CRITICAL INFRASTRUCTURES – OFFSHORE INSTALLATION PROTECTION

Martin A. Sebastian

Centre for Maritime Security & Diplomacy – CMSD

Version : Final Report

Date : January 2015
# Table of Contents

Abstract .............................................................................................................................................. 3

1.0 Introduction .................................................................................................................................. 4

2.0 Problem Statement ....................................................................................................................... 9

3.0 Literature Review .......................................................................................................................... 9

4.0 Area of Study ............................................................................................................................... 10

5.0 Objectives of study ....................................................................................................................... 10

6.0 Significance of the study ............................................................................................................ 11

7.0 Methodology .................................................................................................................................. 11

8.0 Limitations ..................................................................................................................................... 11

   Threats to the offshore industry ...................................................................................................... 11

   Framework for assessment of offshore security threats ................................................................. 15

   Links and overlaps between different types of threats ................................................................. 17

   International Approaches to Protect Offshore Installations ......................................................... 17

      Maritime Constitution. UNCLOS. Safety Zones ........................................................................ 17

      Treatise. SUA Protocol. ............................................................................................................. 21

      Regulatory. The ISPS Code ........................................................................................................ 22


   Security Risk Management – Australian Case Study .................................................................. 24

   Security Risk Management – Indian Case Study ....................................................................... 27

   Security Risk Management – Malaysia Case Study .................................................................... 29

9.0 Recommendation .......................................................................................................................... 31

10.0 Conclusion .................................................................................................................................. 32

11.0 Bibliography ................................................................................................................................ 33

# Table of Figures

Figure 1 Oil and Gas Fields in South East Asia .................................................................................... 4

Figure 2 Floating Production, Storage and Offloading Vessels .......................................................... 5

Figure 3 Floating Production Systems ............................................................................................... 5

Figure 4 Floating Storage and Offloading units ................................................................................ 5

Figure 5 Gomusut-Kakap FPS .......................................................................................................... 7

Figure 6 Gomusut-Kakap Infographics ............................................................................................ 9

Figure 7 Kiikeh FPSO ....................................................................................................................... 12

Figure 8 ................................................................................................................................................ 20

Figure 9 ................................................................................................................................................ 29

Figure 10 ................................................................................................................................................ 30
CRITICAL INFRASTRUCTURES – OFFSHORE INSTALLATION PROTECTION

Martin A. SEBASTIAN

Abstract

The growing reliance of the world’s economy on the energy market, especially fossil fuels as a source of well being makes the source of this energy vulnerable to politically motivated threats. These attacks are not far-sighted in this region as it has happened in other areas and with growing terrorist activities in the world, attacks on these installations to bring nations to their knees has been envisaged by risk consulting companies.

This study examines threats to offshore installations in the past and the proliferation of terrorist organisations and persistent separatist threats. It argues that in pursuit of national and commercial objectives, significant and often shared risks exist to Malaysia’s interest. It then looks at the existing security approaches regarding offshore installation and articulates on their effectiveness. It examines how these approaches are practiced by selected states and contrasts them with national approaches.

Finally the study provides risk mitigating options for Malaysia to be urgently and collaboratively considered by multiple actors such as government as in political will, agencies, cooperative entities, and the industry.
1.0 Introduction

“Critical infrastructure” consists of systems and assets so vital to the nation that their incapacity would harm the nation’s physical security, economic security, or public health. Critical infrastructure is often geographically concentrated; so it may be distinctly vulnerable to events like natural disasters, epidemics, and certain kinds of terrorist attacks. Disruption of concentrated infrastructure could have greatly disproportionate effects, with costs potentially running into billions of dollars and spreading far beyond the immediate area of disturbance. In Malaysia, key offshore installations have been deemed critical infrastructure.
Figure 2: Floating Production, Storage and Offloading Vessels

Figure 3: Floating Production Systems

Figure 4: Floating Storage and Offloading units
The offshore industry boom has been unprecedented in this region covering South Asia to Australasia. In South Asia, Southeast Asia, East Asia and Australasia there are 441 projected shallow (less than 300 metres) and deep water (greater than 300 metres) oil and gas fields involving thousands of exploratory drillings. A total of 387 new sub-sea wells have been contracted with a combined total of 70 floating production, storage and offloading vessels (FPSOs), floating production systems (FPSs), floating storage and offloading units (FSOs) plus over 14,000 kilometres of rigid and flexible flow lines. By far the greater proportion of the activity, 237 fields, are in the South China Sea.¹

Petroleum development and exploration sites are frequently located in remote areas and are characterised by poor transport connections and communication to the authorities and associated security infrastructure. Offshore installations are, in essence, hybrids of vessels and shore facilities. Though stationary, they are emplaced miles at sea away from shore-based support. Some are attached permanently to the ocean bottom. The capital investment for each installation can be enormous. The net revenues these facilities produce are equally impressive. Furthermore, one installation can handle production from as many as 24 subsea wells, which means vast quantities of crude oil are moved and controlled by a single facility.

Over the next 25 years,² oil and natural gas will meet approximately 60 percent of the world’s energy demand, and therefore, remain the prime source of energy for industrialised and developing countries. Since the oil and gas industry is a major component of national critical infrastructure, the probability for terror attacks on energy facilities, and a higher level of their sophistication, will undoubtedly have major impact to the nation. A terrorist attack on an offshore oil or gas platform has potentially devastating effects, both economic and environmental. Additionally, due to their isolation and distance from shore, offshore platforms are difficult to protect and extremely vulnerable to attack. In the current security environment, with the increased military capability of transnational terrorist organisations, preventing an attack on such a critical resource and industry is an extremely challenging endeavour.³

² op cit
Measures to deal with large-scale offshore oil and gas safety and security incidents are often not well developed. As evident elsewhere in the world, responses to catastrophic accidents with significant environmental and human security consequences are unlikely to be adequate. Vulnerabilities arise from the lack of capacity and the lack of coordination regimes to deter, respond to, and recover from incidents; and the lack of cooperative arrangements for maritime safety and security.\(^4\) While maritime piracy most often involves the boarding of vessels on the open seas, it raises a serious concern for owners or operators of offshore oil and gas platforms. If a small group of men in a fast speedboat, with small arms and knives, can commandeer a ship with ease, what could a well-trained and determined terrorist cell with sophisticated weapons and knowledge accomplish against a highly valued asset like an offshore rig?

![Figure 5 Gumusut-Kakap FPS](image)

Offshore platforms constitute high-value targets for terrorist attacks for two main reasons: (1) their importance to many states in generating energy and income and (2) the severe damage an attack on such assets may inflict. The offshore oil and natural gas industry is the world’s largest marine industry, and oil production alone amounts to more than $300 billion per year. Furthermore, natural gas and oil are a significant source of energy and an important source of income to states that control these resources. Consequently, an attack on an offshore oil or gas platform could not only interrupt a nation’s regular supply of energy, but also deprive it of an important source of income.

Yet, the results of a terrorist attack on an offshore platform are not limited to those discussed above. Such attacks, especially when aimed at oil platforms,

\(^4\) Lee Gordner, *Offshore Oil and Gas, Safety and Security in the Asia Pacific; The Need for Regional Approaches to Managing Risks*, RSIS Monograph no. 26, RSIS, 2014, Singapore
could also cause severe and long term environmental damage. Besides the devastating damage they may inflict, attacks on offshore platforms are tempting to terrorists for another reason: **these platforms are difficult to protect.** While attacks on military bases, government installations, and transportation routes are becoming more difficult to carry out due to increased security, **offshore platforms remain rather vulnerable.**

The isolation of these platforms, their distance from shore, and their widespread presence make it virtually impossible for states to protect them completely from attack. Moreover, these platforms are engaged in the exploration and storage of large quantities of flammable liquids or gases that may significantly increase the effect of an attack. Finally, offshore platforms are usually fixed to a permanent location and cannot conduct evasive maneuvers when attacked.

If auxiliary police onboard these installations are perceived as the best choice, they will be unprepared when attackers intrude into the security perimeter as the numerous small crafts are a daily phenomenon around these installations. Terrorists these days will not waste time going onboard as detonation to destroy these targets can be readily planted on the hull nearest to the sea surface. Although the motivation for attacks against energy production operations varies: to make a political statement, gain publicity, or simply destruction for its own sake. There are emerging studies making strong evidence that offshore platforms will eventually become a key target for terrorist organisations. An offshore platform is the only type of energy-related facility that can be attacked from the surface, underwater, or from the air. Therefore, it will be imperative for Petronas and related companies to be concerned with protecting vulnerable offshore installations. Typical threats to offshore operations involve hostile intruders in their perimeter using surface craft. Uninvited guests (such as fishermen) pose additional security risks. These threats can mask terrorists or others bent on targeting these installations or any of its associated fittings within the vulnerable perimeter.
2.0 Problem Statement

Malaysia is dependent on the oil and gas industry as it vital to the economic artery to the nation. Politically motivated crimes are the biggest threat to these installations as they will pose major economic and environmental impact to Malaysia. Currently, protecting are existent only onboard these installations and not perimeter security which may pose a major threat to these installations. To enable such perimeter protection, sound policies that encompass cooperative measures including political will, industry and agencies for risk mitigation and crisis response are vital. The Critical Infrastructure Standard Operating Procedures (SOP) does not address these types of protection.

3.0 Literature Review

This report presents an overview of terrorist and rebel attacks against the petroleum production infrastructure during the past three decades and provides an empirical basis for the development of scenarios for long-term defense and crisis management planning.

Attacks and Protection Priorities. United States CRS Report for Congress. 
This report examines the terrorist threat to maritime activities. Because oil tankers are constantly shipping exports from unstable locations where piracy and attacks are of concern, the report presents potential attack scenarios based on actual past attacks or potential attacks developed for maritime security exercises. It also notes the challenge to maritime security planners and implications for homeland security policy.

This article discusses the management of risks related to terrorism and focuses on North Sea oil and gas production and transportation systems and the European oil and gas markets. The author notes how threats to oil and gas markets have added to a perception of uncertainty regarding supplies, which may already have caused a higher market price for crude oil.

The author asks why there have not been more devastating attacks on energy infrastructure, despite the relative ease in carrying out essential infrastructure (EI) attacks. He points out that the biggest recent interruptions in energy supplies (i.e., Hurricane Katrina and the Moscow blackout of May 2005, which was due to a short circuit) were not caused by breaches to security due to intentional human agency. He notes the availability of softer tourist targets and the recent “hardening” of numerous energy targets, which has made it more difficult for terrorists to hit them successfully. He also notes some other interesting strategic considerations that factor into the targeting of EI.

4.0 Area of Study
The area of study covers terrorist threats to offshore installations in general focusing on vulnerable Malaysian offshore interests in the South China Sea

5.0 Objectives of study
The objectives of this study are to:

a) Examine politically motivated threats to the offshore industry;
b) Identify existing security regimes and available security approaches;

c) Illustrate approaches taken by selected states and contrast them with approaches taken by Malaysia; and

d) Recommend risk mitigating options for Malaysia to be urgently and collaboratively considered by multiple actors: government - as in political will, agencies, cooperative entities, the oil and gas industry, and security industry.

6.0 Significance of the study

There have been many studies illustrating threats to the offshore industry. However, comprehensive security to these installations are still lacking where Malaysia is concerned. This study will complement the legions of maritime security studies already in place so as to provide the government and industry a perspective on the need for offshore installation security.

7.0 Methodology

There were several methods used to achieve the objectives of this study. Literature reviews were used to gain knowledge of the subject matter. In addition, field visits were conducted to government agencies and security structures in Sabah to gain firsthand knowledge.

8.0 Limitations

The information for this study is limited to open sources, interviews with relevant agencies, and data received on restricted basis. The study is not for public consumption. The study focuses on the proliferation of terrorist organizations and the threat to vulnerable offshore installations like FPSOs.

Threats to the offshore industry

There have been surprisingly few major safety and security incidents given the geographical extent, scale, and expanding proliferation of offshore oil and gas exploration and exploitation activities and facilities around the world’s oceans over the past 50 years. However, numerous well publicised major safety and security incidents have produced significant consequences including loss of
human life and environmental disasters. Incidents have also resulted in significant economic impacts with national, regional and global consequences, at least in the short-term. Protection of the offshore oil and gas industry has been considered and debated for more than two decades. Those earlier calls to enhance security arrangements for offshore oil and gas installations were generally seen as unwarranted. That perception changed after the 9/11 terrorist attacks in the United States. Since then, safeguarding offshore oil and gas installations from external and internal threats has become imperative for many states especially those with significant offshore oil and gas operations that are vital to their national economic well being. Concurrently, the offshore oil and gas industry has become more aware of its strategic and economic importance in light of global energy security concerns that these concerns may potentially make offshore installations more attractive targets for attacks.  

When discussing the need for offshore protection, these installations comprise hundreds of one-off design elements, the loss of any one of which could bring operations to a sudden and costly halt. To devise appropriate security strategies, regulatory frameworks, and countervailing measures, and to provide adequate protection for offshore oil and gas installations, key decision makers in both government and industry must have a good understanding of the types of threats faced by these installations. These include the knowledge of various threat groups, the dangers they represent, their goals, intentions, offshore capabilities, opportunities, (in extreme cases past attacks) and interferences with offshore installations and possible future actions.

Attacks on offshore oil and gas installations are not a new phenomenon. The first attack on an offshore oil installation took place more than 100 years ago on 2 August 1899 off the shores of Santa Barbara, California. In the last 25 years

---

5 Mikhail Kashubsky, *Threats to Offshore Industry*, University of Canberra, Australia.
there have been about 50 attacks and security incidents involving offshore installations. These were carried out by various perpetrators with different motivations, objectives, tactics and capabilities. These include terrorists, insurgents, pirates, criminal syndicates, environmental activists, anti-oil activists and other types of protesters, hostile nation-states, and sometimes other unknown groups and individuals.

Offshore security threats may be classified in several ways based on different criteria. One such classification is based on geographical criteria, such as local or global, national or transnational. The attacks may come from various sources, individuals or groups internal or external to a state or a combination of both.

Piracy is one of the most visible security threats to offshore oil and gas installations as exemplified by activities in the Gulf of Guinea. In the last seven years at least six pirate attacks on oil and gas installations have been reported worldwide. Four of these took place in the Gulf of Guinea (the 1 April 2007 attack on Bulford Dolphin mobile offshore drilling rig; 3 May 2007 attack on FPSO Mystras; 5 May 2007 attack on Trident VIII offshore rig; 5 January 2010 attack on FSO Westaf). One attack took place near India in 2007 (the 22 March 2007 attack on Aban VII jack-up rig) and one near Tanzania in 2011 (the 3 October 2011 attack on Ocean Rig Poseidon drill ship).

Terrorism is another security threat to offshore oil and gas installations. Terrorists are extremely patient and utilise their covert skills to identify gaps within offshore platform protection and strategize to exploit security weaknesses to the fullest. Historically, most attacks on the open sea occur during the late evening and early morning hours during which time personnel vigilance is at its lowest and visibility from the platform of an approaching vessel is absolutely zero under certain environmental conditions. This plays to the strength and the most effective element of the terrorist strategy— the factor of surprise. To date, there have been two terrorist attacks against offshore installations. On 24 April 2004, in Iraq, Iraq’s Al Basrah Oil Terminal (ABOT) and the Khawr Al Amaya Oil Terminal (KAAOT) in the Persian Gulf were attacked nearly simultaneously by suicide boats. These attacks were allegedly carried out by the Al-Qaeda-affiliated Zarqawi network based in Iraq. Although largely unsuccessful from a physical asset standpoint, they did result in three fatalities and closure of the terminals for about a day, consequently resulting in lost revenue due to a production shut down.

Insurgency is motivated by political struggle and insurgents often cause destruction, damage and casualties to offshore installations. Insurgency groups are responsible for about one-third of attacks and security incidents involving
offshore installations, most of which occurred in the Gulf of Guinea. For example, between 2006 and 2010, the Movement for the Emancipation of Niger Delta (MEND) insurgency group carried out at least thirteen attacks on offshore oil and gas installations in the Niger Delta region of Nigeria as part of their campaign against the oil and gas industry to achieve fair distribution of oil profits and compensation from oil companies. These include the attack on the Bonga FPSO by militants about 90 nautical miles offshore on 19 June 2008 and the bombing of Forcados offshore oil loading terminal on 29 June 2009.

Among the top 10 terrorist groups making the news in the world, South East Asia’s Jemaah Islamiyah (JI) and it’s splinter group are part of this list. JI is part of the al-Qaeda’s branch in Southeast Asia and was responsible for the 2002 Bali bombing that killed 202 people. JI is based in Indonesia and was formed in the early 1990s with the aim of establishing a caliphate in the region. Many of its key figures, including spiritual head Abu Bakar Bashir and Bali bomb-maker Umar Patek have been captured. JI is a transnational organisation with cells in Thailand, Singapore, Malaysia and the Philippines. In addition to al-Qaeda, the group is also thought to have links to the Moro National Liberation Front, namely Nur Misuari.

Nur Misuari Breakaway Group (MBG). Nur Misuari, the founder of the Moro National Liberation Front (MNLF) which was the sole political representative for the Moros. After some skirmishes with the Philippine Army in 2000, he was listed as a terrorist and was arrested by the Malaysian government in 2001 on Jampiras Island. He was then deported to Philippines, where he was jailed. During his incarceration, MNLF went through a reform where he was ousted. In 2012, the Malaysian government facilitated a peace agreement with the Philippines and Moro Islamic Liberation Front (MILF), a splinter group of MNLF. Philippines, tired of the four decades of war is determined to bring peace to Mindanao. The peace process is going smoothly.

Misuari was responsible for the attacks in Lahad Datu and Zamboanga in 2012. He used the same modus operandi to influence others to pressure the target governments in bringing his long forgotten prominence to life. In Lahad Datu he manipulated the defunct self proclaimed Sulu Sultan to claim Sabah. The Royal Sulu Army (RSA) then intruded into Lahad Datu with catastrophic consequences to life and property. Misuari then went on to manipulate his arch Lieutenant, Uztaz Habier Malik and remnants of the MBG to attack Zamboanga. As a result of a counter offensive by the Philippines Army, Habier Malik was killed with many

---

6 http://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/views/251.
of the attackers. Misuari escaped and has since gone into hiding. He is currently facing charges with a few others in the Zamboanga court, and has vowed vengeance to both Philippines and Malaysia.

Abu Sayyaf, a criminal gang that operates in Sulu, is responsible for frequent kidnappings for ransom along Sabah’s coast and adjacent waters. Set up in 1991 with seed money from al-Qaeda, the group based in the islands of Basilan and Jolo, has been blamed for terror attacks in the Philippines, including bombings and kidnappings of Christians and foreigners. The group has long had links with al-Qaeda and recently pledged allegiance to Islamic State of Iraq and Syria (ISIS) which is waging an Islamic war in the Middle East and is calling for the formation of Islamic Caliphate throughout the world.

Malaysia is pioneering and is a champion of "the Global Movement of the Moderates" in the is fighting a growing security threat from international terrorists using it as a base, homegrown militants, and armed intrusions from Philippines rebels. The majority Muslim-populated Malaysia is seeking to intensify its clampdown of militant and terrorist cells brewing in the country, reported The Malaysian Insider. Deputy Home Minister Datuk Wan Junaidi Tuanku Jaafar told the website that more security officers would be recruited to aid various security agencies in intelligence gathering and espionage. Bukit Aman’s Special Branch Counter Terrorism Division principal assistant director Senior Asst Comm Datuk Ayob Khan has warned that their biggest fear now is “lone wolf” attacks in Malaysia. It said terror attacks need not be carried out by a group because it only takes one person to create chaos. Malaysians have been involved in many terrorist groups ranging from Abu Sayaff, MNLF, JI and recently ISIS. Separatists in Sabah and Sarawak (Sabah Sarawak Keluar Malaysia – SSKM) have been recruiting support asking for Sabah and Sarawak separation from Malaysia. Though they do not pose a threat, it will be important to assess their capabilities whilst protecting vulnerable offshore installations.

**Framework for assessment of offshore security threats**

The following set of factors shall be taken into consideration when assessing offshore security threats: a) geography and other enabling factors, b) motivations and objectives, and c) capabilities and tactics.

Geography and enabling factors. The security environment of the oil and gas

---

7 Fariq Zulkipli, It takes only one pro-Islamic State person to create chaos, says anti-terror cop, The Star, 2014.
industry is largely dependent on the overall security and stability of a given state or region. Security of offshore oil and gas installations should not be considered in isolation from the security and political environment of a state or region. Attacks on oil and gas installations occur in many countries, but oil companies face different security risks depending on the region where they operate. Oil companies that operate in high security risk areas such as conflict zones, and those that operate in economically and politically unstable countries are always at a higher risk of attack. In addition, some types of security threats, such as fish bombing around rigs are often concentrated in certain geographical areas as fishes are lucrative there. Therefore, geography and other enabling factors, such as the presence of armed conflict, are relevant for the purposes of assessing security threats to offshore oil and gas installations.

Motivations and objectives. Motivations for violent actions against offshore oil and gas installations vary. Attacks on and unlawful interference with offshore installations can be carried out for political, religious, financial, ideological or other reasons. Perpetrators do not always state their intentions and objectives, and it may be difficult to understand their motives. Some of the most common motives for attacking and interfering with offshore installations include achieving resource control and what attackers perceive as a fairer allocation of oil and gas revenues, such as in the case of attacks by insurgents in Nigeria. Resource control has been a big issue in Sabah and Sarawak where the states are demanding 20% revenue as opposed to the current 5%. Therefore, an understanding of motivations of the attackers is important in analyzing offshore security threats.

Capabilities and tactics. Capabilities and tactics of perpetrators vary. Offshore capabilities of perpetrators have a bearing on the types of attacks they might attempt. Attacking some offshore installations can be quite complex requiring extensive offshore capabilities, planning, and preparation. Some adversaries have well-developed offshore attack capabilities using a variety of methods and means including various kinds of weapons ranging from pistols to rocket-propelled grenades to improvised explosives devices, sophisticated equipment including high-speed boats, and navigational tools. For example, a group of insurgents with experience and training in attack tactics, access to advanced equipment and weapons may mount an entirely different type of attack against the same offshore installation than a group of environmental activists who do not necessarily have specialized training or access to advanced equipment. Tactics used by various perpetrators include bomb threats, threats of attacks and armed intrusion of offshore installations, abduction of workers, hostage-taking, and the use of explosives and bombings of offshore installations. The most common
tactic of insurgents appears to be armed intrusion and it has been suggested that future attack tactics may include using ships as weapons to ram offshore oil and gas installations and conducting underwater attacks. Different threat groups may employ different attack tactics depending on their capabilities. Accordingly, in assessing offshore security threats, it is important to have an understanding of offshore capabilities and tactics of different threat-groups.

**Links and overlaps between different types of threats**

One of the difficulties in assessing offshore security threats is that there are overlaps and relationships between different categories of offshore security threats. Violent non-state actors are motivated by a range of objectives and the distinction between political and criminal motivations is becoming increasingly blurred.\(^8\) For example, there are links between organized crime and insurgents. Insurgents may engage in criminal activities, sometimes in cooperation with organized criminal groups, to fund their operations and campaigns. There can be possible affiliations between terrorist groups and insurgents, particularly when these groups have similar ideological views or strategic objectives. There can also be links between piracy and insurgency. The practical difficulty of distinguishing insurgency from terrorism and piracy is that often insurgents employ terrorist or piratical tactics to achieve their objectives.\(^9\) Insurgents often operate in the same areas as pirates, and in some regions both piracy and insurgency are serious problems which sometimes tend to overlap.

**International Approaches to Protect Offshore Installations**

**Maritime Constitution. UNCLOS. Safety Zones**

The 1982 United Nations Convention on the Law of the Sea provides the backbone for offshore governance by coastal states and those navigating the oceans. This treaty does not only cover zone coastal states’ offshore areas, but also provides specific guidance for their rights, responsibilities, and jurisdiction in the concentric zones as well as basic legal basis for protecting offshore installations. Offshore platforms are typically located in one of a coastal state’s three main zones: the territorial sea, contiguous zone, or exclusive economic zone (and in special circumstances even further on a state’s continental shelf). Within the territorial sea, the coastal state has full enforcement jurisdiction over

---


all security matters and can take enforcement measures against any vessels not in innocent passage. In the contiguous zone, the coastal state has enforcement powers over law enforcement issues which affect its domestic stability, specifically customs, fiscal, immigration, health, and sanitary issues. Thus, within these two zones the coastal state has broad jurisdiction and ability to secure its offshore assets.

In the Exclusive Economic Zone (200 nautical miles from the baseline) however, a coastal state’s rights are more limited. There, the state has full sovereignty to exploit living and non living marine resources and take protective measures to maintain those operations, yet it cannot generally restrict others’ right to innocently transit the waters.

Although vague, UNCLOS includes a special clause which provides coastal states with the ability to harden offshore structures in the EEZ and beyond* by creating a 500 meter safety zone around them. Article 60 of the Convention stipulates:

"... The coastal State may, where necessary, establish reasonable safety zones around such artificial islands, installations and structures in which it may take appropriate measures to ensure the safety both of navigation and of the artificial islands, installations and structures.

- The breadth of the safety zones shall be determined by the coastal State, taking into account applicable international standards. Such zones shall be designed to ensure that they are reasonably related to the nature and function of the artificial islands, installations or structures, and shall not exceed a distance of 500 metres around them, measured from each point of their outer edge, except as authorized by generally accepted international standards or as recommended by the competent international organization. Due notice shall be given of the extent of safety zones.

- All ships must respect these safety zones and shall comply with generally accepted international standards regarding navigation in the vicinity of artificial islands, installations, structures and safety zones..."

In essence, such a safety zone is an area of restricted navigation. The zone itself may or may not be marked, monitored, or enforced, but ships are expected to
refrain from navigating close to offshore structures. Any uninvited encroachment on the zone by large vessels, small craft, individuals, or jettisoned material is considered a definite safety hazard and potential security concern.

Within the zone the coastal state and potentially the offshore operations team can restrict navigation and take reasonable measures to apprehend and even penalize violators. In more serious situations, especially regarding potentially hostile approaches, they can take measures to prevent approach to the structure including actions to disable the vessel should it ignore good faith efforts to stop it without the use of force. The safety zone was designed with navigational hazards in mind, not prevention of a deliberate hostile attack, whether that is ramming a vessel laden with explosives into a platform or raiding the platform for piracy or any other purpose. As shown in the above illustration, 500 meters is not a large security space within which to operate a defensive strategy. It is not broad enough, for example, to immobilize large ships, which can take some miles to slow down to a complete stop.

The notion of safety zones around offshore platforms was born in the International Law Commission’s (ILC) deliberations on the legal regime pertaining to the Continental Shelf in the early 1950s.\(^\text{10}\) In its report to the UN General Assembly in 1956, the ILC recommended that coastal states be allowed to construct and maintain installations on their continental shelf and to establish safety zones at a “reasonable distance” around these installations. In the ILC’s view, the establishment of safety zones was necessary due to the “extreme vulnerability” of these installations and the need to protect them from shipping.

The ILC further suggested that states be authorised within these safety zones to take measures necessary for protecting offshore installations. As for the breadth of those zones, although the ILC did not consider it essential to specify the size of the safety zones, it stated that generally “a maximum radius of 500 metres is sufficient for the purpose.”\(^\text{11}\) This proposed limit was not based on extensive research on methods for combating threats unique to offshore installations. Instead, it was borrowed from national legislation concerning the protection of oil production facilities on land from the dangers of fire.


\(^{11}\) Ibid
For reference, a Harvard University analysis shows that a vessel traveling at twenty-five knots (29 mph) would cross the outermost limit of the zone and make contact with the platform in about 39 seconds. This timeframe is so limited that it is impossible to realistically identify the vessel as friend or foe, attempt to make communications contact, await response, and if no response or unsatisfactory response is given, then dispatch a security team (which may or may not be onboard the platform) to intercept the vessel if possible, let alone request assistance from state law enforcement or military. This exposes a significant gap in the regulatory framework governing offshore maritime security and warrants further examination and tightening to match today’s threat environment.

While the wording of UNCLOS does allow for extending the breadth of this zone: “safety zone ... shall not exceed a distance of 500 metres...except as authorized by generally accepted international standards or as recommended by the competent international organization.” Increasingly, creeping maritime security jurisdiction in the post-9/11 paradigm has given coastal states substantial latitude to take security measures in their EEZs in the name of national security, based on national decrees or customary international law. And of course the right of self defense to protect life and property from imminent risk of harm is a universally recognized concept. The risk of damage and the subsequent security or environmental consequences that could result from a hostile approach to or takeover of a platform are far too great to ignore. For isolated locations far out at sea, clarifying and possibly enhancing the legal regime which governs security jurisdiction for offshore platforms is crucial to design and deliver appropriate responses to varied threats.

The increased likelihood of unauthorised activities in close proximity to oil and gas installations (e.g., fishing, diving or tourism) presenting safety and security

12 http://cimsec.org/offshore-installations-practical-security-legal-considerations/7872
risks, is a concern in many areas. The mandated 500 meter safety zone is not wide enough to provide adequate space to warn or intercept intruders. This matter was considered at the 56th session of the International Maritime Organization (IMO) Sub-Committee on Safety of Navigation in July 2010, with guidelines to increase awareness and routing around the zones proposed, but not to increase the size of safety zones.

Treatise. SUA Protocol.

The Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (SUA PROT) is a multilateral treaty by which states agree to prohibit and punish behaviour which may threaten the safety of offshore fixed platforms, including oil platforms. Malaysia has acceded to this treaty. The Protocol criminalises the following behaviour:

1. Seizing control of a fixed platform by force or threat of force;
2. Committing an act of violence against a person on a fixed platform if it is likely to endanger the safety of the platform;
3. Destroying a fixed platform or damaging it in such a way that endangers its safety;
4. Placing or causing to be placed on a fixed platform a device or substance which is likely to destroy or cause damage to the ship or its cargo;
5. Injuring or killing anyone while committing 1–4;
6. Attempting any of 1–5;
7. Being an accomplice to any of 1–6; and
8. Compelling another through threats to commit any of 1–7.

The Protocol was concluded at the same time as the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention). As of 2014, the Convention has 151 state parties, where the Protocol sets out the principle of aut dedere aut judicare—that a state party to the treaty must either (1) prosecute a person who commits one of the offences or (2) send the individual to another state that requests his or her extradition for prosecution of the same crime.
Regulatory. The ISPS Code

The December 2002 International Maritime Organization (IMO) Conference of Contracting Governments adopted The International Code for the Security of Ships and of Port Facilities (ISPS Code) and International Convention for the Safety of Life at Sea, 1974 (SOLAS 74) amendments to Chapter XI-1 and a new Chapter XI-2, to be implemented by 1 July 2004. SOLAS 74 was extended to cover port facilities noting that “provisions relating to port facilities should relate solely to the ship/port interface”. Of direct relevance to the oil and gas industry was the inclusion of cargo ships of 500 gross tonnage and upwards, mobile offshore drilling units (MODU) and requirements that Ship Security Plans should contain provisions for a ship when interfacing with “fixed or floating platforms or a mobile drilling unit on location”. IMO Conference Resolution 7 recognised the need to establish measures to enhance the security of mobile offshore drilling units on location and fixed and floating platforms not covered by Chapter XI-2 of SOLAS 74.

However, the ISPS Code and SOLAS 74 fell short of encompassing such offshore facilities. The IMO encouraged Contracting Governments, when exercising their responsibilities for mobile offshore drilling units and for fixed and floating platforms operating on their Continental Shelf or within their Exclusive Economic Zone, to ensure that security arrangements applying to offshore facilities would allow interaction with ships covered by the Convention. Governments were requested to inform the IMO of any actions they have taken in this respect. The IMO, in responding to requests for advice on the application of SOLAS Chapter XI-2 and the ISPS Code to FPSOs and FSUs reiterated the view that such facilities were not “ships subject to the provisions of the ISPS Code”. However they should have security procedures in place to prevent contamination of ships and port facilities subject to the Code. Further, the IMO advised that:

As FPSOs and FSUs operate as part of offshore oil production facilities, it can be expected that the State on whose continental shelf or within whose Exclusive Economic Zone the activity is being undertaken will have developed appropriate security measures and procedures under its national law to protect offshore facilities.

13 Facilities are generally offshore fixed platforms in water depths ranging up to 1,000 feet deep whose primary purpose is the exploration, development, and/or product of offshore petroleum reserves. This definition also includes novel floating design such as, Tension Leg Platforms (TLP), Floating Production Facilities (converted MODUs) and Floating Production Storage Offloading units (FPSO).
The onus is clearly placed on nations to provide legislation that addresses security arrangements for offshore oil and gas facilities operating within a national EEZ or on a continental shelf.


The above document provides mechanisms for risk management communication and cooperation. The Standard presents internationally accepted best practice frameworks and guidelines for action on risk management. ISO 31000 is widely used by industry around the world, is mandated for use in many jurisdictions and by international industry bodies, and is increasingly being adopted for use by governments. Risk management is fundamentally about adopting a structured approach to dealing with uncertainty. ISO 31000 presents a framework that is intended to help “ensure that risk is managed effectively, efficiently and coherently...in a systematic, transparent and credible manner”. Major offshore oil and gas safety and security incidents will have security, economic, environmental and human consequences that are likely to be felt beyond individual national jurisdictions and company operations. This scenario is particularly likely in the interconnected littoral geography found in parts of the Asia Pacific region. Managing the risks to major offshore oil and gas activity has regional, national and industry dimensions. The risk management framework presents a systemised way to identify, analyse, evaluate and treat risks to support strategies for major safety and security incident prevention, response and recovery. Formal risk management approaches to offshore oil and gas security are already in place in some regional jurisdictions, for example Australia but are not yet widely embraced in Asia. A significant benefit of governments adopting formal risk management approaches is that they are well understood and widely used by industry; effective communication and shared responsibilities for managing risk is, therefore, facilitated.

The requirements of effective risk management at the regional and national level includes, in summary:

- Defining the risk context;

---

• Identification of key risks and vulnerabilities that may impact safety and security;

• Rigorous and ongoing assessments by competent and experienced individuals and responsible organisations of the likelihood and consequences of the risks arising;

• The formulation of policy and actions to mitigate risks so that they are reduced to as low as reasonably practicable;

• The acceptance of residual risk (i.e. risk that is unable to be fully mitigated) by responsible authorities, where necessary;

• Formulation of risk prevention, response and recovery options, arrangements, processes and mechanisms; and

• Consideration of regional collaborative arrangements and mechanisms to deal with cross-jurisdictional and multi-jurisdictional risk management and incident prevention, response and recovery.

Other risk management elements that require consideration at the regional and national levels include enterprise risk management (ERM) and the difficult area of understanding and managing cumulative, accumulated or aggregated risks in the offshore oil and gas sector. ERM entails managing the regional, national and/or organisational risks that can impact upon the viability of an enterprise. ERM requires strategic perspectives that comprehend linkages between diverse and inter-related aspects of an endeavour, for example: political, economic, security, environmental, social, cultural, safety, technological, and international relations factors. In the complex world of offshore oil and gas activity all of these areas are relevant as they present risks to the attainment or protection of national and commercial objectives and interests.

Security Risk Management – Australian Case Study

A comprehensive review of the effectiveness of Australia’s approach to offshore oil and gas security was commissioned by the Australian Government in 2011–2012,¹⁵ some eight years after imposition of a mandatory security-regulated

regime. The outcome of that review was released to the public on 25 June 2012.\(^{16}\) The Offshore Oil and Gas Resources Sector Security Inquiry Report\(^ {17}\) advised that a risk-based, intelligence-led approach to security oversight underpins Australia’s offshore oil and gas security regime.\(^ {18}\)

The Australian response to offshore oil and gas industry security must be seen in the context of broader, whole of government approaches to dealing with the threat of terrorism. The responsibilities, authorities and mechanisms to prevent, and if necessary manage acts of terrorism and their consequences are outlined in the National Counter-Terrorism Plan (NCTP). Security of the Australian offshore oil and gas industry is affected by many aspects of the NCTP and related arrangements, summarised as follows:

- Australian government responsibilities include maintenance of counter-terrorism capabilities, prevention strategies and operational responses to threats, leading the management of intelligence, and determining and promulgating the national counterterrorism alert level.

- The Australian government regulates security arrangements for Australian ports, port facilities, ships and offshore oil and gas facilities.

- Responsibilities for critical infrastructure (CI) protection are outlined. These apply to offshore oil and gas facilities that contribute significantly to meeting Australia’s energy needs and/or contribute significantly to export income. A National Committee on Critical Infrastructure Protection (NCCIP) coordinates arrangements with a Critical Infrastructure Advisory Council (CIAC) that includes energy industry advice. A Business Government Advisory Group on National Security is also in place.

- A Trusted Information Sharing Network (TISN) has been established to facilitate the sharing of security information (including intelligence, where

---


necessary) between the Australian Government and owners and operators of CI.

The amended *Maritime Transport and Offshore Facilities Security Act (MTOFSA) 2003*28 and *Maritime Transport and Offshore Facilities Security Regulations 2003*29 provides the remedy. The Act and Regulations require that ISPS Code requirements similar to those for ships and port facilities apply to offshore oil and gas facilities and offshore service providers operating under Australian jurisdiction.

The MTOFSA and Regulations established the regulatory framework for Australian offshore oil and gas security. Compliance by offshore industry participants is mandatory, just as Australia, as a Contracting Government, is obliged to set in place arrangements to comply with the ISPS Code and SOLAS 74 amendments. All offshore industry participants are required to have Government approved offshore security plans in place. Failure to comply satisfactorily is an offence. Approval for offshore security plans that are deemed to be inadequate can be cancelled. Cancellation of an offshore security plan effectively means the industry participant can no longer operate.

Security risk assessment and management of risk management fundamentally underpins the offshore oil and gas industry security processes in the Australian context. Offshore facility operators are required to have a valid security risk assessment as part of an offshore security plan that must include: (i) details of the risk management process adopted; (ii) the risk context or threat situation for each facility; (iii) identification of possible risks or threats, with the likelihood and consequences of their occurrence; and (iv) identification of possible risk treatments and their effectiveness in reducing risks and vulnerabilities.

The Australian government issues and updates Offshore Oil & Gas Risk Context Statements (OGRCS) and the Offshore Security Assessments Guidance Paper (OSAGP). The OGRCS provides a contextual and dynamic overview of the transnational terrorism security environment relevant to the Australian oil and gas industry. The document is intended only to supplement threat and risk assessment information from other sources. The onus remains upon specific owner/operators to determine their own security risks utilising risk assessment processes. These documents outline a coordinated approach to security risk management from a national level through enterprise and organizational levels.
down to individual operations and operators. Specific risk management guidance for the oil and gas sector is provided utilising generic approaches defined by Australian and New Zealand risk management standards and guidelines, which are effectively the same as ISO 31000.

The OSAGP provides concise guidance on security risk assessment processes to assist offshore oil and gas operators to meet the security assessment requirements of the MTOFSA and Regulations. Clearly it is in the interests of industry participants to follow the processes outlined. They are obliged to submit offshore security plans to the Australian Government for approval. Notably, the prescribed process is consistent with risk management processes practiced across the industry for other aspects of operations, including safety. The OSAGP recognises that risk analyses can be qualitative, quantitative or semi-quantitative. It advises that qualitative risk analyses are sufficient for offshore oil and gas security risk assessments as they provide satisfactory indicators of risk levels. Guidance is provided on risk categories, likelihood and consequence estimates, and risk treatments and other factors in the risk management process, along with basic templates that may assist those preparing risk assessments.

**Security Risk Management – Indian Case Study**

The government of India has plans to extend the "safety zone" around the country's offshore oil and gas installations to 5 nautical miles (or 8 km) from the existing 500 meters to strengthen the security and prevent sabotage and terrorist attacks on the offshore installations.19 The 500 meter safety zone around offshore installations in the exclusive economic zone (EEZ) of India was set in 2013 and forms part of the Petroleum and Natural Gas (Safety in Offshore Operations) Rules, 2008. The country's largest oil and gas exploration company, the state-owned ONGC that has 190 offshore installations, has confirmed asking the Petroleum Ministry to extend this 500 meter safety zone.

The officials of private oil and gas companies including Reliance Industries Ltd (RIL) and Cairn India Ltd, having major oil and gas installations on the western and eastern shores, have similar opinion on the need to have a larger designated area around the offshore installations.

The ONGC Chairman and Managing Director RS Sharma said that they have

patrolling boats but due to safety concerns they do not keep firearms. He added if a vessel comes close to their platforms and blows, it can cause a lot of damage and the existing 500 meter safety zone leaves very little time for the company to react or inform the coast guard or the Navy. To strengthen the security of India’s offshore oil and gas installations and prevent sabotage and terrorist attacks on them, the government is extending the “safety zone” around the installations to 5 nautical miles (or 8 km) from the existing 500 metres. The country’s largest oil and gas exploration company, the state-owned ONGC that has 190 offshore installations confirmed that it has been asking the Petroleum Ministry to extend this 500 meter safety zone.

The officials of private oil and gas companies including Reliance Industries Ltd (RIL) and Cairn India Ltd having major oil and gas installations on the western and eastern shores echoed similar sentiments on the need to have a larger designated area around the offshore installations.

“Although we have patrolling boats, due to safety concerns, we do not keep firearms,” ONGC Chairman and Managing Director RS Sharma told Hindustan Times. “If a vessel comes close to our platforms and blows, it can cause a lot of damage. The existing 500 meter safety zone leaves us with very little time for the company to react or inform the coast guard or the navy."

A senior official of the Oil Industry and Safety Directorate in the Petroleum Ministry said, “We have supported the proposal but also feel that this would result in putting extra monitoring liability on the operators.”

“We welcome the proposed initiative of the government in strengthening the security area around nation’s strategic oil and gas assets,” said P.M.S. Prasad, head of RIL’s oil and gas operations. “This will help deal with the perceived challenge from individuals with questionable motive close to the vicinity of offshore installation under cover.”

Refuting these fears a senior private company official said, “Cost will not increase much whether it is 500 meters or 5 nautical miles. If the safety zone is increased, we will get more reaction time. In the 500 meters safety zone, nothing can be done.” The Coast Guard is the principal agency for enforcement of provisions of all national enactment in force in the maritime zones of India and provides following services to the Nation and marine community ensuring safety and protection of the artificial islands, offshore installations and other structure in our maritime zones.
Security Risk Management – Malaysia Case Study

Strategic Levels. Protection of national key infrastructures come under the purview of the Chief Government Security Office (CGSO).\(^{20}\) The document that discusses national key infrastructures is called Arahan Tetap Sasaran Penting (ATSP) 1993. The Government Security Officers are appointed based on the 15 June 1957 Terms of Reference in the Prime Minister’s Department through the “Confidential General Circular No. 1, of 1958, Government Security Officer, Federation of Malaya”.

According to the Strategic Plan of CGSO 2013-2017, the main function of the post is to advise the protection of national key infrastructures in the federal, state departments and agencies from espionage and sabotage.\(^{21}\)


The ATSP is seen as a general Standard Operating Procedure (SOP) which does not have a capstone policy. It has a “one size fits all” approach which makes it difficult where land and sea approaches to security are seen in one lens. With this concern in mind, CGSO has embarked on efforts to amend the ATSP and it is timely that a policy is discussed in a larger sense with a larger audience. Policy recommendations will then be a useful template.

Operational Level. When discussing on the protection of offshore installations, one cannot overlook the industry-agency nexus where cooperative security arrangements will be important. Petronas caters for security arrangements working with the Police on the platforms whilst the Navy, Air Force, and the Maritime Enforcement Agency (MMEA) provide for external security. Currently there are no foreseen threats; however, 70% of the fishing fleets around installations are foreign. Dangers posed by these vessels are fish bombing, naked fires and possible carriage of explosives. Outreach programmes conducted with local fishermen to keep out of the perimeter cannot outscore the lucrative catches within the perimeter of these installations. Offshore staff have perennially raised concerns on this matter.

---

22 Discussions with MMEA, Sabah, October 2013.
Petronas has a number of sensors installed on the platforms although it will be interesting to note the response mechanism in any eventuality. Here is where the gap lies between the size of the maritime real estate (which houses the vulnerable platforms and the assets) versus the number of assets to provide round the clock perimeter security or even timely response in the event of an attack. The Navy and Air Force for instance are combat orientated and not constabulary focused whilst the MMEA has limitations on size, number of assets and funds to maintain presence as their fuel consumption is hedged. These shortfalls need to be urgently addressed when reforms are discussed pertaining to offshore installations security. Threat analysis and existing security regimes need to be considered urgently to identify vulnerabilities, prepare risk mitigation mechanisms and consequence management procedures. The management of three major events in Malaysia: the Lahad Datu incident, the loss of MH 370, and the recent floods on the east coast have much to say about the trust gap between the government, industry, and the people. Therefore, it is timely that the protection of offshore installations be given much thought.

Tactical. There are many scenarios that can be envisaged when it comes to threat to offshore installations. One major threat is the hijacking of a cruise liner to ram on the FPSO, FSO or FSRU. The second threat is the masked carriage of explosives in the Offshore Support Vessels (OSV) and finally the laying of magnetic charges on the hulls. It will be impossible to stave off these attacks until it is too late.

9.0 Recommendation

A policy which identifies vulnerabilities, risk mitigation measures and consequence management is to be developed as a capstone document to affect change to the current Arahan Tetap Sasaran Penting (ATSP) 1993. In the interim, cooperative security architectures culminating in the oil and gas industry, security industry, and agencies to provide perimeter security from three to five nautical miles as a deterrent around FPSO, FSO and FPS are required.

23 Ibid.
10.0 Conclusion

The report provides a brief illustration of the importance of the oil and gas industry as the lifeblood of the nation. It further articulated on the type of vulnerable targets and the possible attacks which can bring the nation to her knees and create irrecoverable environmental damage. Potential threats in the growing proliferation of terrorists and separatists in Sabah pose a grave threat to vulnerabilities where a vulnerability assessment, risk mitigation and consequence management policy has to be in place. The number of security regimes addressing security approaches and the Best Practices by nations are already available.

The potential threats to offshore installations cannot be ignored any longer. Agencies, working with interim security industries and larger safety zones could certainly improve the ability to protect offshore platforms from attack. First, they would enhance the ability to distinguish potential threats that warrant further examination, such as vessels that have entered the safety zone without permission, from other maritime traffic. This would be especially valuable in areas with dense maritime traffic. Second, larger safety zones would provide security personnel on board the platform, and possibly the coastal state’s military or law enforcement forces operating in that area, with a longer reaction time to potential attacks. More time from the moment the safety zone was infringed to the moment the infringing vessel approaches the platform means a better ability to employ defensive measures, such as questioning the vessel’s motives and engaging it upon determination of hostile intent.

Indeed, one could argue that no matter how large safety zones are, they will never be large enough to protect offshore platforms from long range weapon systems. Nonetheless, an expansion of safety zones for example, to a distance of three to five nautical miles could significantly promote the ability to protect offshore platforms from the most common and available methods of attacks, especially the use of vessels mounted with explosives.

Risk mitigating architectures are necessary to create domain awareness and inform on the possible risks posed. Collaborative and cooperative arrangements are to be put in place in order to train towards an event and to have a calibrated response to prepare for contingencies.
11.0 Bibliography

3. Arahan Tetap Sasaran Penting (ATSP) 1993
6. Lindsay, M, The Security Threat to Oil Companies in and out of Conflict Zones, Business Briefing: Exploration and Production: The Oil & Gas Review. 2005
10. Schmid, A.P, Targeting oil and other energy resources and infrastructure. MIPT, 2007
14. Mikhail Kashubsky, Threats to Offshore Industry, University of Canberra, Australia, 2013
17. Lee Gordner, Offshore Oil and Gas Safety and Security in the Asia Pacific - The Need for Regional Approaches to Managing Risks, RSIS Monograph 32. 2014