January / February 2018 - Issue #2

ASPIS

Advanced Superyacht Security

The threat of cyber-attacks

Cybercrime is one of the fastest growing areas of illegal activity worldwide.

FEARS AND FACTS IN MARITIME SECURITY

DRONES: A NEW PRIVACY THREAT

THE VALUE OF ACTIVE LISTENING AND ITS IMPORTANCE IN NEGOTIATIONS

0 74470 26308 1 02

Superyacht Crews Security Training Program 2018

2018 Courses, Clinics & Seminars:

- Perfect Safe Room
- Protection at Anchorage
- Restricting Access Onboard the Yacht
- Boarding Avoidance
- Anti-Robbery Technics
- Spotting the Intruder
- Preventive Actions Prior Sailing
- Evasive Maneuvering
- Bomb Found Onboard
- Immigrants Handling
- Immigrants Confining
- Contagious Agents
- Basic negotiation skills

Playing roles in security scenarios:

A series of specially planned drills and exercises conducted at appropriate intervals taking into account the yacht type, personnel, port facilities to be visited and other relevant circumstances. Debriefing after scenario unfolds – lessons identified – lessons learned together with our experts.

t: +1 786 406 6111
@: info@asd-superyachts.com

ASD-Superyachts.com

Headquarters:
201 S. Biscayne Bvd. 28fl
Miami - 33131FL
Education centers in Monaco.
Offices in America, Europe, and Asia

We are specialized in on board and in class crew training.
Every yacht is different, and every training program is specially designed and customised for each yacht and crew.
Our bespoke education programs are specially written and designed for each particular yacht.

All courses offered by our company are written by security specialists for each yacht, after a deep study of its architecture, crew, uses, and frequent destinations.

Each course includes:

1- On board or in classroom lesson, with instructors who combine over 110 years of experience in maritime security,

2- A printed and digital Quick Reference Guide for the Crew,

3- A printed and digital Step by Step Manual for the Captain,

4- A continuing education program, based on our proprietary online learning platform, where every yacht has its private, secure area, where the crew can access refreshing courses and pass a periodic exam. Captains will have access to the student's information and exams grades to understand the level of training of his crew.

5- A New Crew online training program, where the new crew member has to pass a series of courses as a first approach to understand the security plan for your specific vessel, based on the training program taken by the rest of the crew.

6- Every crew member will receive a certification (Diploma) of every course taken, and will be registered in the database of trained crews.

Our clients receive a 24/7 phone support service available for captains and crews, attended by our maritime security experts, to support the vessel when facing a threat.

Supported by:

NAVIS

ASPIS

A·S·D EDUCATION

FEATURES

FEARS AND FACTS IN MARITIME SECURITY

Page: 8

DRONES: A NEW PRIVACY THREAT

Page: 20

THE VALUE OF ACTIVE LISTENING AND ITS IMPORTANCE IN NEGOTIATIONS

Page: 26

CONTRIBUTORS

NICK KASIMATIS

Captain, Hellenic Navy class 90'. He served in all types of Guided Missile Boats as Commanding Officer. He has extended and specialized professional education by the FOST, UK NAVY on piracy, intruders, VIP protection and immigrant handling. He holds MS of Management from SALVE REGINA Uni. RI, USA, Certification from HARVARD UNIVERSITY, MA USA, YACHTMASTER OFFSHORE diploma (RYA). He speaks English, French and Italian.

OLEG VORNIK

Mr. Oleg Vornik is the CEO and Managing Director of DroneShield Limited, an ASX-listed Australian/US global leader in drone detection and countermeasures. The company is best known for its DroneGun portable rifle-shaped jammer, DroneSentinel five sensor detection system (fusing radar, radiofrequency, acoustic, thermal and optical camera feeds) and an integrated DroneSentry detect-and-defeat system.

EFSTATHIOS PSARIADIS

Efstathios Psariadis is a Captain (Ret) Hellenic Navy. Commanding officer and Executive Officer on various types of war vessels, staff officer to NATO, Director of Departments of the Fleet Command and Navy General staff. He currently is a civilian contractor as scenario scripter and role-player of NATO Operational exercises. He holds a Master equivalent on National Security Policy and Strategy from Supreme War College and a BA on Naval Science from Hellenic Naval Academy.

SUPERYACHTS FACE: THE THREAT OF CYBER-ATTACKS.

Page: 32

ANESTIS ANESTIS

Captain, Hellenic Navy. He graduated from the Hellenic Naval Academy on 1991 and he served in various types of Frigates, Fast Patrol Boats and Replenishment Ship as Operations Officer, Executive Officer and as Commanding Officer. He has a specialized professional education concerning security and intelligence issues. He has the YACHTMASTER OFFSHORE diploma by RYA.

STAFF

ASPIS is a proud member of NAVIS Media Network

Year 1 - Number 2 - January / February 2018

EDITORIAL

General Director: Pablo Ferrero
Editor in Chief: Dimitris Raftogiannis

CONTRIBUTOR

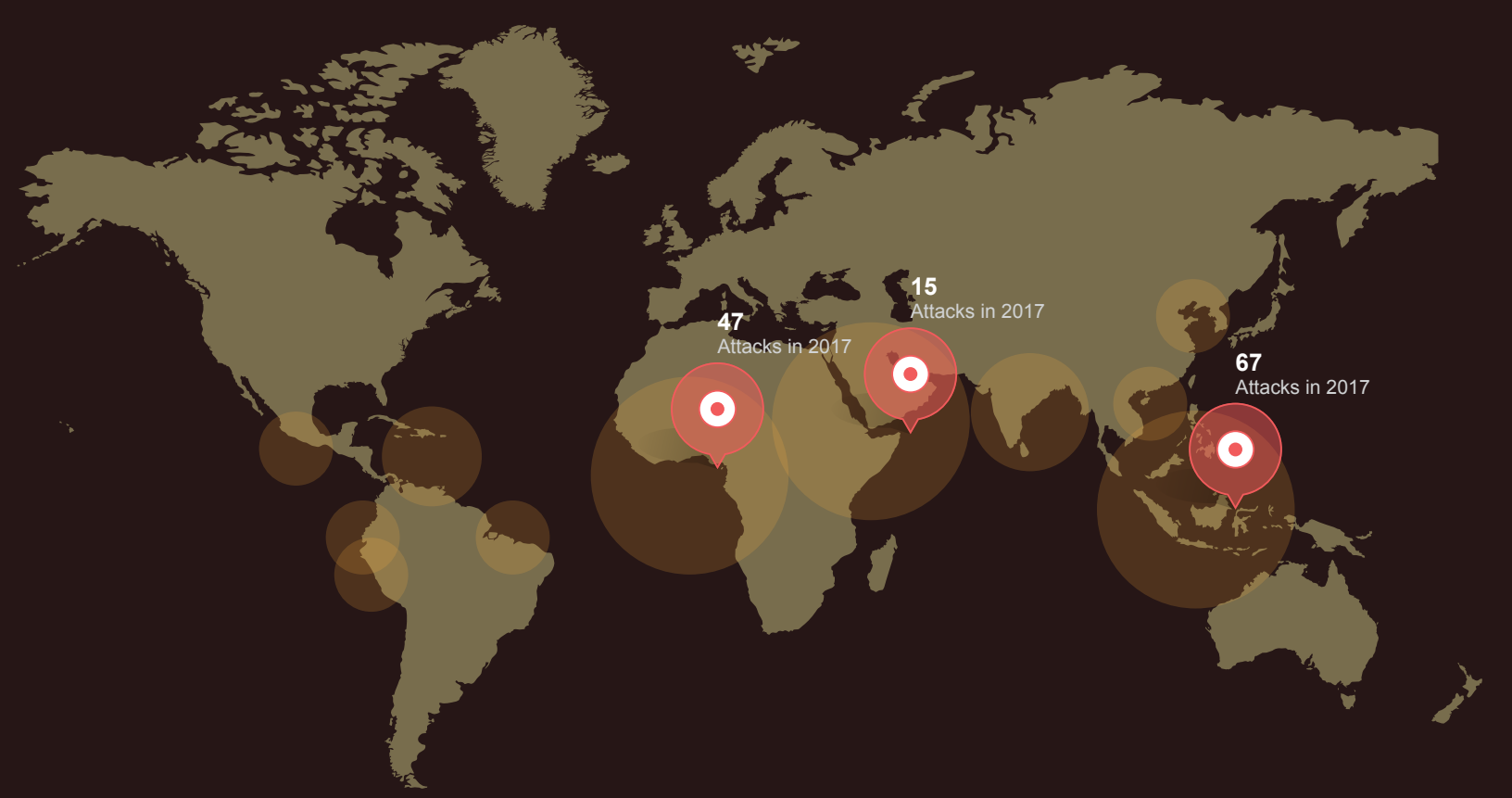
Kleanthis Kyriakidis, Nick Kasimatis,
Anestis Anestis, Oleg Vornik.

Art Director Gabriel Parra
Photography: Pablo Ferrero
Lukas Gojda
Advertising: ASPIS-Superyachts.com

Letters/Comments: info@aspis-superyachts.com
General Enquiries: info@aspis-superyachts.com
Suscription Enquiries: info@aspis-superyachts.com
Telephone: +1 786 406 6111

Website: www.ASPIS-Superyachts.com

ASPIS ISSN 2160-7958 (Print)
ASPIS ISSN 2160-7966 (Online)
ASPIS is a bimonthly publication:
Flat World Communication LLC
201 S. Biscayne Blvd., 28th Fl, Miami, Florida, 33131
t. +1 (305) 913 1337



Maritime Crime Attacks Registered in 2017

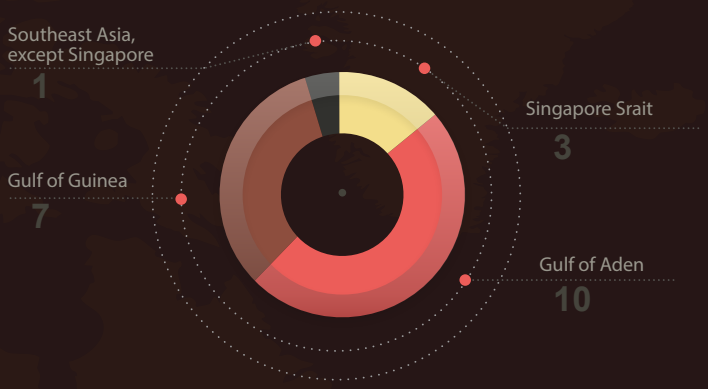
180 Incidents Reported

136 Vessels Boarded

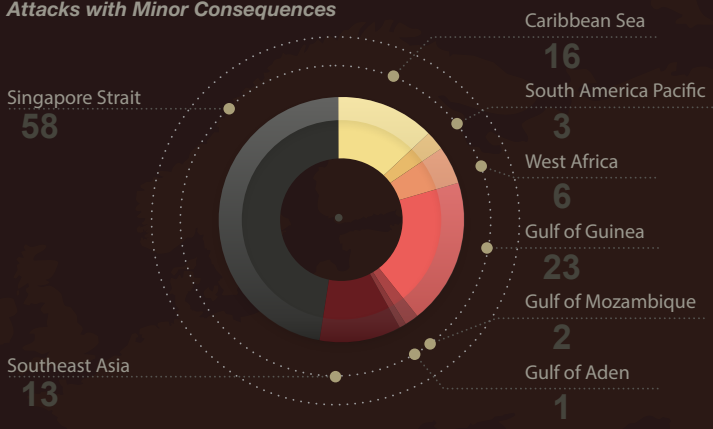
6 Hijackings

16 Kidnapped

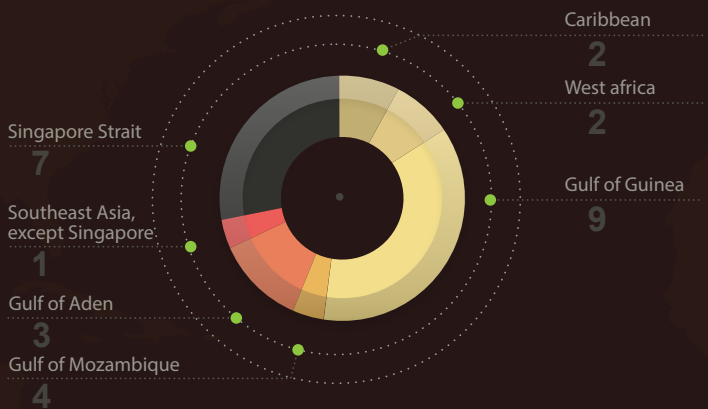
Attacks with Major Consequences



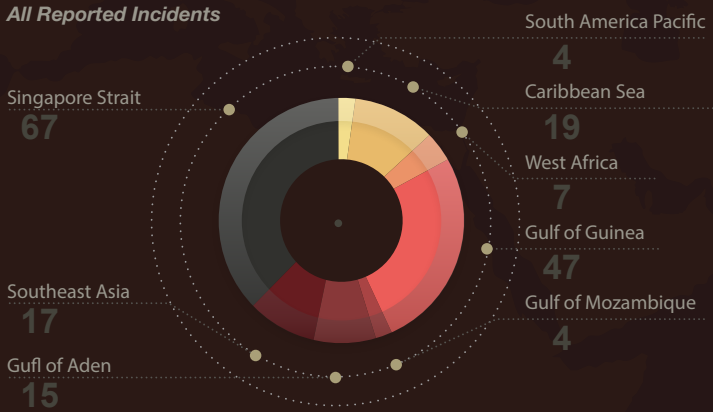
Attacks with Minor Consequences



Foiled Attacks and Suspicious Approaches



All Reported Incidents

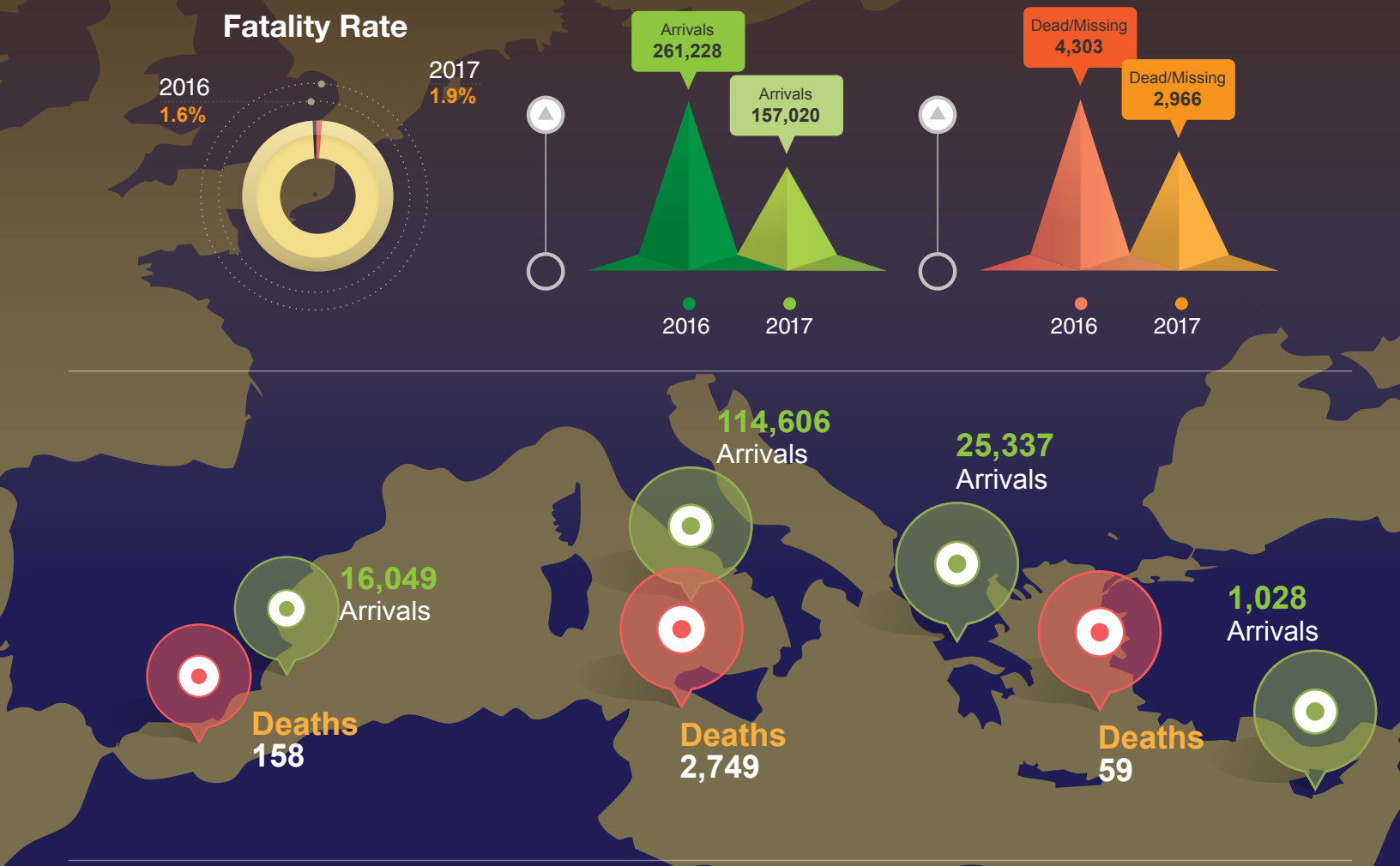


MEDITERRANEAN UPDATE

Migration Flows Europe: Arrivals and Fatalities

International Organizations for Migration - The UN Migration Agency

Published 14 November 2017



Piracy

Despite the international efforts to tackle piracy the phenomenon persists remaining a significant threat for maritime industry.

The number of the overall reported attacks in 2017 were slightly reduced, 180 down from 191 in 2016. 136 vessels were boarded of whom 6 were hijacked in 2017 whereas 150 were boarded in 2016 of whom 7 were hijacked.

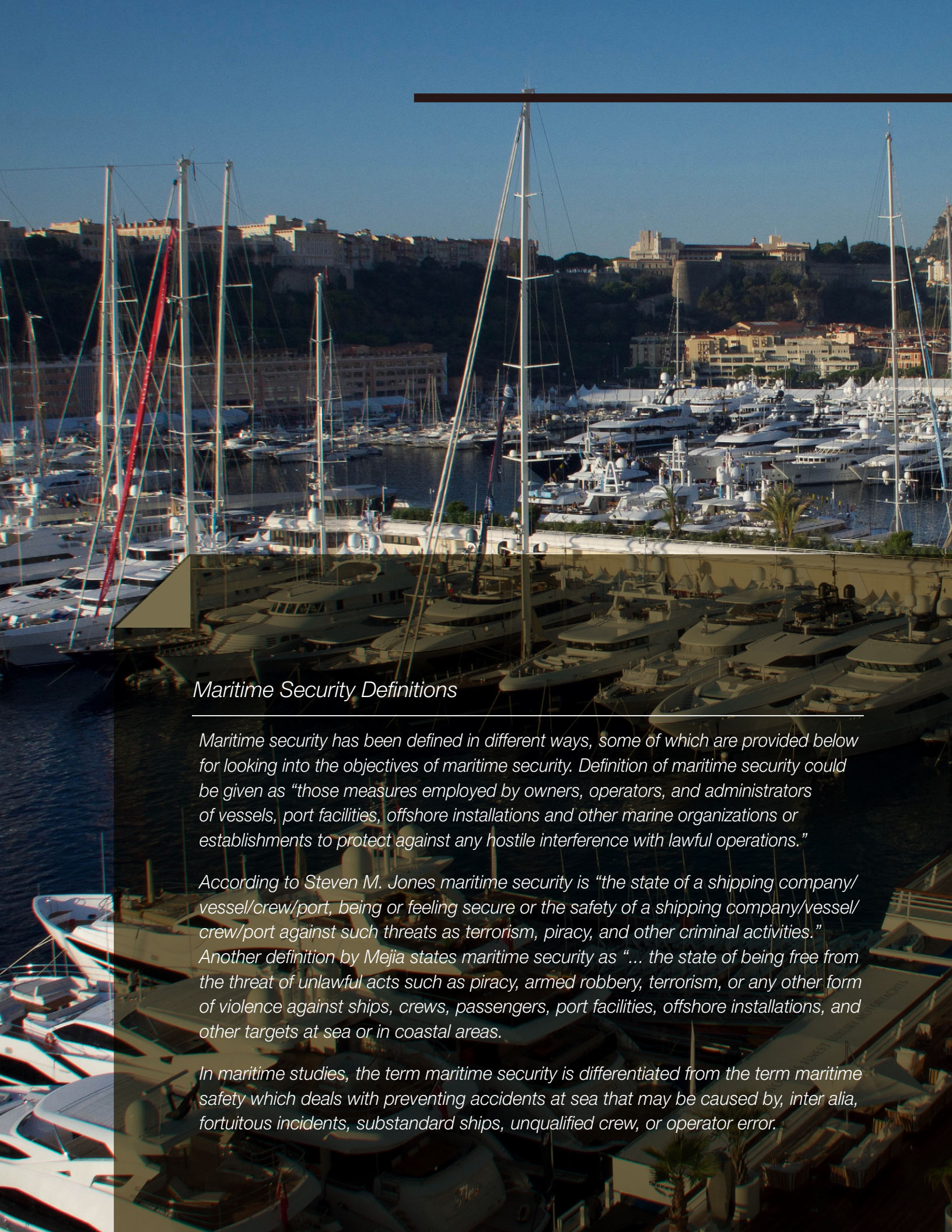
SE Asia recorded 76 attacks and Africa 57 followed by the Americas with 24. 16 vessels were fired upon, up from 12 in 2016, only 1 in 2015 and 13 in 2014. It was the highest number of vessels fired upon since 2013, a worrying trend. 3 seafarers were killed in 2017, none in 2016, 1 in 2015, 4 in 2014 and 1 in 2013. However, less crew were taken hostage, 91, was 151 in 2016. Compared to 2016, slightly more were kidnapped in 2017, 75.

Out of 180 attacks, 75 were against tankers, 50 against bulk carriers and 23 against container vessels up from 10 in 2016.

100 of the victim vessels were controlled/managed by 3 countries: Greece, Germany and Singapore.

Immigration flows

In 2017 immigration flows continued albeit significantly reduced. The Mediterranean Sea is the main sea route which leads to Europe for tenths of thousands of immigrants and refugees/asylum seekers from many African, Middle East and Asian countries. In 2017 there were 157000 arrivals to Europe, down from 261000 compared to 2016. The bulk of the arrivals were by sea. Only in the Mediterranean, 2996 were recorded dead or missing in 2017, 4303 in 2016. The trends allow for optimism as regards flows. However, developments in Middle East confrontations, civil wars, terrorism and social unrest/instability in key - countries will decide what happens short term. The only given is that immigration flows, especially towards Europe, are here to stay for the years to come



Maritime Security Definitions

Maritime security has been defined in different ways, some of which are provided below for looking into the objectives of maritime security. Definition of maritime security could be given as "those measures employed by owners, operators, and administrators of vessels, port facilities, offshore installations and other marine organizations or establishments to protect against any hostile interference with lawful operations."

According to Steven M. Jones maritime security is "the state of a shipping company/vessel/crew/port, being or feeling secure or the safety of a shipping company/vessel/crew/port against such threats as terrorism, piracy, and other criminal activities." Another definition by Mejia states maritime security as "... the state of being free from the threat of unlawful acts such as piracy, armed robbery, terrorism, or any other form of violence against ships, crews, passengers, port facilities, offshore installations, and other targets at sea or in coastal areas.

In maritime studies, the term maritime security is differentiated from the term maritime safety which deals with preventing accidents at sea that may be caused by, inter alia, fortuitous incidents, substandard ships, unqualified crew, or operator error.

BY NICK KASIMATIS

Photography: Pablo Ferrero

FEARS AND FACTS IN MARITIME SECURITY

From the beginnings, International Shipping has been the most liberal form of transportation with a high degree of flexibility in its movement. This very nature of shipping inculcated fearlessness in the system, resulting in lack of investment for the training of personnel and infrastructure development for maritime security, and a general lack of understanding of the threats posed to the ships and their crews. This article will provide an overview of the maritime security and dwell on some definitions, the vulnerability of the maritime sector to the crimes such as piracy, armed robbery against ships and maritime terrorism, and finally the preventive measures that are available in the form of international instruments.

Overview of Maritime Security and Definitions

For ages, shipping has been vulnerable to various maritime crimes. The collected data from maritime security incidents is a clear reflection of the fact that the industry was exposed to multiple maritime crimes year after year. Threats to the maritime industry were also seen during the Iran-Iraq war days. Numerous ships and maritime infrastructure were targeted during the period 1980- 1988. The hijacking of the Achille Lauro on October 7, 1985, an Italian cruise ship carrying 400 passengers by the Palestinian Liberation Front and killing of 69-year-old Leon Klinghoffer, a Jewish-American exposed the lack of security in the industry. This incident raised concerns among the International Maritime Organization member states, as it threatened numerous human lives.

The terrorist attack on the United States in 2001 further drew the attention of the world to the severity of the crime that may be committed and the level of motivation of the perpetrators. The hijacking of an aircraft is rare as it involves the crossing of several security barriers in the presence of security officials. However, no such barriers exist when a ship is at sea. Criminals can easily board a ship, overpower the crew and exploit it for achieving their goals. Some security experts fear that the biggest nightmare would be if a ship carrying explosive cargo, like LNG, were to be hijacked to be used as Weapon of Mass Destruction (WMD). The extent of damage that could be caused in such case can be seen from the collision between Norwegian steamer, Belgian relief ship Imo and ammunition steamer Mont Blanc on December 6, 1917, in Halifax Harbor. The collision resulted in an explosion that destroyed more than 325 acres of Halifax city, killing more than 1600 people, injuring more than 9,000, and destroying more than 12,000 buildings.

Fears and Facts in Maritime Security

Maritime security risks to the industry range from terrorizing of the crew, hijacking of ships and attacks on ships and port facilities to disrupt the supply chain so as to causing economic losses. Ransom money involved for release of hijacked ships and their crews ranges from $1million to $20 million, and some experts estimate that the value of cargo lost per hijacked merchandise ships is between $8 million and $200 million.

In the past, it has been seen that ships have been used for illegally transporting weapons of mass destruction, explosives, illegal materials and contrabands, and terrorists as stowaways. Confiscation of an assembly line for ballistic missiles by Indian customs officials at the port of Kandla on June 30, 1999, and seizure of approximately 8,000 assault rifles and automatic weapons from three cargo containers by Italian customs officials in the port of Gioia Tauro on April 10, 2004, are examples of illegal activities.

Shipping is the most affordable and luxury means of transportation for the more than 12 million passengers cruising each year. Passenger, cruise ships, and yachts are a high profile target. In the past, it has been seen that such incidents gave maximum commercial impetus for media, and thus they exploit the situation through social amplification of risk framework. The hijacking episode of Achille Lauro in 1985 is an example.

The above-listed incidents are clear indications that there is a prevalent threat to the maritime assets. Therefore, there is a need to protect the maritime assets from the perils of maritime crime (Figure 1). The questionnaire survey results also indicate that the respondents feel there is a need to enhance maritime security for protection of maritime assets and its users (Figure 2).

In order to protect these assets, it is important to carry out an analysis of the growth of maritime crimes namely Piracy and Armed Robbery, and Terrorism over the years and the legal instruments developed for enhancing maritime security.

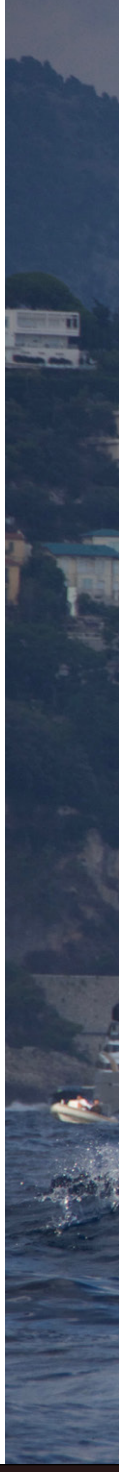


Figure 1: Threat to maritime assets.

Figure 2: Need for enhancing maritime security.

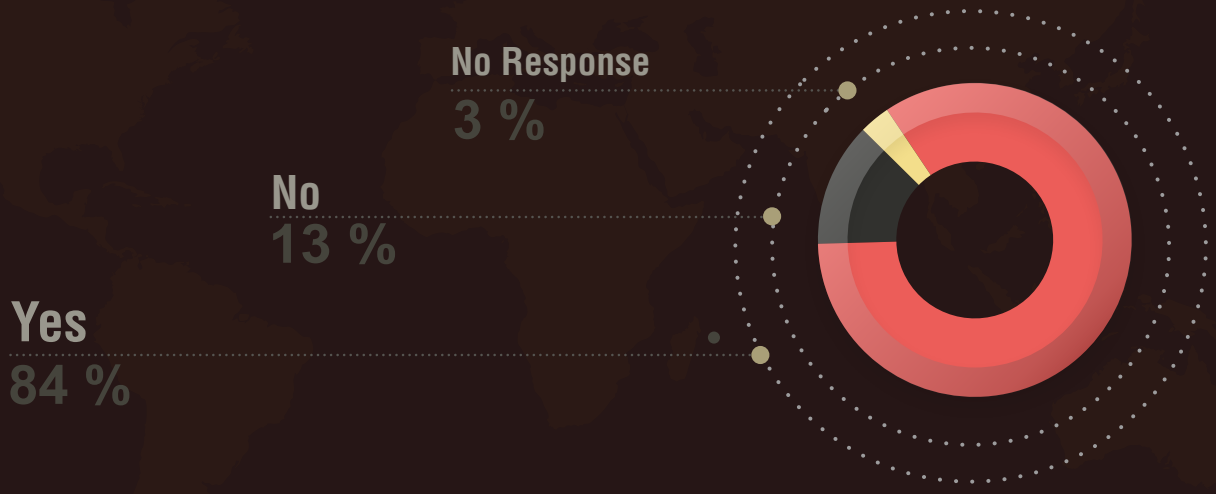
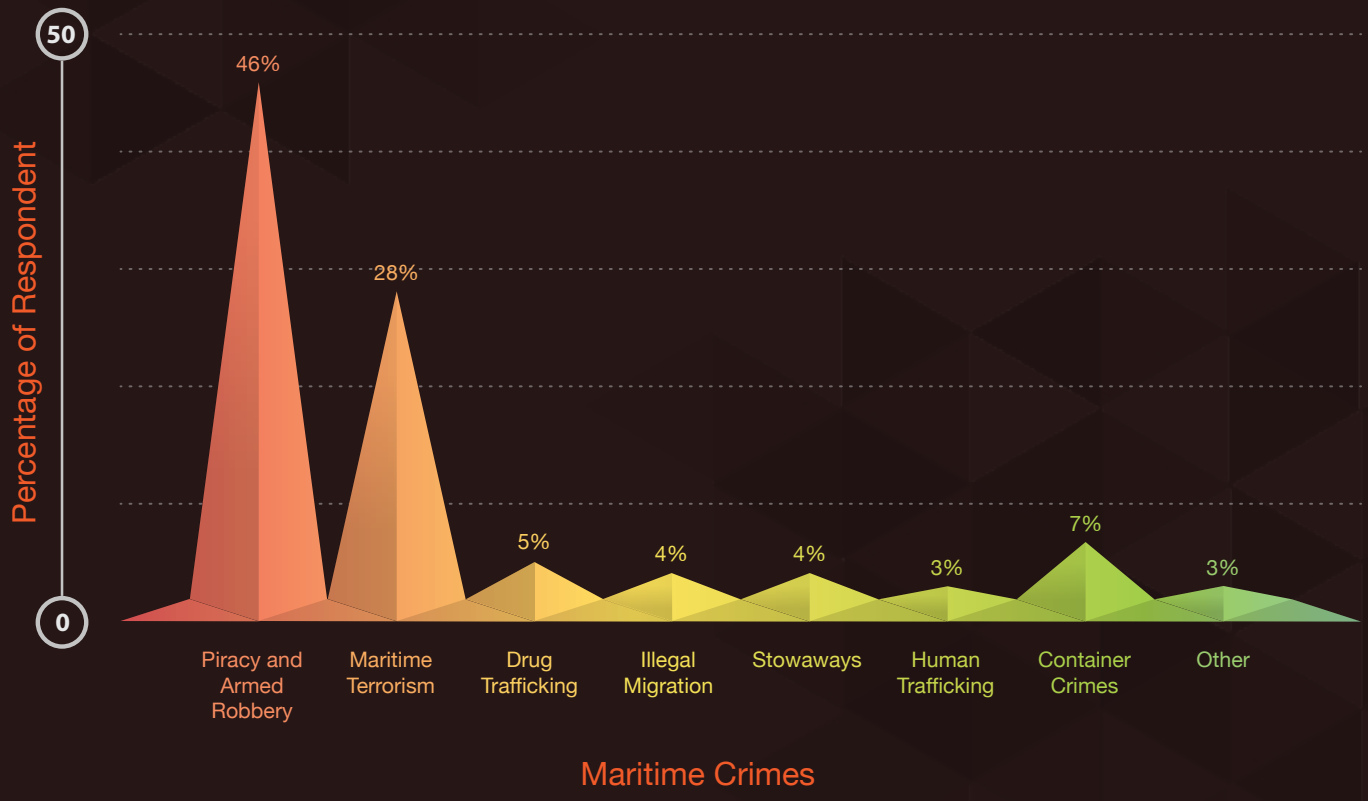


Figure 3: Maritime Crimes posing threat to Maritime Security.

Figure 4: Degree of threat posed by Maritime Crimes to Maritime Security.



Threats to Maritime Security

Today threats to maritime security are posed by maritime crimes shown in Figure3.

With rising incidents of piracy and armed robbery against ships and the consequences of maritime terrorism, experts in the field feel that these are the two crimes that pose the greatest threats to maritime security. The survey results also supplement this view (Figure 4).

Piracy and Armed Robbery against Ships

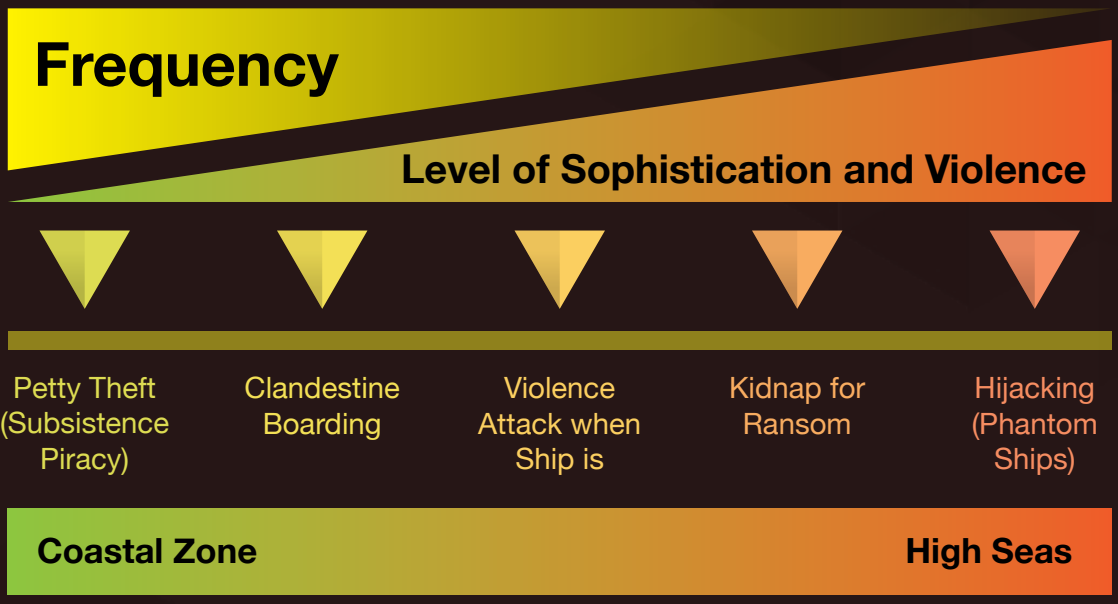
Piracy has been prevailing in some form or the other since ancient times. Thucydides in his book "The History of the Peloponnesian war" which took place in 431 B.C. said "The first person known to us by tradition as having established a navy is Minos. He made himself master of what is now called the Hellenic sea ... and thus did his best to put down piracy in those waters".

Since antiquity piracy has been posing a threat to ships, its crew, and the cargo. It has ridden the tide, becoming a menace at one time and then subsiding during other times. Capitalism and technology have assisted in making piracy and armed robbery against ships bloodier and more violent. Today, the objective of piracy is no longer theft of cash, valuables belonging to the crew, and ships store. According to Chamberlain today's pirates "no longer dress like characters from the Disney film Pirates of the Caribbean, but the Buccaneers of the 21st century have lost none of their taste for a bloodthirsty boarding". He further writes "gone are the cannon and cutlass, which have been replaced by rocket-propelled grenades and automatic rifles,..". The world community has an image of pirates as colorful swashbucklers from the 18th and 19th century Caribbean. Credit for such a portrait goes to the literary and cinematic world that portrays pirates as romantic and rebellious characters. For some, it is a seaborne version of Robin Hood.

Piracy as a menace and its global impact can be seen from the convention on the High Seas, 1958 and UNCLOS 1982. These conventions address the acts of piracy at sea and recognize it to be a universal crime, considering it as a crime and dingus punishable under the laws of every state. It is important to note that this menace started as a maritime mugging, wherein the motive

According to Chamberlain today's pirates "no longer dress like characters from the Disney film Pirates of the Caribbean, but the Buccaneers of the 21st century have lost none of their taste for a bloodthirsty boarding". He further writes "gone are the cannon and cutlass, which have been replaced by rocket-propelled grenades and automatic rifles,..".

Figure 5: Spectrum of violent act against shipping with varying degree of sophistication in different water with frequency of commitments.



was to rob cash and valuables from the ship. However, it grew as an organized crime with hijacking of ships, selling the entire cargo and further operating the ship with fraudulent documentation taking advantage of the administrative lacunae due to lax regulations of the open registers. Piracy has flourished in regions marred by political instability or poor economic growth or bears a complex coastal terrain. To name such regions, Southeast Asia, Caribbean and Africa today are the hotspots of piracy. Poor economic growth drives the coastal community to resort to theft and robbery from the ships for livelihood given their familiarity with the seas. Furthermore, the situation becomes grimmer due to lack of resources with these governments to provide adequate security to combat such incidences.

Jones classifies piracy into four categories, depending on the gravity of crime and its planning, namely:

- Opportunity Crimes
- Low Level Armed Robbery
- Medium Level Armed Assault and Robbery
- Major Criminal Hi-jacking

The International Maritime Bureau (IMB) classifies piracy on the basis of modus operandi of attack:

- Opportunity theft by persons who manage to gain access to the vessel, in port or at anchor, and steal anything handy such as paint or mooring ropes;
- Planned robbery, alongside, at anchor or underway, targeted mainly at money, crews' personal effects, and ships' equipment, often carried out by increasingly organized, determined and well-armed gangs;
- Permanent hijacking of ships and cargoes with crews sometimes being murdered cast adrift or held to ransom.

Today piracy covers a wide range of acts of maritime violence starting from petty thefts of ropes, personal belongings of crew, etc. to hijacking of ships and operating it under a fictitious name and becoming a phantom ship as shown in Figure 5.

The piratical attacks at the three hotspots of the world today are committed with entirely different motives. In the case of piratical attacks in Southeast Asia, the motive is to attack such ships whose cargo is in high demand so that it can be sold in the black market, whereas in Somalia piratical attacks are primarily for ransom. In the Caribbean Sea, the target usually is yachts, and the motive is looting and ransom. Fairplay reported Somali piracy having links with criminal gangs based at Dubai and the attacks being masterminded by them to raise funds for their operations.

Maritime Terrorism

During recent years, maritime terrorism has drawn considerable attention in the maritime sector. Piracy is viewed as a crime solely for private gains, whereas terrorism has a political objective behind it. When looking into the maritime history, hijacking of the passenger liner Santa Maria in 1961 was an incident of maritime terrorism of modern time. Later, the seizure of Achille Lauro in 1985 led to the adoption of 'The Suppression of Unlawful Acts against the Safety of Maritime Navigation' (SUA) Convention in the year 1988.

Maritime terrorism is not restricted to hijacking and seizure of ships. The attack on USS Cole in 2000 by suicide bombers, while refueling in the port city of Aden, Yemen is an example. A similar type of attack on an LNG tanker caused huge panic. According to Professor James Fay, Massachusetts Institute of Technology "Once ignited, as is very likely when the spill is initiated by a chemical explosion, the floating LNG pool

“There have been persistent reports of political extremists boarding vessels in Southeast Asia in an apparent effort to learn how to pilot them for a rerun of 9/11 at sea”.

will burn vigorously...Like the attack on the World Trade Center in New York City, there exists no relevant industrial experience with fires of this scale from which to project measures for securing public safety".

Utilizing a ship as a weapon against another ship or blocking vital choke points on the major sea routes, or attacking port facilities or vital installations on the coastlines, as was done in the case of 9/11 attacks, is very much a possibility. Reports indicate that terrorist organizations intend to disrupt the oil supply by blocking of choke points. Blocking of choke points will cause heavy financial losses as seen in the case of collision of the supply ship Lee with another ship, in the Southwest Pass entrance to the Port of New Orleans on February 21, 2004. The estimated loss to the Port of New Orleans was 3 million dollar every day. Thus blocking of choke points can cause economic recession in many countries.

Incidents of maritime terrorism are very few as compared to piracy; however, it attracts more media attention due to involvement of greater loss of life, property and consequential economic losses. The psychology behind the motive of terrorism is not material or monetary gains, but to create panic in the society for more publicity, and to elicit fear and horror. This is the main reason why a potential terrorist attack on a Superyacht could create huge impact in the worldwide industry of yachting.

Valencia quotes Brian Jenkins, Captain P.K. Mukundan and Admiral Thomas Fargo having said that presently there is no authenticated report that establishes a link between piracy and terrorism. However, a London-based security consultant Aegis Defence Service (ADS), in its terrorism report warns against the threat posed by the partnership between maritime piracy and maritime terrorism. Furthermore, a study carried out by Chalk for RAND Corporation, reveals that favorable environment for terrorists and pirates to operate is mainly due to little government regulation, absence of effective marine policing capabilities, and the necessary adherence of merchant vessels to established international sea-lanes. U.S. intelligence officials have identified 300 ships possibly owned and/or operated by the al Qaeda terrorist group. A recent study by the RAND Corporation indicates, "There have been persistent reports of political extremists boarding vessels in Southeast Asia in an apparent effort to learn how to pilot them for a rerun of 9/11 at sea".

With the ongoing war on terrorism by the United States and its allies, the possibility of terrorists and pirates synergizing against security forces cannot be ruled out. How the two groups will associate with each other, time will testify.

Since terrorism has a political motive linked to it, there has been no consensus on the definition of terrorism at the international level. Neither SUA 88 nor the twelve other international conventions and treaties focusing on terrorism give a final definition of terrorism.

On the other hand maritime terrorism incidents are less; however, maritime terrorism remains high on the risk agenda due to an unprecedented increase of acts of terrorism globally.

Legal Framework for Maritime Security

Present Instruments

Having seen aircraft being used as weapons of mass destruction, the fear of a ship being transformed by terrorists, from a medium of transport to a weapon of mass destruction, in future, cannot be ruled out. While the industry was struggling to tackle piracy, 9/11 took it by surprise. Such an act was unthinkable by the world community. Uncertainty in mind led to intensive negotiations for fostering higher degree of security and the year 2002 resulted in the adoption of maritime security instruments at IMO, amendments to the International Convention for the Safety of Life at Sea (SOLAS) 1974, and the concomitant International Ship and Port Facility Security (ISPS) Code. In addition to these, Articles 100-107 of the United Nations Convention on the law of the Sea (UNCLOS) 1982, and the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) Convention, comprise the international legal umbrella for maritime security.

Future Developments

During recent years, the concept of maritime violence has been gaining focus owing to the need to achieve both common international law and municipal law objectives with respect to piracy, terrorism, armed robbery against ships. Well chalked out laws would save the prosecutors from establishing critical legal intricacies, such as whether the act was on the high seas or in territorial waters, whether the motive was political or for material gains, and ensure successful conviction whenever such crimes are committed.

Conclusion

In this article, a brief attempt has been made to take the reader through the versatility of the maritime industry and vulnerability of its security. The Economic boom, especially in developing countries, has led to manifold increase in international trade and yachting. Ships have become more sophisticated with induction of new technology for improving efficiency and precision.

The industry was focused on safety and environmental protection; maritime security took a back seat. This article reflects that the industry is vulnerable to piracy and armed robbery, and maritime terrorism. Piracy which started off as maritime muggings has become bloodier as it has transformed from the usage of swords to automatic weapons in committing heinous crimes against innocent seafarers.

On the other hand maritime terrorism incidents are less; however, maritime terrorism remains high on the risk agenda due to an unprecedented increase of acts of terrorism globally. Shipping and especially Yachting must be always on alert and well prepared.

BY OLEG VORNIK

DRONES:
A NEW PRIVACY THREAT

Photography: Pablo Ferrero, Lukas Gojda

For years, yachts and oceans have been used to get away from the crowds, media, and various sets of prying eyes. This is rapidly changing with consumer drones that are cheap and easy to obtain and control. They are able to fly kilometers on a single charge and by pilots having minimal training. Powerful cameras are attached to the drone's underbelly and their use is changing what used to be a tranquil space.

While beneficial uses of drones are plentiful, so are the nefarious applications. ISIS has been reported to strap DIY grenades to drones and deploy against Iraqi military and civilian populations. Plane spotters deploying drones have been creating havoc around airports with flights halted until the drones are neutralized. Prisons regularly report that contraband is delivered by drones and there are many other novel uses of this new technology.

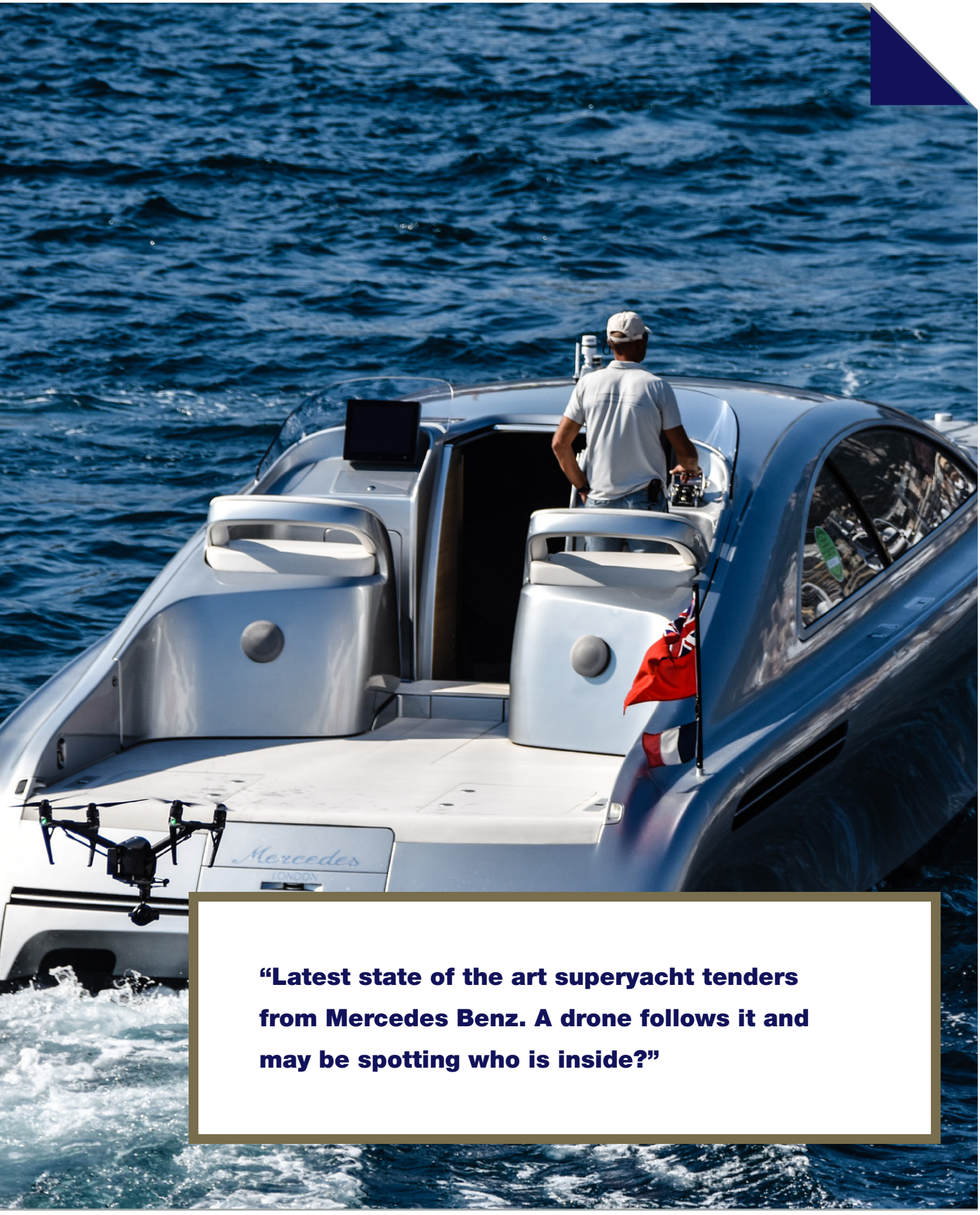
One such nefarious application is the invasion of privacy – much like when the introduction of cameras in the 1900's sparked privacy concerns a century ago. In addition to movie studios being concerned with fan drones flying around production sets, the paparazzi taking celebrity shots using drones, and others use them to peek into the windows of houses; the privacy threat has come to yachts. A drone can easily fly off land or from another yacht towards the target yacht and take photos or a video. This is easily accomplished as the drone is mostly invisible and controlled by a pilot using powerful cameras that can film a long distance from its target. A DJI Phantom drone typically cannot be seen by the naked eye within 200-300 meters in the best conditions. Visibility if further reduced when there is low contrast such as a white drone hovering in front of a white cloud. And if one is not deliberately looking for a drone, it is unlikely to notice even if it is only a few dozen meters away - it is much like focusing on one conversation at a time at a loud party.

On the other end of the drone could be the paparazzi, an industrial competitor seeking to learn trade secrets, an investigator hired by an over jealous spouse, or even a blackmailer going after an unsuspecting target.

With the issue so new, there are no privacy laws available. The illegal surveillance and trespassing laws are generally archaical and do not include aerial sources.

So what can be done to alleviate this threat? Detection is always the first step. Unlike the human mind, which cannot be on alert for drones at all times, machines are an excellent choice to perform continuous surveillance. A combination of sensors is usually best with regard to maximizing the probability of detection while minimizing false alarms. Think of a fire alarm that rings every day without a fire. Eventually the house owner switches off the alarm. The technologies available on the market today include radiofrequency, radar, acoustic, thermal and optical cameras. The range of such sensors can be up to several km, giving some warning time, and in some instances a direction from where the threat is coming.

But what to do next? Unlike detection which is universally legal (with some caveats such as privacy regulations in some situations) countermeasures for non-government users are more complicated legally. Generally speaking, there are three types of responses: (1) avoidance, (2) hard kill, (3) soft kill.



“Latest state of the art superyacht tenders from Mercedes Benz. A drone follows it and may be spotting who is inside?”

Avoidance is essentially going inside, closing blinds, and taking the yacht outside of the area of the drone's operation. Drone batteries are typically too limited today to hover for hours while waiting for the target to re-emerge. Hardly ideal, it is the safest legal approach today until the laws around drones and aviation catch up.

Hard kill includes bullets, nets and the like. While bullets are effective on direct impact, drones are known to be very difficult targets. They are small and fast moving and will likely require multiple shots where collateral damage is likely. Nets also have a very limited range. Additionally, hard kill can be unlawful – especially bullets.

Soft kill is generally recognized today as the best countermeasure where lawful to deploy by the user. A portable rifle-shaped jammer can shoot a jamming signal in a cone and reduces the need for exact targeting. There have been arguments of law regarding the use of jammers on the High Seas and not in port, thus, much like firearms topics, readers should seek their own legal advice. The jammer is effective up to a couple of kilometers. The video transmission of the drone cuts immediately and it responds by either landing down or going back to where it came from. The jamming is effective against both remotely controlled and GPS-controlled drones. Jamming can be modular to either include GPS jamming or not. GPS jamming has its own legalities associated with it and is generally reserved for military and federal agency customers only. After a signal is jammed, if the drone lands on the deck of the yacht it can be retrieved intact and an investigation conducted.

The counter-drone industry is evolving quickly, much like drones themselves with underwater drones becoming the next technology wave to arrive to the scene! Yacht owners need to be aware of the privacy and security issues and be able to take measures.

BY EFSTATHIOS PSARIADIS, CAPTAIN RET, HELLENIC NAVY

The Value of Active Listening and its Importance in Negotiations

Photography: Pablo Ferrero.

On the occasion of people being rescued at sea such as immigrants, some sort of negotiations might be required in order to maintain order and safety onboard a yacht. Likewise, on the occasion of a hostage situation, some basic negotiation skills will be needed to make an understanding of the situation. Though in such cases professional negotiators will be eventually involved as soon as the authorities arrive on the scene, there will always be a critical time gap between the occurrence of the incident and the take-over by professionals.

We negotiate every day, with co-workers, friends, and spouses. Some negotiations might be small, such as what restaurant will have dinner tonight or who will drive the kids to school and some might involve large stakes, such as convince people to stop posing a threat to themselves or others. Situations as the latter go beyond the level of a simple disagreement, they are extremely stressful and could easily end-up in a conflict if not being the result of a conflict that wasn't dealt in a positive and constructive way. Usually, the sooner one deals with a conflict by negotiating the better possibilities will have to resolve it but the timely response will not do only.

AN EFFECTIVE NEGOTIATION IS THE ONE THAT BOTH SIDES REACH A WIN-WIN SOLUTION, A RESULT THAT LEAVES BOTH PARTIES SATISFIED. IN ORDER FOR THIS TO BE ACHIEVED, ONE MUST TRY TO FIND OUT WHAT THE OTHER SIDE'S REAL INTERESTS ARE AND THAT IS SOMETHING THAT WILL NOT BE NECESSARILY VISIBLE FROM THE INITIAL STATEMENTS OR POSITIONS.

Negotiation is nothing but a discussion to reach a result which would satisfy all sides and that discussion can be effective only through effective communication. There is no negotiation without communication. As a matter of fact, the quality of communication has a direct proportional effect on negotiation. Discussion is not about fighting, shouting, raising additional communication barriers and definitely is not one-way communication driven only by emotions. Discussion is the healthy and effective exchange of one's thoughts, ideas and point of views with another. From one's end in order to have an effective discussion, it is important to comprehend the other side's thoughts and ideas, and this could only be possible if one can "read behind the lines."

The cornerstone of an effective communication is active listening, in other words, to understand as much as possible of what really is the context of the situation and to provide feedback to the speaker so that he or she knows the message is received. Active listening is an essential interpersonal skill in the process of communication, trust -building and mutual persuasion, what a negotiation essentially is.

We listen to obtain information, to understand, to learn and given all the listening we do one would think is good at it. Research suggests that after each discussion we merely remember between 25 to 50 percent of what we hear. But communication is not only about what we hear. Many researchers of body language found that a message is not just words and sentences, in a matter of fact words and sentences are a disproportional low percentage of the message one receives. Most of them agree that the verbal channel is used primarily for conveying information, while the non-verbal channel is used for transmitting interpersonal attitudes adding or subtracting credibility to the verbal message.

Professor Albert Mehrabian, known best by his publications on the relative importance of verbal and nonverbal messages, found that the total impact of a message is about 7 percent verbal (words only) and 38 percent vocal (including tone of voice and other sounds) and 55 percent non-verbal. Respectively, Professor Ray Birdwhistell found that the verbal component of a face-to-face conversation is less than 35 percent and that over 65 percent of communication is done non-verbally. Variation on percentages might exist among researchers, but they generally agree that the verbal-only part of a message is significantly low and as mentioned above one remembers only the 25 – 50 percent.

Active listening is a process not limited to "hearing" only. It is a conscious decision to listen, decipher and comprehend the message of the speaker whether this comes with words, facial expressions, gestures or any vocal properties. Neither it is being silent while the other person talks. It is a cooperative interaction where competitive attitudes have no room – as using the time the other side speaks to form arguments, becoming defensive or only try to identify logic errors.

It must involve all senses and give full attention to the speaker as otherwise the speaker might end discouraged to make its point. For that, it will be required to use both verbal and non-verbal

messages such as maintaining eye contact, smiling, agreeing by saying 'Yes' or simply 'Mmm hmm' to encourage them to continue. This feedback from our end will usually help the person speaking to relax and communicate more openly and honestly. One must remain non-judgmental, trying not to take sides or form opinions, especially early in the conversation because in the end is all about patience. An active listener must give the other person time to further explore their thoughts and feelings as if it's allowed to think out loud.

Active listening is an intrapersonal skill and requires to have firm control over oneself emotions, cultural background, prejudices and stress caused by the situation. It also requires from one to have self-awareness and modesty in order to step back when does not have the knowledge of the topic to be negotiated or understand that its intervention is not going to help.

Though this is not an exhaustive list, some active listening guidelines are:

- Focus your attention to the speaker and try to minimize any distraction that comes from the external (e.g., ambient noise, people that "hijack" the discussion) or from your own self (e.g., personal issues not allowing to focus)
- Don't interrupt as this could be perceived as a sign of disrespect.
- Restate, in all cases but more in particular when one or both sides are non-native speakers of the language the discussion takes place.
- Ask as many questions as possible in order to understand. A simple "yes" or "no" doesn't always work and could be perceived by the other side as straightforward agreement or disagreement while that might not be the case.
- Be as much empathetic as possible by understanding the context of the other side's situation.

Some examples of bad listening are;

- Not looking at the speaker.
- Interrupting.
- Body language that signals disinterest.
- Being distracted by doing in parallel something not relevant to the conversation.
- Rushing the speaker and making him feel that he's wasting the listener's time.
- Using emotional words thus obscuring the message.

An effective negotiation is the one that both sides reach a win-win solution, a result that leaves both parties satisfied. In order for this to be achieved, one must try to find out what the other side's real interests are and that is something that will not be necessarily visible from the initial statements or positions. In general, positions tend to be "monolithic" and may be hard or almost impossible to find a solution that will satisfy both sides. On the other hand, there are a number of ways to satisfy the other side's interests let alone that some of those might be in common. In other words, in order to achieve a mutually beneficial solution we need to focus and understand the other side's interests and not the initial position as this will be first stated.

For example, after a rescue operation, a number of immigrants are now onboard and must be handed over to the nearest authorities. Though were provided food or snacks the dissatisfaction of them is hard not to be noticed, in a matter of fact they complain that they were treated with disrespect and they were left hungry. This is their "stated position" that at first wouldn't make any sense given the fact

they were given more than enough food. Maintaining order onboard is of paramount importance hence overseeing the complaints by not trying to understand the real issue could jeopardize the safety of the crew, the immigrants, and the ship. Active listening will allow to comprehend that the real issue is not about the quantity of the food, it is about the conflict created due to their religious or cultural background and the kind of food provided. This is their "interest" and the true source of discomfort that has to be taken care of in order to maintain peace and order onboard.

Active listening is not just to gather or share information and ideas, but mainly to gain perspective and understanding. It is not a skill that comes naturally to everyone, therefore must be cultivated and practiced at each and every opportunity until turns into a habit and this habit have to be reinforced. It is actually a struggle with one's self that requires concentration and determination to be an active listener. The degree this skill will be developed will impact the quality of one's relationships either professional or private.

References

- Nikolopoulos, A. (2014), Negotiating Strategically – One Versus All, AUEB
- An Introduction to Communication Skills, eBook by Skills you need
- Conflict Resolution and Mediation, eBook by Skills you need
- http://www.bakadesuyo.com/2013/06/hostage-negotiation/
- https://www.skillsyouneed.com/ips/active-listening.html
- https://hbr.org/2016/07/what-great-listeners-actually-do
- http://changingminds.org/techniques/listening/bad_listening.htm

Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber discipline.

Stand-alone systems will be less vulnerable to external cyber-attacks.

CAPTAIN ANESTIS ANESTIS

SUPERYACHTS FACE
The threat of cyber-attacks.

Cybercrime is one of the fastest growing areas of illegal activity worldwide. In 2016, climbs to the second most reported economic crime, affecting 32% of organizations[1] and cost the global economy over $450 billion. The recent global malware attack, known as WannaCry[2], infected more than 230,000 computers in over 150 countries, causing mass disruption to banks, hospitals, and other organizations[3]. Some estimate that cybercrime will cost businesses over $2 trillion by 2019[4].

Nowadays most ships are increasingly using systems that rely on digitization[5], integration, and automation. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet. This brings the greater risk of unauthorized access or malicious attacks to ship's systems and networks. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media.

In many cases, a yacht, especially a superyacht, can be managed from one central unit which controls navigation systems, engines, air conditioning/ventilation systems, lighting, and entertainment equipment. While cybercriminals can hack any network in the world, the increased use of computerized systems onboard ship can lead to cyber risks that should be addressed. A ship's vulnerable systems could include, but are not limited to[6]:

a. Bridge systems.
b. Cargo handling and management systems.
c. Propulsion and machinery management and power control system.
d. Access control systems.
e. Passenger servicing and management systems.
f. Passenger facing public networks.
g. Administrative and crew welfare systems.
h. Communication systems.

1- Global Economic Crime Survey 2016.
2- The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.
3- The British National Health Service, international shipper FedEx and Spanish telecommunications company Telefonica were among the targets.
4- https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#347e19a03a91.
5- Digitization, less commonly digitalization, is the process of converting information into a digital (i.e. computer-readable) format, in which the information is organized into bits. The result is the representation of an object, image, sound, document or signal (usually an analog signal) by generating a series of numbers that describe a discrete set of its points or samples.
6- IMO Guidelines on Maritime Cyber Risk Management MSC-FAL.1/Circ.3 5 July 2017

Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber discipline. Stand-alone systems will be less vulnerable to external cyber-attacks compared to those attached to uncontrolled networks or directly to the internet.

In a computing context, security includes both cybersecurity and physical security. **Cybersecurity** is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. **Physical security** is the protection of personnel, hardware, software, networks and data from physical actions, intrusions and other events that could damage an organization. Yacht owners, Masters, and crewmembers must understand their systems in order to use and protect systems, data, and asset functions.

While cybersecurity is concerned with the protection of IT, OT and data from unauthorized access, manipulation, and disruption, **cyber safety** covers the risks from the loss of availability or integrity of safety critical data and OT. Cyber safety incidents can arise as the result of:

- A cybersecurity incident, which affects the availability and integrity of OT, for example, corruption of chart data held in an Electronic Chart Display and Information System (ECDIS).
- A failure occurring during software maintenance and patching.
- Loss of or manipulation of external sensor data, critical for the operation of a ship. This includes but is not limited to Global Navigation Satellite Systems (GNSS).

Cyber risk management means the process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders. Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of a company or yacht and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms. A cybersecurity risk assessment is also necessary to identify the gaps in a yacht's critical risk areas and to determine actions to close these gaps.

Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber discipline.

Cyberattack is any type of offensive action employed by nation-states, individuals, groups, or organizations that targets computer information systems[7], infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.

7- *https://en.wikipedia.org/wiki/Cyberattack.*


TRUE WIND
DIRECTION
191.0 °
SPEED
4.4 kts
GYRO HEADING
75.7 °
A/P SET POINT
261.5
APPARENT WIND
ANGLE
115.3 °
SPEED
4.4 kts
PORT ENGINE
COOLANT
26 °C
OIL
0.0 Bar
STBD ENGINE
COOLANT
25 °C
OIL
0.0 Bar
BOAT SPEED AND DEPTH
0.0 kts
14.9 m
693.8 m
RATE OF TURN
ENVIRONMENT
AIR PRESSURE
1022 mBar
AIR TEMPERATURE
20.7 °C
WATER TEMPERATURE
21.4 °C
POSITION
43°44.088' N
7°25.519' E
RUDDER ANGLE
GPS
COG
285.3 °
SOG
0.0 kts
menu
BRILLIANCE
ON/OFF
NAVnet
416
285.3 COG T
0.0 SOG kt
+21.38 SST °C
0.0 SOW kt
27/Sep/17
19:10:21 TIME
menu

In general, there are two categories of cyber-attacks[8], which may affect companies and ships, **untargeted attacks**, where a ship's systems and data are one of many potential targets and **targeted attacks**, where a ship's systems and data are the intended targets.

Untargeted attacks are likely to use tools and techniques available on the internet which can be used to locate, discover and exploit widespread vulnerabilities which may also exist onboard a yacht. The intent to cause damage to people's software is a driving force behind these attacks, but no particular person or group is being targeted. They tend to take the form of malware, worms, and viruses and, for the most part, they are sent out via the internet. Examples of some tools and techniques that may be used in these circumstances include:

- **Malware:** Malware, or malicious software, is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses, spyware, and ransomware. Ransomware, for example, is designed to infect a user's system and encrypt the data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data.
- **Phishing:** Phishing is a type of security attack that attempts to trick or coerce targets into divulging sensitive/valuable information. Attackers target users' login credentials, financial information (such as credit cards or bank accounts), company data, and anything that could potentially be of value.
- **Water holing:** Setting up a fake website or compromising a legitimate one in order to exploit visiting users.
- **Scanning:** Attacking wide swathes of the Internet at random.

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a yacht. An attack can be considered a targeted attack when it fulfills three main criteria:

a. The attackers have a specific target in mind and has been shown to have spent considerable time, resources and effort in setting up or carrying out the targeted attack,
b. The main aim of the targeted attack is to infiltrate the target's network and steal information from their servers,
c. The attack is persistent, with the attackers expending considerable effort to ensure the attack continues beyond the initial network penetration and infiltration of data.

Examples of tools and techniques which may be used in these circumstances include:

- **Brute force:** Brute force attacks involve a trial-and-error method used to get information such as a PIN or password. In this type of attack, automated software generates several consecutive guesses to try to isolate the correct solution.
- **Denial of service (DoS):** In a Denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email,

8- The Guidelines on Cyber Security Onboard Ships Version 2.0 (Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI).

CONCLUSION

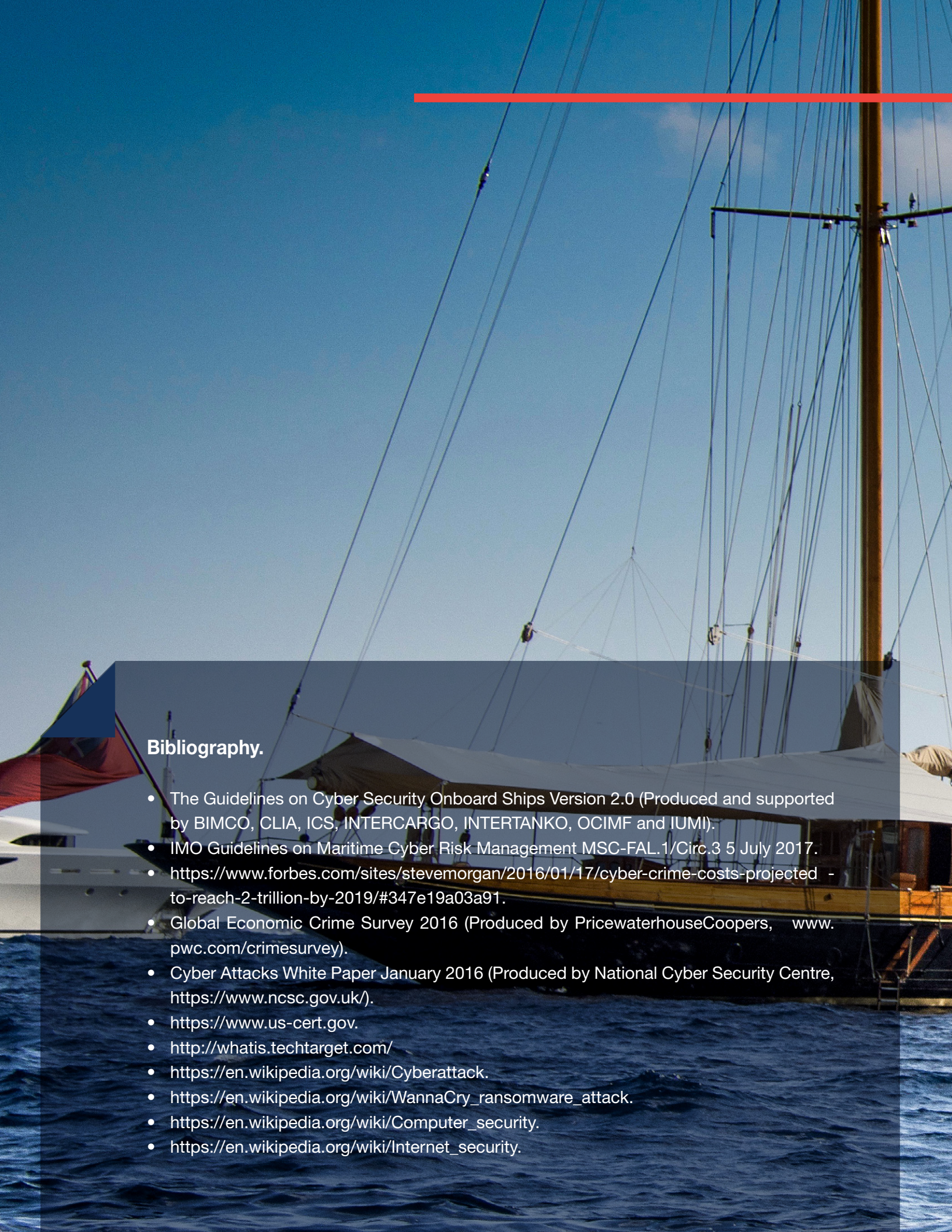
websites, online accounts (banking, etc.), or other services that rely on the affected computer. The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information.

- **Spear-phishing:** Sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software.
- **Subverting the supply chain:** To attack equipment or software being delivered to the organization (ship, company, etc.).

But how can you protect your yacht from cyber-extortion? Here are a few ways that you can use to protect your vessel from a cyber-attack:

a. Develop and implement a cybersecurity plan that clearly outlines best practices for all crewmembers.
b. Protect your valuable data. You must understand what sensitive data is and know what data you need to protect.
c. Determine what risks to your yacht are low, medium, or high-level threats. This will help you prioritize your actions.
d. Educate your crew. The more your crew know about cyber-attacks and how to protect your data, the better off you'll be. Develop Internet security guidelines and educate crew about Internet safety, security and the latest threats.
e. Password protection. Select passwords that will be difficult for attackers to guess, and use different passwords for different programs and devices.
f. Ensure all systems have an appropriate firewall. Firewalls may be able to prevent some types of infection by blocking malicious traffic before it can enter your computer and limiting the traffic you send.
g. Use and maintain anti-virus software. Anti-virus software can often recognize and protect your computer against most known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your definitions up to date.
h. Use with caution email attachments. Do not open email attachments that you were not expecting, especially if they are from people you do not know. If you decide to open an email attachment, scan it for viruses first.
i. Be wary of downloadable files on websites. Avoid downloading files from sites that you do not trust. If you do download a file from a website, consider saving it to your computer and manually scanning it for viruses before opening it.
j. Be careful what information you publicize and avoid posting personal data in public forums. Attackers may be able to piece together information from a variety of sources.
k. Hire a cybersecurity expert. The best solution for such type of problem is to handle the task to any professional company which is dealing with them regularly.

Cybersecurity is a complex subject and one of the most urgent issues of the day. A yacht faces similar cyber threats as any other commercial ship. Owners and masters must realize that a superyacht is an attractive target for hackers who are getting more sophisticated every day. An attack into the yacht's systems and data could give attackers access to critical information that can threaten the security of the ship.



Bibliography.

- The Guidelines on Cyber Security Onboard Ships Version 2.0 (Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI).
- IMO Guidelines on Maritime Cyber Risk Management MSC-FAL.1/Circ.3 5 July 2017.
- https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#347e19a03a91.
- Global Economic Crime Survey 2016 (Produced by PricewaterhouseCoopers, www.pwc.com/crimesurvey).
- Cyber Attacks White Paper January 2016 (Produced by National Cyber Security Centre, https://www.ncsc.gov.uk/).
- https://www.us-cert.gov.
- http://whatis.techtarget.com/
- https://en.wikipedia.org/wiki/Cyberattack.
- https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.
- https://en.wikipedia.org/wiki/Computer_security.
- https://en.wikipedia.org/wiki/Internet_security.

It’s time to start planning your crew training for 2018

Contact us for a free consultation and proposal

t: +1 786 406 6111
@: info@asd-superyachts.com

ASD-Superyachts.com

Headquarters:
201 S. Biscayne Bvd. 28fl
Miami - 33131FL
Education centers in Monaco.
Offices in America, Europe, and Asia

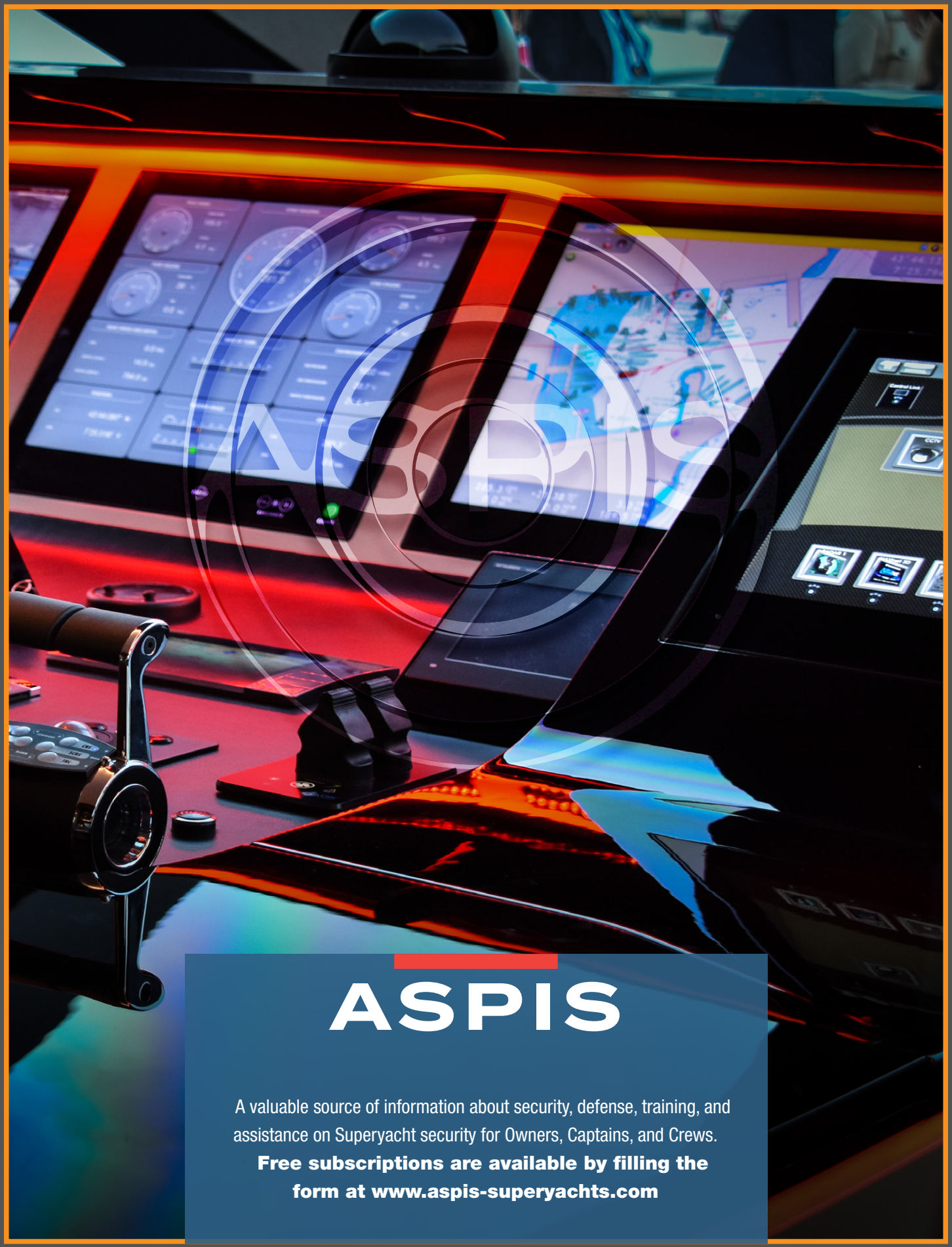
Superyachts bespoke security training programs for captains and crews

Supported by:

NAVIS

ASPIS

A·S·D EDUCATION



ASPIS

A valuable source of information about security, defense, training, and assistance on Superyacht security for Owners, Captains, and Crews.

Free subscriptions are available by filling the form at www.aspis-superyachts.com