MARITIME TERRORISM AND RESILIENCE OF MARTITIME CRITICAL INFRASTRUCTURES

Tonći Prodan[1]

Introduction

After the terrorist attack on the USA on September 11th, 2001, it became obvious that means of transport can be used very effectively as the means of committing terrorist attacks. The surface area of the earth is covered by 71% water, that of which 96.5% is sea water. One particularly interesting thing about this subject is that the oceans are actually the routes of world trade, and any disruption in this domain can be harmful[2]. However, terrorists are also aware of this fact. Counterterrorist experts argue that the maritime transport will be

1 Tonći Prodan, PhD, Portus et Navem Split, e-mail: tprodanportnav@gmail.com

2 Maritime traffic is the bloodstream of Europe's prosperity, and the production of energy and transport, fisheries, the environment and climate change - they all depend and are of close relation with maritime safety, in one way or the other (Drent et al 2013:25).

the first upcoming major terrorist target[3]. Taking into account this information, we have decided to do this (empirical) research aimed at studying the contemporary phenomenon of maritime terrorism within its real life context[4]. The phenomenon of maritime terrorism and the resilience of critical maritime infrastructure will therefore be viewed holistically in this paper in order to understand the overall context of the phenomenon. Thus, we will be able to determine the best real risk[5]of maritime terrorist attacks that can lead to complex and long lasting and negative consequences, some in particular being: on national critical infrastructure, by operating on maritime transport routes, energy installations, the communication industry, financial and administrative structures, and the overall values that support the sustainable development of maritime studies. How likely a specific terrorist attack is to occur can be evaluated through a wide range of different methods; however their detailed analysis goes beyond the scope of this paper.

Major terrorist targets in maritime affairs

Major terrorist targets in maritime affairs can be: sea ports, ships, bridges, oil and gas platforms.

3 It is mentioned in the Al- Qaeda manual, among 10 others, as desirable targets for seaports (WorldNetDaily, 2003).

4 With this method (qualitative) research has dealt with more concrete cases (Yin, 2007). As an analytical technique, time series analysis and case comparison synthesis were used. Regarding the compositional structure of work, we mostly used a comparative structure.

5 Risk is the result of threats with adverse effects on the vulnerable system (Haimes, 2006:293).

In and around sea ports, there are a number of vulnerable facilities, installations, and critical infrastructures such as: navigation infrastructure, cranes, berths, pipelines, railways, bridges, roads, water supply systems, fuel storage and hazardous cargoes, container terminals, pilot ships and more. Bridges are particularly vulnerable to explosives or explosives associated with chemical-biological agents. Al-Qaeda has been known for, among others, targeting the Brooklyn bridge in New York City and the Golden Gate bridge in San Francisco (Goslin, 2008).

Furthermore, all types of ships may be terrorist targets, the most interesting being war ships, supertankers, and passenger ships, due to the fact that the most damage can be done with attacks on these types of ships.

The attack on the US naval warship USS COLE in the seaport of Aden, Yemenin the year 2000 showed that terrorists do not withstand from attacks on the best defended and most dangerous naval ships[6].They also showed that they are ready and able to attack the world's strongest military force. In that attack, 17 crew members were killed, 42 injured, although the ship had taken all the necessary precautionary measures.

The next vulnerable category of sea ships which represent attractive targets for terrorists are tankers. By attacking tankers terrorists are

6 Al Nashiri as Bin Laden's then Chief Operation Officer in the Persian gulf and Yemen set up a suicide attack on the American USS Cole in October of 2000, just like an identical attempt 9 months earlier on the USS Sullivans, which did not succeed because the suicide boat sunk due to overburdening of explosives.

able to achieve higher goals: incur human and material damage, lead to disruption in energy supplies, and pollute the marine environment. An attack like that happened in 2002 not far from the Ash Shihr oil terminal in Yemen, during the time of the terrorist attack on tanker Limburg. On that occasion, one crew member was killed and 90,000 barrels of oil went into the marine environment.

Figure 1. USS Cole after the terrorist attack, 2000

Figure 2. Tanker Limburg after the terrorist attack, 2002

Passenger ships and ferries are the next attractive terrorist target because there are a large number of people in a small area. By attacking these kind of targets, the goal of terrorist organizations are attained, those being causing as much human losses as possible and gaining more media attention. An attack like this took place in 2004, by the organized terrorist group Abu Sayyaf, the target being the Superferry 14 Filipino ship. In this attack, which completely shocked Filipino authorities, there was a death toll of 116 people, and 300 injuries[7].

Figure 3. Superferry 14 after the terrorist attack, 2004

An attractive target for terrorist attacks would also be oil and gas platforms, because an

7 The Philippine governments were in a state of denial about terrorist threats, and due such bad judgments this disaster occurred. The United States, joined by Australia and Great Britain, quietly warned the Philippine government that they did not do enough to break terrorist groups within the country. (Manalo, Eusaquito P.,2004:61). Contrary to the aforementioned approach of "state of denial", terroristic threats in any country need to be constantly evaluated.

attack on such “soft”targets also achieves certain goals: a large number of human casualties and large material damage; damages to the marine environment and disruption in energy supplies.

Certain circumstances indicate that is the reason behind the oil platform of Piper Alpha becoming a target. At the beginning of the official investigation, it was discovered that a year before the accident (in autumn of 1987), Piper Alpha discovered an attempted sabotage that had been denied at the last moment. The sabotage was discovered just prior to the gas being released from the field. This is a very indicative and tragic case which took place on July 6th, 1988 in the North Sea, 200km from the Northeastern coast of Scotland. At that time, an entire series of successive explosions and fires occurred on this oil platform with 230 employees of the American oil company named Occidental Oil. In this tragedy, 167 casualties occurred (including 2 members of the rescue crew), and the platform was completely destroyed[8].

8 Kulišić, Magušić,2007:41-46.

Figure 4. Oil platform Piper Alpha after the explosions and fires, 1998

In addition to ships, suitable targets for naval terrorist attacks could also be fuel warehouses and dangerous heavy loads regularly located in or near seaports[9]. In many countries, such warehouses are considered critical infrastructures.

Terrorist attacks on these warehouses can cause significant human, material and environmental damage, and therefore require good security.

9 Port security in a country or its insecurity relies heavily on the grace and weakness of an organization and functionality of a port security system or lack thereof in another country. Canada admitted, amongst many other Western governments, that their ports and associated facilities are "perverted" to organized crime. Furthermore, it is common knowledge that the USA invest in the safety of the country and its citizens, especially following the terroristic attack on September 11th, 2001. However, analysis of available literature suggests that the safety program of American ports still has not achieved the planned results in the form of real improvement of port security.

To illustrate the possible consequences of such accidents on objects of maritime critical infrastructure, we provide an example of the explosion, sinking and subsequent fire of the ExxonMobile 60 meter long B-125 bunker fuel tank at Arthur Kill (Staten Island, in the Gulf across New York City business center). At the time of the explosions on the barges there were just over 7.5 million liters of fuel. Two crew members were killed, and one person was injured. Only rapid fire-fighting interventions had prevented explosions and fires from reaching nearby large tanks at the oil terminal, having a capacity of about 380 million liters of liquid petroleum products, with a massive amount of stored liquid petroleum derivates.

The effects of the wave from the blast of an explosion have left the effects to a radius of almost 5km around the center of the explosion. The explosion also resulted in panic as a result of speculation of another possible terrorist attack on New York.

Figure 5. Barge 125 after the explosion, 2003

Understanding the dangers of Maritime terrorism

The best insight to the real threats of maritime terrorism is an analysis of organizational structure, tactics and techniques which used by certain terrorist organizations. The Sri Lankan Liberation Tigers of Tamil Elam (LTTE) are a good example of a highly organized terrorist organization which specializes in maritime attacks. In their organization they have: maritime fighting units, submarine destruction teams, attack groups of marine tigers, naval and shipbuilding departments, radar and telecommunication departments, marine armaments departments, naval schools and academies, reconnaissance units, political, financial and propaganda departments, maritime logistics, intelligence departments and the maritime register.

We further outline which tactics and techniques are used by some of the terrorist organizations that have been carrying out terrorism offshore acts so far.

(1) Maritime terrorist tactics and techniques of the Tamil Tigers:

- Blowing up ships filled with explosives near war[10], trade and passenger ships

10 Prior to arriving in Aden for its short supply of fuel, USS Cole, like all American ships visiting, was required to implement the Protection Force Plan for a visit. This plan was approved by senior US military authorities, and was conducted during a ship visit. According to the plan, USS Cole was under threat of "Bravo" at the time of the attack, raising the alertness of possible terrorist attacks. This state of threat includes steps specifically designed to protect against the impact of small ships. (Perl &O'Rourke, 2001: CRS-2). Drawing parallel to the international regulations that entered into the force in 2004 (the ISPS Code) and

- Blowing up ships filled with explosives inside of sea ports.
- Using large boats, including tankers, for ramminginto smaller ships
- Using submarines to hit ships, including air cargo carrying ships
- Use of underwater destruction teams to destroy ships
- Grounding and sinking ships in narrow canals

(2) Maritime terrorist tactics and techniques of Al-Qaeda:

- Attacking vulnerable ships at sea[11]
- Blowing up medium sized ships in ports
- Attacking vulnerable, large freight carriers (supertankers) from the air by small explosive powered aircraft

---

Croatian legal regulations (Article 15 of the Maritime and Naval Safeguards Act N.N. 124/09 and 59/12), the commander and other crew members of the ship are obliged to operate in accordance with the ship safety precautionary plan and degree of safety protection in force at each port..

11 Cruise ships and passenger ferries are, among other things, particularly vulnerable in this regard, because they are populated by a large number of people who are limited to one physical space (Warouw, 2005).

- Underwater attacks by divers or suicide destruction teams using limpet mines

Al-Qaeda encourages the recruitment of agents working as "employees at borders, and air and sea ports". (WorldNetDaily, 2003)

(3) Maritime terrorist tactics and techniques of Jemaah Islamic (JI):

- The main element of this terrorist organization is: Unauthorized access to ships and port facilities for the purpose of placing explosives

The above mentioned tactics and techniques of the terrorist organizations show all possible deadliness of terrorist attacks in the maritime domain, and show possible scenarios.

Maritime terrorism can also be committed in many other ways that are often difficult to detect and prevent. A possible scenario is the theft of a ship by a foreign terrorist organization with which a terrorist attack may then occur. Furthermore, terrorist organizations can register their ships under flags of convenience because there are much less controls there, making it more difficult to detect terrorist activities. The next way is the purchase and use of legitimate shipping companies by terrorist organizations whose ships can load explosives and hit other vessels, port facilities, critical infrastructure facilities, or densely populated town centers on the seashore. Also, tankers or ships carrying dangerous cargoes can be used as terrorist

weapons and naval vessels, oil platforms, large seaports, coastal stockpiles, power plants, bridges can be the ideal targets for such attacks. One of the most intimidating terrorist threats to maritime security includes terrorist smuggling and/or activation of explosives or weapons of mass destruction (WMD) in general, and in particular the dirty bombs which can be brought into containers in any sovereign state.

ISPS RULES

Following the terrorist attack on the USA on September 11th, 2001, the security situation changed significantly and under such circumstances it was important to bring effective legal regulations for the protection of naval ships and ports. In response to this terrorist attack which shook the world, the International Ship and Port Security Code (ISPS) came into effect on July 1st, 2004. The ISPS Code is part of the Safety of Life at Sea Convention[12](SOLAS, 1974) and is binding on 148 SOLAS contracting parties.

The Code, with some exceptions, refers to passenger ships, cargo ships of more than 500 GT in international navigation, mobile offshore facilities for exploration and exploitation of the underwater, harbors and port operational areas in which the said categories of ships comply. Aboard ships, in shipping companies and in

12 The existing Chapter XI of SOLAS was amended in Chapter XI-1. The new chapter XI-2 was established on the basis of special measures to improve maritime safety. Part A of the ISPS code contains mandatory requirements regarding the revised provisions of Chapter XI-2 of SOLAS, 1974; Part B provides guidance on these amended provisions..

seaports, the function of a security officer is introduced. The Code contains a number of other security requirements pertaining to governments, port authorities and shipping, along with a series of guidelines on how to meet these needs. This regulation also introduces recognized port security organizations that deal with port security assessment and the adoption of port security plans and other port security issues. The Portus et Navem company from Split, which as a panelist participated in the work of the Second Zagreb Security Forum and whose director is the author of this text, is one of the currently 3 recognized security organizations (RSO) for port security in the Republic of Croatia.

In order to determine if the number of terrorist offences in the maritime sector decreased after the introduction of the ISPS Code, we conducted an analysis of the number of terrorist attacks committed before and after the Code was introduced; the following results were achieved. From 1970 to 2004, 212 terrorist attacks were committed at sea[13], averaging at 8 attacks per year.

Since the introduction of the Code, to the end of 2015 (2004-2015), 94 terrorist acts[14] have been committed in maritime affairs, averaging 6 attacks per year. Although since the introduction of the ISPS Code the number of terrorist attacks has decreased, the danger of terrorist threats is still very high.

13 The Global Terrorism Database - GTD

14 GTD

The International Maritime Organization (IMO) has highlighted some of the remaining challenges for the ISPS Code:

(1) Lack of National Laws/Guidelines on the implementation of the ISPS Code

(2) The ISPS Code serves as a means to address all maritime security threats

(3) Deciding on appropriate risk assessment methodology[15]

(4) Spreading good security practices in seaports

(5) Who controls controllers?

(6) The ships face difficulties after visiting a high risk port (Shipping and Offshore, 2014).

These needs and disadvantages clearly indicate that further work needs to be done on the development of the ISPS Code, its better implementation and enforcement control.

The consequences of maritime terrorist acts

As we have seen, a large number of terrorist acts are committed in maritime affairs. Terrorists are aware of the fact that the attack on a large port area can paralyze national economies, significantly affect the world's stock markets and cause significant losses and possible long-term damage to the environment.

15 Only a model based on the concrete event of terrorism can provide insight to whether the changes in assumptions or the actual level of threats, vulnerabilities, and consequences affect the level of risk. (Willis et al., 2005: XXII).

Maritime terrorism is therefore the reality of today and is directly related to: loss of human life; great economic damage to the critical infrastructure, the cities, countries and regions where it happens, the world economy; disturbances in production, storage and supply of energy; ecological incidents with long term direct and indirect consequences. Maritime traffic is the bloodstream of Europe's prosperity, and the production of energy and transport, fisheries, the environment and climate change - all depend closely on maritime security, in one way or another (Drent et al 2013). The use of all EU instruments within a comprehensive approach enables Europe to effectively tackle marine and maritime security threats at sea, tackle the causes and restore good governance. The EU's response may relate, inter alia, to EU political and economic activities as well as to the development of co-operation, together with the security sector reform, the building of regional maritime capacities and maritime missions and EU operations (European Union Maritime Security Strategy, 2014).

According to the views of the US Coast Guard, as reported in the Homeland Security Office's 2004 fiscal report, the closure of major ports for a month could end diminish tens of billions of dollars, hinder trade and the US economy as a whole (Wrightson, 2005). The importance of the Croatian economy to the Adriatic Sea is needless to say, which is why issues relating to the protection of the Croatian part of the Adriatic Sea, ports, oil and gas platforms and other facilities of critical infrastructure against terrorism are of paramount importance for Croatian national interest.

Technical Counterterrorism Measures in the Maritime

There are a number of technical solutions that can be used to raise the level of security on ships, ports, oil and gas platforms, other critical maritime infrastructure facilities, and in general in maritime affairs. A more detailed description of these systems and their way of working would require special research, so here we will briefly list some of them. Warships have the option of using a specially designed virtual security shield[16], while for passenger ships[17]there is a specially designed virtual security pertaining to cruise ships.

Harbor facilities are generally vulnerable to terrorist attacks and are considered critical infrastructure facilities. Given their importance, they should be protected by early detection systems for security breaches, among which we especially mention: the security corridor system, the intelligent digital video surveillance system, the "friend or foe"system, the artificial door and artificial security shield. Container terminals can be specially protected by intermodal container exit systems, while fuel and hazardous cargoes are protected by specially designed safety systems for hazardous substances and fuel tank storage[18].

16 The attack on the American destroyer USS Cole in October 2000 showed the vulnerability of warships to the low-tech attacks of proximity suicide bomber during the fuel loading operation at the port.

17 This system archives all events that can later serve as a response to forensics and subsequent event analysis, and also allows alerting and tracking of incidents such as "man at sea".

18 The HAZMAT system provides optical detection and multi-sensor support: chemical, radiological, nuclear, explosive,

With the help of the following technical protection systems it is possible to: detect the entry of unauthorized personnel into the port area or on a ship; detecting unauthorized vehicles approaching a ship or working in a port area; supervise large specific areas of the protected territory; warn of threats to the facility or ship; register suspicious activities or work in the port area; track and classify people, vehicles and planes in low-flying; have a panoramic live image of the object in a 360 degree view. Such systems maintain historical data and images that are automatically archived into easily accessible forensic database and subsequent event analysis. Audible and visual alarms equipped with such systems alert the staff responsible for the security of a particular facility. This system is easy to integrate devices that can be used to make sound notifications, but also flashing or any other device that is suitable for detecting activities and persons who may harm the security of a protected object (Goslin, 2008).

Although they are of great use, technical measures themselves are not enough for an effective fight against maritime terrorism.

Development of a crisis management system at sea

Crisis management is very sensitive and complex, and the terrorist attacks on seafaring cause a number of crisis situations.

---

biometric, radar, biological, meteorological, passive infrared, magnetic, seismic and hydroponic sensors.

In 2013, the Massachusetts Institute of Technology (MIT) developed the concept of a new generation of NICs(Next Generation Incident Command System). The following year, NICS was used in more than 250 different US state organizations. This is a concept based on a multi-agency approach and supports decision-making.

The team of experts from the Split company Portus et Navem, who participated in the work of the Second Zagreb Security Forum, are developing a Web application to address the crisis situations at sea. It is characterized by multi-agency multicriteria, different tools and decision-support algorithms in crisis situations. This program uses sophisticated computer management of human resources, technical vessels and equipment at sea. The interface between the system operator and the commander of the ship is easy and affordable, all in order to provide quick and easy communication. Resolving a security or ecological incident at sea is performed through the algorithm, using plans and procedures with a clear sequence of precisely defined orders.

It is a new generation of systems that, using multicriteria analysis, represents a new, modern approach to managing risks and crises that pose the greatest risks to human lives, human health, the environment, and equally represents the added value of an effective response to the crisis within the European Union.

Conclusion

Since its inception, man has always had the need to sail, and the safety of navigation and human life at sea has always been endangered.

Today 90% of the world's trade takes place by sea. By using the research design used in this paper, we have been able to gain insight into the explored maritime terrorism problem and have proved that maritime affairs with all its critical infrastructure were indeed endangered by terrorism and will continue to pose as a target for terrorists in the future for many reasons.

Using concrete examples, we have been able to provide the description of terrorist attacks showing that targets can be warships, tankers and ships for the carriage of passengers and vehicles. Furthermore, we have shown that no oil and gas platforms have been spared from terrorist attacks, as well as ports, port facilities and many other critical infrastructure facilities. By describing the possible scenarios, we have demonstrated ways to carry out terrorist attacks with or to ships, ports, and in general maritime affairs, and shown that these scenarios are very numerous and realistic, especially when considering the high level of specialization of individual organizations for attacks with maritime goals and critical infrastructure.

Each scenario of potential terrorist attacks in the maritime sector involves significant human and material losses, major economic damage to critical infrastructure, energy supply disturbance and large pollution of the sea with catastrophic direct and indirect consequences. Terrorists are also aware of the fact that the attack on the large port area and all the relevant facilities of critical infrastructure can paralyze national economies and have a significant impact on world stock markets. As previously mentioned in the sector of the paper dealing with the application of the ISPS Code, since 2004

terrorism has tried to be prevented through the applications of this Code, however, terrorist acts are still taking place. We have particularly looked at the technical systems of maritime protection and critical infrastructure: warships, cruisers, and large ships for passenger and vehicle transport, and more technical systems for the protection of ports and port facilities and containers, pipelines, chemical and other dangerous cargoes placed therein. By using these technical solutions in synergy with other security measures and procedures such as providing naval navigation, tanker protection, LNG and LPG ships and other ships carrying strategic burdens, many terrorist attacks could in time be prevented, detected and stopped. Technical solutions that characterize a multi-agency multicriteria approach and various tools and decision supporting algorithms in crisis situations are also being developed by Portus et Navem.

Technology itself cannot ensure safety for ports and shipping, nor can it be achieved by implementing additional security procedures, physical barriers, or additional workforce to completely reduce the risk. An effective counterterrorism system in maritime affairs would be a complete, carefully planned approach which combines the greatest elements: technical, physical, procedural and informational security disciplines as a comprehensive whole.

References

1. *Douglas, J., Johnston, D. (2004). "In Video Message, bin Laden Issues Warning to U.S.".The New York Times, October 30, 2004, p. 1.*

2. *Drent, M., Homan, K., Zandee, D. (2013). Case Study on Maritime Security. Civil–MilitaryCapacities for European Security, Clingendael Report, December 2013.*
3. *Frey, B.S., Luechinger, S., Stutzer, A. (2004). Calculating Tragedy: Assessing the Costs of Terrorism. Munich: CESifo Working Paper, No. 1341, Center for Economic Studies and Ifo Institute for Economic Research, 2004.*
4. *Goslin, C. (2008). Maritime and Port Security White paper. Jacksonville: Duos Technologies, Inc. Page 2 -16*
   Gunaratna, Rohan (2006). The Threat to the Maritime Domain: How Real Is the Terrorist Threat? Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency.
5. *Haimes, Y.Y. (2006). On the Definition of Vulnerabilities in Measuring Risks to Infrastructures. Risk Analysis, Vol. 26, No. 2. 293–296.*
6. *Köknar, A. M. (2005). Maritime Terrorism: A New Challenge for NATO. Energy Security, January 24, 2005. Prepared by the Institute for the Analysis of Global Security (IAGS).*
7. *Kulišić, D., Magušić, F. (2007). O aktualnim općim pristupima i elementima za raščlambe opasnosti od zlonamjernih ugroza sigurnosti prometnih tokova. Policija i sigurnost, godina 16. broj 1-2. 41-66.*
8. *Manalo, E.P. (2004). The Philippine Response to Terrorism: The Abu Sayyaf Group. Master's thesis. Monterey, Calif.: Naval Postgraduate School.*
9. *Perl, R., O'Rourke, R. (2001). Terrorist Attack on USS Cole: Background and Issues for Congress. Washington, D.C.: Congressional Research Service, 01-RS20721, January 30, 2001.*

10. *van Ginkel, B. (2014). EU Governance of the Threat of Piracy Off the Coast of Somalia. Govaere I. i Poli S. (ed.) EU Management of Global Emergencies: Legal Frameworks for Combating Threats and Crises (2014, pp. 330–350). Presentation held in Brussels on 22-23.10. 2012.*
11. *Warouw, M. (2005). The Threat Against Maritime Assets: A Review of Historical Cases, Operational Patterns and Indicators,unpublished paper prepared for the Institute of Defense and Strategic Studies.*
12. *Willis, H. H., Morral, A.R., Terrence, K.K., Jamison J. M. (2005). Estimating Terrorism Risk. Santa Monica, Calif.: RAND Corporation, MG-388RC, 2005.*
13. *Wrightson, M.T. (2005). Maritime Security: New Structures Have Improved Information Sharing but Security Clearances Processing Requires Further Attention: Report to Congressional Requesters. Washington, D.C.: U.S. Government Accountability Office, GAO-05-394, 2005.*

STRATEGIES, LEGAL REGULATIONS

14. *Maritime and Harbor Security Act of the Republic of Croatia- Zakon o sigurnosti pomorskih brodova i luka (NN 124/09, 59/12 2009,2012:par.15).*
15. *International Ship and Port Security Code – ISPS, 2004.*
16. *European Union Maritime Security Strategy, 2014.*