

CHENS

MARITIME SECURITY

**BEST PRACTICE
GUIDELINES**

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

PREFACE

BACKGROUND

1. During the last decade, but most notably following the terrorist attack on New York in September 2001, a great many national and international initiatives have been put in place to enhance security in the maritime domain resulting in the ongoing development of *Maritime Security (MS)*.
2. *Maritime Security* is, so far, a mostly ad hoc attempt to combine civil and military efforts to ensure the legal use of maritime spaces and prevent unlawful activities such as terrorism, proliferation of weapons of mass destruction, piracy, illegal immigration, narcotic trafficking and the like, being spread across the oceans and projected into territorial areas.
3. *Maritime Security* requires a solid legal basis therefore the first international initiatives have been oriented towards the creation of such a framework. The establishment of the Automatic Identification System (AIS), the International Ship and Port Security (ISPS) Code, by the amended Safety of Life at Sea (SOLAS) Convention or the 2005 Protocols to the Suppression of Unlawful Acts (SUA) Convention are some examples of measures taken by the International Maritime Organization (IMO), on behalf of the United Nations.
4. Together with these legal tools, new organizational models have been proposed to enable the correct combination of efforts and capabilities by those agencies entitled to act against the various threats that have emerged in recent years. The large number of agencies involved in maritime activities is itself a challenge when it comes to co-ordinating the required defensive measures, yet co-ordination is essential to achieve sufficient unified action and avoid undesired security gaps.
5. At the same time, in the wake of *Maritime Security*, a better understanding of the maritime domain has been found to be critical, calling for increasing information exchange by all involved agencies, which has resulted in the expansion of a further concept, *Maritime Situational Awareness*.
6. These ideas have not remained unnoticed by world navies. Navies have traditionally been charged with the protection of the Sea Lines of Communication and, although many other agencies (such as Coast Guards, Police Forces and Border Guards) now have *Maritime Security* tasks, the naval contribution to *Maritime Security* will be crucial for the maintenance of a safe maritime environment; therefore they must be prepared to contribute to and create the correct co-operation atmosphere both at inter-agency and at international levels.
7. For this reason, the Chiefs of European Navies (CHENS) forum decided that supporting *Maritime Security* should be one of its principal challenges in the future.

SCOPE

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

8. Since May 2006, CHENS has been working on *Maritime Security* concepts through a working group (CHENS MSO WG) created for that purpose and which has benefited from the participation of the majority of European navies.
9. The findings of the CHENS MSO WG were compiled in a document entitled "Developing a European Interagency Strategy for Maritime Security Operations, a Paper Supported by the Chiefs of the European Navies" (the Paper) that was approved by CHENS during the annual meeting in May 2007.
10. The document advocates the need for Europe to develop a Maritime Security Strategy and recognizes the role of the European navies in its development and promotion.
11. The Interagency Strategy provides four Lines of Development to contribute to the CHENS vision of *Maritime Security* which are: Diplomatic and Co-operation, Information, Operational and Economic.
12. As a result, following the approval of the Paper, the CHENS MSO WG met in Amsterdam in July 2007 and assigned responsibilities in order to influence progress along those Lines of Development (LoD). As far as the Operational LoD is concerned, a significant workstream was the development of a set of Maritime Security Best Practice Guidelines, through the work of the specifically established "Maritime Security Best Practice Sub-WG".
13. This document presents the findings of the Best Practice Sub-working Group.

OBJECTIVE

14. During recent years a great deal of Maritime Security discussion has taken place in, and many initiatives have been launched from, a variety of maritime related fora - one such being CHENS, whose Maritime Security Interagency Strategy paper provides a sound basis of how European Maritime Security should be taken forward and what the involvement of the navies should be. To date only a few nations have developed Maritime Security Interagency concepts and structures.
15. Maritime Security is not only a vision into the future but a living operational activity and most European navies routinely participate in Maritime Security activity to a greater or lesser extent.
16. For this reason and while the political process for the development of a European Maritime Security system is discussed, navies must be prepared to participate in this activity, which is only partially new, with the same professionalism as they apply to more traditional conventional warfare tasks.
17. The objective of this document is to provide European navies with guidelines for the implementation of naval Maritime Security structures and the execution of naval Maritime Security missions. The content is not intended to be regarded as doctrine but may be used by European navies in the development of their own doctrine. The national organizational and legal differences are acknowledged and therefore, the implementation of a single common rule for all the nations is not possible at this time.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

CONTENTS

LIST OF ABBREVIATIONS

THE MARITIME SECURITY FRAMEWORK

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES: OPERATIONAL LEVEL.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES: TACTICAL LEVEL.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

ABBREVIATIONS USED IN THIS DOCUMENT

| Abbreviation | Meaning |
|--------------|--|
| AIS | Automatic Identification System |
| COI | Contacts of Interest |
| COLREGs | International Regulations for Preventing Collisions at Sea 1972 |
| DC | Damage Control |
| HIV | High Interest Vessel |
| IDCRIT | Identification Criteria |
| IMO | International Maritime Organization |
| ISPS | International Ship and Port Security |
| LRIT | Long Range Identification and Tracking |
| MIO | Maritime Interdiction Operations |
| MS | Maritime Security |
| MSA | Maritime Situational Awareness |
| MSO | Maritime Security Operations |
| OGD | Other Government Departments |
| POS ID | Positively Identify |
| PIM | Position Intended Movement |
| PSI | Proliferation Security Initiative |
| RFA | Fleet Auxiliary |
| RFI | Requests for Information |
| RMP | Recognized Maritime Picture |
| ROE | Rules of Engagement |
| SAR | Search and Rescue |
| SOA | Speed of Advance |
| SOLAS | Safety of Life at Sea |
| SOP | Standard Operating Practice |
| SPECTK | Special Track |
| SUA | Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988 |
| TSS | Traffic Separation Schemes |
| TTW | Territorial Waters |
| UNCLOS | UN Convention on the Law of the Sea |
| WMD | Weapons of Mass Destruction |

THE MARITIME SECURITY FRAMEWORK

TACTICAL - 5

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

INTRODUCTION

1. As stated in the preface to this document, a great deal of intellectual activity has been taking place in the field of Maritime Security. Most of the Maritime Security related terminology is relatively well known yet only a few countries have officially developed Maritime Security concepts, either within navies or in an interagency framework, to support it.
2. Maritime Security is not only made up of new concepts and ideas but also comprises traditional doctrine and activity.
3. From a naval perspective, the mixture of traditional doctrine with some of the new ideas is creating some misunderstanding and an undesired lack of standardization.
4. Some new concepts such as *Maritime Security Operations*, *Maritime Domain Awareness*, *Maritime Situational Awareness*, *Sense Making*, and some traditional terms such as *Recognized Maritime Picture*, *Maritime Interdiction Operations* and *Surveillance*, are relatively well known but when it comes to dealing with the differences among them, their relationships and interconnections, it is soon found that the overall picture is rather confusing and a common framework is therefore required.
5. Achieving a common European Maritime Security concept and terminology is a reasonable objective in the medium or long term but in the meantime European navies need a common basis to work with and the objective of this chapter is to provide it.

BASIC TERMINOLOGY

6. Regardless of the absence of Maritime Security concepts at all levels, there are four basic terms: *Maritime Security*, *Maritime Safety*, *Maritime Security Operations* and *Maritime Situational Awareness* in use across the international maritime and naval communities.
7. Yet, and depending on the context, the meaning of these basic terms are frequently confused or even referred to as the same thing.
8. For this reason and considering the leading role of CHENS in the development of views and ideas within this emerging conceptual area, it is very important to define these terms, for the purpose of this document, in developing these Maritime Security guidelines. Therefore, in the context of this document, the following terms should be understood to mean:

Maritime Security (MS) is an international and interagency, civil and military, activity to mitigate the risks and counter the threat of illegal or threatening activities in the maritime domain, so that they may be acted upon in order to enforce law, protect citizens and safeguard national and international interests. Maritime Security will therefore concentrate on the unlawful use of the maritime domain.

Maritime Safety encompasses the measures taken by the appropriate national and international authorities in order to ensure the safe navigation of ships and transport

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

of goods at sea and prevent accidents, pollution and the undesired and accidental effects of legal maritime activities.

Maritime Security Operations (MSO) relates to the action carried out at sea by those military and civil authorities equipped with the appropriate assets and empowered to act upon Maritime Security related risks and threats.

Maritime Situational Awareness (MSA) is the management of information related to the maritime domain that can have an impact on Maritime Security. Ideally, Maritime Situational Awareness should include as many international and interagency information sources as possible; furthermore Maritime Situational Awareness requires the timely exchange and analysis of different pieces of information, coming from different sources, in order to obtain actionable conclusions that might otherwise remain unnoticed.

9. Notwithstanding the interagency nature of Maritime Security, these Guidelines are developed from a naval perspective; therefore, only the naval aspects of Maritime Security will be covered in these Guidelines, while the civil side will be taken for granted and not examined in detail.

THE MARITIME SECURITY CONCEPTUAL FRAMEWORK

10. The definitions above are widely understood within the naval community, with some minor variations, but some misunderstandings are still being generated.

11. Even where these definitions are agreed there seem to be differing interpretations of the relationships among them. This paragraph sets out a Maritime Security Conceptual Framework for the common use of all European navies and it provides a general view of how Maritime Security works, the processes involved and how those processes relate to each other.

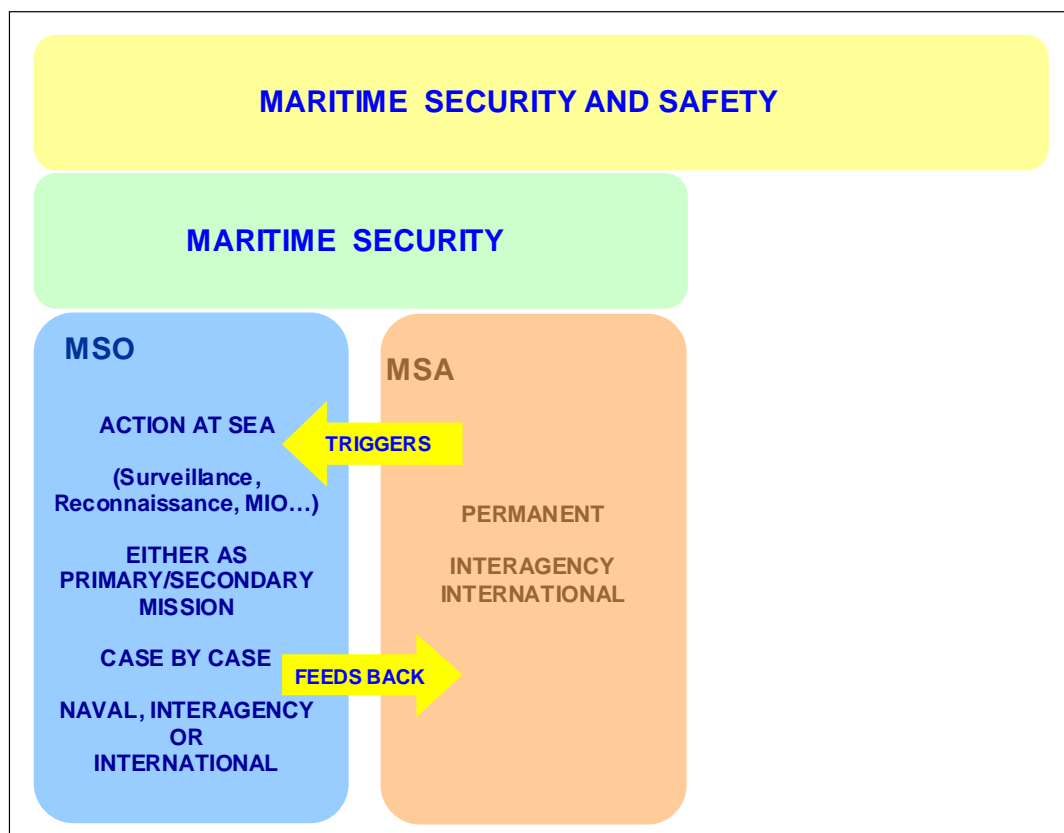
12. Before concentrating on Maritime Security, that is, on the fight against unlawful activities in the maritime domain, it is important to note that Maritime Security and Maritime Safety, as defined above, are very much interconnected and although the natural working context of navies is Maritime Security, in most cases Maritime Safety activities and information should be taken into account to aid better planning and understanding of Maritime Security missions.

13. Looking closely at the definition of Maritime Security above it is easy to appreciate the complexity of such an activity where a large number of organizations, working processes and an ambiguous legal framework are involved.

14. In order to simplify, Maritime Security is to be considered the combination of Maritime Security Operations and Maritime Situational Awareness. In other words, Maritime Security implies information analysis and action at sea, and both complement each other.

15. Maritime Security requires much more than just those two components but, as far as navies' participation in the overall Maritime Security system is concerned, those are the two main ones to consider and that will require specific doctrine. Therefore, we can start by stating that:

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES



This means that MSA and MSO work together to accomplish Maritime Security but also that they are two independent activities. MSA and MSO may be carried out by

different authorities that will in turn depend on a higher authority responsible for Maritime Security as a whole. It also means that they both need specific procedures and doctrine for their execution.

THE MARITIME SECURITY CYCLE

16. MSA and MSO, besides being independent activities, ought to be very closely related and the authority responsible for Maritime Security must ensure the efficient coordination of both.

17. MSA is related to MSO because operations at sea must, in most cases, be based on the results of the information analysis conducted in the maritime domain. In other words, MSA triggers MSO.

18. On the other hand, the information obtained during Maritime Security Operations (mostly Maritime Surveillance) will be a very valuable input to MSA. In other words, MSO feeds back into MSA. This relationship is clearly represented in the following figure:

19. There are other important MSA and MSO characteristics that are represented in the figure:

- a. Maritime Security Operations take place on a case by case basis, while MSA is a permanent activity.
- b. Maritime Security Operations can be carried out as a primary mission, which means that the main role of the units or forces at sea is Maritime Security related, or as a secondary mission, when the units or forces are at sea for any other type of

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

naval operation but are assigned a Maritime Security role to be executed at the same time or when possible.

c. In general terms, Maritime Security Operations may be classified as Surveillance, Reconnaissance and Maritime Interdiction Operations. The first two, Surveillance and Reconnaissance, generally known as “Scouting”, are directed to the gathering of information on a particular geographical area or on a particular suspected contact. Maritime Interdiction, in turn, implies action on the particular suspicious contact, either to board and search, seize or take her to port.

d. Finally, and this will be very much dependent on the internal inter-agency arrangements of the different countries, Maritime Security Operations can be carried out by navies alone, in co-operation with other civilian national agencies or in co-operation with other nations or international organizations. The same is true of Maritime Situational Awareness although, in this field, the co-operation with other agencies and international actors should be considered as essential because, without it, the quality of the resulting product would be very limited.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

OPERATIONAL LEVEL GUIDELINES

INTRODUCTION

1. The international and interagency dimension of Maritime Security is strategic in nature because of the global effects of the existing risks and threats and the enormous amount of security activities that need to be coordinated.
2. The general arrangement of such activity is beyond the reach of European navies, yet the international and interagency implications of Maritime Security must be present in the military contribution to overall Maritime Security and therefore in this work.
3. Within this context, European navies need to agree on a common concept of use for naval assets, gather expertise and develop specific capabilities to confront their responsibilities in the field of Maritime Security.
4. Before dealing with the more detailed tactical considerations some broader operational guidelines must be established. That is the purpose of this chapter.

THE MARITIME SECURITY SPECTRUM

5. Figure 1 below summarizes the wide range of operational scenarios that can be found in Maritime Security and the potential involvement of navies within that.
6. The participation of navies in the wide spectrum of Maritime Security missions varies from country to country and very much depends on the national distribution of responsibilities within the maritime domain.
7. Nevertheless, there seems to be a common relationship between navies' involvement in Maritime Security missions and the level of the risks and threats; the higher the risks and threats the more likely it is that navies will be involved in maritime security missions.
8. This is true because navies are provided with military capabilities that in some situations could be the only effective means to counter the existing dangers (e.g: it may only be possible to neutralize a *renegade ship* with conventional weapons such as torpedoes or missiles).
9. We can therefore establish three basic levels:
 - Standing Security Control Measures.
 - Law Enforcement Operations against Organized Crime.
 - Maritime Security against Global Threats.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

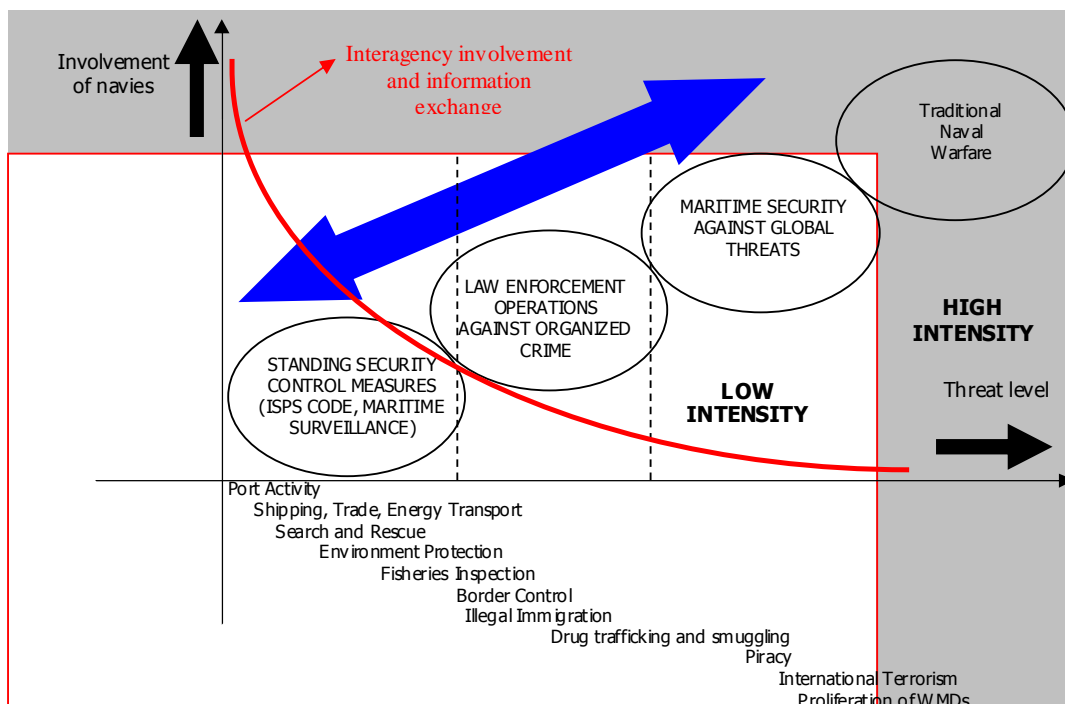


Figure 1 - The Maritime Security Spectrum

10. The boundaries between each of these three levels are not well defined. They are instead ambiguous and vary from nation to nation depending on internal legal arrangements. That said, the higher the continuity across the Maritime Security Spectrum (along the blue double arrow towards the right) the higher the level of defence required against the risks and threats and thus, naval involvement is increasingly more likely.

11. That continuity is based on effective interagency co-ordination of security activities and a high degree of information exchange.

12. It is also important to note that although a high degree of interagency co-operation and information exchange is desirable across the whole spectrum, as the level of risks and threats increases the number of actors involved will necessarily decrease and the confidentiality of the exchanged data will be higher, in order to maintain the operations within an appropriate context (Interagency involvement and information exchange red curve).

13. No matter how deep each European navy's involvement is within its own nation's Maritime Security Spectrum there are some recommended Guidelines to consider within each level below:

STANDING SECURITY CONTROL MEASURES

14. The normal maritime activities that take place everyday, covering different fields such as sea trade, fishing, energy, leisure, etc. These were put under a higher state of

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

alert following the terrorist attacks in New York on 11 September 2001. The international community reacted in different ways and numerous initiatives were launched to enhance security in the maritime domain.

15. Most notably, the International Maritime Organization (IMO) amended the Safety of Life at Sea (SOLAS) Convention and some new mechanisms, such as the International Ship and Port Security (ISPS) Code and the Automatic Identification System (AIS), were put in force.

16. The goal was to allow the normal flow of maritime legal activities whilst increasing both the security of critical points, such as ports and ships, and the information about them, in order to be able to detect any possible attempt to cause damage by criminal or terrorists groups in advance.

17. Although the approach to these security areas is mostly civilian, navies must be involved as much as is permitted by their different national legislation, not only to provide support to the general defensive system but also to be prepared for their possible participation in the other two, higher, levels.

18. In this regard, European navies should consider:

a. orientating traditional surveillance missions into the field of Maritime Security. This means that naval assets should focus surveillance on the detection across the whole spectrum of Maritime Security threats, and all naval assets should be assigned a Maritime Security role, whatever its main task.

b. orientating the structure, procedures and systems of existing Maritime Surveillance Centres to the management of Maritime Situational Awareness (MSA). This will require access to the new information sources developed in the field of Maritime Security, such as AIS, and LRIT in the future, and the appropriate technical tools to analyze such information in order to obtain actionable conclusions.

c. developing, national legislation permitting, interagency co-operation agreements and mechanisms in order to enhance the co-ordination of the different Maritime Security activities, including MSA. This will provide a comprehensive and multiplying effect, both for the efficiency of the defensive measures and for situational awareness.

d. actively co-operating with each other, from the international perspective, in order to improve their MSA and to engage in combined Maritime Security Operations (MSO), mostly in sub-regional scenarios where risks and threats are often shared by neighbouring nations.

LAW ENFORCEMENT OPERATIONS AGAINST ORGANIZED CRIME

19. For the same reasons, the international community has also reacted to provide new legal tools to nations to facilitate the fight against organized crime, in its different forms (Illegal Immigration, Smuggling, Narcotics, etc.), in the maritime domain.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

20. This type of operation is normally under the responsibility of Police Forces, Coast Guard or the like, especially inside territorial waters, and navies' participation varies from nation to nation.

21. Nevertheless, and regardless of the level of navies' involvement in this type of mission, there are some considerations that should be taken into account:

a. A close relationship should be maintained between navies and Law Enforcement agencies, either to provide the required support or at least to avoid interference by any naval asset in the area of operations for other reasons.

b. Consider the possibility and convenience of developing interagency agreements for the execution of joint civil and military Maritime Security Operations. The combination of naval capabilities and the judicial powers of Law Enforcement agencies is a very effective tool for nations to consider.

MARITIME SECURITY AGAINST GLOBAL THREATS

22. The worst and most dangerous scenarios, as far as Maritime Security is concerned, are the ones represented by the Proliferation of Weapons of Mass Destruction, Terrorism or the combination of both.

23. In order to prevent and avoid these, the United Nations is trying to improve the mechanisms provided by the SUA Convention, for the Suppression of Unlawful Acts at Sea, to empower nations to interdict ships suspected of carrying nuclear components and to avoid attacks on platforms at sea.

24. To this extent, and mostly on the high seas, navies will, without doubt, have a very important operational role to play and therefore they must prepare to act by:

a. developing Maritime Interdiction Operation (MIO) capabilities. This will require specific doctrine and training and the creation of professional MIO teams. It is also important to gain access to new technological tools such as nuclear radiation detectors, night vision devices or ship to ship communications systems.

b. Engaging with national legal and jurisdictional structures in order to establish the appropriate links to enable such operations to proceed as required.

c. Actively participating in those international fora created for the enhancement and promotion of concepts and measures related to the fight against this specific type of risk and threat, such as the Proliferation Security Initiative (PSI).

POSSIBLE MARITIME SECURITY SCENARIOS FOR NAVAL FORCES

25. The previous paragraph defines the levels that could be considered within Maritime Security in regards to the threat and navies' involvement in such activity.

26. It is also important to define different naval approaches to Maritime Security in regards to the planning and conduct of missions, no matter what the nature of the risks and threats to counter is.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

27. Maritime Security, and the participation of navies in it, can take many possible forms, from routine activities inside its own territorial waters to specific deployments in distant locations. There are a number of possible situations but, overall, European navies are likely to find themselves in one of the four following types of Maritime Security scenarios.

BASELINE MARITIME SECURITY

28. Baseline Maritime Security is that part of Maritime Security that takes place on a permanently ongoing basis. Returning to the principles set in the Maritime Security Framework chapter and considering that MSA, one of the two components of Maritime Security, is also a permanent activity, it follows that Baseline Maritime Security will be related to the gaining of awareness of the security situation in the maritime domain.

29. That part of the process is normally carried out in Maritime Surveillance Centres and requires a great deal of technological developments, interagency information exchange and international connections, amongst other tools.

30. Baseline Maritime Security is not achieved through information management alone. The presence of naval assets at sea is a Maritime Security multiplier. That means that some Maritime Security Operations will be part of this baseline scenario. Surveillance or Reconnaissance Operations, conducted on a routine basis or just as a secondary task for any other type of mission, will help to build the awareness picture.

31. In some cases naval units, whilst executing routine activities, may find themselves encountering unexpected Maritime Security violations and will need to be prepared to act on them. That is to say that Baseline Maritime Security may go beyond the information or surveillance line and become interdiction, when unexpected situations develop.

32. As far as guidelines for European navies is concerned, apart from the ones included in the Standing Security Control Measures paragraph, the need to provide clear orders for commanders at sea, to cover unexpected interdiction operations, must be considered.

PRE-PLANNED MARITIME SECURITY

33. Baseline Maritime Security calls for a proactive attitude by all naval units at sea, even when no risks or threats to Maritime Security are evident. It is when some form of warning is detected as a result of this routine activity that the normal Maritime Security cycle, as described in the MS Framework chapter, begins.

34. The goal of MSA is to identify individual risks and threats from a large amount of information. Once a specific threat is evident, it is likely that naval units will be called upon to carry out a MSO.

35. MSO may take different forms. Depending on the desired end state, they may range from simple reconnaissance, to marking or shadowing up to MIO or neutralization of the threat. All these different types of operations, triggered by MSA results, are termed Pre-planned Maritime Security Operations.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

36. The next chapter of this document includes Tactical Level Guidelines and provides further doctrinal detail for the planning and conduct of such operations.

MARITIME SECURITY IN SUPPORT OF EXISTING SECURITY STRATEGIES

37. The first two scenarios described above apply to regional and sub-regional theatres, whether national or international. They are the reason why Maritime Security has been developed and in response to which most Maritime Security related activity will take place.

38. Risks and threats to Maritime Security exist in distant areas as well but their impact on the prosperity and stability of our nations and citizens can be very high.

39. The dangers represented by the increase of Piracy in certain parts of the Globe and the indiscriminate attacks on Oil Tankers and Platforms are two good examples of why Maritime Security must be exported abroad. These types of scenarios are especially relevant for navies because, in most cases, only naval forces are provided with the appropriate capabilities and therefore may be requested to act upon them.

40. In this regard European navies should consider activity to:

- a. determine and analyze which scenarios are more vulnerable from the Maritime Security point of view and more critical to the national and international interests.
- b. study and engage in possible international initiatives to apply Maritime Security to such scenarios.
- c. study and consider the scope and development of appropriate Maritime Security capabilities to complement those traditionally provided by naval forces.
- d. be prepared to participate in Capacity Building initiatives as a prerequisite to being able to extend Maritime Security.

MARITIME SECURITY AS PART OF ANOTHER OPERATION

41. During the last decade many naval operations have been carried out in different parts of the Globe to exercise sea control in a particular area. The recent development of Maritime Security provides new technological and legal tools to enhance such control.

42. To this extent, the following guidelines could be used by all European navies:

- a. Fit all units (surface and air) with AIS receivers in order to be able to create a local MSA picture, especially in those areas where the required coastal infrastructures are not available.
- b. Consider the possibility of liaison with theatre coastal authorities in order to support the development of such capabilities (MSA Capacity Building).

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

- c. Consider the particular Maritime Security requirements of such deployments (systems, training, etc.), not only during the planning phase of the mission but also during the design of future naval units (MIO personnel and material oriented compartments, communication systems, etc).

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

TACTICAL LEVEL GUIDELINES

INTRODUCTION

1. The maritime environment forms a global continuum, which is vital to national and international economies. It, together with the littoral, provides a focus for population, trade and the production and movement of energy supplies world-wide. The high seas are an area where governance is weak, allowing almost unlimited freedom of movement to both legitimate and illegal activities.

2. The high seas are an unevenly regulated highway that lack effective global monitoring and therefore provide the least discriminating avenue for international communications and trade and an attractive environment to support illegal activity. We know that the sea has been used to enable terrorist attacks that elements of Weapons of Mass Destruction (WMD) material are transported by sea and illegal activity from human trafficking to drug smuggling has a strong maritime element. Therefore, in recognition of the strategic context and acknowledgement that threats to national economic and physical security are being enabled by the maritime environment, Maritime Security Operations (MSO) offer a relevant and important military contribution.

3. MSO is to be considered as core business, the concept merely accepts the fact that the presence of naval assets at sea, whether in transit, on exercise, or defined operation, create an effect and have an outcome upon maritime traffic in a global context. The purpose of this chapter is to formalize elements of this line of operation and to commend a mindset to those who have a responsibility and input into this process.

4. The success of MSO is dependant upon the clarity of the Recognized Maritime Picture (RMP) and the quality of the intelligence feeding it. Every unit already contributes to this process in the form of standard reports (such as NATO Form GOLD), Intelligence Reports and the sharing of their own validated, localized maritime picture product. These disparate inputs are then fused and correlated to produce the global RMP; the aim is to also create an unclassified, secure white shipping picture to complement the classified RMP.

5. The employment of the "Surface Investigate" procedure must become as instinctive as the "Investigate" procedure is in the air environment. This procedure must be employed as a generic Standard Operating Practice (SOP), whether on passage, transit, exercise or operation since MSO is always a live, ongoing, operation whether or not directly related to individual unit missions or tasking.

6. MSO will seek to improve military unit's ability to contribute to countering illegal activity and protecting legal activity.

FRONTLINE IMPLICATIONS OF MSO

7. There are a number of areas in which units can take action in support of MSO:

a. Planning. During the planning process, the Command team should consider how the ship can best contribute to MSO whilst meeting primary tasking. Taking the Regional Maritime Intelligence Reports and Contacts of Interest (COI) lists into consideration in navigation and operational planning is essential. Ships should

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

adjust their routing to take into consideration MSO hotspots. Some examples are disputed fishing grounds, known smuggling routes, Oil Refineries, Major Ports and Nuclear installations. Requests for Information (RFI) should be considered where gaps in information exist, but it is recommended that ships approach national intelligence sources at an early stage.

b. Posture at Sea. Whenever at sea, be it on Transit, Training or on Operations, the ship's SA should be expanded to the maximum extent possible. This should not require a change to the posture required for the ships primary task, instead there needs to be a proactive and inquisitive ethos with sufficient flexibility in passage planning to allow units to investigate suspicious contacts. COI lists should be well promulgated and areas known to be of interest should be highlighted to the bridge and ops room teams. It is important to place activity in perspective and recognize that a ship must be ready to conduct Maritime Interdiction Operations (MIO) and boarding although they will be infrequent occurrences.

c. Action Required. Use of the investigate procedure is the first step in ensuring that the maximum amount of information is collected on individual contacts. Reference to all available information including AIS, COI databases, interagency data, pre-sailing briefs and as well as having an instinctive knowledge of the operating area, must be made at this point to avoid nugatory questioning of legitimate vessels. Should sufficient doubt or suspicion exist; investigation by AIS Text, VHF query or dispatch of a boarding team should be considered. If this is not possible within the operational constraints of the programme, the operational commander should be passed all relevant information so that consideration can be given to what, if any, follow on action should be taken in consultation with all interested parties and Other Government Departments (OGD).

e. Understanding Maritime Law. The legal framework in which maritime units operate is complex and demands careful study and should be table-topped if actions are to be instinctive and forward leaning. Further guidance is at Annex B.

f. Capability. Ultimately, ships may be tasked to Interdict, Question or Board a vessel. There will not be a single formula for boarding party capability that meets all requirements. Although the traditional visit and search is still valid, the majority of boarding's today are centred on HUMINT rather than search.

g. Equipment and Training. It is recognized that equipment and training are key enablers to successful MSO. All units must ensure that they have the minimum equipment required and conduct training to ensure that core skills are maintained.

ANNEXES

- A. MSO - COMMAND TEAM CONSIDERATIONS
- B. LEGAL FRAMEWORK
- C. SUSPICIOUS VESSEL DELEGATION AND ACTION MATRIX
- D. PICTURE COMPILATION
- E. AVIATION SUPPORT
- F. SUBMARINE PLANNING AND SUPPORT

MSO - COMMAND TEAM CONSIDERATIONS

INTRODUCTION

1. The application of the options for various courses of action to successfully conduct MSO is well understood however, the key to operational success is the accurate assessment of the relevant factors and appreciation of the difficulties associated when balancing the correct political, legal and military decision. There will be a requirement for a comprehensive threat and risk analysis, and Rules of Engagement (ROE) will need to be considered early. Whilst inevitably the main focus in MSO will be Search, Report, Track etc, a typical operation could follow a sequence of:

- a. Intelligence gathering and management.
- b. Assessment and recommendations.
- c. Political decision-making and direction.
- d. Establishing the Command Organization.
- e. Allocation of assets.
- f. Search, Identification, Track and Report.
- g. Interdiction, Boarding, Inspection and possible diversion.
- h. Transfer operation to law enforcement authorities.

2. The following are a number of factors for consideration and possible maritime courses of action. Of note, chain of command (i.e. CTF/CTG) should always be consulted at an early stage if a unit is involved in any MSO incident that may escalate beyond normality.

| Factors for Consideration | Maritime Actions |
|---|--|
| Strategic considerations <ul style="list-style-type: none"> • Which nations are involved • What is the media position • What open source information is available • How much time is available • Any requirement for specialist expertise (industry) | Monitor the consignment Customs search in port Commercial / Law enforcement / Diplomatic / Intelligence request |
| Intelligence <ul style="list-style-type: none"> • What intelligence do we / other nations have • What intelligence can be shared • How accurate is the intelligence | <ul style="list-style-type: none"> • Stop shipment being loaded • Redirect shipment • Prevent onward shipment • Return cargo to origin |

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

| | |
|--|--|
| <p>Cargo</p> <ul style="list-style-type: none">• Check cargo definition (Human, drugs, WMD etc)• What is the target cargo• What is the destination of the cargo• What is the destination organization• Does the cargo present a hazard• What is the risk assessment, who will decide if it is safe to escort into port• What is the significance of the cargo <p>Location & Routing</p> <ul style="list-style-type: none">• What is the method of transportation (Type of vessel)• What was the last port of call• What is the next port of call• Where is the vessel• Where is the nearest Coastal State <p>Legal Aspects</p> <ul style="list-style-type: none">• What information is available to be used as evidence• What are the National legal issues (particularly jurisdiction)• What are the international legal issues• Is the vessel a warship, auxiliary, or commercial vessel• Does the vessel have a flag – What is the flag• Is there a boarding agreement with the Flag State of the vessel• What nationality is the owner, master, crew, charter• Is it legitimate trade• What are the legal aims – seizure, forfeiture, prosecution <p>Diversion</p> <ul style="list-style-type: none">• Are we going to divert the cargo• Where is the cargo to be diverted to• Who is going to divert the cargo• Do other nations need to assist in diverting the | <p>Divert ship into port to conduct search alongside</p> <p>Locate, identify and track shipment vessel</p> <p>Conduct Boarding</p> <ul style="list-style-type: none">• Aim of Boarding – confirm flag, search, seize, divert etc• Type of Boarding – Compliant, Non-Compliant or Opposed• Provide enabling capabilities in support boarding by other agencies e.g. CBRN search <p>Stop shipment vessel</p> <ul style="list-style-type: none">• To secure vessel, cargo and/or crew• To await law enforcement authorities <p>Destroy shipment</p> <ul style="list-style-type: none">• Legal implication |
|--|--|

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

cargo

- What are the consequences of diverting the cargo
- Where is the most suitable diversion port
- What is the domestic legal position of the diversion port

Boarding

- What is the legal basis for boarding
- Nature of the boarding - Compliant, Non-Compliant or Opposed
- Who will conduct the boarding
- What is the aim of the boarding
- What is the capability of the search team
- What are the security considerations
- What is the status of the target vessels crew / passengers
- Will the search team be able to identify the cargo
- Are there search capabilities available
- Is there a technical reach back from the target vessel to national resources

Disposal

- Where is the vessel to be taken
- Who will handle disposal
- What are the compensation / disposition issues

Decisions

- What is the mission
- What strategic effect are we trying to achieve
- What is the legal basis for action
- Who is the lead nation
- What is the political aim
- What is the end state
- What is the course of action
- What nations are / will participate
- What handovers of responsibility are required
- How will participating nations communicate
- Which is the lead department within each nation
- Which assets are required

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

- | | |
|---|--|
| <ul style="list-style-type: none">• What ROE is required• What is the C2 structure• What is the media impact likely to be• What is the operational impact likely to be• What is the legal and political impact likely to be | |
|---|--|

REQUEST FOR BOARDING

3. The conduct for Boarding Operations is in accordance with National procedures. The following information may be required in order to consider a request for boarding:

- a. Name of ship to be boarded and IMO identification number (if known).
 - b. The flag of the vessel.
 - c. Location of the vessel at the time of the request and its predicted location when the boarding is planned to occur.
 - d. The grounds for the boarding / legal aspects.
 - e. Which State is requesting consent to board the vessel.
 - f. Confirmation that the nation will be informed of the results of the boarding.
 - g. Where the ship is in the territorial sea of a State that is not requesting consent to board that ship, confirmation that the boarding would only be conducted when the Coastal State has also given consent.
4. In all cases where consent is given to boarding it will be on the understanding that:
- a. The consent is given solely and exclusively for the requesting State to board that ship.
 - b. That such boarding can only be undertaken if the Flag Consent has been received.
 - c. Any boarding is undertaken only within the ROE agreed / approved for that specific operation.

SHIP'S POSTURE

5. It is not intended that commanders will detail MSO posture to be assumed by units, nor is it likely that there will be any additional allowance within the SOA/Fuel allowance while on operational transit unless units are specifically tasked. However, experience shows that for specific operations, it is useful for individual units or CTG's to establish a MSO Posture to allow autonomous ops. Example postures are shown below:

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

- a. MSO 1. Units are to attempt to identify all vessels to the required recognition level without deviating from navigational track or jeopardizing Speed of Advance (SOA). SOA is the over riding priority.
- b. MSO 2. Units are to attempt to identify all vessels to the required recognition level but may deviate no more than 2 nautical miles from navigational track and are not to jeopardize SOA. SOA is considered to have been jeopardized if units were unable to regain position intended movement (PIM) without requiring un-economic engine configuration.
- c. MSO 3. Units are to attempt to identify all vessels to the required recognition level but may deviate no more than 5 nautical miles from promulgated navigational track and are not to jeopardize SOA without informing CO/CTG.
- d. MSO 4. Units may deviate up to 10 nautical miles from navigational track in order to identify vessels to required recognition level but they are to report the impact on SOA to CTG. It is anticipated that this posture would normally only used in response to request for particular intelligence whilst on passage or if supporting Commander Task Force (CTF) 320.
- e. MSO 5. Units are to identify all vessels to required recognition level within patrol area. This would be the posture of choice during MIOs.

LEGAL FRAMEWORK

1. The legal framework in which maritime units operate is complex and demands careful study and should be table-topped if actions are to be instinctive and forward leaning. Guidance is also available within national references.

2. In general terms, vessels that merit close attention / interest should be those suspected of being in contravention of the UN Convention on the Law of the Sea (UNCLOS¹) rules on Piracy, Slavery, Drug Trafficking and Illegal Broadcasting, and those suspected of involvement in Terrorism, Smuggling (personnel or goods), Proliferation or Maritime Crime (that is, Piracy but within another nation state's Territorial Waters). Table 1.1 gives jurisdiction guidance provided under UNCLOS or other conventions on the powers for naval forces on the high seas against different crimes.

Table 1.1 – Powers of Naval Forces on the High Seas

| | Legal Instrument | Naval Powers on High Seas | Flag State approval Required for arrest, etc? | Jurisdiction |
|-----------------------------|---|---|--|--|
| Piracy | UNCLOS 105 / 110 | 1. Right of Visit. 2. Arrest 3. Seizure | No (UNCLOS 110, 105) | Crime of Universal Jurisdiction |
| Illegal Broadcasting | UNCLOS 109 / 110 | 1. Right of Visit. 2. Arrest. 3. Seizure | No | |
| Slavery | UNCLOS 110 | 1. Right of Visit. 2. Release slaves. | Not for visit and Freeing slaves. | Only Flag State may seize ship and arrest. |
| Drugs | UNCLOS 108 Vienna Convention Criminal Justice (International Co-operation) Act 1990 'Co-operate' in the suppression of drug trafficking | 1. Stop. 2. Board. 3. Search 4. Arrest 5. Divert 6. Detain | Yes for boarding and subsequent Action. | Flag State – until relinquished |
| Illegal Immigration | | | | |
| Flag Verification | UNCLOS 110 | Right of Visit | No (UNCLOS 110) Flag State (once verified). | Nations may Have jurisdiction over Stateless vessels depending on facts. |

¹ Turkey is not a state party to UNCLOS as such, Turkey supports countering piracy, slavery, narcotics trafficking, smuggling and illegal broadcasting, based on Customary International Law.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

3. Future changes to the legal framework. Recently, many nations have signed a Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988, known as SUA. When this protocol is brought into National law, it is likely to provide navies with increased enforcement powers on the high seas to deal with a number of offences, including terrorist related offences, transportation of WMD and piracy. The Protocol will establish a comprehensive set of procedures and protections, designed to facilitate the boarding of a ship suspected of being involved in a SUA offence. Consistent with existing international law and practice, SUA boarding can only be conducted with the express consent of the Flag State. It is anticipated that there will be an expedited process of seeking Flag State consent. The Flag State may authorize the requesting Party to detain the ship, cargo and persons pending disposition instructions.

SUSPICIOUS VESSEL DELEGATION AND ACTION MATRIX

1. Table 1.2 provides proposed delegations for expected actions in MSO activity; this is provided for guidance only and should be read in conjunction with Table 1.3. This table provides guidance on the identification and subsequent response to suspicious vessels and has incorporated recent practical experience and is a generic SOP in MSO recognized language, utilizing known terms: INVESTIGATE, QUERY, REPORT, TRACK, ASSESS, LOCATE, CLASSIFY and RECOMMEND:

INDICATORS OF SUSPICIOUS INTENT

2. Indicators that could draw attention to a vessel that requires further investigation include (list not exhaustive):

- a. Vessel not taking action to avoid collision in accordance with International Regulations for Preventing Collisions at Sea (COLREGs).
- b. Vessel not following COLREGs adopted Traffic Separation Schemes (TSS) / recognized traffic route / shipping lane.
- c. Vessel loitering for no obvious reason.
- d. Indications that rendezvous/transfer with another vessel have taken/are about to take place.
- e. Vessel stops in water on sighting own vessel.
- f. Vessel attempts to evade – turns away on sighting own ship / on own ship closing (not including manoeuvres in accordance with COLREGs).
- g. Vessel manoeuvres to enter nearest Territorial Waters (TTW) on sighting own vessel.
- h. Vessel on a route known for illegal activity.
- i. Vessel out of place against background traffic.
- j. Number / type of personnel / equipment fit / cargo / weaponry not consistent with stated role.
- k. Crew attempt to hide themselves / personnel / cargo from view, or do not respond in normal manner
- l. Vessel ditching equipment over ship's side.
- m. Vessel ditching personnel over ship's side / Persons located in water (apparent Search and Rescue (SAR)).
- n. Vessel requests assistance for onboard emergency / breakdown.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

- o. Vessel on reliable Intelligence source Contact of Interest (COI) / High Interest Vessel (HIV) list.
- p. Suspicious response to hailing procedure.
- q. Vessel attempting to operate covertly.
- r. Vessel follows / manoeuvres towards own vessel and / or increases speed.

TABLE 1.2 - SUSPICIOUS VESSEL DELEGATION MATRIX

| Intent Indicator | Delegation of Expected Action | | | | | | | | | | | | | | | | | | | |
|------------------|-------------------------------|---------|-----------|----------|-----------|-------|----------------|-----------------|-------------------|--------|------------|---------------|-----|--------------|----------------|-----------|---------------|-------|--------|--------|
| | Initial Intentions | Request | Full Hail | Position | Stand-off | POSID | Check database | Recover objects | Recover Personnel | Assist | Inform CTG | Inform OP COM | SAC | Inform Local | Issue Warnings | Compliant | Non-Compliant | Diver | Detain | Arrest |
| 1 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | ? | ++ | ++ | ++ | ++ | ++ | ++ |
| 2 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | ? | ++ | ++ | ++ | ++ | ++ | ++ |
| 3 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | + | ++ | ++ | ++ | ++ | ++ | ++ |
| 4 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | + | ++ | ++ | ++ | ++ | ++ | ++ |
| 5 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | + | ++ | ++ | ++ | ++ | ++ | ++ |
| 6 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | + | ++ | ++ | ++ | ++ | ++ | ++ |
| 7 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | + | ++ | ++ | ++ | ++ | ++ | ++ |
| 8 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | + | ++ | ++ | ++ | ++ | ++ | ++ |
| 9 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | + | ++ | ++ | ++ | ++ | ++ | ++ |
| 10 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | ? | ++ | ++ | ++ | ++ | ++ | ++ |
| 11 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | + | ++ | ++ | ++ | ++ | ++ | ++ |
| 12 | √ | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | √ | √ | √ | √ | ++ | ++ | ++ | ++ | ++ | ++ |
| 13 | √ | √ | √ | √ | √ | √ | √ | N/A | √ | N/A | √ | √ | √ | √ | ++ | ++ | ++ | ++ | ++ | ++ |
| 14 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | √ | √ | √ | √ | + | ++ | ++ | ++ | ++ | ++ | ++ |
| 15 | ? | ? | ? | ? | ? | ? | √ | N/A | N/A | N/A | √ | √ | √ | ? | ++ | ++ | ++ | ++ | ++ | ++ |
| 16 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | ? | ++ | ++ | ++ | ++ | ++ | ++ |
| 17 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | √ | ++ | ++ | ++ | ++ | ++ | ++ |
| 18 | √ | √ | √ | √ | √ | √ | √ | N/A | N/A | N/A | √ | √ | √ | √ | ++ | ++ | ++ | ++ | ++ | ++ |

Notes:

1. Number in left hand column refers to numbers in Table 1.3 'Summary of Indicators of Suspicious Intent' list.
2. Symbol decodes (Example to be modified IAW national criteria):
 - √ = Delegated to COs.
 - +
 - ++ = Held above CTG level.
 - ? = Situation dependent (at CO's discretion)

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

TABLE 1.3 - SUSPICIOUS VESSEL ACTION MATRIX

| Indicator Number | Action by Suspicious Vessel | Response | Comment |
|-------------------------|--|----------------------------|---|
| 1 | Manoeuvres not in accordance with International Regulations for Preventing Collisions at Sea (COLREGs) | INVESTIGATE, QUERY, REPORT | <p>1. If response during hailing raises suspicion consider further questioning for standard hailing data</p> <p>2. Consider reporting larger vessels to IMO for contravention of COLREGs</p> <p>3. Be aware of fishermen who use small, fast boats to follow shoals of tuna and hence appear to manoeuvre erratically</p> |
| 2 | Not following recognized Traffic Separation Schemes or common shipping routes | INVESTIGATE, QUERY, REPORT | If response during hailing raises suspicion consider questioning for standard hailing data |
| 3 | Vessel loitering for no obvious reason | INVESTIGATE, QUERY, REPORT | If response during hailing raises suspicion consider questioning for standard hailing data |
| 4 | Indications that rendezvous / transfer with another vessel have taken / are about to take place | INVESTIGATE, QUERY, REPORT | If response during hailing raises suspicion consider questioning for standard hailing data |
| 5 | Stops on sighting own vessel | INVESTIGATE, QUERY, REPORT | <p>1. Monitor movement if ship adjusts course to avoid. Commence hailing process. IMO Number to be correlated with Automatic Interrogation System (AIS) and checked against COI / HIV database</p> <p>2. Stand-off position should be consistent with ship safety in relation to hand-held / shoulder launched weapon ranges.</p> <p>3. Warn OPCOM & Local SAC if remain concerned.</p> <p>4. In case of a small vessel not responding to radio hailing, there may be a requirement to use a boat for vocal hail. Boat should hail from maximum safe distance and not go directly alongside suspect vessel.</p> |

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

| Indicator Number | Action by Suspicious Vessel | Response | Comment |
|-------------------------|---|--|--|
| 6 | Turns away on sighting own ship / Turns away on own ship closing (not including alterations of course in accordance with COLREGs) | INVESTIGATE, QUERY, REPORT close to safe distance to positively identify (POS ID), maintaining overt presence as this may give further indication of intent. | <ol style="list-style-type: none"> 1. Positively ID vessel using Helo, or close if Helo unavailable 2. Check details given with COI / HIV databases 3. Report details to OPCOM & Local SAC |
| 7 | Vessel manoeuvres to enter nearest TW on sighting own vessel | INVESTIGATE, QUERY, REPORT close remaining inside international waters limits to support query and support POS ID. | <ol style="list-style-type: none"> 1. POS ID vessel using Helo, or close if Helo unavailable 2. Check details given with COI / HIV databases 3. Report details to OPCOM & Local SAC |
| 8 | Vessel on a route known for illegal activity | INVESTIGATE, QUERY, REPORT, TRACK (close to safe distance) | Report details to OPCOM & Local SAC |
| 9 | Vessel out of place against background traffic | INVESTIGATE, QUERY, REPORT (as necessary) | <ol style="list-style-type: none"> 1. Establish details from hailing, report to OPCOM & local SAC 2. Indicators that vessel out of place: Vessel characteristics (class / equipment fitted / condition / location) do not correspond with others in vicinity, e.g. speed-boats among fishing dhows, etc. Beware of the overly bland vessel, or vessels which have a high speed for their size / type. It must be noted that fishing dhows regularly employ speedboats / skiffs to return fresh catch to shore and should be a consideration when assessing the area of interest. |
| 10 | Number / type of personnel / equipment fit / cargo / weaponry not consistent with stated role | INVESTIGATE, QUERY, REPORT | <ol style="list-style-type: none"> 1. Establish details from hailing, report to OPCOM & local SAC 2. If vessel proven state sponsored, i.e. Coastguard withdraw to approved minimum distance in accordance |

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

| Indicator Number | Action by Suspicious Vessel | Response | Comment |
|-------------------------|--|---|---|
| | | | with operating orders. 3. Note that, in areas of increased piracy threat (e.g. Gulf of Oman, Malacca Straits) carrying small arms for self-protection is the considered normal and is not a sole indicator of malicious intent |
| 11 | Crew attempt to hide themselves / personnel / cargo from view, or do not respond. | INVESTIGATE, QUERY, REPORT, AND TRACK. Respond as directed | Establish details from hailing, report to OPCOM & local SAC |
| 12 | Vessel ditching equipment over ship's side | INVESTIGATE, QUERY, REPORT, AND TRACK. Respond as directed | 1. Establish details from hailing, report to OPCOM & local SAC 2. Do not attempt to recover objects, monitor and then respond as directed by higher authority. 3. When authorized , attempt to recover objects by sea boat (primary) / Helo grappling hook (secondary) - Beware booby traps (sharp objects, chemicals, biohazards, etc) |
| 13 | Vessel ditching personnel over ship's side / Persons located in water (apparent SAR) | Recover person(s) (save life) once complete, if possible, close to safe distance, query and report. | 1. Establish details from hailing, report to OPCOM & local SAC 2. Attempt to recover personnel by sea boat (primary) / Helo strop (secondary) - Beware suicide booby-trap (Bulky clothing, person suspicious prepared to enter water (well-dressed, lifejacket) etc) – unlikely if person discovered out of usual operating area |
| 14 | Vessel requests assistance for onboard emergency / breakdown | INVESTIGATE, QUERY, REPORT, TRACK ASSESS, RECOMMEND, RESPOND | 1. Establish nature of problem. Report to OPCOM and Local SAC 2. Consider graduated response to situation post-ID |

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

| Indicator Number | Action by Suspicious Vessel | Response | Comment |
|-------------------------|--|--|--|
| | | | <p>3. Use Helo / Sea boat to assess potential threat prior to closure</p> <p>4. Force Protection of personnel/unit needs to be considered. Once approval authorized, armed security sweep to be conducted prior to assistance team embarkation.</p> <p>5. If ship required to approach, point bows at contact, approach slowly, assume appropriate Damage Control (DC) state, clear upper deck of non-essential personnel, position armed lookout on Foc'sle, use longest practicable tow-line</p> |
| 15 | Vessel on reliable Intelligence source Contact of Interest (COI) / High Interest Vessel (HIV) list | LOCATE, INVESTIGATE, CLASSIFY, REPORT | <p>1. Report to OPCOM, Local SAC and other authorities as required by guidance / allowed by security classification</p> <p>2. Respond as directed by Higher Authority / Standing or any extant Special Instructions.</p> <p>3. Do not raise suspicions by not hailing if have been routinely hailing other vessels</p> |
| 16 | Suspicious response to hailing procedure | TRACK, REPORT | <p>1. Report to OPCOM and Local SAC</p> <p>2. Respond as directed by Higher Authority / Standing or any extant Special Instructions.</p> |
| 17 | Vessel attempting to operate covertly, e.g. lack of Navigation Lights at night, no response to hailing, etc. | INVESTIGATE, QUERY, MANOEUVRE, REPORT, TRACK | <p>1. Report details to OPCOM & Local SAC</p> <p>2. Respond as directed by Higher Authority / Standing or any extant Special Instructions.</p> <p>3. Consider POS ID vessel using Helo, or close if Helo unavailable.</p> |

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

| Indicator Number | Action by Suspicious Vessel | Response | Comment |
|-------------------------|---|--|---|
| | | | 4. Check details given with COI / HIV databases |
| 18 | Vessel follows / manoeuvres towards own vessel and / or increases speed | Initiate QUICKDRAW, concurrently INVESTIGATE, QUERY, MANOEUVRE, REPORT | 1. Report to OPCOM and Local SAC 2. Increase own / TG Force Protection measures as deemed appropriate 3. Be wary of over-reacting to vessels closing out of genuine interest, or small fishermen who may wish to shelter in lee while on transit in rough weather |

PICTURE COMPILATION

INTRODUCTION

1. The successful conduct of MSO is reliant upon comprehensive surface picture compilation together with timely intelligence and an understanding of the environment including common and expected shipping patterns as well as MSO “hot-spots”.
2. ‘Traditional’ surface picture compilation has been focused towards the recognition and identification of enemy combatants by organic sensors. This Annex aims to reiterate the principles of picture compilation and provide an overview of utility of Automatic Identification System (AIS). It is meant to be carried out both, onboard units (MSO) and in Maritime Surveillance Centers.

PRINCIPLES

3. Picture compilation can be subdivided into 5 processes;
 - a. Detection. The detection process involves the employment of sensors in a certain area to determine the presence or absence of contacts or contact-related data. The probability of gaining contact depends on a range of factors including:
 - (1) Accuracy of intelligence.
 - (2) Sensor coverage and level of confidence.
 - (3) Type and behavior of target.
 - (4) Time late and last known position.
 - (5) Operator performance.
 - (6) Environmental and geographic factors.Within MSO the detection process is likely to be cued by;
 - (7) Intelligence.
 - (8) Deviation of vessel movement from typical shipping pattern.
 - b. Localization. The localization process involves the use of sensors to determine the positional information and movements of a contact. During MSO it is likely that information from the ‘traditional’ organic sensors (e.g. radar, ESM, visual) will be combined with data from other sources e.g. AIS, or local intelligence to assist the localization process. It is important that all available information is reviewed, including that provided by outside sources such as N2 when determining if further investigation and hailing of a particular vessel is required.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

c. Recognition. Recognition describes the interpretation of data collected by sensors to determine the characteristics of a contact and compare it with reference data in order to lead to correlation with an associated level of confidence:

(1) **Certain**. Positively recognized by type, visually or electro-optically and by a competent person and continuously tracked after initial recognition.

(2) **Probable**. A certain contact that has been tracked intermittently and is confidently considered the same contact or a contact that has displayed strong cumulative information based on any two of the following:

(a) Electronic emission unique to a type of unit. This could include an AIS transmission.

(b) In a position predicted by intelligence reports. This could include Contact of Interest (COI)/High Interest Vessel (HIV) details.

(c) Sighted visually or by using EO but not positively recognized.

(d) Radar contacts with tracking and/or formation consistent with that expected of an externally reported contact.

(e) Weapon release by contact.

(3) **Possible**. A contact that has a lower degree of recognition than that required for “probable”. The confidence of the recognition should be amplified as follows:

(a) High Confidence: Only one of the criteria for probable is satisfied.

(b) Low Confidence: A contact that has indications that it may satisfy the criteria and further investigation is required.

d. Identification. This process results in the assignment of one of 6 standard identities:

(1) Hostile or confirmed Contact of Interest (COI)/High Interest Vessel (HIV).

(2) Suspect COI or HIV.

(3) Unknown.

(4) Neutral.

(5) Assumed Friend.

(6) Friend.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

e. Identification Criteria. A defined authority (possibly the ASUWC (when working as part of a TG) within a MSO context) should define a set of Identification Criteria (IDCRIT) that should be applied to a contact prior to assigning an identity. Within MSO examples of possible track identification means and associated IDCRIT are given below:

- (1) Visual.
 - (a) Vessel positively identified.
 - (b) Vessel identified, but not positively.
 - (c) Opening of fire.
 - (d) No or wrong reply to visual identification signal.
 - (e) No lights being shown.
- (2) Electronic.
 - (a) Vessel giving incorrect AIS information.
 - (b) Vessel less than 10 degrees from a communications intercept bearing
- (3) Behavior.
 - (a) Vessel in position predicted by intelligence reports.
 - (b) Vessel deviating from standard shipping route or traffic separation scheme.
 - (c) Vessel altering course for no obvious reason.
 - (d) Vessel not adhering to COLREGs.
 - (e) Vessel rendezvousing or conducting transfer with another vessel.
 - (f) Vessel attempts to turn away following detection.
 - (g) Vessel on a route known for illegal activity.
 - (h) Cargo or crew inconsistent with apparent role of vessel.
 - (i) Suspicious response to hailing.
 - (j) Vessel seen to be ditching equipment, cargo or personnel.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

f. During MSO it is vital that the ASUWC (or designated commander) issues a clear set of IDCRIT to cover a specific AOR and time period as they could act as triggers for ROE and subsequent actions. Examples include;

(1) **Reporting.** SUSPECT vessels are to be reported IAW CTG instructions. SUSPECT is defined within the IDCRIT as a vessel showing at least two of the following characteristics;

- (a) Vessel in position predicted by intelligence reports.
- (b) Vessel deviating from standard shipping route or traffic separation scheme.
- (c) Vessel on a route known for illegal activity.

(2) **Boarding.** These may only be permitted against SUSPECT vessels. SUSPECT is defined within the IDCRIT as a vessel showing at least two of the following characteristics;

- (a) Incorrect transmission of AIS data.
- (b) Suspicious response to hailing.
- (c) Ditching equipment, personnel or cargo.

g. Where special instructions have not been promulgated through a higher authority, a generic Surface IDCRIT for passage / transit operations may be appropriate. Table 1 provides an example:

| | |
|-----------------------------|--|
| COI/HIV (Hostile) | Pos Vis ID, Correlation of ESM, Query Discrepancies Hostile Behavior – Hostile Intent, Hostile Act Additional off board source info. |
| Possible COI/HIV (Suspect) | Behaviors, Low Confidence suspect ESM, unconfirmed ID, off board source info. |
| Unknown – pre QUERY | No indication of suspicious behavior or suspect ESM |
| Neutral – post QUERY | Response correlates to behavior positioning and off board source info (AIS) |
| Assumed Friend – post QUERY | Results correlate with supplementary information from off board sources |
| Friendly – post QUERY | Pos ID UK or Coalition Asset |

Table 1: Example of Generic Surface IDCRIT

h. Dissemination. Consideration should be given to the most effective means of disseminating surface picture information across a force whilst conducting MSO. Pre-designated Special Track (SPECTK) numbers are appropriate for passing COI and HIV information via voice cross-tell and tactical data links.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

SURFACE INVESTIGATE PROCEDURE

4. The Surface Investigate Procedure is an efficient method of collating information on a specific track. It is ideally suited for use within MSO but it should include, when available, information from systems such as AIS. A typical Surface Investigate Procedure is given at Table 2 below. The Investigate Procedure is inherently flexible; for example, some ships have reported a preference to delay the OOW report until the end of the procedure.

| BY WHOM | TO | CIRCUIT | STATEMENT | REMARKS |
|---------------|------|---------|---|--|
| ANYONE | ALL | COMMAND | ALL POSITIONS INVESTIGATE UNKNOWN SURFACE CONTACT BEARING _____ RANGE _____ START RECORDING | |
| TPS / ORS | PWO | COMMAND | RECORDERS RUNNING | |
| PWO | ALL | COMMAND | ALL POSITIONS REPORT TRACK BEARING _____ RANGE _____ | |
| SPS | PWO | COMMAND | TRACK _____ BRG _____ RNG _____ COURSE _____ SPEED _____ CPA _____ RXD ON LINK FROM PU/JU...(IF APPLICABLE) SQUAWKING/ NOT SQUAWKING MODE 1 2 3 4 | |
| OOW | PWO | COMMAND | NOTHING VISUAL/OR CONTACT BRG VISUALLY HELD ID'D AS _____ CONFORMING/NOT CONFORMING TO SEALANES | |
| GPEOD/ DAS | PWO | COMMAND | GPEOD/ DAS TRAINED _____ NOTHING VISUAL/OR CONTACT BRG ID'D AS _____ | ADDITIONAL INFO MOVING FROM LEFT TO RIGHT AS REQUIRED |
| SPC/AIS OP | ALL | COMMAND | TRACK _____ TYPE _____ NAME _____ TONNAGE _____ DESTINATION _____ CPA TO HVU/OPLAT _____ | AIS INFORMATION |
| EWD | PWO | COMMAND | TRACK _____ ESM DETAILS _____ MTP _____ CSS _____ INTELLIGENCE _____ | USING UAT/IAE/MTP/CSS HIGH INTEREST SHIPPING LIST |
| PWO | CAPT | COMMAND | TRACK _____ DETAILS & ASSESSMENT RECOMMENDATIONS | OOW STANDBY TO READ WARNINGS ON VHF CH CONSIDER QUICK DRAW SURFACE |

Table 2: SURFACE INVESTIGATE PROCEDURE

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

AUTOMATIC IDENTIFICATION SYSTEM (AIS)

5. AIS data may be provided via a number of integrated and stand-alone systems. Irrespective of the host system, AIS data can provide a significant contribution to the development of a comprehensive surface picture. The following paragraphs provide a summary of AIS and its potential impact on MSO.

6. AIS uses two common digital VHF channels (161.975 & 162.025MHz) to transmit and receive data automatically in precise time slots referenced against a GPS time signal.

a. Standard AIS information transmitted by a ship includes:

(1) **Static.** Fixed information, entered into the AIS on installation. Should remain unchanged unless a ship changes its name or undergoes major conversion.

(2) **Dynamic.** Data which, apart from 'Navigational Status' information, is updated automatically from the ship sensors connected to AIS.

(3) **Voyage Related.** Information that is manually entered and updated as required by ship's staff.

b. Details of information passed are given in Table 3 below:

| DATA IDENTIFIER | DATA DESCRIPTION |
|---|--|
| STATIC – Transmitted every 6 minutes | |
| Maritime Mobile Station Identifier (MMSI) Call sign/ Ships name IMO number Length and beam Type of ship | Set on installation. Data protected by an installation password. Selected from a pre-installed list, options include: <ul style="list-style-type: none"> • Tug • Passenger • Cargo • Tanker • Pilot boat • Tender Amplifying or further information may be added. RFAs include the statement 'Military Operations'. |
| Location of position fixing antenna | Set on installation. |
| DYNAMIC – Transmitted at intervals of 12 secs or less (Every 3 mins if at anchor) | |
| Ship's position | Updated automatically from the position sensor connected |

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

| DATA IDENTIFIER | DATA DESCRIPTION |
|--------------------------------|--|
| Time (UTC) | to AIS. |
| Course over ground (COG) | |
| Speed over ground (SOG) | |
| Heading | Updated automatically by the ship's heading sensor (Gyro compass). |
| Navigational status | Entered manually by OOW, options are: <ul style="list-style-type: none"> • Underway by engines • At anchor • Not under command (NUC) • Restricted in ability to maneuver (RAM) • Moored • Constrained by draught • Aground • Engaged in fishing • Underway by sail. |
| Rate of turn (ROT) | These all relate to COLREGs and should therefore be changed at the same time as lights or shapes. Updated automatically by ROT sensor if fitted. |
| VOYAGE RELATED | |
| Draught | Entered manually at start of voyage using anticipated max draught. |
| Hazardous cargo | Entered manually at start of voyage confirming if hazardous cargoes are borne as follows: Dangerous Goods (DG), Harmful Substances (HS), and Marine Pollutants (MP). |
| Destination and ETA | Entered manually at start of voyage and updated as required. |
| Route plan | Entered manually at start of voyage at CO's discretion. |
| SAFETY RELATED MESSAGES | |
| | Free format text messages that are entered manually addressed either to a specific addressee or broadcast. |

Table 3: AIS Data

7. AIS SURVEILLANCE. Both remote and organic AIS sensors can contribute to the effective surveillance of the area of interest however the ***potential for spoofing plus incorrect data should always be considered when using AIS to compile a surface picture.***

8. The following factors should be considered during operational planning;

a. Remote Open Source Data. Availability of remote open source AIS data (e.g. www.aislive.com) should be considered. Choke points and coastal areas are increasingly well covered and valuable traffic information may be provided however the timeliness of data received may require careful monitoring. Although it may be possible for ships to gain access to www.aislive.com (and other shipping data provided within the www), bandwidth limitations are expected to reduce easy

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

access. It is expected that in the future open source data such as that from aislive.com will be provided to the front-line within a fused picture either within the RMP or alternatively within a separate 'white shipping' picture.

b. Remote Classified Data. AIS data may be received within the Recognized Maritime Picture (RMP). Within each operation early liaison should be established with the appropriate organization in order to establish procedures for the reporting of AIS tracks to the RMP manager. Indiscriminate reporting of AIS tracks could rapidly overload the RMP production process. AIS sourced tracks within the RMP should be clearly annotated. The RMP manager may direct ships to tailor reports to provide coverage of a defined geographical area or specific Contacts of Interest (COI).

c. Organic AIS Coverage. AIS information will typically be gathered via WECDIS and a NAMESIS/AIS fit. AIS detection ranges vary widely depending on environmental conditions. Experience shows AIS coverage is rarely less than 30nm from own ship. Ranges of 40-60nm are typical, but under very good conditions, coverage beyond 150nm can be achieved. It should be noted that the extended ranges achieved may be due to 'skipping'; full surface coverage may therefore not be available out to the most distant track. Coverage has been seen to increase around sunrise and sunset.

d. Disposition of AIS fitted units within a force. In order to gain the maximum benefit from AIS, consideration should be given to the stationing of an AIS fitted unit within a force. Stationing the AIS fitted unit at the centre of the force allows the AIS range advantage (over radar) to be exploited. Non-AIS fitted units can be directed towards AIS contacts and make early identification. Hailing can be based on background data passed from the AIS fitted unit.

e. AIS & Hailing. If AIS data is available within the force all ships can dramatically reduce the requirement for VHF hailing. If hailing is required, name and/or call sign from AIS should be used to enable a short and precise call. Experience has shown that 'short calling' is appreciated by merchant shipping. Care should also be taken to ensure that merchant ships are not subject to repeated VHF hails from different warships; pre-assigned Link Special Track numbers can be used within a force to indicate ships that have been hailed.

AVIATION SUPPORT TO MARITIME SURVEILLANCE

1. Aviation has a significant role to play in Maritime Security Operations (MSO) whether providing embarked support to Force Elements afloat or providing shore-based coverage both overseas and at home (in the context of Homeland Security). The skills required of flying crews are largely those employed in traditional ASuW and therefore does not require specialist training, however, the key component to the employment of aircraft in MSO tasking is the timely flow of information pre-flight, in-flight and post-flight.
2. Maritime helicopters possess a range of sensors and dynamic capabilities that enable them to make a key contribution to MSO² as follows:
 - a. Surface picture compilation. Most modern maritime helicopters are capable of high endurance, possess long-range radar system and a tactical data link to contribute to the building of the RMP. Older aircraft offer reduced endurance and may lack data link but can offer beyond visual range detection.
 - b. Marking/shadowing. Maintaining station to report on a contact designated a Vessel of Interest. The different sensor suite capabilities may dictate which aircraft type is particularly suited to a shadowing mission.
 - c. Information/intelligence gathering. All aircraft types can provide varying degrees of support, whether merely traffic pattern monitoring with radar or gaining more detailed data/evidence at closer range visually or with camera equipment.
 - d. Interdiction. Most helicopters possess the ability to conduct rapid roping to vessels underway as a component of boarding operations.
 - e. Presence. A helicopter's range and speed advantage allows a visible (and audible) presence at a place and time of MSO benefit far in advance of surface ships.
3. AIS provides valuable surface picture to aircrew. The system is currently fitted on some aircraft with a wider implementation planned.
4. It is not intended within this Annex to provide guidance on the coverage that each platform can provide in directed MSO tasking, as this is directly related to the specific aim of a mission, target size and the operating environment. A tasking authority should seek guidance from flying crews, using the current guidance within their tactics manuals (TACMANs), to advise on the coverage that can be delivered on a case-by-case basis. For directed MSO tasking, flying crews will require clarification on the information (content, quality, format) plus the timeliness and method of its delivery.
5. To fully exploit the value of maritime helicopters in delivering MSO effect, their ability to provide presence, gather information or to contribute to the RMP during routine (non-MSO related) flying ops must be utilized. For example, a long-range Helicopter

² The contribution from shore based aircraft including routine training sorties should not be Overlooked but is not the focus of this Annex.

CHENS MARITIME SECURITY BEST PRACTICE GUIDELINES

Delivery Sortie (HDS) may allow the aircraft to cover an area far away from the immediate focus of MSO and therefore provide an added dimension. Key to this is ensuring adequate information flow to all Force Elements all of the time. Procedures are required to ensure the aircraft can rapidly report back a Vessel of Interest or for aircrew to be made aware of emerging activity. The latter is operationally essential for an aircraft not directly engaged in MSO that, unless adequately briefed/updated, may unwittingly operate in an area where an overt presence is not desirable.

6. Connectivity is critical and the dissemination of the Intelligence product is essential. For aircraft embarked in ships, this process should be catered for by the guidance within this guidance. Finally, use of support vessels as helicopter operating bases requires careful consideration to the dissemination of information to and from these vessels where the N2/N3 infrastructure is likely to be limited.

7. Co-operation with assets from Other Government Departments (OGDs) and international partners will be an increasing feature of MSO. The disparity in secure communications fits between aircraft and platforms of OGDs/other nations will drive the need for procedures to be implemented (such as the use of low-grade codes) to ensure the security of radio transmissions.

8. All types of aircraft, rotary and fixed wing, whether embarked in ships or based ashore operating in the maritime environment have a significant role to play in both data collection to improve Shared RMP and conduct of Operations. All commanders must be fully aware of the capabilities of the aircraft in his force and ensure that best use is made of this valuable asset.

SUBMARINE PLANNING AND SUPPORT GUIDANCE FOR MSO

INTRODUCTION

1. Whether forward deployed on routine operations or deployed rapidly in response to a developing crisis, submarines have a range of capabilities that enable them to contribute to, and benefit from, Maritime Situational Awareness. Maritime Security Operations may be conducted in the homeland littorals and the approaches but may also be undertaken worldwide.
2. The ability to gather and manage information in a manner that leads to decision superiority is key to operational success. Submarines provide a crucial strategic, operational and tactical intelligence gathering capability that cannot be replicated by other means. Employing multiple sensors, submarines can monitor events in the air, surface, or subsurface littoral domain providing a complete picture of an event across a wide spectrum of intelligence disciplines. They are also capable of providing cueing of high interest events to other assets, whether it is for further intelligence collection or actual prosecution.
3. Submarines are able to conduct extended, covert operations in areas inaccessible to other platforms or systems. The ability to dwell covertly for extended periods defeats efforts to evade collection or deceive satellites and other sensors. The look angle provided by a submarine enables it to intercept high interest signal formats that are inaccessible to reconnaissance satellites. The intelligence gleaned from submarine operations ranges from highly technical details of platforms, command and control infrastructure, and sensors to information concerning potential adversaries' operational and tactical intentions.

INITIATION AND PLANNING

4. Submarines can receive the RMP either via a HF aerial or INMARSAT. When connected via INMARSAT the submarine will be viewed as any other fixed user on the system network.
5. Prior to deploying, submarines are to request a tailored RMP from the Operating Authority. This is to be incorporated in the SUBNOTE REQUEST. The tailored RMP will match the ordered submarine broadcast communications schedules. The radius of this service will be dependant on other operations. As this will be a 'directional' tailored service, it may not be available to all deployed submarines and will be determined on a 'case by case' basis.
6. INMARSAT capable deployed submarines should be provided with an 'always on' RMP feed. This will remove the need to establish communications with the operating authority request the INMARSAT RMP feed to be enabled. Submarines receiving this 'always on' service should make full use of the filters available to ensure they only receive a local (as necessary) RMP and not the full 'worldwide' RMP. If the submarine is receiving a tailored HF RMP, it is recommended that the 'full' RMP from the INMARSAT feed is not used.

7. The conduct of MSO requires active planning and operational support. To ensure submarines are provided with comprehensive intelligence management and support throughout their deployment, it is vital that early and robust liaison between Intelligence agencies, the Operating Authority communications officer and the submarine occurs. The Operating Authority will play a key role in co-ordinating the necessary arrangements and explain the support available.

OPERATION

8. As submarines become fitted with the Automatic Identification System (AIS) and training and support is provided, submarines should be more readily able to contribute to, and benefit from, the RMP. To scope the submarines' contribution to the RMP, the following procedure is provided for initial guidance;

- a. Based on the SUBNOTE Moving Haven, ensure a tailored RMP is provided to the submarine.
- b. Whilst at PD, the submarine may 'receive only' the AIS data stream through VHF Maritime system and display the information.
- c. Submarine is to produce reporting messages encompassing any contacts held and signal this via normal channels.
- d. Submarine receives an updated tailored RMP. This should now include all contacts generated by the submarine (See Para 9).
- e. In addition to AIS, traditional submarine methods of contact identification and tracking can be used and reported.

9. There will be periods, during certain operations, when information received from the submarine by operating authority will not be included in the generation of the RMP. This will usually be because, if included, it could provide indication of a submarine presence. This information will, however, be channelled to the appropriate authority depending on the operation. Although MSO relates primarily to operations before getting 'in theatre', the transmission of any information, remaining cognizant of EMCON and Command authority, is highly desirable either pre or post CHOP into the area of operation.