

Protection of the offshore oil and gas industry has been considered and debated for more than two decades. However, 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. 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. At the same time, the offshore oil and gas industry has become of greater strategic and economic importance in light of global energy security concerns. This may have potentially made offshore installations more attractive targets for attacks.

In order to devise appropriate security strategies, regulatory frameworks, 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 offshore installations including knowledge of various threat groups, the dangers they represent, their goals, intentions, offshore capabilities, opportunities, past attacks and interferences with offshore installations and possible future actions. However, the media and some writers tend to generalize threats often giving them a 'label of terrorism' which is misleading and obscures the nature of different types of threats faced by offshore oil and gas installations. This also creates a perception that terrorism is the most significant threat to offshore oil and gas installations which is not necessarily the case.

This article shall focus on offshore security threats. It will identify the types of threats to offshore installations, discuss potential links and overlaps between different types of offshore security threats and shall propose a framework for a consistent approach to the assessment of these threats. Included in this analysis shall also be a review of international legal responses and security measures adopted by governments and industry to safeguard offshore oil and gas installations.

## **Types of offshore security threats**

Attacking offshore oil and gas installations is not a new phenomenon. In fact, 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 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.

# Protecting Offshore Oil and Gas Installations: Security Threats and Countervailing Measures

Written by Dr Mikhail Kashubsky  
Tuesday, 13 August 2013 00:00

---

Offshore security threats are activities that pose a risk to operations of offshore oil and gas installations. Any unlawful interference with offshore oil and gas operations or an act of violence directed towards offshore installations is considered an 'offshore security threat'. 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.

This article categorizes threats faced by offshore oil and gas installations based on activity type. The categories utilized are: 1) piracy, 2) terrorism, 3) insurgency, 4) organized crime, 5) civil protest, 6) inter-state hostilities 7) vandalism, and 8) internal sabotage.

## Piracy

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 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 (floating production, storage, and offloading vessel) 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). Apparently there was another attack off Tanzania on a drillship contracted to Ophir Energy in September 2010; however, that attack is not reported in the International Maritime Organization reports on piracy.

## Terrorism

Terrorism is another security threat to offshore oil and gas installations. To date, there have been only 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

## Protecting Offshore Oil and Gas Installations: Security Threats and Countervailing Measures

Written by Dr Mikhail Kashubsky  
Tuesday, 13 August 2013 00:00

---

Insurgency is motivated by political struggle and insurgents often causing 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.

### Organized crime

Organized crime can also interfere with offshore oil and gas operations. The types of crimes that have relevance to the oil and gas industry include oil theft, extortion, armed robbery, theft of property and other forms of criminal profiteering. There have been at least two reported attacks on offshore installations involving organized criminal groups. These are the attack on the mobile offshore drilling rig Allied Centurion in Malaysia on 26 December 2008, where a group of armed robbers boarded the drilling rig and stole stores of goods and property. Another incident which can be attributed to organized crime is the [attack on the offshore Moudi oil terminal](#) in Cameroon on 17 November 2010 by a 'hybrid criminal/separatist' group called Africa Marine Commando (AMC), apparently for failure to pay a 'security tax' previously demanded by the perpetrators.

### Civil protest

Civil protest also poses a security threat to offshore oil and gas installations. Interferences with offshore operations can be caused by non-violent environmental activists, indigenous activists, labor activists, striking workers, and anti-government protesters. There have been at least ten security incidents where operations of offshore oil and gas installations were affected by the actions of protesters and activists. Greenpeace activists have caused interferences with operations of offshore installations on several occasions including an attempt to board an oil rig about 170 nautical miles off the coast of Massachusetts in the United States on 25 July 1981, the unauthorized boarding and occupation of [Shell's Brent Spar](#) floating offshore oil storage facility in the North Sea on 30 April 1995, an unauthorized boarding of the

#### [Stena Don](#)

offshore drilling rig off the coast of Greenland on 31 August 2010, interference with operations of the

#### [Stena Carron](#)

drillship in the waters off the Shetland Islands north-east of mainland Britain in the UK on 21 September 2010, and the unauthorized boarding of

#### [Leiv Eiriksson](#)

offshore drilling rig in Turkish waters. There have been other offshore security incidents caused by civil protest such as an unauthorized boarding of

#### [Parabe](#)

# Protecting Offshore Oil and Gas Installations: Security Threats and Countervailing Measures

Written by Dr Mikhail Kashubsky  
Tuesday, 13 August 2013 00:00

---

offshore oil production platform by protesters in Nigeria on 25 May 1998, and the seizure of offshore installations by striking oil workers off the coast of Nigeria in April 2003.

## Inter-state hostilities

Certain conduct or actions of Nation-States may also represent a security threat to offshore installations. These can be in the form of interstate armed conflicts and wars, maritime boundary disputes, and state terrorism. There have been at least six security incidents involving actions of hostile states including the attack in March 1983 by Iraqi planes on the Iranian offshore platform at the Nowruz oil field; the 19 October 1987 attack on the Iranian R-7 and R-4 offshore oil platforms in Reshadat and the 18 April 1988 attack on Iranian offshore oil complexes, Salman (aka Sassan) and Nasr (aka Sirri) by US military. Other examples are the 3 June 2000 incident where the Suriname Navy ordered American-owned and operated offshore oil drilling rig, CE Thornton, to stop drilling and leave the area and threatened to use force if its demands were not complied with.

## Vandalism

Vandalism is another security threat to offshore oil and gas installations. Vandalism can be referred to as 'damaging cargo, support equipment, infrastructure, systems or facilities' (Australian Government, Department of Transport and Regional Services, Offshore Security Assessment Guidance Paper (2005): 15). This category of threat can include violent actions of radical environmental and animal rights groups and acts by members of local populations intended to cause damage to company property. There has so far been only one reported incident involving offshore installations that can be categorized as vandalism. On 2 August 1899, in the US, when an oil company began to construct an oil derrick off the shores of Montecito, an affluent suburb of Santa Barbara, California, a local mob attacked the rig and demolished it (Harvey Molotch, William Freudenburg and Krista Paulsen, "History Repeats Itself, But How? City Character, Urban Tradition, and the Accomplishment of Place" American Sociological Review 65 (2000): 804).

## Internal sabotage

Internal sabotage is also a potential security threat to offshore oil and gas installations. Sabotage can be defined as 'the deliberate destruction, disruption or damage of equipment' by dissatisfied employees. The threat of internal sabotage comes from 'insiders' such as current and former employees of oil companies, contractors, offshore service providers, and other trusted persons affiliated with the offshore oil and gas industry. For the purposes of this analysis, intentional disclosure of sensitive/confidential information to third parties is also considered to be a form of internal sabotage. Malicious actions of disgruntled, dishonest or terminated employees or other insiders, including collusion between insiders and external adversaries in carrying out or planning an attack can cause serious disruption to oil and gas installations and operations. There have been several reported instances of participation of

insiders in attacks against the oil and gas industry, but none of those specifically involved 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

Geographical considerations are relevant to the assessment of security threats and these factors should be taken into account. The security environment of the oil and gas 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 they operate in. 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 piracy, are often concentrated in certain geographical areas. 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, raising the awareness of marine pollution from the offshore oil and gas industry as in the case of actions by Greenpeace, financial gain for example in the case of piracy, and causing disruptions to oil supplies and oil price fluctuations. For example, if financial gain is the primary objective of the attackers, they may seek to carry out attacks with minimal damage to offshore installations and avoid unnecessary human casualties. 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, unauthorized boarding 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 abduction of offshore workers, while the usual tactic of environmental protesters is unauthorized boarding and occupation of offshore installations. 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 and other factors such as existing countervailing measures. For example, an organized criminal group will not necessarily use explosives to attack an offshore installation, but may simply make a threat of attack to extort money from a company that operates the installation. 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**

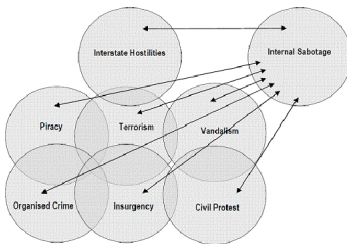
One of the difficulties in assessing offshore security threats is that there are overlaps and relationships between different categories of offshore security threats. Violent non-state actors are motivated by a range of objectives and the distinction between political and criminal motivations is becoming increasingly blurred (Jennifer Giroux, "Global Platforms and Big Returns: Energy Infrastructure Targeting in the 21st Century" CTN Newsletter Special Bulletin Protecting Critical Energy Infrastructure from Terrorist Attacks (2010): 18). 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 (see Martin Murphy, *Small Boats, Weak States, Dirty Money: Piracy & Maritime Terrorism in the Modern World* (Hurst & Co: 2009) 161). 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.

Written by Dr Mikhail Kashubsky  
Tuesday, 13 August 2013 00:00

---

Hansen proposes a ‘four circles model’ (Hans Tino Hansen, “Distinctions in the Finer Shades of Gray: The ‘Four Circles Model’ for Maritime Security Threat Assessment” in Lloyd’s MIU Handbook of Maritime Security, eds. Rupert Herbert-Burns et al. (Florida: Taylor & Francis, 2009), 74-78) for the assessment of maritime security threats, arguing that understanding different categories of threats, as well as their distinctions and interrelationship between them is important. In the assessment of security threats to offshore oil and gas installations, it is possible to add three or four circles to Hansen’s model. For example, the circles that can be added are ‘vandalism’, ‘civil protest’, ‘inter-State hostilities’ and ‘internal sabotage’. As shown in Figure 1 below, vandalism and civil protest overlap with terrorism and insurgency respectively, and with each other. A threat of inter-state hostilities overlaps with terrorism to some extent, particularly in the case of terrorist acts committed by or on behalf of states, but inter-state hostilities do not overlap with any other categories of threats. The internal sabotage threat category can overlap with any or all of the other categories of threats, but for ease of reading, it is shown separately from all other threats in Figure 1.

**Figure 1: Offshore Security Threats Nexus**



Source: Author

## Conclusion

Offshore oil and gas installations face a number of different security threats. In this article threats are grouped into eight categories based on the type of activity. Offshore security threats have become more complex and are often interrelated which makes it more difficult to categorize and analyze them. The above framework for assessment of threats is proposed for assessment of threats faced by offshore oil and gas installations generally. For the purposes of the protection of offshore installations, specific threat assessment for each offshore installation must be undertaken using industry-standard risk management methodologies taking into account the specific threat environment of the area where an offshore installation is located, specific vulnerabilities, and any countervailing or mitigating measures that are in place.

## Protecting Offshore Oil and Gas Installations: Security Threats and Countervailing Measures

Written by Dr Mikhail Kashubsky  
Tuesday, 13 August 2013 00:00

---

Oil companies face different security threats depending on the country or region they operate in, and accordingly they face a different level of risk of being attacked. Companies operating in economically and politically unstable countries and in countries with some kind of civil unrest or armed conflict are more prone to attacks on their offshore installations than in more stable regions.

After 9/11 the governments and industry responded to the changed threat environment with a number of international and national regulatory measures and initiatives to enhance security of offshore installations have been introduced.

*Contributor Mikhail Kashubsky is Senior Lecturer at the Centre for Customs and Excise Studies, University of Canberra, Australia and Head of Secretariat of the International Network of Customs Universities (INCUI). This article is based on part of PhD thesis completed at the Australian National Centre for Ocean Resources and Security, University of Wollongong, Australia*