Chapter 18: Security of Maritime Energy Assets

Nir Zarchi

Introduction

Throughout modern history energy has been an essential basis of social prosperity and economic development and serves as a key component of the country's power and sovereignty.[1] Accordingly, many countries regard the maintenance of energy security – and in particular the aspects of reliability and continuity of supply – as key elements in their national security policy.

Over the course of recent decades, global dependence on energy has been increasing, leading to a substantial rise in demand and necessitating the development of additional or alternative supply sources. This need, along with the development of advanced detection, production and generation technologies, leads to the emergence of a **maritime energy economy**. At present, this economy represents the source of over 30% of all global energy[2] and this trend is expected to intensify over the course of the coming years.[3]

Since the 1999 discovery of the 'Noa' reservoir, large reserves of natural gas have been found offshore of the State of Israel, in the Exclusive Economic Zone (EEZ). These reserves serve as the central energy source for generating electricity in Israel and in the future they are expected to be one of the main energy sources for domestic transport and industrial purposes. Moreover, the intention is to export some of the gas reserves. Estimates indicate that the proceeds from these reserves will be a significant source of revenue for the national economy.[4]

However, along with the many opportunities inherent in the development of the maritime energy economy, significant challenges are emerging[5] regarding the

1 Dannreuther and Ostrowski, 2013

2 Kaiser 2007, Robertson 2013

3 It is quite possible that in the future the mid-sea will become the principal source for energy production, both from fossil sources and from renewable sources found in the sea, such as the kinetic energy of waves, or sources that in order to produce energy from them open spaces are required, such as solar energy or electricity produced from wind.

4 Bank of Israel. "*Bank of Israel's comments to the draft outline with regard to development of the gas fields discovered in the economic waters of Israel*",pg. 9. 2015.

5 It should be noted that damage to the energy infrastructure could be intentional (a terror incident for example) or unintentional (technical failure, natural force, etc.). The implications for the national energy economy, as well as the environmental implications, do not depend on the cause of the damage. Nevertheless, the present chapter discusses the intentional threat protection policy.

manner of coping with possible threats to the infrastructures found there, the potential economic implications of the resulting damage for the national energy economy, as well as the environmental implications.

Characteristics of the Maritime Domain and its Existing Security Threats

The maritime domain has several unique characteristics which differentiate it from other domains, particularly the terrestrial domain. The main ones are: its physical size;[6] its low congestion – both in terms of human presence and in terms of the number of installations and facilities found there; its morphological characteristics and its geological features that differ from one another in its three layers – the subsea, the sea and the sea surface; and its special legal status, which is based on international treaties, such as UNCLOS and Freedom of the Seas, attempts to regulate with the aim of finding a balance between the whole spectrum of interests and needs of many different countries.[7] These and other characteristics have a considerable effect on the range and gravity of threats. In fact, the situation may provide attackers with advantages in reaching and attacking their target, while on the other hand preventing attacks in good time, or providing an adequate response during and after their occurrence, is very challenging.

The phenomenon of attacking maritime oil and gas installations is certainly not new. The first such attack took place more than a hundred years ago off the coast of the United Stated and involved the destruction of a rig.[8] Over the years there have been a significant number of security incidents involving maritime installations. In the last 25 years alone there were roughly 50 such incidents, which were perpetrated by diverse entities with a range of motives, objectives, capabilities and tactics.[9] Figure 18.1 shows the various types of threats and the threat realization process flow.

6 For example, roughly 71% of the earth's surface is covered by water (CIA, 2009). In the case of the State of Israel, its exclusive economic zone is slightly larger than its land area (Haifa Center for Maritime Strategy, 2015).

7 UNCLOS is a compromise between many interests of a variety of countries. In essence, it attempts to create a better state foothold in the waters. Nevertheless, a variety of issues, among them the piracy issue, were hardly addressed (Nyman, 2013)

8 The foregoing references an attack on an oil rig that was perpetrated on August 2, 1899 off the coast of Santa Barbara, California. The attack was perpetrated by a criminal organization and caused total destruction of the platform (Kashubsky, 2011).

9 Kashubsky, 2013

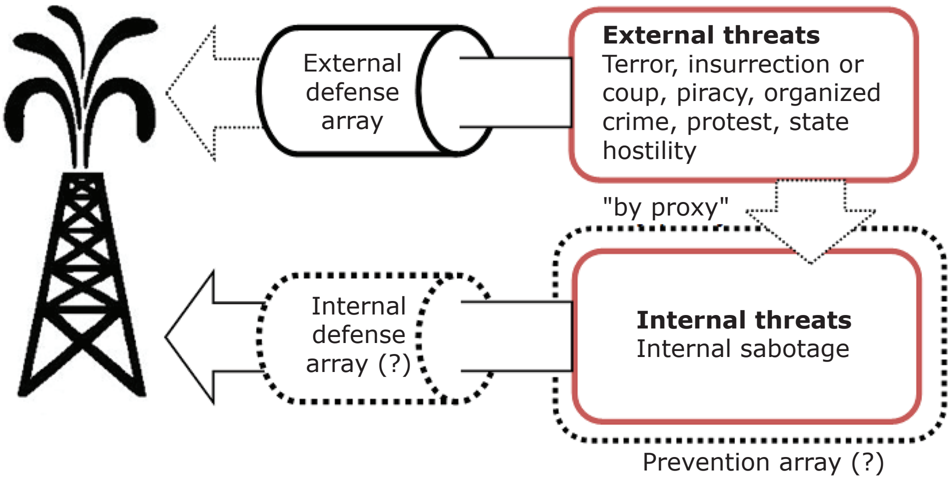

Diagram 18.1 Groups and families of threats

Methods of Protecting Critical Infrastructure in the Maritime Domain

Before dealing with the subject of critical infrastructure protection in general and in the maritime domain in particular, we must first define the target for protection, and consequently its extent and its manner of implementation. Protection targets can be classified according to two levels: tactical level targets – where the purpose is to prevent any damage to the critical installations themselves; and strategic level targets – where the purpose is to maintain critical interests at the systemic level and in the case under discussion, National Energy Security.[10] Therefore, the response for tactical level targets will generally focus on frustrating or preventing an attack, while the response for strategic level targets will also include elements of robustness – elements that give the system the ability to recover rapidly from shock and thus maintain a reasonable level of service in terms of of time-frames and cost-effectiveness.[11]

Tactical level protection targets include all those installations and critical infrastructures located in the maritime environment and in particular the energy installations, where the protection concept focuses largely on prevention and frustration of attacks. In cases of malicious internal threats, a variety of methods and tools can be used, for example to restrict the entry of unauthorized entities and to

10 It should be noted that there may be additional implications at the strategic level, apart from maintaining energy security, such as image or economic damage.

11 Sauser et al., 2011

create capabilities of identification and response to possible scenarios. Furthermore, it is possible to develop a system for coping with external threats that could include measures to create 'full situational awareness',[12] along with the ability to implement an operational engagement process that includes detection, identification, decision making and action (known as: 'OODA Loop'[13]). Thus, there is effectively an effort to maintain the functional continuity of the infrastructure components.

At the strategic level, the discussion of Israel's energy security is beyond the scope of the present discussion on the protection of maritime energy infrastructures. As a rule, a state's energy security is based on three elements: reliability of supply, affordability and sustainability.[14] Accordingly, the degree of damage to national energy security can be expressed in terms of the scale of the gas shortage in relation to demand in the domestic market and the duration of the shortage, and to examine the full range of methods and measures required in order to protect energy security.

Since it is unlikely that attacks on energy facilities can be totally prevented, it may thus be more effective to implement policy tools aim at minimizing the extent of damage to supply once an attack occurs, rather than focus solely on ensuring an attack’s interception. First, an emergency plan can be implemented15 for coping with energy crisis situations, which will handle both the renewal of supply and the moderation and balancing of consumer demand in all sectors of the economy, in accordance with national interests. Furthermore, it is possible to provide natural gas consumers, and particularly electricity producers, with the ability to make use of a variety of energy resources16 ('alternative fuels'), such as gas, coal and fuel oil and thereby to ensure the continuity of their operations. It is also possible to prepare additional energy supply sources17 – suppliers from different geographic regions, both from Israel and abroad – by developing the necessary infrastructures for this purpose. Such infrastructure may include, inter alia, liquefied gas receiving buoys (STL), pipelines to transmit oil and gas from neighboring countries, fossil fuel receiving platforms, etc. An additional effective tool for dealing with an energy

12 A situation characterized by a high level of integration between a variety of military, police and civilian entities.

13 Observe-Orient-Decide/Delay-Act

14 Shaffer, 2009

15 Emergency plans for coping with energy crisis situations are implemented within many countries around the world, sometimes independently and sometimes through umbrella organizations such as the International Energy Agency. Israel may benefit from implementation of such an emergency plan. An example of key principles for an emergency plan may be found at – (IEA, 2013).

16 Or: 'Resourse Diversity'.

17 Or: 'Supplier Diversity'.

crisis – particularly in the initial stages, until the alternative system is stabilized and begins operation – is the maintenance of appropriate emergency stock levels of fuel and gas storage. Finally, is essential to define principles within the energy policy that will ensure the establishment of infrastructures with interchangeability, flexability and redundancy.

Theoretical Framework for Analyzing Methods of Protecting Critical Infrastructure Installations

Below is a proposal for a model that strives to connect between the analytical research methodologies of military threat evaluation[18] (including physical security risk assessment of facilities) and the theoretical tools of political science uses to ensure energy security. To this end, the first phase consists of an infrastructure review and critical assets characterization, followed by identification of events that can cause infrastructure functioning failure. Then, possible threats to the infrastructure are examined, while assessing the likelihood of their occurrence and the level of risk that they constitute to the facility. According to the results, the degree of damage to energy supply capabilities is calculated, while taking into account the measure of impact on the infrastructure. The degree of damage is defined in terms of quantity of time. The last phase examines policies that can minimize the extent of impact caused by reduced supplies, while making 'cost-benefit' considerations. Figure 18.2 below presents this analysis model. Further details on this topic can be found in the research of Zarchi, 2014.

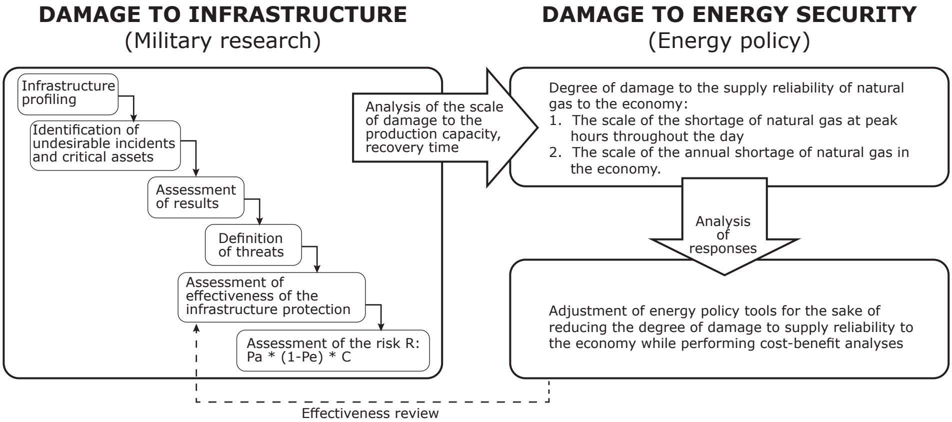

Diagram 18.2: Theoretical framework for analyzing methods of protection of critical infrastructure installations

18 A centeral methodology used by this model is a methodology developed by the Sandia Institute (Sandia, 2000)

The Case of Israel – Initial Situation Assessment

The energy economy and the maritime infrastructure

In recent years, supply and demand for natural gas have been on a steady upward trend. In 2015 alone total natural gas consumption rose by 11% compared with 2014. This trend continued in 2016,[19] and forecasts predict that by 2024 demand will have increased by 75% compared to the present level.[20]

Accordingly, the State of Israel is developing its maritime energy infrastructure. Currently, gas supply to the Israeli economy is based on the Tamar reservoir, with assistance by the Buoy[21] as a routine supplementary supply source and as a partial backup array[22] in times of crisis. For example, last year's gas supply mix consisted of production of approximately 8.3BCM from the Tamar reservoir and the balance, approximately 0.13BCM, was supplied through the buoy.

The gas in the Tamar reservoir is produced by five wells[23] and makes its way through two pipelines, each about 140 km in length, to the Tamar Rig,[24] which is located approximately 25 km west of the coast of Ashkelon (adjacent to the Gaza Strip fishing zones). When the main treatment is complete, the natural gas is transmitted through a pipeline to the onshore receiving terminal in Ashdod. Figure 18.3 illustrates the structure of the current gas infrastructure.

In fact, under the current situation, Israel's maritime energy economy is based on a single primary reservoir – the Tamar Reservoir – and on infrastructure characterized by a low level of robustness.

19 In the present year there has been an increase of approximately 14.5% in gas consumption by the electricity generation sector. In the industrial sector, by contrast, a scope of consumption similar to the scope in 2014 was maintained.

20 The Ministry of National Infrastructures, 2015

21 This refers to a marine buoy that enables reception of natural gas from an LNG regasification vessel, at a rate of 0.57 million cm of gas per hour (The Ministry of Energy and Water Resources, 2013).

22 The gas supply rate of these two sources together comes to approximately$2_{MCM/h}$, where approximately 75% is supplied from the Tamar Reservoir, while only approximately 0.25% is supplied by the buoy.

23 The wells were built in a manner that would enable production of from 7.1–8.5 million cubic meters of gas per day each.

24 The rig constitutes the initial and primary treatment installation. It is located at a water depth of 237 meters and rises to a height of approximately 60 meters above sea level.

Figure 18.3 Tamar Reservoir infrastructure

Vulnerability of the Maritime Infrastructure and its Significance

In order to examine the degree of vulnerability of the infrastructure in various scenarios, we must first define three levels of vulnerability, referring to the degree of damage to production capacity and to its duration:

- Low level – partial damage to production capacity and a short time frame required for repair (up to a few months).
- Moderate level – significant damage to production capacity and short time frame for repair; or partial damage to production capacity and long time frame for repair (several months or more).
- High level – significant damage to production capacity and long time frame for repair.

Based on these definitions, the components of Israel's maritime infrastructure can be classified according to their level of vulnerability:

- The production wells – low level of vulnerability: decentralized and modular infrastructure with high redundancy (5 wells). The time required for any repairs is relatively short.
- Underwater pipeline – low to moderate level of vulnerability: modular infrastructure with partial decentralization and limited redundancy (2 pipelines). The time required for any repairs is relatively short.
- Tamar Rig – high level of vulnerability. Infrastructure characterized by a lack of redundancy, interchangeability and resilience. The time required for any repairs is long.[25]

Accordingly, it is possible to define the **Tamar Rig as the critical component of the maritime energy infrastructure of the State of Israel**. A preliminary analysis

25 It can be estimated at about a year and a half.

of supply versus demand reveals that significant damage to the Tamar Rig would lead to a shortage of roughly 50% of the total fuel mix required for generating electricity.

Key Threats and Protection Methods

In the case of Israel, intentional damage to the gas infrastructures could be caused by an attack carried out by states or by non-state entities. Several non-state entities have even recently declared their intention to carry out physical attacks against Israeli infrastructures in general[26] (such as the threat to damage the ammonia tank in Haifa Bay) and against maritime energy installations in particular.[27] For example, the Secretary General of Hezbollah, Hasan Nasrullah, has expressed explicit threats to damage Israel's gas rigs. [28]Along with this, we can see ongoing efforts by Hamas to acquire maritime and subsea capabilities.[29]

As a rule, the threats can be classified into a number of key groups: (a) attacks by booby-trapped vessels; (b) firing of coast to sea missiles - with the emphasis on 'Yakhont' (P-800 Oniks) and C802 class missiles; (c) damage by means of subsea capabilities;[30] (d) Cyber damage – particularly by powerful entities in this field.[31]

Israel operates a multi-layer defense array against the range of threats as a whole. The external layer is based on existing state defense and intelligence capabilities, which are operated by the military and the various security officials in routine and emergency times alike. This defense layer includes, inter alia, the air defense array (anti-aircraft, RPVs and missiles), an array of routine land and marine security patrols[32], visual (detection and identification) and control activity in the field, various kinds of intelligence activity, plus surveillance and enforcement of civilian

26 An interview with Hezbollah leader Hasan Nasrullah on the Walla website http://news.walla.co.il/item/2945637

27 An interview with Rear Admiral Dror Friedman, head of the navy's sea division in the Globes newspaper 19/01/2015.

28 State Comptroller. The protection of installations and infrastructures for gas and oil production at sea, Annual Report 64 in 2014.

29 An example of this can be seen in the terrorist infiltration by sea of Zikim Beach in the course of Operation 'Protective Edge' (5/7/2014).

30 These capabilities become more and more available within the framework of the commercial market.

31 To date, a real capacity of causing physical damage – which combines accurate intelligence and high technological capability – is mainly prevalent among state entities. However, this field is gaining momentum among additional entities. Moreover, it is quite possible that in certain cases a sub-state actor will be assisted by a state entity (by proxy).

32 Hereinafter: Routine security measures.

entities (such as commercial ships). Along with these, new subsea and cyber defense capabilities have recently been developed. An additional defense layer is a designated maritime defense system which is currently being established by IDF through the Israel Navy, with the aim of protecting Israel's critical interests in the energy sphere within the exclusive economic zone (in accordance with Cabinet Decision 53/b[33]). In order to accomplish this mission, the Navy has acquired four corvettes. The first corvette is due to arrive in Israel in the course of 2020. This is being accompanied by a review of measures and technologies in the air defense and subsea spheres which can be operated using these boats.[34] Finally, there is an internal defense layer – in the immediate vicinity of the installation – which consists of a local security team that operates on behalf (and under the responsibility) of the gas production company.[35]

Despite the defense array that is currently taking shape, it seems that in the present security reality there are several significant threats to Israel's maritime energy infrastructure, with the major ones being attacks perpetrated by a sub-state entity. A study that examined the degree of vulnerability of Israel's maritime gas infrastructure to acts of terror, with reference to potential threats and defense capabilities, found that there are several possible scenarios for significant and long term damage to gas production capacity. The major threats that were identified related to the use of explosive boats, booby trapped planes and predator merchant ships (Zarchi, 2014).

Accordingly, along with the physical defense array it is advisable to also develop energy policy tools aimed at reducing the extent of damage to the supply capability in the event of damage to the maritime installations.

Summary and Recommendations

Over the course of recent years, the extent of supply and demand for natural gas in the State of Israel has been on a steady upward trend. In 2015 alone the total

33 On 13.11.13 the Security Cabinet decision was made (no. 53/b) with regard to 'protection of the critical interests of the State of Israel in the energy sector in the Mediterranean Sea ('economic waters'). Which regulates the protection and the security of the maritime gas installations (hereinafter – decision 53/b). This decision imposed on IDF 'to take action to protect the critical interests of the State of Israeli in the energy sector in the exclusive economic zone [economic waters]".

34 The cost of establishing the array for protecting the economic waters is estimated at three billion dollars (Bamahane, 2012), (Katz, 2012).

35 From the State Comptroller Report 64b pg. 21: "Private security companies perform the local security for the gas production installations at sea, routinely and in emergencies".

natural gas consumption rose by 11% compared with 2014 and the forecast is that demand will only continue to increase.

Accordingly, the State of Israel is developing its maritime energy infrastructure. Currently, the gas supply to the Israeli economy is based on the Tamar reservoir, with the Tamar Rig constituting the critical component of its maritime energy infrastructure. Significant damage to the Tamar Rig would lead to a shortage of roughly 50% of the total fuel mix required to generate electricity in the coming years.

It seems that in the present security reality there are several significant threats that may cause such damage, with the major ones being acts of terror by sub-state entities. In particular, we can point to a number of major possible scenarios for significant and long term damage to gas production capacity: use of explosive boats, use of booby trapped planes, or use of 'predator' merchant ships.

Since it is probably impossible to completely prevent attacks on energy installations, and particularly maritime energy installations, it may thus be more effective to implement policy tools aim at minimizing the extent of damage to supply once an attack occurs, rather than focus solely on ensuring an attack’s interception. These tools may include an emergency plan for coping with crisis situations, the ability to use a variety of alternative energy resources, preparation of additional energy supply sources and development of the necessary infrastructure to this end, maintaining appropriate emergency stock levels of fuels, and finally, defining principles to ensure the establishment of an infrastructure with interchangeability, flexability and redundancy.