SECURITY CHALLENGES AND GUIDELINE PROPOSALS FOR THE DEVELOPMENT OF UNDERWATER SECURITY

Tonći Prodan[1], Josip Kasum[2,] Marin Stošić[3], Ćiro Ugrin[4]

[1] Tonći Prodan, PhD, Portus et Navem Split Ltd.; University Department of Forensic Sciences, Split, Croatia, e-mail:tprodanportnav@gmail.com. Tonći Prodan, (born 1965), graduated from the Split Faculty of Maritime Studies. He worked for a number of years in the field of maritime affairs, first as a merchant naval officer in international traffic, then as crew member on oil platforms, and later as employee and manager in the area of maritime economy. He resumed his studies by enrolling at the Faculty of Criminology from which he graduated and earning a bachelor's degree in criminology. Furthermore, he obtained a master's degree at the Faculty of Political Science with thesis titled Common Foreign and Security Policy of the European Union and Combat against Terrorism and later received PhD in Comparative Politics with a doctoral thesis titled The USA and the EU in the Combat against Terrorism – Strategies, Models and Results. After his maritime service, he had been professionally involved in issues related to national and international security for a number of years as member of the Croatian security system. He published a several scientific articles in the fields of terrorism and counterterrorism in journals and proceedings

[2] Josip Kasum, PhD, Full Professor, University Department of Forensic Sciences, Split, Croatia, e-mail: jkasum@unist.hr

[3] Marin Stošić, Rear admiral (lower half-ret), e-mail:marinstosic56@yahoo.com

[4] Ćiro Ugrin, President of Diving Club Veterans 4th Brigade, e-mail:diving4.brigada@gmail.com

Abstract:

Maritime affairs are of great importance to the world economy, which is why the security of this area is of the utmost importance. Maritime security can be disrupted in a number of ways, and in this paper the greatest emphasis is placed on underwater security. Although states are making efforts to safeguard maritime and underwater security, there is still plenty of room to raise underwater security to a much higher level.

Keywords: Maritime, underwater, security, critical infrastructure, protection.

1. INTRODUCTION

According to the United Nations Conference on Trade and Development (UNCTAD, 2019), maritime transport is an essential branch of the world economy, because it accounts for almost 90% of worldwide trade. During 2018, around 11 billion tonnes of goods have been transported worldwide by sea. This form of transport and trade is the most cost-effective and most economical compared to the transportation of goods and people by air and land.

Due to its economy and cost-effectiveness, which enables the transportation of goods (which consequently provide better services) to all parts of the world, maritime transport is the key to the sustainable and constant development of the global economy, and it contributes to the eradication of economic deprivation and inequality worldwide.

According to UNCTAD international maritime transport and trade have been growing year by year, and in 2018 it has increased by 2.7 percent compared to 2017. UNCTAD announced that international maritime traffic will be in the constant positive raise in the period from 2020 to 2024.

1.1 MARITIME SAFETY THREATS

Maritime safety threats can be divided into two categories: deliberate offenses against maritime objects and maritime accidents.

1.1.1 DELIBERATE MARITIME OFFENSES

In the domain of deliberate delicts, we include acts of terrorism, piracy, sabotage, organized crime, etc.

As the target, terrorist actors in the maritime sector can take ports, ships, bridges, oil rigs, pipelines, and all other facilities that are somehow connected to the sea and maritime industry. According to the Global Terrorism Database (GTD), 377 maritime-related incidents occurred from 1970 to 2018.
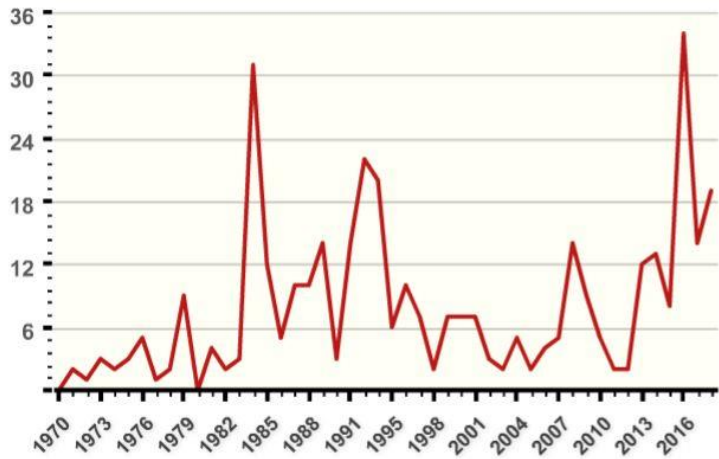
Picture 1. Maritime terrorist attacks, period from 1970 to 2018

The proportion of terrorism-related incidents in the maritime sector is up to 2% of the total number of committed terrorist acts, but the consequences of such acts remain far greater than the acts of terrorism committed ashore. One reason for this is the fact that executing a terrorist act successfully at sea, especially in undersea regions, requires extremely good preparation and good logistics.

Acts of piracy and attempted robbery are also present in maritime affairs, and from 2008 to 2017 there were 3016 such acts (Tumbarska, 2018).

Organized crime in the domain of trafficking in persons, drugs, weapons, and other illicit substances is also present in maritime traffic, and these offenses can be committed using various vessels and several types of underwater vehicles

(small submarines, autonomous underwater vehicle, etc.) (UNODC, 2013).

1.1.2. MARITIME ACCIDENTS

A maritime accident is a specific, identifiable, unexpected, unusual and unintentional event caused or related to a maritime object that results in material and/or human casualties.

Each maritime accident has its cause and each must be viewed separately and in the context in which it occurred. A maritime accident can occur for a variety of reasons, some of which include: sensory system errors, errors in data interpretation, human errors (inexperience, etc.), inadequate surveillance, or inadequate safety-at-sea (Prodan; Stošić, 2018).

2. CRITICAL UNDERWATER INFRASTRUCTURE AND HAZARDS

2.1 PORT FACILITY INFRASTRUCTURE

The security of the port and port areas is an important aspect of the security of a particular state and interstate community as a whole. Ports and port areas are potentially attractive target for terrorist organizations and organized crime groups due to the flow of large numbers of people and goods. Jemaah Islamiyah, Tamil Tigers, and Al-Qaeda have underwater terrorist capability and professionally trained underwater attacking teams (Prodan, 2017).

The biggest threats to the underwater security of port critical infrastructure are autonomous underwater vehicles, professionally trained swimmers and divers, and they all can attack by using explosive devices and in any other way. Targets of the port attacks can be the ships themselves or critical infrastructure of the port (berths, pontoons, coastal areas, etc.).

2.2 UNDERWATER SHIP PARTS

Due to their operational nature, ships are very attractive targets to terrorists, extremists and other actors as they transport valuable resources and/or passengers. Ships are an attractive terrorist target because their destruction may result

in potentially big human and material casualties, and/or big ecological disaster. Ships can also be interesting to destroy because the ship can be perceived as a state symbol. The consequences described here represent a security threat to the economy at national and international levels for the legal order as a whole.

Terror and sabotage acts on underwater ship parts cannot and should not be separated from the security threats to the port infrastructure. By their nature, ships spend a certain period of their life in ports, which is why there is an interdependence between the protection of the port, port areas, and underwater ship parts.

Ship sabotage and assault carried from underwater can be done by divers, swimmers or personnel who remotely operate autonomous underwater vehicles. Each of the actors involved in the sabotage or assault can use limpet mines, and the same mines are relatively easy to handle since the smallest variants can weigh only two kilograms. For example, we can take the VS-SS-22 (Valsellina), limpet mine which can destroy a ship that weighs 400 tons and do serious damage to the ship of up to 1500 tons. Valsellina weighs only 20 kilograms of which 10-12 is explosive. (Croatian MoD, 1995)

A new generation of limpet mines (and the old ones that can easily be upgraded to modern standards), from the perspective of members of terrorist organizations, have many advantages compared to other explosive devices and sabotage methods. The terrorists see the benefits of using limpet mines in the following:

- demining requires a certain amount of time and proper professional training,

- multiple people can quickly set up large numbers of mines,

- setting up the timer and connecting it to all mines can produce a simultaneous explosion, causing massive casualties to a ship, port infrastructure or human casualties (Murphy, 2007).

Public awareness of the underwater acts of terrorism manifested itself in 2002 when reports came to the media that Al-Qaeda is preparing divers and that they are planning an attack on US warships that visit the Indonesian ports. In 2005, the operative of the Jemaah Islamiyah terrorist group

revealed that he had been hired and sent to training where he was preparing for underwater terrorist activities (Murphy, 2007).

Recent activities in the Gulf of Oman are a real example of using limpet mines for maritime sabotage purposes. On May 12, 2019, four merchant ships were damaged by such attacks, and the quick response of the world stock market manifested itself in soaring of crude oil prices. This attack is an example of the extremely rapid and significant impact of security hazards on the economy as a whole and exemplifies that preventive activities and enhanced security measures in the field of underwater security are very important to achieve adequate underwater security protection. (UNSC, 2019).

2.3 OFFSHORE INFRASTRUCTURE

Offshore research, oil, gas and other exploitation platforms and wind farms represent critical infrastructure and they are an important segment of energy security of a particular state. The security of offshore facilities is part of the state national energy security, and it is also of interest to the international community as a whole.

Between 1975 and 2010, about 60 attacks, unlawful interferences, and security incidents related to offshore facilities were reported (Kashubsky, 2011). Swimmers and divers (alone or in a "sabotage group") and an autonomous underwater vehicles pose potential security threats to an offshore facility because they can place an explosive device on the construction above the water lines or they can perform a sabotage act within the underwater part of the facility (attacks on underwater structures, on pipes through which oil/gas flows, etc.).

Due to the operational nature of the oil/gas platforms, any sabotage, explosive device activation, or deliberate fire setting can have devastating consequences on the environment, economy and the legal order of the country.

Picture 2. Illustration of the consequences of a security-compromised offshore facility (oil platform) Source: Wikimedia Commons

2.4 UNDERWATER PIPELINES

Underwater pipelines are used for the transmission of oil and gas and in some cases water. A fluid that passes through the pipeline makes them a critical infrastructure, and any obstruction to the oil and gas flow poses a security threat to the millions of citizens in the particular area of pipeline supply. There are estimates that the value of oil production from offshore wells alone exceeds $ 300 billion a year (Wrathall, 2010). Also, any security risk or threat in the domain of underwater pipelines used for oil and gas transmission is a potential environmental catastrophe that hurts the environment and the national and international economy.

The safety risk for underwater pipelines is primarily the nature of the material that is used to build pipelines and the nature of the environment in which the pipeline is installed. The natural erosion of the materials of which the pipelines are built, changes in the sea soil, earthquakes, tsunamis, and similar events are of great security importance for the maintenance and pipeline sustainability. Also, the demanding and difficult maintenance of pipelines in inaccessible underwater areas that are difficult to dive into represents an additional challenge in achieving the effective sustainability of the entire system. Obsolete pipes already weakened by natural processes represent an easier target for attack than pipes recently installed that meet the standards of modern technology.

Also, the potential safety risk is posed by fishing boats and boats that unlawfully anchor near such installations. Heavy fishing nets used for bottom trawling or heavy anchors can pose a safety problem for pipelines.

2.5 UNDERSEA CABLES AND COUNTERINTELLIGENCE

Undersea cables are a vital skeleton of informatization (World Wide Web), digitalization (financial services, operation of state institutions, global trade, etc.), electricity supply, etc. and as such are of great strategic importance for the global economy. Commercial underwater communication cables carry about 97% of intercontinental electronic communications and as such are extremely tempting and vulnerable to acts of terrorism, illegal fishing activities, illegal anchoring, cyber-attacks, etc. (Green; Burnett, 2008); (Wrathall, 2010).

Sabotage activities of undersea cables can affect critical economic and financial national and interstate affairs. Also, undersea cables can be vulnerable to intelligence and espionage actions by states, groups, and individuals by compromising electronic data, and those activities are a threat to political stability and order of states and they can compromise international relations (DNI, 2017) ; (Matis, 2012).

Picture 3. Diver during inspection of underwater cable
Source: CTBTO Preparatory Commission (CC BY 2.0)

3. CHARACTERISTICS OF UNDERSEA ACTIVITIES

All undersea systems share certain characteristics that make them extremely important and place them in the category of critical processes/infrastructure. An undersea operating environment is physically extremely demanding. Water that slows down movement, pressure, environmental salinity, etc. often offers distorted, incomplete and ambiguous information, and without proper equipment, it is almost impossible to interpret that information. Even when information is properly collected, the problem lays in the transfer of information to land (to the human). Transmission problems are especially present in the modern undersea systems because critical infrastructure is placed at ever greater depths (Wrathall, 2010).

Undersea sabotage and assault differ from land sabotages and assaults. The undersea environment allows the attacker to be more inconspicuous when performing the act (the attacker is operating near the target, he is unnoticed and he will more likely to bypass defensive measures), and after the offensive act, the attacker will have relatively easy way out of the action zone (Wrathall, 2010). For the country where the act was executed, undersea acts often result in the inability to prosecute those responsible because of difficulties in locating the object that was used in an attack, and the perpetrator himself.

Also, all construction and defense activities in the sub-sea are economically and technically challenging, while sabotage and/or attack activities are relatively inexpensive, and with a good organizational structure of assault teams are very easily realizable. Modern autonomous underwater vehicles achieved worrying features - the basic models cost only a few hundred US dollars, and some "mid-cost underwater vehicle" is about 90 centimeters long, with no additional surface accessories, can dive about 300 meters and can develop speeds of up to 10 knots with a range of about 50 kilometers.

Picture 4. Autonomus underwater vehicle
Izvor: Wikimedia Commons

4. PROPOSAL FOR THE DEVELOPMENT OF THE UNDERWATER SAFETY GUIDELINES

4.1 ESTABLISHMENT OF THE WORKING GROUP FOR THE PURPOSE OF UNDERWATER SECURITY PROPOSALS

In order to operationalize security proposals and measures, it would be desirable to set up the working group for the purpose of underwater security and to forward its proposals to the European Commission, IMO, IHO and other relevant maritime and safety organizations.

4.2 NATIONAL AND INTERNATIONAL LEGISLATIVE AND REVISION OF ISPS REGULATIONS

In order for the safety solutions to be implemented, they need to be legally standardized in international and national legislation governing maritime safety. In this regard, amendments to the ISPS rules would be proposed, with particular attention to underwater security.

4.3 INTERDISCIPLINARY AND MULTIDISCIPLINARY APPROACH TO PROVISION OF SECURITY PLANS AND ASSESSMENTS

For each individual ship and critical infrastructure facility (ports, offshore objects, etc.), it would be necessary to make

a security assessment and based on that conclusions develop a security plan for the specific facility. Given the complexity of the risks and dangers that may come from undersea, security assessments and plans would be made by a team of experts on interdisciplinary and multidisciplinary principles.

4.4 APPLIED FORENSICS

Forensic science could be used in the underwater security aspect as a preventative tool with the help of which the hazards and risks threatening protected objects could be predicted, based on previous forensic practice and in the specific case of possible threat scenarios.

4.5 UNDERWATER TEHNICAL PROTECTION

Implementation of up-to-date techical security solutions in order to increase the safety of the subsea. This equipment would be used to monitor safety-indicative activities in the underwater area near critical infrastructure facilities.

4.6 FORMATION OF UNDERWATER PROTECTION TEAMS

Formation of underwater security teams that would assess the underwater security of ports, ships, offshore objects (platforms, etc.) and will develop and implement security plans for these critical infrastructure facilities.

4.7 EDUCATION OF CREW AND STAFF THAT ARE INCLUDED IN MARITIME, UNDERWATER AND PORT SAFETY PROCESSES AND ACTIVITIES

Given the introduction of new technologies and procedures, it would be necessary to provide training for all participants in the maritime economy (ports, shipping companies, ship crews and others).
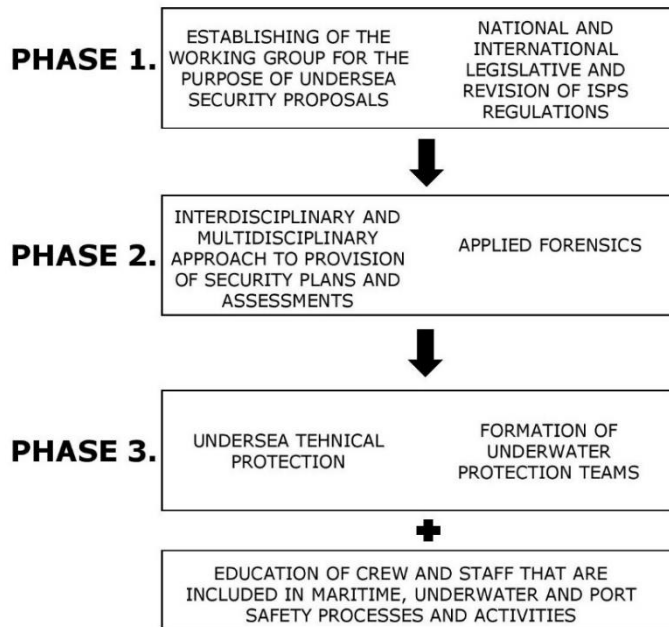
Picture 5. A conceptual example of undersea safety developmental phases

5. CONCLUSION

Maritime affairs and its security are of high importance to the world economy, as almost 90% of the world's trade is done by the seas. There are numerous safety threats to maritime transport, as evidenced by the fact that in the last 50 years 377 terrorist incidents have been linked to maritime affairs. Also, there are numerous acts of domestic organized crime and piracy, and they number surpass terrorist acts by multiple times.

Critical maritime (undersea) infrastructure is an attractive terrorist target, but even though the state is taking action and measures for undersea risk mitigation, there is still room for greater improvement. There are numerous scenarios of underwater attacks on critical infrastructure and ships, and one of the most striking examples is the limpet mine attack in the Gulf of Oman on May 12, 2019, which damaged 4

merchant ships, which prompted an immediate rise in the global crude oil price.

In addition to the assault targets already stated, the target may be offshore objects, undersea pipelines, and underwater cables. The consequences of possible attacks on those targets are multiple because they represent critical infrastructure and are of particular importance for the economy and security of the state. Underwater attacks are vastly different from land attacks, and with the advancement of technology, they become relatively inexpensive and, with good organizational structure, are relatively easy to perform.

In the light of all that has been elaborated, we consider it necessary to continue theoretical and practical research into this area of safety and to develop guidelines for raising the level of undersea security for which purpose we propose the following:

- setting up a working group to develop proposals for underwater security and forward its proposals to the European Commission, IMO, IHO and other relevant maritime and safety organizations,

- drafting national and international legislation and revising ISPS regulations,

- use an interdisciplinary/multidisciplinary approach when making security plans and assessments,

- develop models of underwater forensics through applied forensics,

- use of modern underwater technical protection,

- formation of underwater protection teams,

- training crews and personnel involved in maritime, underwater and port security.

6. REFERENCES

1. Croatian Ministry of Defence, Hrvatski vojnik (1995). Mine – jeftino i učinkovito oružje – 1. dio

2. Green, M., Burnett, D (2008). Security of International Submarine Cable Infrastructure: Time to Rethink? at International Cable Protection Committee.

3. Kashubsky. M (2011). A Chronology of Attacks onn and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975 – 2010

4. Matis, M. (2012). The Protection of Undersea Cables: A Global Security Threat by United States Navy

5. Murphy, M. (2007). The Adelphi Papers: Contemporary Piracy and Maritime Terrorism: The Threat to International Security

6. Office of the Director of National Intelligence (2017). Threats to Undersea Cable Communications

7. Prodan, T., Stošić, M. (2018). Endangering maritime security – risk scenarios and countermeasures

8. Prodan, T. (2017). Maritime terrorism and resilience of maritime critical infrastructures

9. Tumbarska, A. (2018). Maritime Piracy and Armed Robbery Evolution In 2008-2017 at Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A. Balevski", at the Bulgarian Academy of Sciences

10. United Nations Conference on Trade and Development (UNCTAD). Review of Maritime Transport 2019

11. United Nations Office on Drugs and Crime (2013). Combating Transnational Organized Crime Committed at Sea

12. United Nations Security Council (2019). Initial report on the oil tanker attacks off the port of Fujairah, United Arab Emirates, on 12 May 2019

13. University of Maryland, College Park. Global Terrorism Database

14. Wrathall, L. (2010). The Vulnerability of Subsea Infrastructure to Underwater Attack: Legal Shortcomings and the Way Forward