (EEZ). Seismologists have recorded sizeable explosions of about 100 kilograms of TNT, suggesting underwater sabotage of the Nord Stream 2 pipelines underneath the Baltic Sea. These were potentially less damaging to

Europe's energy security, as the Nord Stream 2 was lying in disuse for some time. It is likened to the potlatch ceremony, where Native Americans used to destroy dysfunctional assets and wealth. Nevertheless, the environmental impact is substantial. Unlike an oil spill, gas leakage does not pollute the sea, but the methane released could significantly impact climate change. According to one estimate, 500 million cubic meters of gas leaked is the equivalent of eight million tons of carbon dioxide or 1/5000th of annual global CO2 emissions.[1]

Resembling an Agatha Christie novel, this incident is one in which nearly everyone could be involved with a motive in the ongoing Russia-Ukraine war. According to satellite data monitoring private firm SpaceKnow, 25 large cargo ships had passed through the region weeks before the blasts, of which two were Darkships. These two ships had their Automatic Identification System (AIS) switched off, violating international law. Such Darkships are usually involved in maritime crime.[2] One thing that has become clear from the explosions is that maritime infrastructure like the oil and gas pipelines, electricity grids, and underwater communication networks are the new frontlines of future conflict.

An apparent disruption of two major submarine cables, Asia-Africa-Europe 1 (AAE-1) and SeaMeWe5 near Egypt on 06 June 2022 had restricted internet access for several hours simultaneously to many countries in Asia and Africa. AAE-1 and SeaMeWe5 are consortium cable of length over 20,000 kilometres and connects scores of landing points across Africa, Europe, and Asia. Of course, natural disasters, fishing boats, shark attacks, and volcanoes can cause outrage. However, the possibility of intentional subversion in prolonged and desperate conflict adds a new dimension to maritime security.[3]

Arguably, the character of warfare has changed significantly in the past few decades. Belligerents do not feel encumbered to inflict pain on the civilian population as it strikes at the legitimacy of a government in power, unable to protect the lives and livelihoods of its people. Such methods are now employed by extremists against civilian targets for political aims. Violent extremists of all backgrounds frequently choose critical infrastructure systems essential for the normal functioning of day-to-day life within a country.[4]

Commercial offshore infrastructure like undersea internet cables, power cables and oil and gas pipelines have become potential targets. The advantages of underwater commercial warfare are their deniability and the ability to disrupt the opponent economically before or during a war. The increasing vulnerabilities of these offshore assets have spurred the French to unveil a new Strategic Seabed Warfare Doctrine in February 2022[5]. Immediately

[1] Sergey Vakulenko, Shock and Awe: Who Attacked the Nord Stream Pipelines? *Carnegie Endowment for International Peace,* 30 September 2022, https://carnegieendowment.org/politika/88062

[2] Matt Burgess, Dark Ships' Emerge From the Shadows of the Nord Stream Mystery, *Wired,* 11 Nov 2022, https://www.wired.co.uk/article/nord-stream-pipeline-explosion-dark-ships

[3] Andrea Peterson, Disruption to submarine cables degrades internet for parts of Africa and Asia, *The Record,* 07 June 2022, https://therecord.media/submarine-cables-cut-egypt-disruption/

[4] Ilana Krill & Bennett Clifford, Mayhem, Murder, and Misdirection: Violent Extremist Attack Plots Against Critical Infrastructure in the United States, 2016-2022, George Washington University, 2022, https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/CriticalInfrastructureTargeting09072022.pdf

[5] Xavier Vavasseur, France Unveils New Seabed Warfare Strategy, Naval News, 16 February 2022, https://www.navalnews.com/naval-news/2022/02/france-unveils-new-seabed-warfare-strategy/

after, the Royal UK Navy reviewed its undersea vulnerabilities with private operators in May 2022[6].

States increasingly depend on infrastructure and assets partially or completely located outside their jurisdiction and over which they have little or no control. Most of the critical infrastructure is owned by the private sector. Consequently, the State itself may no longer be able to ensure comprehensive security and may be largely dependent on the private sector. Therefore, a well-defined public/private partnership is essential to design effective policies on the protection of critical infrastructure.

There are several difficulties in determining which assets should be considered *critical*. Because of the dense interconnections, it is often difficult to prioritise. Moreover, the criticality of an infrastructure might change over time. Decision-makers are often unwilling to assume the political risk of removing items from a *critical list* or including one due to financial constraints, resulting in the waste of resources. These ambiguities will hamper the development of security measures.

<u>Proposal 1</u>*:* National Maritime Security Coordinator (NMSC) needs to review India's undersea vulnerabilities with private operators and prepare:

(a) A well-defined public/private partnership is essential for a policy on drawing a **critical list** and protection of Commercial Offshore Infrastructure Systems (COIS). This needs to be reviewed periodically.

(b) A Seabed Warfare **Doctrine** and **Strategy** in collaboration with the Indian Navy. Collaborate with or learn from the French or Royal Navy. Integrate the INTEG, IFC-IOR, NIOT, or any other agencies necessary.

India's Commercial Offshore Infrastructure Systems (COIS)

The damage of COIS that could disrupt economic and political stability includes undersea communication cables, undersea power cables, and undersea energy infrastructure. Some of the infrastructure already exists, whilst some would be created in the future.

Undersea Energy Infrastructure

The offshore Exploration and Production (E&P) commonly known as the 'upstream' sector comprise a large variety of drilling rigs, processing and control platforms, pipelines and numerous types of support ships and vessels. Transportation of petroleum-based energy involves specialised ships, pipelines and associated manifolds, dedicated oil terminals and berths in ports, Single Point Moorings (SPMs), etc.

[6] Andrew Salerno-Garthwaite, Seabed warfare is a 'real and present threat', Naval Technology, 20, December 2022, https://www.naval-technology.com/features/seabed-warfare-is-a-real-and-present-threat/

According to DG of Hydrocarbons, the offshore oil and gas fields under the Production Sharing Contract (PSC) regime are areas E, F, G and H, illustrated in **Figure 1**. PSC is a special agreement with foreign contractors for exploration and development in the country. https://dghindia.gov.in/assets/downloads/56cef5b69043edghwebsite9.pdf

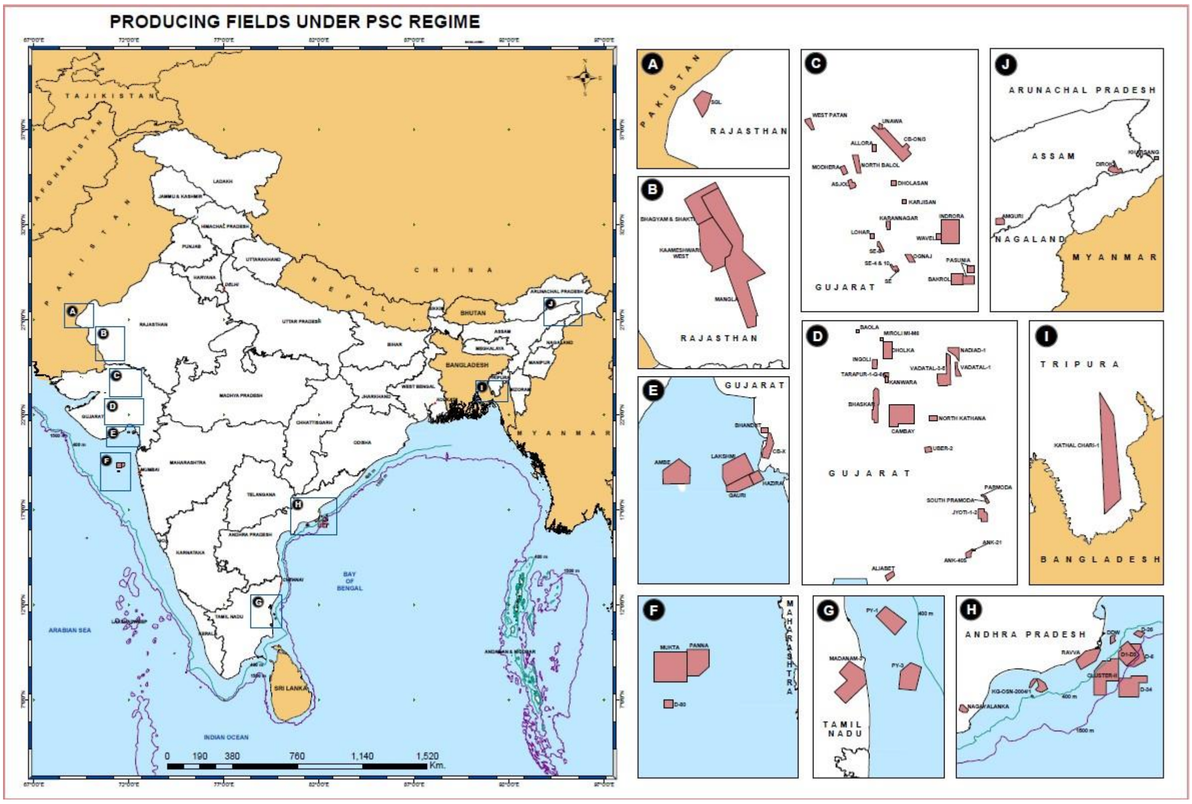


Figure 1: Producing Oil and Gas Fields *(Source DGoH)*

Additionally, India is offering 26 blocks for exploration and production of oil and gas in a mega offshore bid upstream. Out of the 26 blocks, 15 areas are in ultra-deepwater, eight are in shallow seas and three are on land. The bid rounds held under the 2016 policy are called the Hydrocarbon Exploration and Licensing Policy (HELP). Since then, seven bid rounds of the Open Acreage Licensing Programme (OALP) have been concluded, which led to the award of 134 blocks for exploration and production awarded.[7] The offshore blocks are:

(a) Blocks D, E, F and G under the OALP I.
https://dghindia.gov.in/assets/downloads/56cef5b69043edghwebsite6.pdf

(b) Blocks B, E, F, and G have been awarded under the OALP II.
https://dghindia.gov.in/assets/downloads/56cef597bce77dghwebsite7.pdf

(c) Blocks C, D and G in OALP III.
https://dghindia.gov.in/assets/downloads/56cef5a59811bdghwebsite8.pdf

[7] PTI, India offers 26 oil, gas blocks in mega offshore round, The Economic Times, 12 October 2022, https://energy.economictimes.indiatimes.com/news/oil-and-gas/india-offers-26-oil-gas-blocks-in-mega-offshore-round/94798375

The progress of exploration and production in these OALPs have to be monitored. Interestingly, Block G of OALP II corresponds to Andaman and Nicobar Islands (**Figure 2**). India is set to complete an exhaustive survey of its Exclusive Economic Zone (EEZ) in a few months, after the central government aligned all stakeholders, including defence and space agencies, to release 99% of the areas prohibited for oil exploration and production due to security concerns. An empowered coordination committee oversaw the process and the **National Maritime Security Coordinator**, part of the National Security Council Secretariat, played a critical role in expediting security clearances. In the past, 42% of the Indian EEZ of 2.36 million square kilometers was under a 'no-go zone'.[8]

Susceptible to Sabotage 1 - Given the size of the discovery and proximity to the international shipping lane, the offshore energy infrastructure will be susceptible to sabotage. Hence, these fields could be included in the **critical list** and will need robust UDA for defence. Other high-yield offshore fields in the EEZ also may be included in the critical list.

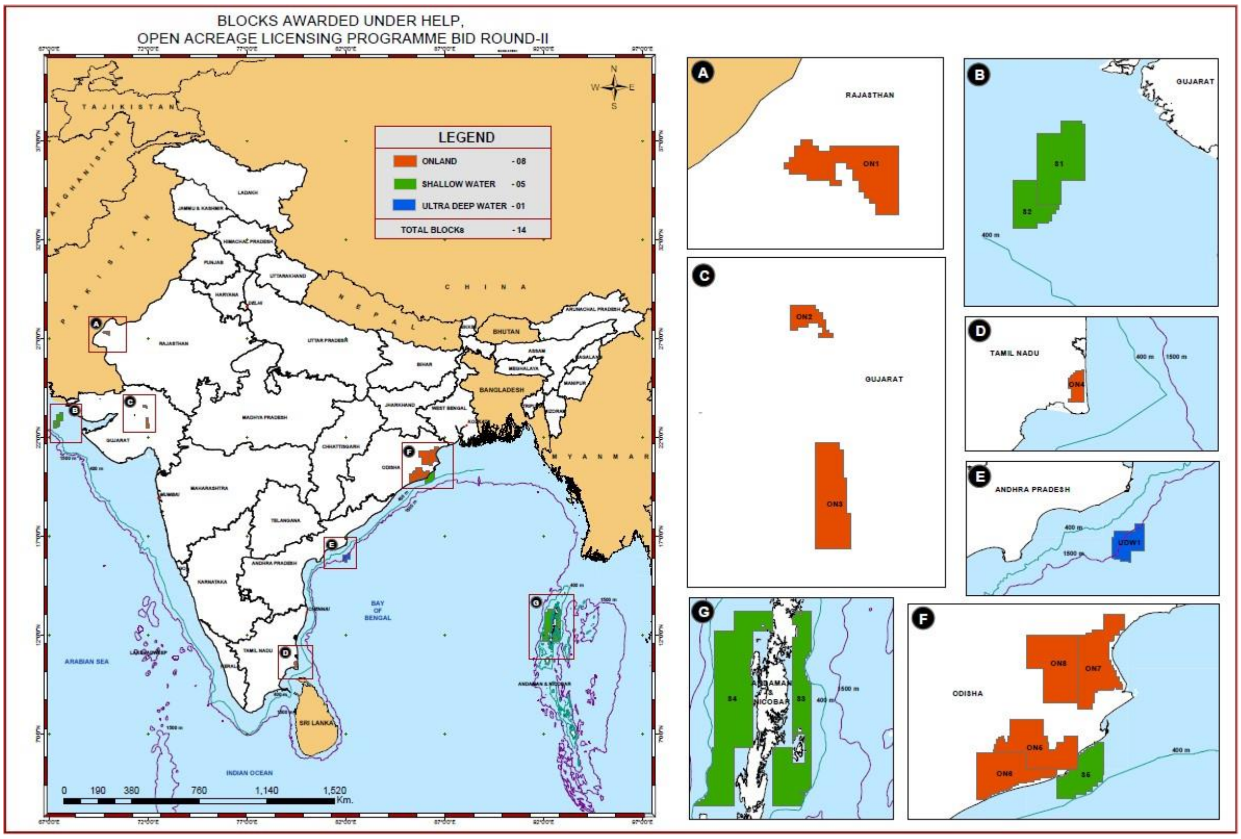


Figure 2: Blocks Awarded Under OALP II *(Source DGoH)*

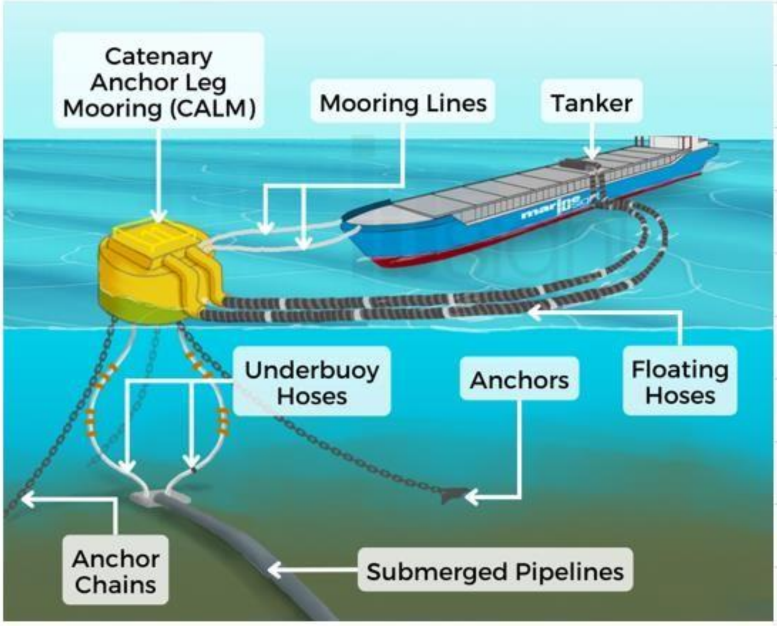
Unconventional Gas Hydrates - Gas hydrate is a crystalline solid. Each molecule of Gas hydrate contains up to 164 m3 of Methane (CH4). Initial work in India on Gas Hydrates as energy resource, was done by GAIL and the National Institute of Oceanography (NIO). These will be critical when they start production.[9]

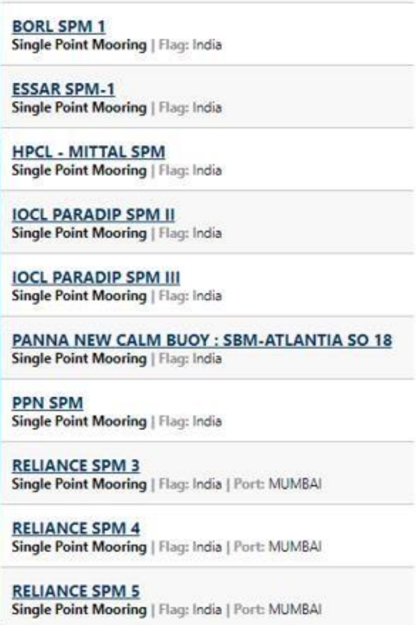
[8] Construction World.in, India EEZ survey expected to yield significant oil and gas, 31 May 2023, https://www.constructionworld.in/energy-infrastructure/oil-and-gas/india-eez-survey-expected-to-yield-significant-oil-and-gas/41260

[9] DGoH, Gas Hydrate, https://dghindia.gov.in/index.php/page?pageId=39

Single Point Moorings – Single-point mooring (SPM) systems are designed to accommodate deep-draft tankers while they transfer crude oil and fuel oil to and from shore. According to Marine Directory, there are 10 SPMs (**Figure 3**).

Susceptible to Sabotage 2 - All 10 SPMs can be considered to be on the **critical list** as they handle major imports of crude from Very Large Crude Carriers (VLCC).




BORL SPM 1
Single Point Mooring | Flag: India

ESSAR SPM-1
Single Point Mooring | Flag: India

HPCL - MITTAL SPM
Single Point Mooring | Flag: India

IOCL PARADIP SPM II
Single Point Mooring | Flag: India

IOCL PARADIP SPM III
Single Point Mooring | Flag: India

PANNA NEW CALM BUOY : SBM-ATLANTIA SO 18
Single Point Mooring | Flag: India

PPN SPM
Single Point Mooring | Flag: India

RELIANCE SPM 3
Single Point Mooring | Flag: India | Port: MUMBAI

RELIANCE SPM 4
Single Point Mooring | Flag: India | Port: MUMBAI

RELIANCE SPM 5
Single Point Mooring | Flag: India | Port: MUMBAI

Figure 3: SPMs in India *(Source: Maritime Directory)*

Offshore Trunk Pipelines (**OTPs**) – There is a need to map all the trunk pipelines connecting offshore oil and gas rigs to the on-land processing complex. ONGC commissioned the Mumbai High Uran Trunk (MUT) pipeline project on 8 June 2005. The 504.95 km pipeline was built at a cost of Rs.2,638.20 crore. Built by Hyundai Heavy Industries, the trunk pipelines were designed to transport 3.27 lakh barrels of oil per day and 12.24 mmscmd of gas from the western offshore to the Uran terminal.[10] Similarly, private sector company like Reliance has a 24 km offshore trunk pipeline in Jamnagar.[11] There would be many more OTPs.

Susceptible to Sabotage 3 - All OTPs need to be studied and a few might have to be included in the **critical list** based on cost-benefit analysis.

Undersea Communication Infrastructure

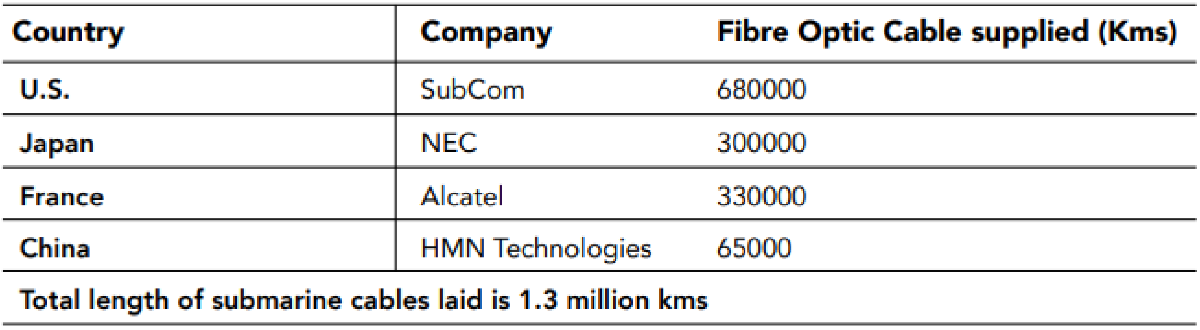
India is barely present in undersea fibre-optic cables despite being one of the world's largest telecom and data markets and having the world's second-largest digitised citizenry (after China). Since 95% of international internet data including cloud and digital communication are transmitted through undersea fibre-optic cables, India must develop a submarine cable network as part of its critical national infrastructure. Since investments in

[10] Projects Today, Mumbai High Trunk pipeline commissioned, 09 June 2005, https://www.projectstoday.com/News/Mumbai-High-Trunk-pipeline-commissioned

[11] Saipem Today, https://www.saipem.com/sites/default/files/2019-03/2330spm_SEAlin_L01_1.pdf

the undersea cable might take some time, India needs to at least invest in the protection of physical infrastructure and the data flowing in it.

There are just three major players in undersea cables: Japan's NEC, U.S.-based SubCom, and France-headquartered Alcatel Submarine Networks. They are the world's top three suppliers of optical cables, with an over 90% market share. They also own much of the technological elements of undersea networks across the entire spectrum, including subsea geological survey, cable laying, and repair capabilities. A fourth player is emerging, i.e., China's Huawei Marine Networks, rebranded as HMN Technologies in Oct 2020.[12] Table 1 shows the length of Fiber Optics laid by these major players as of 2021.



Country	Company	Fibre Optic Cable supplied (Kms)
U.S.	SubCom	680000
Japan	NEC	300000
France	Alcatel	330000
China	HMN Technologies	65000
Total length of submarine cables laid is 1.3 million kms		

Table 1: Undersea Cables laid by major players *(Source: Gateway House Research)*

At present, India has around 17 submarine cables terminating at 14 distinct cable landing stations in five cities—i.e., Mumbai, Chennai, Cochin, Tuticorin, and Trivandrum. The existing cable landing stations are owned by Tata Communications (5), Bharti Airtel (3), Reliance Jio (2), Global Cloud eXchange (formerly Reliance Globalcom) (2), and others including Sify, BSNL, and Vodafone. By 2025, India is expected to have the following additional cable links[13]:

(a) **India-Asia Xpress (IAX) and India-Europe Xpress (IEX)** by Reliance Jio's connecting Singapore to the Persian Gulf and Europe.

(b) **MIST** connecting Mumbai and Cochin to Myanmar, Thailand, Malaysia, and Singapore.

(c) **Blue-Raman** from Italy to India.

(d) **SEA-ME-WE 6** upgrades from Singapore to Marseille.

(e) **2 Africa Pearl** connecting India and Pakistan.

[12] Gateway House, Quad Economy, and Technology Task Force Report, 23 August 2021, https://www.gatewayhouse.in/wp-content/uploads/2021/08/Quad-Economy-and-Technology-Task-Force-Report_GH_2021.pdf

[13] Kaush Arha, India at the Centre of the Indian Ocean Submarine Cable Network: Trusted Connectivity in Practice, 06 April 2023, https://www.orfonline.org/research/india-at-the-centre-of-the-indian-ocean-submarine-cable-network/#:~:text=At%20present%2C%20India%20has%20around,124%20and%2084%20Tbps%2C%20respectively.

An illustration of subsea underwater communication cables connecting with India is in **Figure 4**.

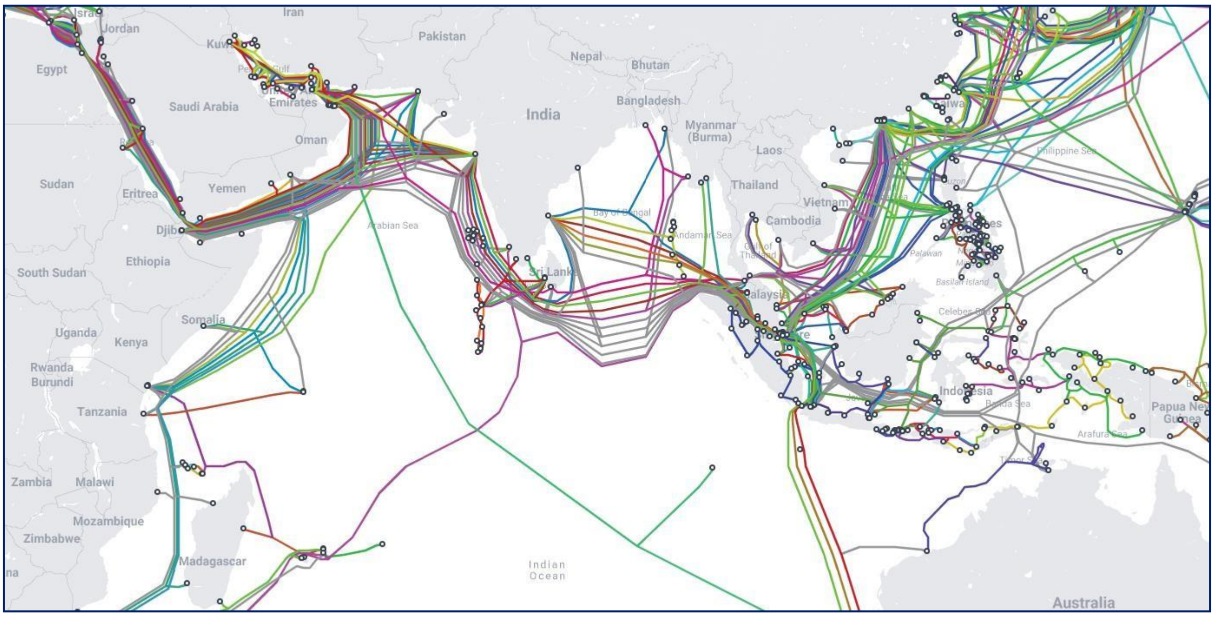


Figure 4: Undersea Communication Cable Connecting with India
(Source: https://www.submarinecablemap.com/)

Sniffing Devices – In 2022, Mauritius was embroiled in a political controversy, the government was under pressure to install sniffing devices at undersea cable landing stations which connect the country to the global internet. Sherry Singh, the Chief Executive Officer of Mauritius Telecom had to resign due to the political fallout. Such surveillance devices can be installed undersea by adversaries and is a major national security concern.[14]

Susceptible to Sabotage 4 - In 2021, the available and used capacity of these cables amounted to 124 and 84 Tbps, respectively. The main subsea cables will be difficult to disrupt unless a belligerent nation becomes desperate, like the blowing of the Kakhovka dam in southern Ukraine. However, sniffing devices can be installed on them. In addition, the isolated cable branches that connect the landing stations to the main network will be especially vulnerable to physical damage from underwater sabotage.

Undersea Power Cables

Power cables are still a continental phenomenon. A few undersea power cables can be found in Europe and North America (**Figure 5**) connecting windmills grids and islands**.** The current research could not locate undersea power cables in South Asia. However, the Honourable Prime Minister's clarion call for One Sun One World One Grid (OSOWOG) will eventually result in undersea power cables in the tropical region connecting sub-continents and landmasses across gulfs and straits. Such projects will need to have in-built standards for protection against sabotage and surveillance.

[14] Aroon Deep, Is India tapping undersea internet cables? Telcos and DoT won't say, EN Trackr, 26 July 2022, https://entrackr.com/2022/07/is-india-tapping-undersea-internet-cables-telcos-dot-wont-say/

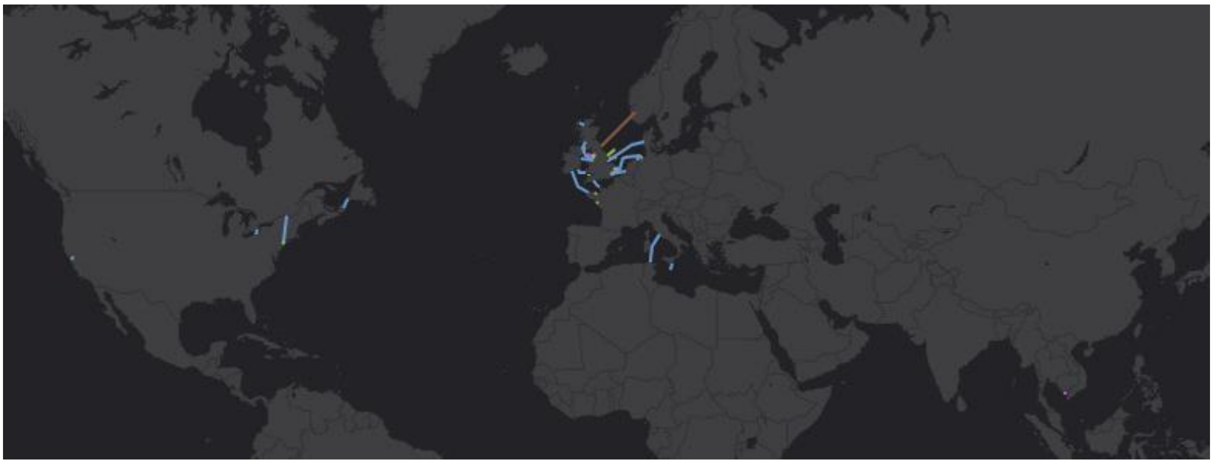


Figure 5: Undersea Power Cable Globally
(Source: https://www.intertek.com/energy-water/subsea-power-cables-project-map/)

Proposal 2*:* There is a need to formulate the necessary doctrines, standards, and strategies for deterrence, defence, mitigation, and resilience against the damage of COVAs. These will include:

(a) **Mapping** - mapping of all major production rigs, SPMs, and offshore trunk pipelines.

(b) **Standards** - Future COIS will have to be built per the promulgated security standards.

(c) **Deterrence** - Deterrence will have to be accompanied by strategic signalling and punishment. India should, therefore, develop the undersea capabilities to punish an adversary. It will be necessary for effective strategic signalling.

(d) **Defence** – The defence of COIS will need a review of organisation, infrastructure, and logistics. It will also need a vulnerability assessment and a technology scan.

(e) **Mitigation** - Mitigation might involve the repair and revival of the damaged facility if found to be cost-effective. Agencies responsible for the mitigation of environmental disasters also have to be involved.

(f) **Resilience** - In the event of a major disruption of a COIS, suitable fallbacks, and alternatives have to be identified. Such contingencies have to be tested regularly to check for resilience.

India's Civil-Military Fusion (CMF) – A Journey to iCET

When the Cyberspace Administration of China (CAC) requested user data from DiDi, a Chinese car-rental company, the latter was initially reticent. Then, upon insistence by the regulatory authorities, it reluctantly complied by providing hardcopy printouts of the customer data, thus avoiding digital forms for data analysis. DiDi's defiance eventually forced the company to delist from the New York Stock Exchange and was fined 1.2 Bn Euros by the CAC in July 2022[15]. In another Apple-FBI standoff, the manufacturer has refused access to the iPhone used by a terrorist in the San Bernardino shooting. It was eventually unlocked by a small Australian hacking firm Azimuth Security in 2016, ending a momentous standoff between the U.S. government and the tech titan Apple[16]. Essentially, these two incidents demonstrate that achieving CMF is easier said than done. However, CMF is also the way forward and Indian Public Sector Units (PSUs) have made efforts, albeit with little success.

During the formative years after independence, State Public Sector Units (PSUs) and Council of Scientific and Industrial Research (CSIR) laboratories took the lead in space, nuclear energy, and defense sectors. However, in the 1980s, self-reliance petered off unsuccessfully due to decreased support for PSUs and their inability to upgrade technologies. Even the liberalisation of Indian industries in the 1990s did not bring new technological knowledge into India. The private sector in India showed little interest in R&D and was content with collaborating with foreign Original Equipment Manufacturers (OEMs) on the latter's terms. India thus wholly missed out on the Third Industrial Revolution, characterised by semiconductors, mass manufacturing, electronics, white goods, etc. Years of enticing foreign defence majors to set up shops in India also came to naught. As a result, India has emerged as the largest defence importer in the bargain, causing a big drain on taxpayers' money and strategic dependence on foreign countries.

Hon'ble Raksha Mantri's call for 'Civil-Military Fusion' (CMF) in September 2022 is meant to correct this. However, India's experiment with Atmanirbhar Bharat and CMF@75 is relatively normative and will need real-time knowledge absorption by the Indian private sector from high-tech foreign firms. In this context, The National Security Advisors of India and the US launched the initiative on Critical and Emerging Technologies (iCET) on 01 February 2023, which promises to foster an open, accessible, secure technology ecosystem. iCET is the fruition of the intent expressed at the Biden-Modi meeting in May 2022 to further and elevate the US-India strategic partnership and defence industrial cooperation.

iCET - President Biden and Prime Minister Modi announced the U.S.-India initiative on Critical and Emerging Technology (iCET) in May 2022 to elevate and expand strategic technology partnership and defense industrial cooperation between the governments, businesses, and academic institutions of the two countries. This was followed by a roundtable on 30 January 2023 between U.S. Secretary of Commerce Gina Raimondo, U.S. National Security Advisor Jake Sullivan, and Indian National Security Advisor Ajit Doval, and other

[15] Vincent Brussee, Didi fine marks new phase in Beijing's rectification of tech sector, 09 August 2022, https://merics.org/en/short-analysis/didi-fine-marks-new-phase-beijings-rectification-tech-sector

[16] Ellen Nakashima and Reed Albergotti, The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm, *Washington Post,* 14 April 2021, https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/

senior U.S. and Indian officials. It was attended by more than 40 CEOs, university presidents, and thought leaders from both countries to accelerate opportunities for increased technology cooperation. India-US iCET has opened opportunities to develop an ***innovation bridge*** for cutting-edge commercial technologies in artificial intelligence, quantum technologies, advanced wireless, jet engines, munition-related technologies, maritime security and intelligence surveillance reconnaissance (ISR), space, and resilient semiconductor value chains.[17] During the interaction with Jake Sullivan, the US National Security Advisor on 13 Jane 2023 in New Delhi, the Indian business leaders proposed several industrial sectors for cooperation under the iCET. However, there was no specific proposal on underwater technology, including underwater exploration, cable laying, or surveillance.

A Wakeup Call for UDA – Need for INNOVATION through iCET

Marine infrastructure has become the backbone of our modern economy. But the security of these vital systems has become essential. Sightings of undetected Russian ships in both Dutch and Belgian waters have prompted intelligence officials to question if Moscow was spying on the North Sea's offshore wind farms. Both countries launched investigations into claims that Russia might have tried to map out the wind farms and other infrastructure elements in a bid to understand how these energy systems work in the North Sea. These incidents were detected after the alleged sabotage of Nord Stream 1 and 2 last September 2022[18]. So, espionage and sabotage by the enemy to vital infrastructure on the sea bottom is ***not a hypothetical threat anymore, it's a real danger***.

iCET Skill, Technology and Production Corridors. One of the main uses of subsea technology is for offshore drilling and cable laying. Indigenised technologies produced by the DRDO or NIOT have neither been commercialised nor have been inducted into defence. iCET provides excellent option for creating skill corridors and development corridors for seamless innovation and production of scale. The underwater technologies for collaboration are:

Remotely Operated Vehicles (ROVs). ROVs are widely utilized robots to overcome the shortcomings or inefficiencies of human subsea divers in underwater activities for development, repair, and maintenance operations. Deep sea ROVs form a critical part of advanced navies, especially the US. ROV technology has become increasingly affordable due to oil and gas producers in the United States for obtaining data and carrying out routine maintenance work on subsea assets and surfaces[19]. Soon deep sea ROVs will be required to address emergent underwater threats. Therefore, ROVs will need collaboration through iCET to stop imports and maintain long-term sustainable underwater security.

[17] The White House, FACT SHEET: United States and India Elevate Strategic Partnership with the Initiative on Critical and Emerging Technology (iCET), 31 January 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/31/fact-sheet-united-states-and-india-elevate-strategic-partnership-with-the-initiative-on-critical-and-emerging-technology-icet/

[18] Denis Loctier. 'A wake-up call': How to protect Europe's vital marine infrastructure from emerging threats? Euronews, 30 May 2023, https://www.euronews.com/green/2023/05/30/the-threat-of-sabotage-to-critical-infrastructure-is-real-belgian-navy-official-warns

[19] Mordor Intelligence, Rov Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028), https://www.mordorintelligence.com/industry-reports/rov-market

Autonomous Underwater Vehicles (AuV). While ROVs made up approximately 86% of the market share, their dominance is challenged by the rise in Autonomous Underwater Vehicles (AUVs). As the safety and security industries look to enhance their competitive edge in surveillance, mine counter-measures, and anti-submarine warfare applications, the demand in AUVs is predicted to have significant growth over time. By 2025, the value of AUVs is expected to reach over USD 1.48 billion. This growth in demand is fuelled primarily by commercial markets. AUVs are better equipped to explore deeper ocean depths and are cheaper to deploy than ROVs. Soon AUVs will be able to replace fully manned vessels tasked with surveillance and reconnaissance, deep-sea data gathering, and discrete payload delivery.[20] **Imported shallow water AUVs are already in use in the Indian Navy**. iCET could enable collaboration for shallow and deep water AUVs. A typical application AUV vs ROVs is illustrated at **Figure 6**. Component level technologies of an AUV is illustrated at **Figure 7**.

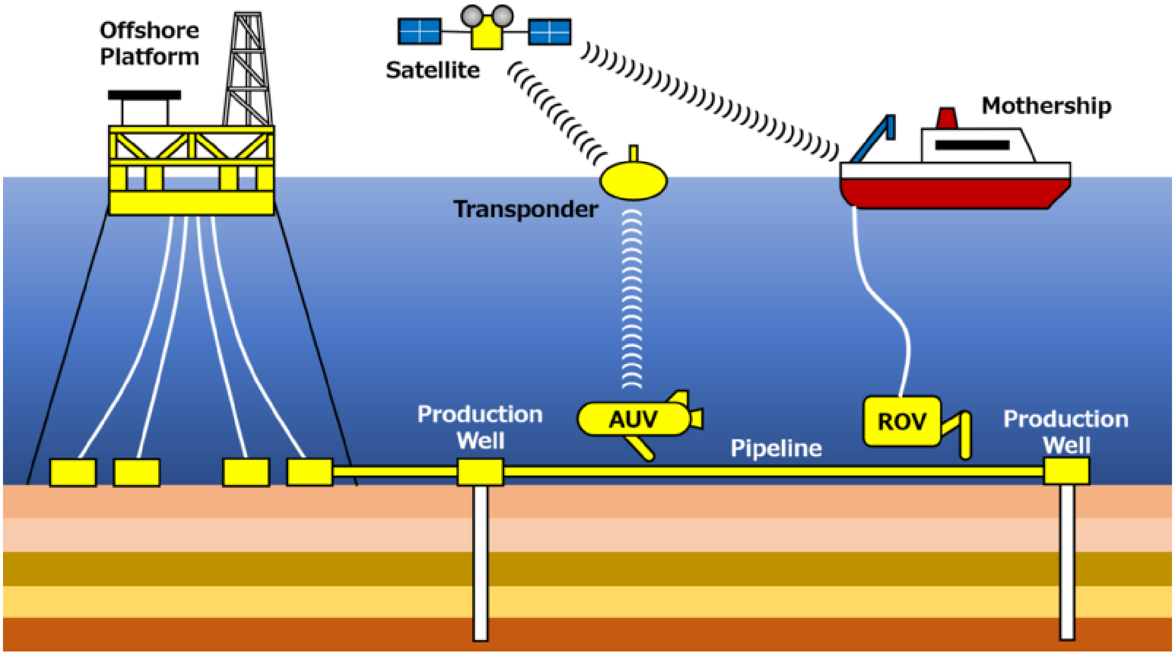


Figure 6: Application of ROVs and AUVs
(Source: http://dx.doi.org/10.1177/0278364912461059)

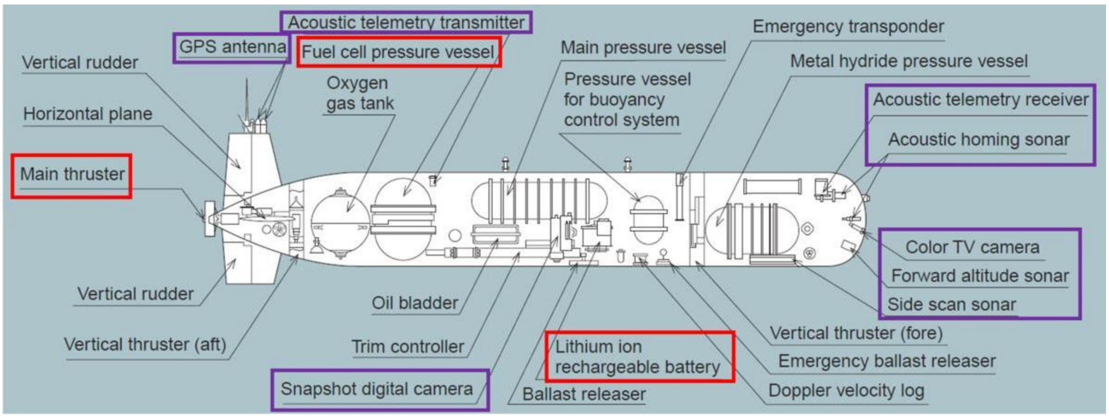


Image Source: Mitsubishi Heavy Industry
https://www.mhi.co.jp/technology/review/pdf/e431/e431024.pdf

Figure 7: Component Level Technologies in an AUVs

[20] Gov of US - International Trade Administration, https://www.trade.gov/underwater-technology

Port, Oil Rig and Cable Defence Systems. Israel Aerospace Industries (IAI) has developed and delivered comprehensive security and protection systems, known as the Integrated Underwater Harbour Defence and Surveillance System (IUHDSS) to the Indian Navy. The IUHDSS comprises surveillance, observation, surface and underwater sensing arrays that can detect, locate, and track various threats whether from small boats and submersibles, swimmer delivery vehicles (SDV), swimmers or divers. The system includes an advanced command and control system, a range of coastal surveillance radars, diver-detecting sonars, electro-optical sensors, and automatic threat identification systems. The central command and control system provides automatic integration of all sensors, creating a common situational picture for port defence.[21] An illustration of IUHDSS is at **Figure 8**. Ironically these shallow water systems had to be imported. In future India will ned deepwater systems to protect its oil rigs and communication cables in the East, West and Andaman coasts. iCET could be the launchpad for design and development of such underwater technology.

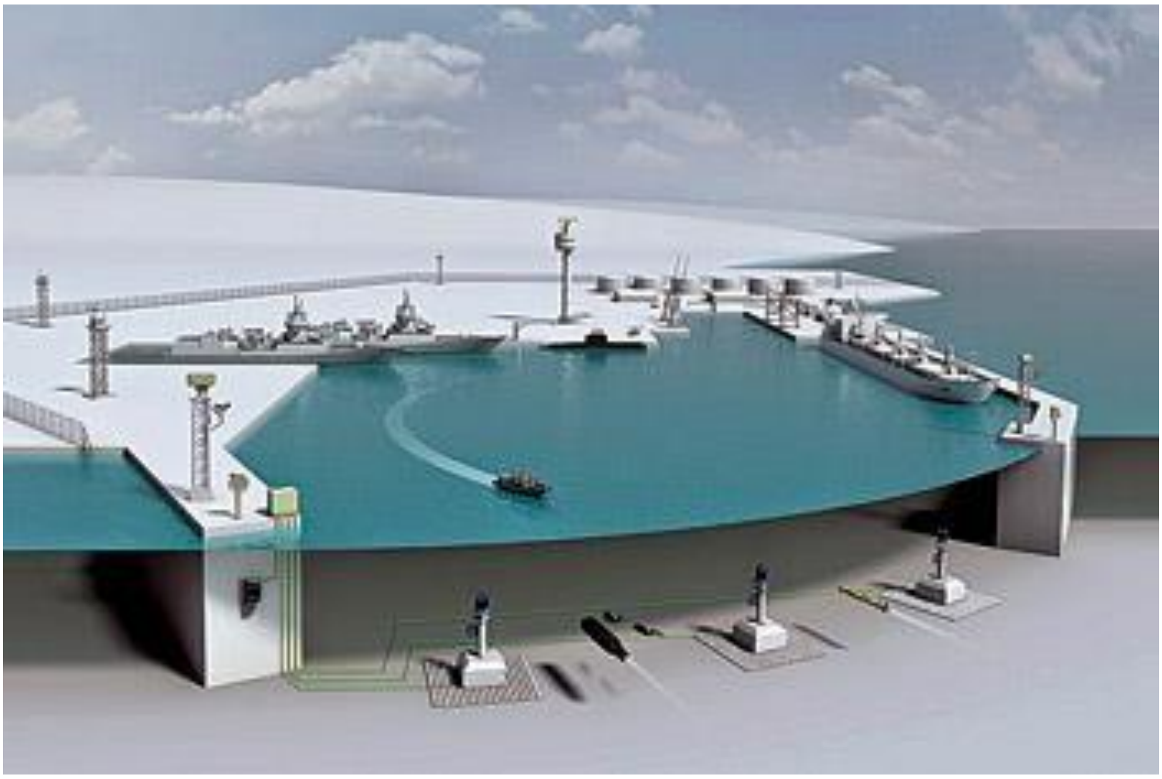


Figure 7: An IAI Harbour Defence System for India
(Source: IAI)

Synthesis of <u>ORGANISATIONS</u> with Policies

While maritime security and cyber security are the most notable policy fields for underwater security, a broader policy understanding is essential for a more comprehensive security of Commercial Offshore Infrastructure Systems (COIS). It will need ocean governance,

[21] Military Aerospace Internal Security, IAI completes Port Security and Defence Project in India, 16 February 2017, https://www.spsmai.com/military/?id=4316&q=IAI-completes-Port-Security-and-Defence-Project-in-India

digital policy and external action. **Figure 8** is a suggested collaboration between policies and agencies for underwater maritime security.

Ocean Governance – The expected outcome of ocean governance is **maritime security** of communication cable, rigs and oil and gas pipelines. Collaboration between the Indian Navy, Coast Guard, NIOT, MoPNG, and MoIC have to be cultivated for ocean governance. Currently, a modicum of collaboration is already provided by the Flag Officer Defence Advisory Group (FODAG) the Indian Navy and ONGC at offshore oil rigs in the Bombay High. A FODAG like organisation will have to be extended to included other agencies for tackling the emergent threats. The Indian Navy will be the natural and lead agency and executer for governance as it is their primary function. Whereas, security is a secondary function for other collaborating agencies. This is also the reason why such a collaboration can be clubbed as **Civil-Military-Fusion (CMF)**.

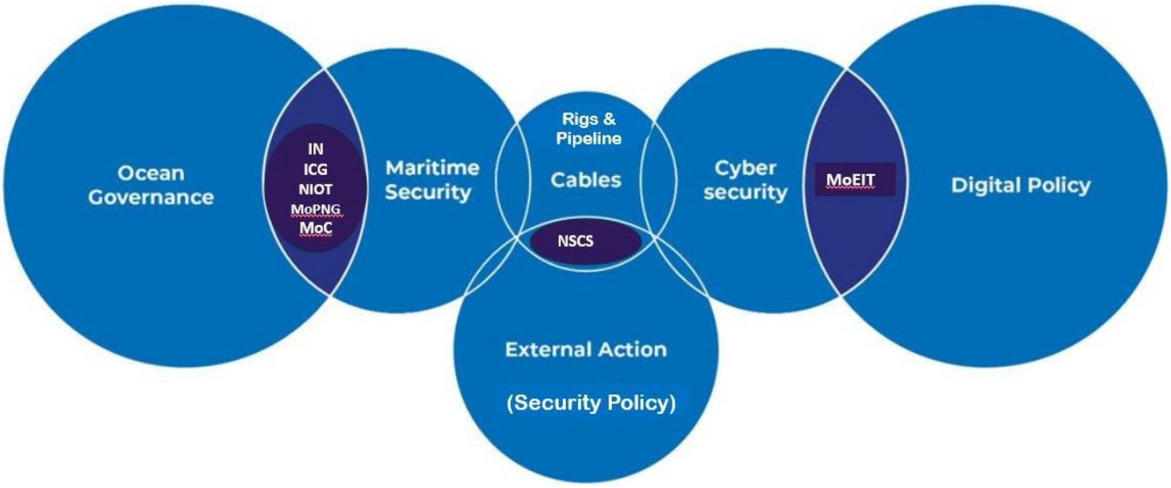


Figure 8: Collaboration between Policy and Agencies

Digital Policy - In the digital domain, insertion of foreign technologies is inexorable and omnipresent. There is a need to reduce vulnerabilities to external influence and dependencies as a potential security threat by harnessing control over key critical technologies and infrastructures. This will ensure **digital sovereignty** over data. The ***proposed Digital India Act 2023*** will need to mitigate the possibilities of sniffing and evolve with AI enable cyber-attacks. The MoEIT will be the primary coordinator to ensure cyber security of data traversing through the undersea cables.

External Action – This is the most important link between governance and policy making. To ensure national and transnational resilience of Commercial Offshore Infrastructure Systems (COIS), the NSCS will have to be the nodal points, directing actions, when necessary, especially in the even to contingencies. It will also have to review preparedness, and strategies periodically. It will also coordinate with foreign partners to mitigate possible global threats like sabotage and cybercrime.

Logistics of Underwater Security

From the perspective of operational-logistics, the enormity of sea area and depth to be protected will require considerable logistical support. Some are already available, while others will have to be created. For example, the primary method of navigation is not the GPS. For navigational accuracy of AUVs new array of transponders will have to be deployed. Maintenance of the deployed underwater surveillance devices will need equipment and specially trained people. Such equipment and trained people are available with the private sector. An effective CMF will be able to integrate these tools into underwater security.

Proposal 3 - iCET provides excellent option for creating skill corridors and development corridors for seamless innovation and production of scale. The underwater technologies include ROVs, AUVs, and Harbour/ Rig/ Cable/ Pipeline Defence Systems.

Proposal 4 - While maritime security and cyber security are the most notable policy fields for underwater security, a broader policy understanding is essential for a more comprehensive security of Commercial Offshore Infrastructure Systems (COIS). It will need ocean governance, digital policy and external action.

Ocean Governance – Collaboration between the Indian Navy, Coast Guard, NIOT, MoPNG, and MoIC have to be cultivated for ocean governance. Currently, a modicum of collaboration is already provided by the Flag Officer Defence Advisory Group (FODAG) the Indian Navy and ONGC at offshore oil rigs in the Bombay High. A FODAG like organisation will have to be extended to included other agencies for tackling the emergent threats.

Digital Policy - There is a need to reduce vulnerabilities to external influence and dependencies as a potential security threat by harnessing control over key critical technologies and infrastructures. This will ensure digital sovereignty over data. The proposed Digital India Act 2023 will need to mitigate the possibilities of sniffing and evolve with AI enable cyber-attacks. The MoEIT will be the primary coordinator to ensure cyber security of data traversing through the undersea cables.

External Action – This is the most important link between governance and policy making. To ensure national and transnational resilience of Commercial Offshore Infrastructure Systems (COIS), the **NSCS** will have to be the nodal points, directing actions, when necessary, especially in the even to contingencies. It will also have to review preparedness, and strategies periodically. It will also coordinate with foreign partners to mitigate possible global threats like sabotage and cybercrime.

Conclusion

The character of warfare has changed significantly in the past few decades. Belligerents do not feel encumbered to inflict pain on the civilian population as it strikes at the legitimacy of a government in power, unable to protect the lives and livelihoods of its people. Such methods are now employed by extremists against civilian targets for political aims. Violent extremists of all backgrounds frequently choose critical infrastructure systems essential for the normal functioning of day-to-day life within a country.

Commercial offshore infrastructure like undersea internet cables, power cables and oil and gas pipelines have become potential targets. The advantages of underwater commercial warfare are their deniability and the ability to disrupt the opponent economically before or during a war. The increasing vulnerabilities of these offshore assets have spurred the French to unveil a new Strategic Seabed Warfare Doctrine in February 2022. Immediately after, the Royal UK Navy reviewed its undersea vulnerabilities with private operators in May 2022.

States increasingly depend on commercial infrastructure and assets partially or completely located outside their jurisdiction and over which they have little or no control. Most of the critical infrastructure is owned by the private sector. Consequently, the State itself may no longer be able to ensure comprehensive security and may be largely dependent on the private sector. Therefore, a well-defined public/private partnership is essential to design effective policies on the protection of critical infrastructure.

The modern trends of warfare and sabotage have re-kindled the importance of Underwater Domain Awareness (UDA) after the Cold War. However, the mere absorption of advanced underwater technologies would be inadequate for optimal defence for critical underwater national assets, constituting an effective deterrence, or conducting an offensive/covert action against an adversary. There will be a need to synthesise the existing Organisations, Innovations, and Logistics, or the OIL of CMF for enhancing the UDA. This paper has explored the necessity of critical list of underwater infrastructure, and need to review India's underwater threats and preparedness. Further, it has suggested the necessity to build standards, deterrence, defence and resilience. Finally, the paper suggests that India-US collaboration on iCET provides a good window of opportunity to address the innovation gaps.

Critical List **-** There are several difficulties in determining which underwater assets should be considered *critical*. Because of the dense interconnections, it is often difficult to prioritise. Moreover, the criticality of an infrastructure might change over time. Decision-makers are often unwilling to assume the political risk of removing items from a *critical list* or including one due to financial constraints, resulting in the waste of resources. These ambiguities will hamper the development of security measures. A critical list on Commercial Offshore Infrastructure Systems (COIS) needs to be drawn based on their susceptibility to sabotage.

Susceptible to Sabotage 1 - Given the size of the discovery and proximity to the international shipping lane, the offshore energy infrastructure will be susceptible to sabotage. Hence, these fields need robust UDA for defence. Other high-yield offshore fields in the EEZ also may be included in the **critical list**.

Susceptible to Sabotage 2 - All 10 Single Point Moorings (SPMs) can be considered to be on the **critical list** as they handle major imports of crude from Very Large Crude Carriers (VLCC).

Susceptible to Sabotage 3 - All Offshore Trunk Pipelines (OTPs) need to be studied and a few might have to be included in the **critical list** based on cost-benefit analysis.

Susceptible to Sabotage 4 - The main subsea cables will be difficult to disrupt unless a belligerent nation becomes desperate. However, sniffing devices can be installed on them. However, the isolated cable branches that connect the landing stations to the main network will be especially vulnerable to physical damage from underwater sabotage and should be included in the **critical list**.

Proposal 1*:* National Maritime Security Coordinator (NMSC) needs to review India's undersea vulnerabilities with private operators and prepare:

(a) A well-defined public/private partnership is essential for a policy on drawing a **critical list** and protection of Commercial Offshore Infrastructure Systems (COIS). This needs to be reviewed periodically.

(b) A Seabed Warfare **Doctrine** and **Strategy** in collaboration with the Indian Navy. Collaborate with or learn from the French or Royal Navy. Integrate the INTEG, IFC-IOR, NIOT, or any other agencies necessary.

Proposal 2*:* There is a need to formulate the necessary doctrines, standards, and strategies for deterrence, defence, mitigation, and resilience against the damage of COVAs. These will include:

(a) **Mapping** - mapping of all major production rigs, SPMs, and offshore trunk pipelines.

(b) **Standards** - Future COIS will have to be built per the promulgated security standards.

(c) **Deterrence** - Deterrence will have to be accompanied by strategic signalling and punishment. India should, therefore, develop the undersea capabilities to punish an adversary. It will be necessary for effective strategic signalling.

(d) **Defence** – The defence of COIS will need a review of organisation, infrastructure, and logistics. It will also need a vulnerability assessment and a technology scan.

(e) **Mitigation** - Mitigation might involve the repair and revival of the damaged facility if found to be cost-effective. Agencies responsible for the mitigation of environmental disasters also have to be involved.

(f) **Resilience** - In the event of a major disruption of a COIS, suitable fallbacks, and alternatives have to be identified. Such contingencies have to be tested regularly to check for resilience.

<u>Proposal 3</u> - iCET provides excellent option for creating skill corridors and development corridors for seamless innovation and production of scale. The underwater technologies include ROVs, AUVs, and Harbour/ Rig/ Cable/ Pipeline Defence Systems.

<u>Proposal 4</u> - While maritime security and cyber security are the most notable policy fields for underwater security, a broader policy understanding is essential for a more comprehensive security of Commercial Offshore Infrastructure Systems (COIS). It will need ocean governance, digital policy and external action.

<u>Ocean Governance</u> – Collaboration between the Indian Navy, Coast Guard, NIOT, MoPNG, and MoIC have to be cultivated for ocean governance. Currently, a modicum of collaboration is already provided by the Flag Officer Defence Advisory Group (FODAG) the Indian Navy and ONGC at offshore oil rigs in the Bombay High. A FODAG like organisation will have to be extended to included other agencies for tackling the emergent threats.

<u>Digital Policy</u> - There is a need to reduce vulnerabilities to external influence and dependencies as a potential security threat by harnessing control over key critical technologies and infrastructures. This will ensure digital sovereignty over data. The proposed Digital India Act 2023 will need to mitigate the possibilities of sniffing and evolve with AI enable cyber-attacks. The MoEIT will be the primary coordinator to ensure cyber security of data traversing through the undersea cables.

<u>External Action</u> – This is the most important link between governance and policy making. To ensure national and transnational resilience of Commercial Offshore Infrastructure Systems (COIS), the **NSCS** will have to be the nodal points, directing actions, when necessary, especially in the even to contingencies. It will also have to review preparedness, and strategies periodically. It will also coordinate with foreign partners to mitigate possible global threats like sabotage and cybercrime.

***Disclaimer**: The views expressed in this paper are of the Author and not of MRC.*

***Funding**: No funding has been received for this research*

Author

Commodore (Dr.) Somen Banerjee (Retd.) is an Anti-Submarine Warfare specialist and has commanded three worships of the Indian Navy. He has served as Senior Fellow at the Vivekananda International Foundation (VIF), and the National Maritime Foundation (NMF) in Delhi. As an academic, he conceived and executed the idea of India joining the Indian Ocean Commission and the Djibouti Code of Conduct as an Observer.

He has authored two books - Maritime Power through Blue Economy and Sea of Collective Destiny: Bay of Bengal and BIMSTEC, published papers in Taylor & Francis, SAGE, and IFAJ, and written several issue briefs and commentaries. His recent paper, entitled Civil-Military Fusion, was published by CENJOWS in March 2023.

He is a MSc form the Madras University and a MPhil, PhD from Mumbai University in Defence and Strategic Studies.