Safety Science 68 (2014) 222–230

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

A Bayesian network to manage risks of maritime piracy against offshore oil fields

Amal Bouejla *, Xavier Chaze [1], Franck Guarnieri [2], Aldo Napoli [3]

Crisis and Risk Research Centre (CRC), MINES ParisTech, 1 rue Claude Daunesse, BP 207, F-06904 Sophia Antipolis Cedex, France

ARTICLE INFO

Article history:
Received 9 September 2013
Received in revised form 8 April 2014
Accepted 14 April 2014
Available online 7 May 2014

Keywords:
Oil platforms
Offshore oil fields
Pirate attacks
Bayesian networks
Quantitative and qualitative knowledge

ABSTRACT

In recent years, pirate attacks against shipping and oil field installations have become more frequent and more serious. This article proposes an innovative solution to the problem of offshore piracy from the perspective of the entire processing chain: from the detection of a potential threat to the implementation of a response. The response to an attack must take into account multiple variables: the characteristics of the threat and the potential target, existing protection tools, environmental constraints, etc. The potential of Bayesian networks is used to manage this large number of parameters and identify appropriate counter-measures.

1. Introduction

Currently there are over seven thousand oil platforms scattered throughout the world, each of which requires on the one hand, equipment for the extraction, processing and temporary storage of petroleum, and on the other hand shipping capable of transporting crude oil between production and consumption sites.

Modern piracy is currently the major threat to the security of these energy production sites and maritime crude oil transport. In 2011, 552 attacks on ships and platforms were registered with the International Maritime Bureau[4] compared to 487 reports in 2010. At production sites, monitoring methods are a major weakness in the detection of a threat, and the procedures to be applied in the event of an attack are often inefficient and inappropriate. It is therefore essential to have a system that ensures the security of oil fields and offers them appropriate protection and effective crisis management.

The SARGOS[5] system, funded by the National French Research Agency[6] (*Agence Nationale de la Recherche*) and recognised by regional organisations addresses this need by offering a global protection system in the fight against oil infrastructure piracy.

This article is organised into three parts. It first addresses the issue of acts of piracy against oil fields. Next the method used for the planning of counter-measures is described in detail. This includes notably, the construction of Bayesian networks from two datasets: the "Piracy and Armed Robbery" database of the International Maritime Organization (IMO) and the collection and formalisation of the knowledge of domain experts. Finally, the article describes how the model was tested using realistic and comprehensive pirate attack scenarios and the results are discussed.

2. Piracy against oil installations: a serious threat and limited defences

Offshore oil infrastructure is subject to a constantly increasing risk of piracy. The consequences of these actions have repercus-

* Corresponding author. Tel.: +33 4 93 67 89 14; fax: +33 4 93 95 75 81.
E-mail addresses: amal.bouejla@mines-paristech.fr (A. Bouejla), xavier.chaze@mines-paristech.fr (X. Chaze), franck.guarnieri@mines-paristech.fr (F. Guarnieri), aldo.napoli@mines-paristech.fr (A. Napoli).

[1] Tel.: +33 4 93 67 75 77; fax: +33 4 93 95 75 81.

[2] Tel.: +33 4 93 67 74 72; fax: +33 4 93 95 75 81.

[3] Tel.: +33 4 93 67 89 15; fax: +33 4 93 95 75 81.

[4] International Chamber of Commerce International Maritime Bureau's Piracy Reporting Centre (http://www.icc-ccs.org).

[5] The Offshore Warning and Graduated Response System (*Système d'Alerte et de Réponse Graduée OffShore*).

[6] The SARGOS project includes participants from private sector organisations such as DCNS (a French naval shipbuilder) and SOFRESUD (a supplier of high-tech equipment to the defence industry), and public research centres including ARMINES (a French contract research organisation) and TéSA (Telecommunications for Space and Aeronautics).

http://dx.doi.org/10.1016/j.ssci.2014.04.010
0925-7535/© 2014 Elsevier Ltd. All rights reserved.

sions as much at a local level (on operations) as globally (on distribution). This section highlights both the economic and the political implications of pirate attacks and describes an increasingly insecure context where actors in the offshore oil and gas industry, without effective tools to protect themselves, find themselves helpless. Finally, it presents the SARGOS system and describes the contribution that this new system is expected to make to dealing with the problem of maritime piracy.

2.1. Economic and political issues

Offshore oil exploration is expanding rapidly. The exploitation of offshore oil resources currently represents about a third of global petroleum production. This energy resource, despite its scarcity, is being explored in many areas some of which are located in dangerous territorial waters, notably the Gulf of Guinea. In the offshore waters of politically unstable countries, attacks on oil field infrastructure generate significant additional costs – caused by, for example the payment of ransoms, increased insurance premiums and the installation of security equipment. The annual cost of piracy is estimated at 7–12 billion United States dollars (BMI, 2011). These additional costs directly affect the international price of oil.

Moreover, oil fields form the interface between the maritime world and the oil and gas industry. The heterogeneity of applicable regulation (rather than the absence of law) makes the status of installations a legal headache. Moreover, this complexity can lead to political conflicts between nations; when the nationality of the company operating the platform does not correspond to physical location of the installation, the problem arises of who has responsibility for the protection of the area (Schroeder and Love, 2004).

The importance of oil installations in the global economy and industry and the potential political consequences of piracy therefore require that such assets are better protected.

2.2. Violent attacks

Although attacks against oil fields are infrequent and mostly low-profile, they are extremely disturbing because of the severe impact on the crew and infrastructure.

The following examples demonstrate the point:

- On 22nd September, 2010 the tug Bourbon Alexandre located in the Addax oil field off the Nigerian coast was attacked by four speedboats; three French sailors were taken hostage. This was the fourth attack against the Bourbon Company since 2009.
- The attack on the Exxon Mobil platform off the coast of Nigeria, led to the kidnapping of nineteen of its employees and significant damage to the oil facility caused by explosive devices used by the pirates.
- Finally, on 17th November, 2010 pirates aboard a speedboat attacked a ship owned by the French company Perenco that was carrying Cameroonian security forces near an oil platform in the Gulf of Guinea. The attack killed six people.

Infrastructure managers, employees and safety officers do not want to continue to see their ships or other assets become the subject of substantial ransoms, nor crewmen injured, killed or kept in extreme conditions for days or even weeks. At the same time insurers are unwilling to continue to provide cover for such high risks indefinitely. Finally, nations do not want to continue to see the price of oil affected by such events.

2.3. Emerging operational requirements

The attacks described above are a perfect illustration of the weakness of current anti-piracy tools. At the present time, there is no comprehensive system capable of managing the entire threat processing chain. Current systems treat the detection of a threat and the response to it as independent operations. Among the available detection tools, radar-based (pulse) systems[7] can spot large or medium-sized cooperative mobile objects but perform poorly in the detection of small craft (e.g. fishing boats and motor boats) in a rough sea; moreover the analysis of a large domain is relatively slow. There are also optronics surveillance systems[8] that, despite their ability to detect small targets at long-range, are handicapped by the problem of solar reflection from the sea and are very sensitive to weather conditions. As for the tools used to counter an attack, they are often inadequate or incorrectly used (e.g. water jets, Ship Security Alert System).

In terms of the threat response, the targets in danger can currently send alert messages to other units in the area but this diffusion is restricted to a very small geographic area. Moreover, even if a security vessel is alerted to a threat, it cannot be assumed that it will be able to intervene, particularly if it is not close to the location of the attack.

Therefore, the aim of the SARGOS system is to offer a new method that is able to both detect threats and plan a response. The response implements a graduated series of non-lethal counter-measures (sonic cannons, barring infrastructure access, etc.) that can be applied in order to eliminate the danger.

2.4. The contribution of the SARGOS system

The SARGOS system addresses the need to protect civilian infrastructure that is vulnerable to acts of piracy or terrorism at sea. It is a global system that takes into account the whole threat processing chain, from the detection of a potential danger to the implementation of the response. It can be integrated into the operations of the installation and takes into account regulatory and legal frameworks at both national and international level. The creation of the system, which involved the development of an overall protection method, automatic threat detection and identification, risk assessment and management of an appropriate response, required professional skills from many domains.

The functional diagram of the SARGOS system (Fig. 1) describes the threat processing cycle. The overall system operates as follows: when the detection module instruments (Frequency Modulated Continuous Wave radar, infrared cameras, etc.) identify a vessel in an area near to the oil field, the system evaluates the threat and the potential danger and generates an alert report containing comprehensive data describing the scenario. This information includes details such as visibility, time of day, the speed, longitude and latitude of the detected vessel and its potential target, etc. The distance between the two entities and the theoretical response time of the security vessel is also calculated from this data. If the threat is identified as suspicious or hostile, the system generates an alert report every second. The alert report is used in the planning stage where external and internal means to respond to the attack are mobilised. This paper particularly addresses this aspect of response planning and the management of internal and external resources available on the installation (such as searchlights or sonar alarms).

[7] In these systems, a radar antenna emits microwave pulses towards the target. These signals are reflected back, and then intercepted by the radar receiver, which collects an electrical signal called the echo.

[8] These electronic and electrical systems generally consist of an optical sensor, an image processing system and a data storage, or display device.