PROMERC

Protection Measures for Merchant Ships

EUROPEAN COMMISSION

SEVENTH FRAMEWORK PROGRAMME
SEC-2013.2.4-2
GA No. 607685

Protection Measures for Merchant Ships

Deliverable No.	ProMerc D1.1	
Deliverable Title	Counter-Measures Database	
Dissemination level	Restricted (RE)	
Written By	Ronald Funk (CMRE) Huw Davies (FLIR) Adrienne Turnbull (CMRE) Francesca de Rosa (CMRE)	2014-05-29
Checked by	WP leader Ronald Funk (CMRE)	2014-05-29
Approved by	Huw Davies (FLIR) - Coordinator	2014-05-29
Status	FINAL	2014-05-30

SEC-2013.2.4-2 - Protection Measures for Merchant Ships

Acknowledgement:

The author(s) would like to thank the partners in the project for their valuable comments on previous drafts and for performing the review.

Project partners:

1 – FLIR – FLIR Systems LTD - EN
2 – CMRE – NATO Science and Technology Organisation - BE
3 – WMU – World Maritime University - SE
4 – UoA – University of the Aegean-Research Unit - GR
5 – SAMI – Security Association for the Maritime Industry Limited - EN
6 – UNR – Uniresearch B.V. - NL
7 – TNO – Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek - NL
8 – EII – Engineering – Ingegneria Informatica Spa - IT
9 – Oldendorff – Oldendorff Carriers GMBH & Co KG - DE

Disclaimer:

This project has received funding from the European Union’s Seventh Framework Programme for research; technological development and demonstration under grant agreement no 607685. The contents of this publication is the sole responsibility of the project partners involved in the present activity and do not necessarily represent the view of the European Commission and its services nor of any of the other consortium partners.

Executive Summary

Introduction

The PROMERC Description of Work (DOW) Task (T) 1.1 is a Counter-Measures[1] (CM) survey to "create a capability catalogue of available and emerging active and passive counter measures which will be assessed in subsequent tasks and developed into a database in WP3. This report scope is limited to the PROMERC Deliverable (D) 1.1 "A capability catalogue of available and emerging active and passive counter measures" that documents the results of Task 1.1 CM Survey.

The CM catalogue is a list of potential CMs that covers the range of technical capabilities intended to reduce the observed risk of piracy events that would otherwise succeed. T1.2 will review the piracy event data, T1.3 will look at the training implications and T1.4 will determine how to combine the CM usage into an evidence-based utility assessment using quantitative data and qualitative estimates when data is limited. The achievable technical risk is the CM value to reduce technical aspects of a piracy event. An important aspect to consider is that the merchants' assessment of their requirement for CMs needs to be done twice because the decision of when to obtain the CM must often take place well in advance of actually using it. This applies equally to procuring physical CMs as it does to training the crew in defensive procedures.

The consideration of externally imposed constraints from Political-Economic-Ethical-Social-Legal-Environmental (PEESLE) factors modifies what is allowed to happen. The effect is to modify the cost/utility of technology to the PEESLE limited net CM utility that it is based on. These PEESLE considerations are part of a separate work package, WP 2, and are not considered in T1.1.

CM Data

The CM catalogue that has been compiled for T1.1 is the combined effort of many different entities using a wide variety of sources. The major references used to derive the information are BMP4, IMO publications, and Subject Matter Experts (SME), such as ship masters and trainers. The organizations who provided the majority of the input are FLIR and WMU.

The CM aspects of the PROMERC database (DB) starts with the CM List. It acts as the hub to associate the CM entity with details, products and vendors. Within the larger data architecture, the CM portion interfaces with external information through the CM List. The key external interfaces are the Scenario and Threat information, and the PEESLE List where CM and PEESLE considerations are linked together.

The CM can be categorized in different ways. The most important categorization is the layered defence that is presented in the PROMERC DOW. It illustrates how layered defence is like an onion of progressively more defensive activities designed to mutually support each other. The three PROMERC tools under development will improve each layer of defence in distinctive ways.

CM Activation Process

The categorization factors of Layered Defence point to the time dependent nature of applying CM to the piracy threat. If this is the case, then there should be a corresponding time dependency associated with considering what CMs to use. This further implies that the CM decisions must be made early enough and acted upon in an appropriate manner to ensure the investment is ready when needed. The decision to use any CM starts with the actions needed to obtain and use the CM. The consequences of CM decisions consume time and resources to ensure the CM is properly integrated into vessel operations. The cumulative effect is a set of context sensitive decisions linked to each CM.

[1] "Throughout this document Counter Measures refer to the measures taken to prevent/deter piracy and not to the legal use as defined within the Responsibility of States for Internationally Wrongful Acts – 2001"

There are four separate types of counter-piracy capability are considered when a CM decision is made, including what actions are required to obtain the CM and what training is needed to use the CM effectively:

1. Ship physical capabilities require procurement decisions to be made long enough before the voyage to allow for installation and specialist training.

2. Ship preparations are oriented towards company and ship SOPS that can occur before and during a voyage, but before the ship enters the area, because the crew must train with the new SOPS as a team;

3. Proactive defence heavily depends on the master having learned and practiced SOPS that allow the ship to stop the pirates from being able to successfully board the vessel.

4. Reactive defence involves last ditch attempts by crew members showing individual initiative to thwart pirates who are in the process of successfully boarding the vessel. Each crew member must also have clear direction about when they are to abandon defensive actions to seek refuge in the citadel.

Ranking CMs

During the project planning phases, the anticipated method for determining the utility of CMs was from the analysis of piracy events. The effect of each CM would be determined by comparing the rate of failure of pirate attacks when the CM is used and not, with all other CMs remaining the same within the comparison. Unfortunately this detailed quantitative analysis was not possible due to the lack of information about how the CMs were used during the piracy events, nor how well they worked.

In order to mitigate these deficiencies in the data, it was decided to solicit the advice of merchant SMEs to state the order they would prefer to select CMs. Rather than hold a group discussion to determine this order – a method which rarely gives equal weight to each participant’s opinion – a quantitative assessment was used to generate a consensus ranking of SME preferences towards each CM.

A software application called Multi-criteria Analysis and Ranking Consensus Unified System (MARCUS was used to do the consensus ranking. A copy of the document provided to the SMEs is in Appendix 3. Each SME used the CM List, divided up into the relevant defence layer, to anonymously rank their preference of CM within each layer. They provided basic data on their experience with merchant shipping and counter-piracy to group cohorts. The criterion used was:

“Which CM has most value (irrelevant of cost) to you in a piracy-prone area?”

The ranking exercise was conducting by a group of 12 participants composed of five master mariners, 2 SMEs with shore-based counter-piracy experience and five PROMERC partners. The results were visualized for the audience at the end of the same day for each layered defence having its CMs ranked in the order from most to least preferred CM, with ties allowed.

During a subsequent review it was confirmed that partners without a merchant ship or piracy experience had CM rankings quite different from those with merchant ship or counter-piracy operations experience. It was judged that only the seven responses from experienced merchant ship or counter-piracy operations SMEs are suitable to report here.

Conclusions & Recommendations

The conclusions about the D1.1 report are:

1. The CM catalogue is a relevant list of sensible CM's extracted from BMP4, IMO and NATO sources. It includes PROMERC stakeholder and SME inputs from the Kick Off meeting and the first Workshop (WS1);

2. The CM catalogue analysis points to a major "bottom-line" consideration about CMs where the early counter-piracy preparations <BEFORE> encountering pirate, that leads to options that reduce the probability of success <DURING> a piracy attack;

3. CM packages documented during WS1 have facilitated the logical grouping of many related CMs described by the SME's;

4. The CM activation process documents the key parameters required to make timely and operationally relevant decisions about by each CM in the list.

5. The CM catalogue requires further validation using stakeholder reviews;

The report recommends that:

1. The CM catalogue consolidation be finished no later than 15 August 2014 to ensure there is sufficient time to complete the cost-benefit analysis that follows;

2. The CM activation process should be considered as a context sensitive basis for the T3.5 CM manual;

3. The implications of the CM activation process should be factored into the Benefits Realization in T3.6.

4. SAMI should pursue the implications of the CM activation process with the maritime industry.

THIS PAGE INTENTIONALLY LEFT BLANK

Acronym List

ADS	Active Denial System
AIS	Automatic Identification System
BMP4	Best Management Practices (version 4)
CCTV	Closed Circuit Television
CM	Counter-Measure
CSO	Company Security Officer
D	Deliverable
DOW	Description of Work
DP	Defence Phase
EEI	Essential Elements of Information
EUNAVFOR	European Naval Force Somalia
FRA	France
GOG	Gulf of Guinea
HOA	Horn of Africa
HRA	High Risk Area
IMO	International Maritime Organization
IO	Indian Ocean
IRTC	Internationally Recommended Transit Corridor
ISM	International Safety Management
ISPS	International Ship and Port Facility Security
LD	Layered Defence
LNG	Liquefied Natural Gas
LRAD	Long Range Acoustic Device
LRIT	Long-Range Identification and Tracking
MARCUS	Multi-criteria Analysis and Ranking Consensus Unified System
MSCHOA	Maritime Security Centre – Horn of Africa
MSEC	Maritime Security Executive Committee
NLD	The Netherlands
NMIOTC	NATO Maritime Interdiction Operational Training Centre
NVG	Night Vision Goggle
PCASP	Private Contracted Armed Security Personnel
PEESLE	Political-Economic-Ethical-Social-Legal-Environmental
PM	Person Months
PMSC	Private Maritime Security Company
PPE	Personal Protective Equipment
PROMERC	Protection Measures for Merchant Ships
PTSD	Posttraumatic Stress Disorder
ROE	Rules of Engagement
RFUF	Rules For Use of Force
RPG	Rocket Propelled Grenade
SECTRONIC	Security System for Maritime Infrastructures, Ports and Coastal Zones
SME	Subject Matter Expert
SOP	Standard Operational Procedure
SPAR	Suppress Piracy and Robbery
SSAS	Ship Security Alert System
STS	Ship to Ship operations
SVSRA	Ship and Voyage Specific Risk Assessment

T	Task
TDA	Tactical Decision Aid
TTPs	Tactics Techniques and Procedures
VLCC	Very Large Crude oil Carrier
VOI	Vessel of Interest
VPODS	Military Detachment Onboard
UAV	Underwater Autonomous Vehicle
UOF	Use of Force
UKMTO	UK Maritime Trade Operations
WMU	World Maritime University
WP	Work Package
WS	Work Shop