Acting as the voice of the **security industry**

Confederation of European Security Services

White Paper on Passenger Ship Security

WHITE PAPER

CONFIDENTIAL

May 2019

Table of Contents

Publishers: **Catherine Piana,** Secretary General, CoESS

Authors: **Antoine COUDRE, Guido FALLENTHEYN, Cornelius TOUSSAINT,** CoESS Maritime and Port Security Committee

Abbreviations

BMP 5	Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea
CBRN	Chemical, biological, radiological and nuclear
CEMT- Class	A set of standards for interoperability of large navigable waterways, created by the Conférence Européenne des Ministres des Transports, CEMT in 1992
CoESS	Confederation of European Security Services
CQB	Close Quarter Battle
DG MOVE	The European Commission department responsible for the policies on mobility and transport
FPOS	First Person on Scene
GewO – SeeBewachV	*Gewerbeordung* – Trade Regulation *Verordnung über die Zulassung von Bewachungsunternehmen auf Seeschiffen* – Regulation on the approval of security companies on seagoing vessels
HME	HomeMade Explosives
HRA	High Risk Area (as defined in the BMP)
IED	Improvised Explosive Device
IMO	International Maritime Organisation
ISPS	International Ships & Ports Security Code
MARSEC 1, 2, 3	Reference to the threat levels defined in the ISPS code
NIJ Lvl	[US] National Institute of Justice - standard levels for the body armour worn by law enforcement officers
OSINT	Open Source Intelligence
PRT	Physical Readiness Tests
ROPAX	Ro-Ro vessel also carrying passengers
SBS	[UK] Special Boat Services
SSA	Ship Security Assessment
SSP	Ship Security Plan
STCW	Standards of Training, Certification and Watchkeeping for Seafarers
SWAT	Special Weapons and Tactics team
TCCC	Tactical Combat Casualty Care
UMS	Universal Measurement System – measurement system of the cargo-carrying capacity of a ship

1. Introduction

The European Maritime infrastructures are vulnerable. The evolving terrorist threat on means of transportation, maritime piracy, illegal immigration, the proliferation of arms and hazardous substances, unlawful intentional acts by means of cyberattacks and drones – these increasingly complex risks and challenges to maritime security makes it necessary to review the implementation of the ISPS code and European Port Security policies.

From a risk perspective, we distinguish between:

Passenger ships (such as ferries or cruise ships)

With hundreds of million Euros invested in each vessel and the congregation of a large number of passengers, ferries and cruise ships represent a vulnerable target for terrorist groups – similar to airplanes and mass land transportation networks. Means of attacks can include firearms, HMEs, IEDs, or even CBRN.

Up until now, there has not been a terrorist attack on board of a passenger ship in Europe. However, the bomb attack on the Philippine Superferry14 in 2004 shows that such an incident would immediately affect a large amount of people, attract a lot of media attention, and would have severe consequences for tourism, mobility and trade.

Cruise ships therefore have very strict security guidelines based on the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code. Even at MarSec threat level 1, 100% of the passengers and their hand-luggage must be screened.

While **ferries** operate in a similar threat environment, they do not systematically screen boarding passengers, their hand-luggage and vehicles; thus leaving people on board vulnerable to attacks with firearms and explosives.

Seaports & Terminals

Many European terminals and ports function as trade hubs and are critical infrastructures that face similar threats as airports do. They are key facilitators in European trade, logistics, and transportation. But today, they also continue to be vulnerable to security incidents, especially intrusions in IT systems and terrorist attacks, which can disrupt traffic and trade flows, with significant economic impact.

Minor incidents can quickly escalate to a major crisis, having an impact on a large amount of passengers and personnel, the environment, trade, and national security.

Examples of incidents can include the invasion by large groups of illegal migrants, the loss of electrical power, fire and explosions, major structural failure, spills of flammable or CBRN substances, and criminal activities including involving / targeting port personnel and passengers.

Recent threat developments include drones, which can circumvent security measures around port security perimeters, severely compromising security, and the Insider Threat.

Following repeated terrorist attacks on passengers as soft targets, studies are being made and specialist workgroups are set up to improve the security of passengers at sea. Their focus is mainly securing the ship / port interchange, i.e. strengthening the security in the port facilities receiving various types of passenger ships.

The security of the passenger ships at sea is disregarded, as attacks on ships underway between ports are – wrongly – considered as "unlikely".

2. Summary

This White Paper contains recommendations on how to improve maritime security measures on board the passenger ships based on our experience and the identified gaps.

> “Every year **400 million** passengers pass through EU ports and harbours. [...] *Available capabilities must match the scale, complexity and potential impact of maritime risks.*
> *Prevention is the foundation of protection. A higher degree of preparation, anticipation and responsiveness can be achieved if all actors adopt the duty of sincere cooperation, assessing risk and resilience to develop precautionary measures, common risk management procedures and joint contingency plans.”*
>
> in “Responding Together to Global Challenges, A Guide for Stakeholders”, European Union Maritime Strategy

Transports and leisure activities are considered as primary targets for 3rd generation terrorist organizations. Passenger ships perfectly this description, both as transportation modes (Ferries) and leisure activities (Cruises).

For a long time, sailing outside the coastal waters has been considered as inherently secure. Somalian piracy has proved this wrong. Although the risk of an attack at sea – using concealed weapons or boarding teams with speedboats – is considered low, a successful attack would result in mass casualties and greatly affect the economy of EU Member States.

In case of a terrorist act on board ships at sea, even with units on stand-by, there will be a minimum of 2 hours delay between the first alert and the drop of Special Forces on board. At sea or even on a river, the passengers would not be able to escape and the death toll would be very high.

CoESS recommends the use of ship security teams or “Sea Marshalls” on board of ROPAX, Sea & River Cruise and other passenger ships. During the critical minutes and hours following an initial event, the ship’s security crew will be the only force available and should be trained and equipped to deal with any plausible foe or event.

The objective of having on-board security is not to handle and resolve the full situation but to mitigate the risk and minimize the impact on life until the Specialized Forces reach the ship.

The costs for the Sea Marshalls can be limited. As first responders, they should also be able to assist with ship safety tasks currently carried out by other staff.

The size of the team and the type of arms / equipment must be established in the SSP, based on Ships Security Assessments that include also the risks of attacks on passengers when the ship is underway.

3. Scope

Risk management relies on the probability of occurrence and the consequences of an incident. An attack on a passenger ship in European waters is less likely to happen than on a cargo ship in the East or West African High Risk Areas (HRA) but the consequences of such an attack would be more detrimental regarding the number of potential casualties and the impact on the EU economy.

This document suggests and specifies the minimum requirements to assure the security of the passengers of cruise and ferry ships with on-board Security Teams.

This document focuses on 3 most common cases:

- National and international passenger transportation such as ferries, ROPAX, …
- International high sea cruises with stopovers in different countries
- Inland national transportation such as Rhine or Danube cruises

The topics of our proposed measures are:

- Basic doctrine
- Minimal training
- Equipment
- Organization and integration

Cargo ships, not carrying passengers, are not covered by this document. However, for those vessels we strongly recommend the generalisation of BMP5 and the possibility to use armed guards on the ships, mainly in function of the MarSec risk level (2 and 3), and not solely based on the waters they are sailing.

4. The risk: today and tomorrow

The ISPS code has greatly improved ships' security, especially by introducing of training standards and the multiple layers security system. But unlike the safety threats, security threats evolve much faster and adapt to counter the security measures in place.

The rise of soft target terrorist attacks on Western soil tells us that it is a matter of time before terrorist groups start aiming at passenger ships such as ferries. The attacks seen since the highlights of the 2nd generation terrorism have slipped from highly valuable hard targets, like the USS Cole, Pentagon and WTC to less valuable but softer targets, such as the trains in Madrid, London Public Transport, concert halls like in Manchester and Paris etc.

Transports and leisure activities are considered as primary targets for 3rd generation terrorist organizations. Passenger ships perfectly fit this description, both as transportation mode (Ferries) and leisure activity (Cruises). Even after the introduction of the ISPS code, cruise ships are still to be considered as soft targets, especially since most of the ISPS guidelines and Ship's Security Plans have been designed to deal with 2nd generation terrorism.

Today, small groups of terrorists can rent small motorboats near ports with passenger traffic lines and can easily board a cruise ship or ferry to execute their murderous plans. Somali or Guinean local pirates do this on a regular basis; there is no reason why this cannot take place in Europe.

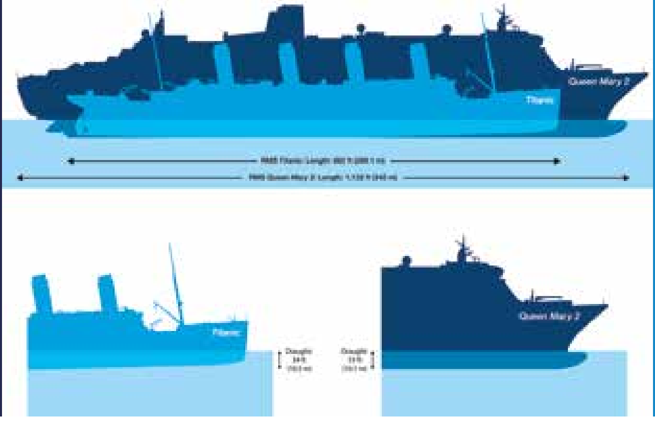
Even in an area with an extensive surveillance network, such as the North Sea, there are not enough public security vessels to expeditiously enforce security.

Actually, as shown in Paris in 2015, the authorities are well organized to face a 1st or 2nd generation terrorist attack. Special Forces are well trained to deal with hostage taking situations or hijacking. However, they do not have the real possibility to counter a 3rd generation massive terrorist attack like the Bataclan Concert Hall.

What is worse still, at sea or even on a river, the passengers would not be able to escape as some managed to do, and the police response time would take much longer. The death toll therefore would be much higher.

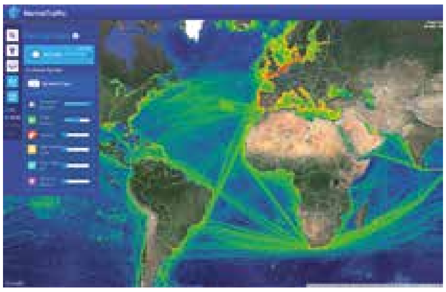
4.1. Passenger ships

Cruise ships are following the same path of gigantism as tanker and container vessels. Many giant cruise ships over 300m long are already in service, with others under construction. What is now the biggest cruise ship in the world will soon become the standard for this type of ship, with over 8 000 people on board, like the *Oasis of the Seas (6.300 passengers + 3.000 Crew).*


Queen Mary 2
Titanic
RMS Titanic Length: 882 ft (269.1 m)
RMS Queen Mary 2 Length: 1,132 ft (345 m)
Titanic
Draught
Draught
Queen Mary 2

European ferries are not as big, but they transport more passengers in comparison to their size and are easier targets, since they navigate every day on fixed routes. This predictability offers ample time and data to plan, with extreme efficiency, a devastating attack.

These kinds of ships offer a large amount of undefended potential victims as well as a very large economic sector to strike, requiring limited resources to achieve this agenda.



The cruise & ferry ships can easily be targeted when underway between ports. Even if the intervention of national security forces can occur in less than two hours in European waters, this leaves the attackers plenty of time to perform their ignominious task.

For a long time, sailing outside the coastal waters has been considered inherently secure. Somalian piracy has proved this wrong.

ROPAX (Ro-Ro with passengers) are very **valuable** and **vulnerable targets**. This is one of the reasons why the EU DG MOVE launched a study about their vulnerability in 2018. They have relatively low accesses above the waterline, with easily accessible open decks and large public areas. They also embark hundreds of vehicles, each one requiring substantial efforts when checked for concealed weapons.

Even if ROPAX sail relatively close to the shore making an intervention of public security forces faster than on high seas, one can hardly qualify an armed intervention by Special Forces at sea as easy.

While cargo ships of similar size, following the BMP 4 & 5 recommendations, have citadels for the protection of the seafarers, passenger ships lack secure and easy to defend zones.

4.2. Inland passenger ships

Although Inland Passenger or River Cruise Ships do not fall under the ISPS code or the EU Regulation 725/2004, we included them in our study.

In many ways, the inland water passenger ships are more vulnerable than the blue water ships. Actually, it is far easier to get aboard inland water ships because they sail with a regular schedule on thousands of kilometres of unmonitored and unprotected waterways.

The ISPS code and Regulation 725/2004 clearly state in article A 3.2 and B 4.20, for example, that contracting government security measures should apply in the most extensive way as possible, especially in case of interactions with ships or ports used by ISPS compliant ships.

Even if the Inland Ports consider the ISPS security measures as "less relevant", these measures are not "useless".

Ideally, river cruise ships and ports receiving them should be submitted to the EU regulation 725/2004, with specific items designed to meet inland ship and port specificities.

Why?

- → Europe possesses one of the biggest networks of inland waterways in the world, most of which are directly connected to major ISPS ports.
- → The European inland waterways are relevant critical infrastructures for industrial and transport services[1]. They flow directly through major European capitals such as: Paris, Amsterdam, Strasbourg, Brussels, Berlin, Stockholm, Warsaw, Bucharest, Budapest, Bratislava, Prague, Vienna … , which also happen to be some of the most urbanized and crowded areas in the world. Furthermore, other critical infrastructures such as nuclear power plants and chemical factories are located along these waterways.
- → CEMT 2 class ships and above are over 500 UMS and can sail in the same ports and coastal waters as those covered by the ISPS code. Technically speaking, they are ships that should comply with the ISPS code except for the waterways they are using.
- → The Port Security Directive and ISPS code are primarily risk- based, with the protection of human life and the environment as a priority.
- → The ISPS code states that infrastructure or ships not submitted to the code should not be allowed to interact with compliant ships and infrastructure without equivalent security measures.
- → The CEMT in 2002 has stated that inland waterways are a privileged way to bring terrorism into the heart of Europe.
- → Passengers on board river cruise ships are usually elder, sometimes with reduced mobility, and can't escape an attack, similar to those sailing in blue waters.

[1] This was noticed in 2018 by the low water levels during summer time and the resulting logistic problems to supply areas with petrol and other regularly shipped goods.

5. Security forces intervention

Let’s take a look at France. The country has been the target of various terrorist attacks during these last years and it has taken many steps to enhance its overall security.

When including the overseas territories, France has one of the largest maritime areas in the world.

We take France as an example, but there is no single reason to believe that reaction times in other EU Member States will be sensibly faster.

5.1. Reaction times

Based on OSINT, the French maritime security response capacity consists of 6 dedicated platoons for maritime security.

1. Le Havre (French main container port – 2006)
2. Port-de-Bouc (Fos-sur-Mer – 2009) Mostly an oil & gas port
3. Marseille (Main Mediterranean port – 2010)
4. Dunkirk (English Channel multipurpose port – 2017)
5. Nantes St-Nazaire (Gas, oil & chemicals port – 2018)
6. Calais (Main passenger port, English Channel – 2019)

Each platoon should have:

- 40 military law enforcement officers,
- A 13 metres surveillance and security boat,
- A 9 metres speedboat,
- A 6.5 metres semi-rigid speedboat.

Beside these platoons, which are in charge of everyday surveillance and low level intervention like smuggling control, France has also reinforced its security Special Forces.

French military Special Forces can be mobilized, especially the “Commando Marine” (Seal or SBS type units), with two units dedicated to counterterrorism on board ships: “Commando Trepel” & “Commando Jaubert” and Underwater actions “Commando Hubert”.

The French doctrine about maritime actions relies on the usual small boats delivered units, helicopters airborne assault or swimmers/divers for amphibious infiltrations.

2016 and 2017 exercises show a helicopter delivered unit dropped on a ferry off the coast of Brittany making it the preferred type of action, without doubt, because of the speed of the airborne delivery.

In case of terrorist acts on board ships, even with units on stand-by at +30’, good weather conditions and quick political decisions, there will be a minimum of 2 hours between the first call from the ship and the drop of Special Forces on board; this will more than likely rise to 3 hours before they access the ship’s plans to prepare correctly for operations.

As a comparison: during the Paris attack of 13 November 2015, the first police officers arrived 20 minutes after the beginning of the attack. However, the first SWAT trained elements arrived approximately within 60 minutes and a full unit, 90 minutes after the first call. The assault finally began 150 minutes after the initial attack. These units were stationed at a driving distance to the attack of 15 to 35 minutes only.

In case of terrorist actions on board ships, even with units on stand-by, there will be a minimum of 2 hours between the first alert and the drop of Special Forces on board.

5.2. The risk

The English Channel is a very busy maritime zone and it is heavily monitored, but mostly for safety reasons. A disabled ship in this area could easily lead to catastrophic consequences.

The area is closely watched by French and British monitoring and rescue centres. The security network is clearly designed for a basic law enforcement duty dealing with smugglers and illegal fishing.
The same applies to the Mediterranean and Baltic seas.

5 scenarios have been studied in 2018 by ICF under a DG MOVE project. One of the most likely scenarios is the attack of a ferry ship by a lone active shooter or a small group armed with handguns or assault rifles ("Bataclan de la mer").

Security professionals familiar with this study consider that the threat assessment underestimates some scenarios, as the study was based, amongst others, on interviews (the fears expressed by the interviewees) rather than the worst and technically feasible threats.

One of the main objectives of the ISPS code is "Preventing the introduction of unauthorised weapons, incendiary devices or explosives to ships or Port Facilities."

From a risk point of view, we see 3 possibilities of introducing arms:

→ **Via the terminal:** weapons concealed by passengers or personnel.

- The mitigation measures for the risk posed by passengers will be addressed by the specific Working Group on Passenger Ship Security.
- For the Insider Threat we refer to the EU-funded project coordinated by CoESS. It provides a simple and concrete web-based set of tools (**https://Help2Protect.info**) for use by transportation ecosystems, but also other critical infrastructure environments.

→ **Water-borne:** Increased searches in the terminals can dissuade criminals to use this way of boarding the ships. The delivery of a small armed team with a fast boat while the ferry is underway is technically possible and not too difficult to organize, especially for ferries always following the same routes and schedules.

→ **Air-borne:** drones represent another threat for the vessel security, not sufficiently covered in the recent studies. Due to the development during the last years, piloting drones with payloads up to 10 kg from the coast line over a couple of kilometres is neither a high financial investment, nor a highly technical task. Drones may be used by terrorists of 3rd[2] or even 4th[3] generation:

- To transport weapons, grenades or any other kind of explosives on board of vessels to be received and used by terrorists.
- As a carrier for explosive or chemical bombs for direct attacks on the ships and passengers.

[2] 3rd generation: Targeting civilians in the transport and leisure industry

[3] 4th generation: Decentralized warfare; the fight which used to be carried with traditional weapons has shifted into potential technology driven attacks.

5.3. Risk mitigation

To mitigate the risks of armed attacks on passengers, strengthening security measures in the port facilities alone are not sufficient, as weapons can be introduced via sea or air into the ship after the departure from the port.

Similar to cruise ships, ROPAX ships and River Cruise boats should have on-board security, sufficiently trained and equipped to deal with the risks of an attack at sea. The size of the team and the type of arms / equipment must be established in the SSP; based on Ship Security Assessments that include also the risks of attacks on passengers when the ship is underway.

During the critical minutes and hours following the initial event, the ship's security crew will be the only force available and should be trained and equipped to deal with any plausible foe or event.

6. Recommendations

In the case of today's most feared scenario, i.e. massive shooting in a confined area with no means of escape, early intervention in the seconds or minutes following the beginning of the event has proven to be the best way to avoid mass casualties.

We have the perfect demonstration of this. During the Brussels-Paris Thalys train attack, US Armed Forces reservists, unarmed, took the lead and neutralized the threat with minimum casualties after the first individual interventions from other passengers.

The ISPS code states that specific ship security measures belong to the Ship Security Officer's responsibilities. With few guidelines and even less regulations, the risk management of those threats is almost non-existent. Even insurance companies, who are the usual capstone of risk management and motor of security, have not imposed additional measures.

Far from emergency security and safety forces, embarked security staff should be able to deter, delay or at least mitigate any attack on ships and threats to its crews and passengers.

CoESS recommends the use of ship security teams or "Sea Marshalls" on board of ROPAX, Sea & River Cruise and other passenger ships.

6.1. Organisation of security

The objective of having on-board security is NOT to handle and resolve the full situation but to mitigate the risk and minimize the impact on life until the Specialized Forces reach the ship. To achieve this objective, the principles as described in IMO BMP 5 apply since it is unlikely to completely avoid boarding by one or more motivated attackers.

If the Citadel doctrine, based on a security zone, which prevents the control of the ship by an attacker, is relatively efficient in countering a piracy threat, it is totally inadequate to counter a terrorist attack aiming to cause many casualties aboard passenger ships.

The protection of the passengers should be achieved both by:

- Protecting the access to the ships' controls (bridge & engine)
- Creating passenger "safe zones" on board

At least until emergency security forces can intervene.

The composition of the on-board security should also take into account the organisation of the transport of passengers as well as provide room for each ship and type of exploitation specific needs.

The organisation of the transport of passengers can be with:

- Short voyages not requiring a 3-watch system
- Long voyages which requires continuous watch-keeping systems

The on-board security teams can be:

- **Vessel Protection Detachments:** Uniformed law enforcement or military personnel embarked on a vessel with explicit approval of the Flag State (as already used on board of some ferries between UK & France).
- **Private Maritime Security:** Embarked private security force personnel hired by the shipping lines, similar to the PMSC teams operating in the High Risk Areas (Indian Ocean).
- **In-house Security:** ship's crew with specific security duties, similar to the teams on-board of the ocean-going cruise ships.

On board security forces should always become a full part of the ship's crew even if they are contracted by external private security companies and not by the ship operator. As proven for the security of merchant vessels, the Ship Master will always be the person to decide about armed actions.

The security of people on board is definitely something to be considered as a "service on its own"; and the team should wear a uniform that clearly distinguishes them.

- **At Marsec 1**, the tactical gear should be concealed under the clothes, like soft NIJ LvL2 bulletproof and slash proof body armour, and the gear needed at the belt.
- **At Marsec 2**, the tactical gear could be reinforced with a tactical jacket and individual kits needed to match the likely threat. At this point, public will certainly be aware of the risk. Seeing visible security measures should reassure them and help keep the passengers feel secure to use ship transport.

- **At Marsec 3** or when the ship is considered to be under clear and present danger[4], it would be preferable to wear fire resistant coverall suits and tactical gear including NIJ Lvl3 or 4 tactical bulletproof jackets.

An observation & reaction team of two persons, equipped with counter boarding equipment and placed on the upper deck, can ensure an effective watch of ship approaches. This support team represents the capstone of the ship security force.

The rest of the protection force should be organized in teams of 3[5] offering the optimal tactical versatility in a mission of protection; one member to manage passengers whilst the two others face and handle the threat. This means that the protection team should be built around a multiple of 3. The number of security personnel should be determined by the number of people aboard, the size of the ship, the number of decks and the length of the trip (watch-keeping or not).

As minimum staffing requirements we recommend:

- River cruise boats: a team of 3 security officers
- ROPAX & Ferries[6]: an observation & reaction team of 2, and an intervention team of 3 security officers
- Ocean going cruise ships: an observation & reaction team of 2 and 1 intervention team of 3 security officers per 1000 passengers

A ship should not have less than one security team for three decks.

When the ships are over 300 m long, a second observation & reaction unit should be deployed on the upper deck to ensure good coverage of ship approaches.

[4] At this threat level, most flag countries will asks to immobilize their ships. But it is still very possible that a rise to Marsec 3 will occur when the ships are actually at sea.

[5] Following the requirements of German BAFA (GewO (SeeBewachV and SeeBewachDVO) teams may also consist of 4 members to allow first responder activities by a team member under the surveillance of a 2nd member.

[6] Upto 1000 passengers and maximum 3 decks.

6.2. Training

The training should follow IMO security and safety model courses and the highest international standards in order to be efficient and meet legal requirements.

We recommend that the “Ship Marshalls” should be trained with a mix of close protection officer and ship security guard. The guidelines could be inspired by USN VBSS training.

STCW:

- STCW A-VI/1: Basic Safety Training
- Crowd management & Passenger safety
- Security Training for Seafarers with designated Security Duties
- Maritime English
- Offender profiling training for the recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security

As first responders, the Sea Marshalls should also be able to back up ship safety and emergency operations, especially passenger health issues and firefighting.

Armed Security Training:

- International rules of engagement and BMP5
- Precision shooting at 800m following NATO Marksmanship standards, to deter unwanted approach of boats while at sea
- Tactical analytic shooting and CQB training: “Ship in a box” training centre
- FPOS or TCCC training
- Unarmed self-defence and non-lethal means

Physical Training / Fitness:

- As per Navy PRT (Physical Readiness Testing)

7. References

- ISPS Code
- EU Regulation 725-2004
- Best practice in transport security – CoESS 2017
- Guide to maritime security and ISPS code – IMO 2012
- French Department of Transport - Security Guidelines for non ISPS ships – 2016
- ISO 16747 standard for Port Security
- IMO Best Management Practices - BMP5
- German Regulations for Security on Seagoing Ships (§ 31 GewO SeeBewachV and SeeBewachDVO)
- Help2Protect - Insider Threat Program funded by the Internal Security Fund (ISF) of the European Union
- Identifying Capabilities Gaps in Shipboard Visit, Board, Search, Seizure (VBSS) teams, Kevin M. Ray, 2010

Photo credits:
©Depositphotos: p. 1 sewer12, Stahlpix, p. 8 Furian, p. 9 phb.cz, p. 13 sewer12 - ©Marine Traffic: p. 8

Acting as the voice of the **security industry**

Confederation of European Security Services

coess.eu

Jan Bogemansstraat | rue Jan Bogemans 249
B-1780 Wemmel
Belgium
chantal@coess.eu

T +32 2 462 07 76
F +32 2 460 14 31

acapella.be