

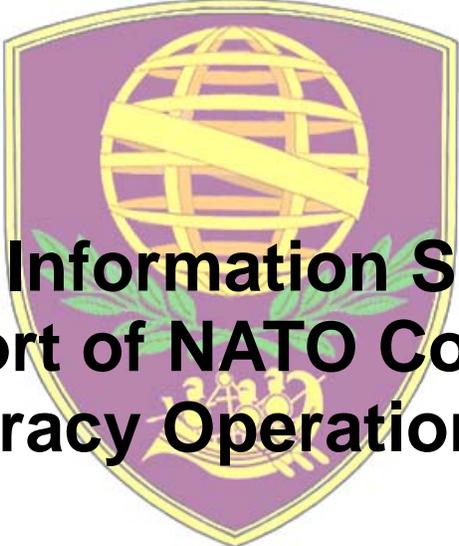


A Report by NATO's
Joint Analysis and Lessons Learned Centre



JALLC/CG/11/163

15 July 2011



**External Information Sharing in
Support of NATO Counter-
Piracy Operations**

Non-Classified Extract

External Information Sharing in Support of NATO Counter-Piracy Operations

15 July 2011

FOREWORD FROM THE COMMANDER

I am pleased to forward this report on the external sharing of information in support of NATO's counter-piracy operation: Operation OCEAN SHIELD. This JALLC study is focused on operational and tactical levels of command, and its purpose is to identify recommendations for improvement within NATO. However, the findings are broader in scope and some of the recommendations are pertinent to all levels of command. Some may even be applicable outside NATO, although we were constrained to make these recommendations exclusively to a NATO audience.

A particular feature of current counter-piracy operations off the Horn of Africa is the multitude of participating maritime forces: in addition to NATO's Operation OCEAN SHIELD, there is the EU Operation ATALANTA, Combined Maritime Forces, and independent national deployments. A key finding of this report is the need for improved shared situational awareness through information assurance and an enhanced ability of these counter-piracy forces to exchange information. Additional findings include the need for clearly articulated information exchange requirements, a tenable approach to classifying information and consistent means of handling criminal evidence. Several of these findings echo findings in earlier studies related to other theatres of operation, indicating we could do better in our lessons learned process.

In addition to examining shortfalls, this report contains identified best practices. I am especially pleased to note that professionalism has been identified as a best practice. In line with the NATO's new Strategic Concept, this professionalism is a realization of NATO's commitment to work more closely with our international partners—in this case, in the complex environment of counter-piracy operations.

Peter SONNEBY
Brigadier General, Danish Air Force
Commander JALLC

External Information Sharing in Support of NATO Counter-Piracy Operations

This report prepared by:

Project manager: MCNICHOL Douglas – LCDR CAN N – JALLC Staff Officer
for Joint Operational Logistics
PRZYMANOWSKI Marek – LTC POL F – JALLC Staff
Officer for Joint Plans
ROSS David – COL USA F (retired) – JALLC Contractor for
Operations Analysis

From August 2010 to June 2011 at multiple locations including Portugal, the United Kingdom, Middle East, Africa, NATO HQ, SHAPE, and HQ SACT.

Joint Analysis and Lessons Learned Centre

Avenida Tenente Martins, Monsanto
1500-589 Lisbon
Portugal

Tel: + 351 21 771 7002

Fax: + 351 21 771 7098

www.jallc.nato.int

The recommendations included in this report require endorsement by the Strategic Commands and/or its principal customer. To know which recommendations have been endorsed, please contact SHAPE FOR RER FSL Lessons Learned or HQ SACT CAPDEV PPM LLI or check the NATO Lessons Learned Database.

Executive Summary

BACKGROUND

Counter Piracy (CP) operations are being conducted off the Horn of Africa and in the Indian Ocean by many separate forces operating under a variety command arrangements. NATO's involvement began in late 2008 under UN remit to protect humanitarian assistance vessels and expanded during 2009 to become Operation OCEAN SHIELD (OOS) with the task to combat piracy and build regional capacity to combat piracy.

This analysis project was originally proposed by Admiral Luciano Zappata, then Deputy Supreme Allied Commander Transformation (DSACT), who had observed CP operations during NATO's initial involvement. At the time, DSACT observed that there was considerable confusion, duplication of effort and poor coordination among these forces.

MISSION

The Joint Analysis and Lessons Learned Centre (JALLC) was tasked by HQ Supreme Allied Commander Transformation (SACT) in the 2010 Programme of Work with the following analysis requirement:

Analysis Requirement: With respect to the operational and tactical activities of OOS since the North Atlantic Council Initiating Directive, analyze information sharing between NATO, EU Operation Headquarters, and other major actors in the CP effort with the aim of identifying any NATO best practices for sharing information, as well as any shortfalls in NATO doctrine or policies for information sharing that may be detrimental to planning or execution of operations.

The agreed analysis objectives (AO) were:

- AO-1.** Within the framework of OOS, identify what information is and should be shared, as well as how, between NATO and external entities.
- AO-2.** Examine the conduct of sharing information with external entities in that context and with respect to existing policy, doctrine, and directives within NATO.
- AO-3.** Recommend courses of action to facilitate information sharing to enable coherent planning and execution of NATO maritime operations in which cooperation with external entities is necessary.

METHODOLOGY

The team collected data—including mission documents and orders—from all headquarters involved in, or associated with, NATO's counter-piracy effort, as well as other entities such as the EU, Combined Maritime Force (CMF), independent national deployers, merchant liaison organizations, and Interpol.

The project team reviewed and discussed work initiated by NATO Centres of Excellence (COE), such as the COE for Combined and Joint Operations from the Sea, and the NATO Maritime Interdiction Operational Training Centre (NMIOTC). In addition, the project team used information from previous JALLC analysis projects that had examined information sharing in Afghanistan and in Operation ACTIVE ENDEAVOUR.

MAJOR CONCLUSIONS AND KEY RECOMMENDATIONS

Sharing situational awareness information and operating pictures

Military forces conducting CP operations lack common, shared situational awareness, and their situational awareness is often based on inaccurate and/or outdated information. There is a lack of a common network available to all CP forces, meaning that for information to be shared it must be input into multiple networks, increasing the risk of errors, data loss and delay. Different forces process and interpret data differently; a problem best solved by cooperation and coordination to create a common situational awareness database rather than simply sharing data points. Formal software tools would likely be needed to create a common situational awareness database in a timely fashion. Unity of effort in theatre is also hampered by not knowing the capabilities and intentions of other forces, resulting in lost opportunities and inefficient use of critical resources.

Recommendations

HQ SACT should accelerate, where possible, the implementation of Baseline for Rapid Iterative Transformational Experimentation (BRITE) as a standard Maritime Command and Control Information System (MCCIS) application, and in collaboration with SHAPE and Joint Force Command Lisbon, consider offering BRITE to CMF and the EU.

Considering the strategic benefits of accurate and common knowledge, SHAPE should consider proposing to their CMF and EU counterparts that the NATO-EU-CMF group establish a joint cell or centre, with rotational lead, to fuse situational awareness data.

To share classified information with non-NATO entities, HQ SACT should accelerate efforts to obtain authorization by the NATO Investment Committee for the capability package(s) for the implementation of Secure Maritime Releasable CIS.

Sharing information with Interpol

Interpol has been cited repeatedly as a key agency in the final resolution of the maritime piracy problem. Sharing information with Interpol is complicated by a myriad of different national policies and laws on what can and cannot be shared, and a single over-arching framework for NATO has not been established. However, even though the national mechanisms differ, each nation does have a way to share with Interpol. The overall effectiveness of OOS could be improved by encouraging participating nations to share their information with Interpol to the full extent allowed by their national laws. Additionally, NATO does not currently provide comprehensive training in law enforcement activities to its maritime forces and such training is needed, especially on the collection and preservation of evidence needed by foreign or international courts for the prosecution of suspected pirates. Finally, there is presently no NATO concept of operations for the handling of biometric data, leading to uncertainty and inconsistency in dealing with information that could be used by Interpol.

Recommendations

JFC Lisbon should propose a policy encouraging Nations participating in OOS to use national frameworks to provide information about suspected pirates to Interpol, either directly or via their National Central Bureaus.

In coordination with the International Military Staff, SHAPE should consider inviting and enabling Interpol to provide maritime law enforcement training, possibly by enhancing NMIOTC curriculum.

SHAPE should continue its endeavour to establish an ACO Concept of Operations for Biometrics in Support of Operations.

Sharing information with merchant mariners

There is a need to improve the situational awareness of merchant mariners; whose safety is the primary purpose for NATO's CP operations. CP forces have been proactive in providing information to merchants, but their efforts have been hampered by not fully understanding the merchant mariners' situations and limitations. During the course of this analysis project, Maritime Command (Mar Cmd) HQ Northwood implemented a procedure to push vital information to merchant mariners when necessary, but at least once each day. This improvement has been described in this report, partly to document the process for future maritime operations.

Recommendation

Mar Cmd HQ Northwood should provide a periodic (daily) summary of pirate group locations and movements/intentions. This needs to be broadcast (pushed) to ships at sea in a short, concise teletype message.

Contents

Foreword from the Commander.....	i
Executive Summary.....	iii
1 Introduction.....	1
Background.....	1
Analysis Requirement and Analysis Objectives.....	1
Purpose of the Report.....	1
Methodology.....	2
Factors Affecting the Analysis.....	3
Other Factors Observed.....	3
2 Sharing Situational Awareness Information and Operating Pictures.....	5
Introduction.....	5
What is Situational Awareness.....	5
Entities Involved in Providing Situational Awareness Information.....	6
Challenges to common situational awareness.....	6
Conclusions.....	10
Recommendations.....	10
3 Sharing with Interpol.....	11
Introduction.....	11
Contact with Interpol.....	11
Information Exchanges.....	12
National Dealings with Interpol.....	12
NATO–Interpol Relations.....	13
Training.....	14
Notes.....	14
Conclusions.....	15
Recommendations.....	15
4 Sharing with Merchants.....	16
Introduction.....	16
Limitations of the Merchant Mariner.....	16
What merchants need from CP forces.....	17
What CP Forces need from Merchants.....	17
Conclusions.....	18
Recommendations.....	18

5	Best Practices	19
	MultiLateral Shared Awareness and Deconfliction.....	19
	“Best Management Practices” Booklet.....	19
	Multilateral Air Coordination Element.....	19
	European Union “MERCURY” System.....	19
	Professionalism.....	20
	References	21
	Annex A Glossary of Acronyms	1



TF 508 Manoeuvres at Speed¹

¹ Photo courtesy of Maritime Command Northwood Public Affairs

BACKGROUND

1. This project was initiated as part of Joint Analysis and Lessons Learned Centre's (JALLC) 2010 programme of work (Reference A). The project was initially proposed by Admiral Luciano Zappata, then Deputy Supreme Allied Commander Transformation (DSACT), who had observed counter-piracy (CP) operations during NATO's initial involvement. CP off the Horn of Africa is being conducted by many separate forces operating under a variety command arrangements. At the time, DSACT observed that there was considerable confusion, duplication of effort and poor coordination among these forces.

2. The multinational forces—NATO Operation OCEAN SHIELD (OOS), the European Union Operation ATALANTA and the Combined Maritime Forces (CMF) Combined Task Force (CTF) 151—are comprised of nations that have frequently worked together in alliances or combined missions and many of these nations are participating in all three of these forces. These three forces are referred to in this report as the NATO-EU-CMF group or *N-E-C group*.

3. At the time the project was initiated, there had been considerable changes and improvements to coordination the CP effort since DSACT's original observations. As such, the project was refined to analyse the information sharing at the operational and tactical levels according to the requirement below. Also, Joint Force Command (JFC) HQ Lisbon assumed the role of customer from DSACT, with Maritime Command (Mar Cmd) HQ Northwood as a co-customer.

ANALYSIS REQUIREMENT AND ANALYSIS OBJECTIVES

Analysis Requirement: With respect to the operational and tactical activities of OOS since the North Atlantic Council (NAC) Initiating Directive, analyze information sharing between NATO, EU Operation Headquarters, and other major actors in the CP effort with the aim of identifying any NATO best practices for sharing information, as well as any shortfalls in NATO doctrine or policies for information sharing that may be detrimental to planning or execution of operations.

4. The Analysis Objectives (AO) were defined as:

AO-1. Within the framework of OOS, identify what information is and should be shared, as well as how, between NATO and external entities.

AO-2. Examine the conduct of sharing information with external entities in that context and with respect to existing policy, doctrine, and directives within NATO.

AO-3. Recommend courses of action to facilitate information sharing to enable coherent planning and execution of NATO maritime operations in which cooperation with external entities is necessary.

PURPOSE OF THE REPORT

5. This report has been written to document the results of this analysis project. The project team has benefitted from working closely with the customer throughout the project from initiation through to completion. As a result, many of the operational- and tactical-level recommendations were discussed as they arose and, where within the

purview of the customer, actions based thereon haven been initiated or implemented. For these situations this report documents issues that should be considered in future operations when unity of command is lacking. The recommendations may also serve to support actions and requests from the customer, JFC HQ Lisbon to higher headquarters in respect to OOS.

6. The report begins with the need to document commanders' information exchange requirements, and the project team's research on what some of those requirements external to NATO should be. This is followed by the need for common understanding and awareness of the CP forces, with an examination of the means available or that could be available.

7. The report then focuses in on key issues such as classification and release, sharing with Interpol and sharing with merchant mariners. The report then documents some of the key initiatives and actions taken by OOS and other CP forces that have worked well and which may be beneficial to emulate in future operations.

METHODOLOGY

8. The analysis began with a review of documentation about the issue and mission. The team reviewed mission documents and orders issued by SHAPE, JFC HQ Lisbon, Commander Maritime Command (COM MCC) Northwood, and Commander Task Force (TF) 508, NATO's CP task force. The project team also reviewed and discussed work initiated by NATO Centres of Excellence (COE), such as the COE for Combined and Joint Operations from the Sea (CJOS), and by the NATO Maritime Interdiction Operational Training Centre (NMIOTC). Coincidentally, both CJOS COE and NMIOTC held CP-related conferences during the project period, which provided the project team additional opportunities for data collection that might not have been possible otherwise. In addition, the project team used information from previous JALLC analysis products that had examined information sharing in Pakistan, Afghanistan, and NATO's Operation ACTIVE ENDEAVOUR.

9. The team then met with the customer to review findings to date and compile a list of agencies with which NATO shares or should share information, and then established a data collection plan to enable the team to meet and interview as many of those people as possible. In addition to JFC HQ Lisbon and Mar Cmd HQ Northwood, the team visited the following locations:

- a. NATO HQ, Brussels;
- b. HQ Supreme Allied Commander Transformation (SACT), Norfolk, United States;
- c. SHAPE, Mons;
- d. Mar Cmd HQ Naples;
- e. International Criminal Police Organization (Interpol) HQ, Lyon, France;
- f. EU Military HQ, Brussels;
- g. EU Naval Force (NAVFOR) HQ, Northwood, UK;
- h. EU NAVFOR Forward Logistics Cell Djibouti;
- i. CJOS COE, Norfolk, United States;
- j. NMIOTC, Chania, Greece;
- k. CMF HQ Bahrain;
- l. UK Maritime Trade Organisation (UKMTO), Dubai, UAE;
- m. Maritime Information Exchange Vessel Operators Meeting (MIEVOM) Dubai, UAE;

- n. Shared Awareness and Deconfliction (SHADE) meeting, Bahrain;
- o. Standing NATO Maritime Group (SNMG) 2 while inport Lisbon, Portugal;
- p. SNMG1 while inport Oman;
- q. Spanish Air Detachment Djibouti;
- r. Japanese Air Detachment Djibouti;
- s. Civil-Military Cooperation Fusion Centre, Norfolk, United States.

10. The collected data was then reviewed. In support of the customer's requirements, the team documented external information exchange requirements as commented upon by OOS participants at all levels. These requirements were then compared against methods and means for information sharing, both those currently available to and used by OOS (and other CP forces) and those that could be used or made available. This allowed for analysis to describe the need, benefit, and shortfalls of the status quo and potential alternative methods and means. The requirements were also compared to NATO security policies and regulations.

FACTORS AFFECTING THE ANALYSIS

11. It was agreed with the customer that this project would focus all recommendations upon what NATO could do to improve information sharing. Any observations or recommendations that reflected upon actions that other entities could take were not followed up or addressed in this report.

12. While the Analysis Requirement refers to the EU in particular, the project team and the customer agreed that with respect to the "other major actors", the project would focus on the N-E-C group from a military perspective. The inclusion of CMF on the military side reflects its size and sophistication and the substantial overlap it has with OOS and EU Operation ATALANTA. There was also a need to keep the project to a manageable size. As such, with respect to civilian information exchange, the project focused on Interpol and merchant mariners. Interpol was chosen for its role in the overall effort against piracy. Since the purpose of the military CP effort is ensuring safety of merchant mariners, information exchange with them is a key aspect of the mission.

OTHER FACTORS OBSERVED

13. At the time of project initiation and transfer of primary customer status to JFC HQ Lisbon, JFC HQ Lisbon observed that OOS would benefit from a related, but different analysis question, how to improve integrated and/or cooperative planning with the EU. As this was outside the scope of this project as defined in the 2010 POW, this was not addressed by this project. However, JFC HQ Lisbon proposed this second question for the JALLC 2011 programme of work (Reference B) which was initially accepted. Aspects of integrated planning and the supporting operational information exchanges were deferred to this project. This project has been recently postponed until further notice, as the engagement between NATO and EU on the intervention in Libya has expanded the scope of such a study.

14. There is a great deal of commonality within the forces involved in CP. Figure 1 shows membership in NATO, the EU and CMF. It shows, for example, that the EU and NATO share a common 75% of their membership, and ten nations are common to all three. This commonality brings opportunities to facilitate exchanges of information through common systems, procedures policies and pre-established levels of trust. This perspective should be considered throughout this report.

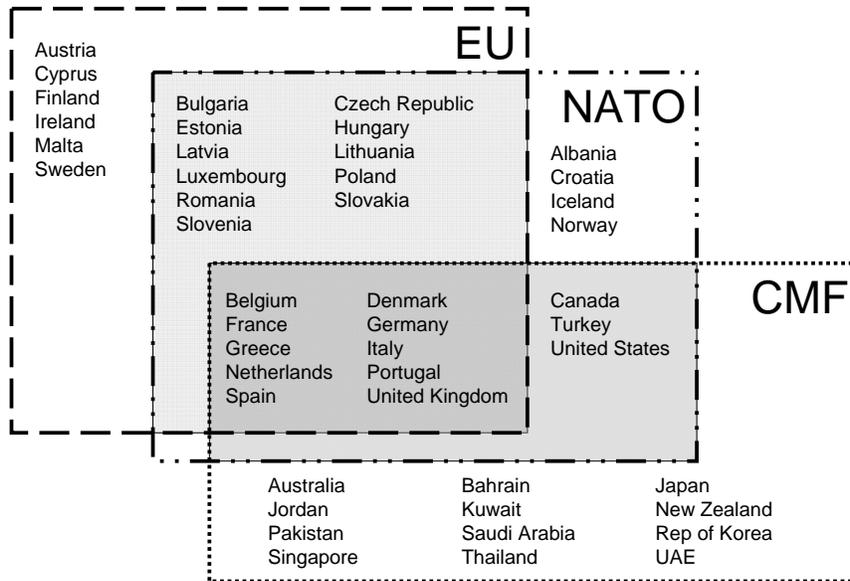


Figure 1: Venn Diagram showing N-E-C Group membership commonality

Sharing Situational Awareness Information and Operating Pictures

INTRODUCTION

15. Everyone in the region needs information to help them understand the situation, and that information needs to be accurate and timely. Sharing accurate and timely situational awareness information is essential to counter piracy forces and the mariners (merchant and private) they support; sharing decreases the risks to the lives of those at sea. It is quite appropriate, therefore, that situational awareness information be shared externally more than any other type of information in the region. As observed by the project team, though, and as confirmed by interviews with nearly 150 military and civilian persons involved in CP, situational awareness information being shared among CP forces and with merchant and private mariners is often inaccurate. Accordingly, the topic of sharing situational awareness information, including operating pictures as components of that awareness, deserves careful examination.

WHAT IS SITUATIONAL AWARENESS

16. In any context, situational awareness is knowledge and understanding of the environment. In the context of CP operations, situational awareness information should include facts about suspected pirates, merchant ships (white shipping data), CP forces, and the operations areas. For CP forces, it should also include details about each commander's own forces, as well as details (including intentions and capabilities) about other forces operating in the area. As described in the NATO Concept for Maritime Situational Awareness (Reference G), the objective of situational awareness in a maritime environment is to gain *"the required information superiority ... to achieve a common understanding of the maritime situation in order to increase effectiveness in the planning and conduct of operations"*. It is important to note that situational awareness is not only relevant to military forces, but also to non-military entities in the region.

17. An operating picture is a subset of situational awareness, often referred to as the common operating picture (COP) or, for the maritime component, the recognized maritime picture. When there is more than one operating picture (e.g. a NATO operating picture, a CMF operating picture, and an EU operating picture), the operating picture that is common to all entities can simply be called the COP. For CP operations in the Gulf of Aden and off the Horn of Africa, the COP should include all available air and maritime pictures. Classification issues preclude the possibility of having a single COP for counter-piracy operations; however they should not preclude the possibility of having multiple COPs wherein data which is not classified is common to all operating pictures.

18. The sharing of information necessary to achieve and maintain situational awareness is a component of the overall interaction that takes place between all CP entities. For complete situational awareness, though, there are more interactions needed than simply sharing information. For this, it is important to note certain characteristics of interacting. These characteristics were described by the NATO Senior Civilian Representative in Afghanistan in a recent report² to the NATO Secretary

² "Comprehensive approach – Lessons Learned in Afghanistan"; Report, submitted to Secretary General under Cover Memorandum, 15 July 2010

General. With the exception of *collective decision making*, they equally apply to the CP environment:

Depending on the type of outcome desired by each actor, the level of interaction and effort will occur over a spectrum, ranging from awareness, to deconfliction, to cooperation, leading eventually to coherence. Modalities for interaction should be viewed as a set of functions or mechanisms that promote transparency and trust that enable a given level of interaction, e.g., information sharing, planning coordination, cooperative problem solving, collective decision making, and mutual situational assessments.

ENTITIES INVOLVED IN PROVIDING SITUATIONAL AWARENESS INFORMATION

19. Within NATO, situational awareness includes military intelligence, which is normally provided by NATO nations, NATO commands and NATO agencies and is subject to agreed policies on its control. It also includes situational awareness obtained from open sources, commercial agencies (Reference H), as well as a number of other means that are not subject to control through NATO policy. For OOS, situational awareness is developed not only from information obtained from NATO sources, but also from other CP actors including national assets and international organizations³.

20. Each organization's situational awareness is part of the common awareness or, as previously described, as the *common understanding of the maritime situation*. In line with AO-3 of this analysis project (*recommend courses of action to facilitate information sharing to enable coherent planning and execution of NATO maritime operations in which cooperation with external entities is necessary*), an objective of this analysis on sharing situational awareness information and operating pictures has been to indicate a way in which to expand the level of common understanding. We propose to do this by examining the challenges to achieving common situational awareness.

CHALLENGES TO COMMON SITUATIONAL AWARENESS

21. The Project team identified six areas wherein challenges influence the ability to achieve comprehensive and common situational awareness. These areas are the following:

- a. Geography
- b. Multiple Sources of Information and Limited Capacity for Information Correlation
- c. Different Communities of Interest

Geography

22. Since Somali piracy first became of worldwide interest, the area in which these pirates operate has expanded significantly. In 2005, for example, acts of piracy were reported up to 165 nm off the coast of Somalia. By 2008, this range had already increased to 445 nm off the coast; and, by 2010, it had increased to 1430 nm. The left side of Figure 3 illustrates this geographic expansion of pirate activity; the right side compares it to the size of Europe.

³ Ideally, regional CP actors (e.g. Somali and Yemeni authorities) would also be key players in contributing to situational awareness, but NATO's ability to exchange information with many of those actors is limited. See the latest Periodic Mission Review and resulting decisions of the NAC (Reference I).

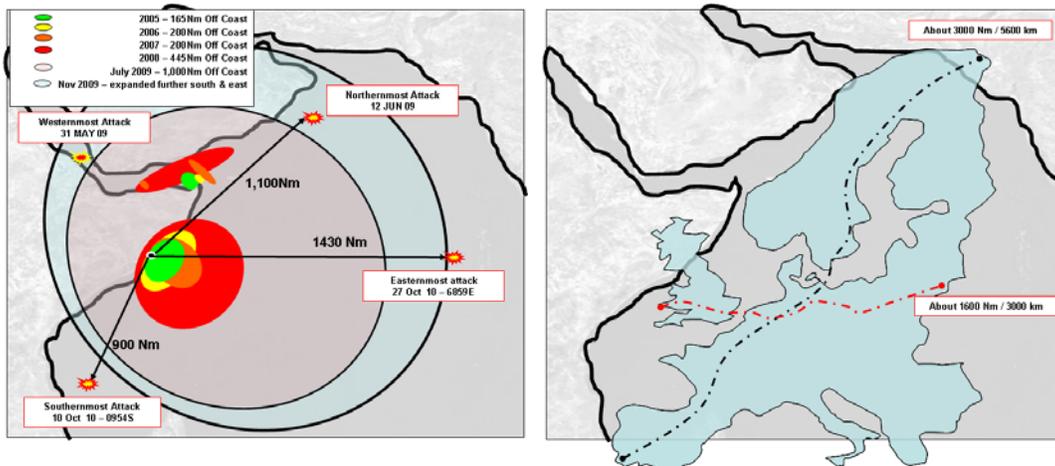


Figure 3: Map of CP danger areas

23. Such expansion of the area of pirate activity significantly increases the amount of information needed to enable situational awareness. Without an increase in situational awareness information or improved capabilities to process additional situational awareness information, the geographic expansion increases the likelihood of there being significant gaps in the CP forces' awareness. These are challenges which underline the importance of close cooperation between CP forces, including the independent deployers, and they highlight the importance of full and common situational awareness.

Multiple Sources of Information and Limited Capacity for Information Correlation

24. Situational awareness information for CP operations comes from a vast number of sources; moreover, each participant in CP operations has a different set of sources. There are some primary sources for the information and some of those are common to all CP forces. For much of the situational awareness information, though, there are multiple raw sources:

25. For example, a single merchant vessel might provide multiple situation reports—automatic identification system (AIS) reports to local AIS reporting stations every few minutes, long range identification and tracking transmissions to its flag nation less periodically, voluntary reporting to entities such as the UKMTO⁴ or the NATO Shipping Centre as agreed or deemed necessary, and voluntary sighting reports when they see something significant⁵. Similarly, different Intelligence sources often provide slightly different information about pirate camps or mother-ship locations.

26. As situational awareness information from these many sources is compiled, its complexity is compounded in several ways, all of which require that situational awareness information be carefully correlated (by correlation we mean any activity to clarify and reconcile data, including data fusion, recovery, extrapolation, and correction). The following are some of the challenges that arise in correlating data:

- a. Different sources typically use different reference numbers for the same ship. Additionally, different sources normally report different information, and with different

⁴ UKMTO requests voluntary message updates at least once each day from ships transiting the Red Sea, Indian Ocean, and Arabian Gulf.

⁵ Merchant mariners are encouraged by the handbook *Best Management Practices, Third Edition* (BMP3) (Reference K) to report suspicious activities. These reports are sometimes filed with parent shipping companies instead of CP agencies.

degrees of accuracy or timeliness. Accordingly, to maintain good situational awareness, it is necessary to repeatedly correlate multiple reports for each ship into a single set of data.

b. Information gaps often occur when reports are not submitted for any reason (e.g. the captain might turn off the AIS transceiver). Thorough correlation would allow for recognition of such situations and extrapolation of available data to cover these gaps.

c. It is quite common for reports about any given ship to arrive out of sequence, meaning what appears to be the most recent report does not contain the most current information. Proper correlation would catch such discrepancies and help ensure that the most current data is not replaced by less current data.

d. Finally, there are instances of situation reports containing detailed information about ships being automatically over-written by reports containing very little information. Valuable information can be lost in this process. Again, proper correlation would catch such discrepancies help ensure that the more detailed data is not overwritten.

27. The following are some examples that illustrate deficiencies that can arise when information is not correlated rapidly and accurately:

a. Inconsistency in operating pictures: As just one example, it was observed that information being shown to merchant mariners is sometimes as much as 40 hours older than information being used by CP force commanders.

b. Insufficient detail in reports: Situation reports do not uniformly describe situations (event or ship), even when they are accurate. Many maritime reports, for example, give little information more than location, course, and speed. A full, quality portrayal of a situation normally requires the fusion of several reports.

c. Information latency: The most significant deficiency noted among CP forces was the routine delay of sharing situation reports (e.g. intelligence, surveillance, and reconnaissance reports). According to interviews with staff officers on TF 508, for example, Intelligence information is sometimes delayed up to 72 hours.

28. Many of those interviewed indicated that the process of sharing situational awareness information between the different entities is good in many respects, but bad in the sense that it generates more information that commanders and their staffs must assimilate when making decisions. Throughout the course of interviews and observations, it was reported that the different CP forces frequently base decisions about the same situations (e.g. a specific hijacking event) on different, or even conflicting, situational awareness information. In some situations the raw data is different; in others, however, the raw data was often the same but each force drew different conclusions from it. It would seem that the need for correlation goes beyond just a single force doing it for itself. There should instead be common correlation efforts to provide each force commander a common baseline of information and lead in turn to more coordinated action by these forces.

29. The speedy correlation of multiple data sources requires effort and is facilitated by strong IT Systems. Yet it would appear that the capacity of the N-E-C group to provide the necessary level of correlation does not meet the need. To some extent, these challenges could be mitigated by designating a common CIS for exchanging situational awareness information, but not completely. There would still be the reality that situational awareness information comes from different sources and is often interpreted differently by the different forces. One senior leader in theatre suggested as a solution a combined fusion centre, staffed by all N-E-C group forces. COM MCC Northwood also underlined the importance of building a shared intelligence capability in Annex D of his 2009 OPLAN for Commander TF 508 (Reference L).

30. An example of the CP forces combining their efforts already exists. The Air Coordination Element (ACE) in Bahrain is operated by personnel assigned from each of the N-E-C group entities, as well as from independent nations providing air assets to the overall CP effort. The ACE coordinates all air assets that are assigned to support CP. Chief ACE is assigned on a rotational basis between NATO, CMF, EU, and the independent nations. Moreover, the requirements to be met by air assets are managed in a cooperative manner by the same entities (i.e. NATO, CMF, EU, and independent nations offering air assets). That management is overseen by the Joint Coordination Management Board (JCMB)⁶ which meets weekly via secure video-teleconference.

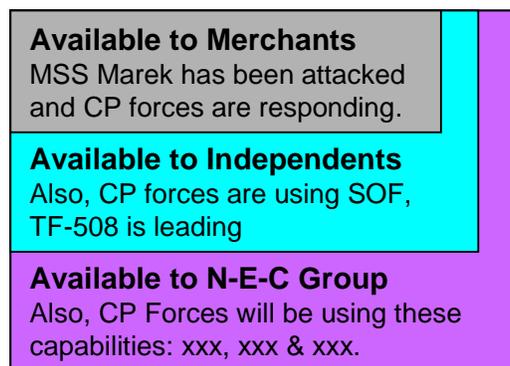
31. A Combined Fusion Centre could meet the need to ensure that situational awareness information is as accurate and timely as possible, correlating information from different sources item-by-item in order to provide all CP commanders and staff involved with a common view of the most accurate and timely information possible. Although it would be naive to suggest that such a fusion centre could completely mitigate all problems with regard to accuracy, quality, and timeliness of information; it would go a long way towards providing decision makers with the best information possible as a common baseline on which to base decisions.

Different Communities of Interest

32. Finally, as noted in several places in this report, there are at least three communities of interest that need correlated information. These communities are:

- The N-E-C group which have reasonable means of sharing classified information,
- The independent deployers that need information about military operations but do not have a reasonable means to share classified information with the N-E-C group and
- The merchant mariners which primarily need to know information about pirate activity (confirmed and suspected).

33. These communities can be represented from the bottom to the top by the classified domain, the unclassified domain, and the non-classified domain. As previously stated, though, the information needs of these communities should not be met with three separate sets of data. Instead, the needs should be met with a single set of data that includes permission characteristics. In this way, the communities would have common information that would be as accurate and timely as possible. The concept is illustrated in figure 4, below.



⁶ The project team believes the JCMB is a best practice that should be considered for future operations where NATO is working closely with other forces toward common aims. See Chapter 7 for further details.

Figure 4: Three communities of interest needing correlated situational awareness information in the context of OOS

CONCLUSIONS

34. Military forces conducting CP operations lack common situational awareness and the situational awareness that is available is often based on inaccurate and/or outdated information; reasons why include:

- a. Information is shared but not processed, or is processed independently by different CP forces, leading to different, sometimes contradicting, situational awareness.
- b. No current deployable capability for sharing classified information with non-NATO entities in OOS.

35. Transparency between forces with regard to their capabilities and intentions is essential to unity of effort.

RECOMMENDATIONS

36. Considering the strategic benefits of accurate and common knowledge, SHAPE should consider proposing to their CMF and EU counterparts that the N-E-C group establish a joint cell, with rotational lead, to fuse situational awareness data.

INTRODUCTION

37. NATO counter-piracy forces will sometimes collect information⁷ about suspected pirates and pirate activity that could be used in courts of law to prosecute suspected criminals, and which could be used by proper authorities to investigate the criminal networks supporting piracy at sea. This chapter examines the pragmatic aspects of NATO forces providing such information to the International Criminal Police Organization (Interpol).⁸

38. Existing guidance for the conduct of OOS does not specifically mention the need to exchange information with Interpol, but it does give direction to provide evidence to designated authorities. As noted by several key leaders during data collection, though, NATO forces are not consistent in their conduct of sharing evidence with Interpol. Every key leader interviewed expressed the opinion that the net effect of this inconsistency is that NATO is not doing as much as it could to counter piracy.

CONTACT WITH INTERPOL

39. Interviews with many senior leaders and staff officers responsible for conducting OOS⁹ revealed strong agreement that NATO counter-piracy forces need to provide information about suspected pirates and pirate activities to Interpol. In fact, interviews at all levels of command revealed consensus that a successful end state for OOS will largely depend not only on growth of regional capacity, but also on prosecution of suspected pirates. Interpol is actively involved in both in a number of ways.

40. Interpol is the world's largest international police organization, presently having 188 member countries. Membership includes every member country of NATO and every country identified as involved in international counter-piracy activities.

41. Interpol is already working with a variety of UN entities including the Political Office for Somalia, UNDP, the Department for Peacekeeping Operations, and CGPCS to broaden the exchange of information between all key players affected by piracy. Also, Interpol provides investigative and operational police support on an ongoing basis to all member countries affected by maritime piracy in the Gulf of Aden and off the coast of Somalia. With its worldwide networks of member nations, reporting mechanisms, and databases, Interpol is able to conduct in-depth analysis of piracy activities, facilitate arrangements for detention and prosecution, and provide legal evidence to prosecution authorities.

42. The UN Security Council unanimously agreed to Security Council Resolution (UNSCR) 1950 (Reference Y) on 23 November 2010 recognizing the efforts that various entities, especially Interpol, have made to bring suspected pirates to justice. The resolution urges member states to cooperate with Interpol to support their efforts against maritime piracy.

⁷ With the exception of training to protect criminal evidence, which is addressed in this chapter, activities leading to the collection of pirate-related evidence are beyond the scope of this report.

⁸ It should be noted that many of the findings of this study are in line with an HQ SACT legal study for Maritime Situational Awareness development (Reference X) which was endorsed by the International Military Staff on 04 October 2010.

⁹ Based on interviews with 17 senior leaders and more than 50 staff officers involved in the conduct of OOS: there were no dissenting views.

INFORMATION EXCHANGES

43. Sharing information with Interpol is not about whether or not information should be provided, but rather what information should be shared and by what authority NATO forces should share it. Based on observations and interviews, the project team discovered three factors contributing to inconsistencies in fulfilling these needs:

a. The first factor regards the legal basis for collecting information and sharing that with any external entity. Presumably, that legal basis would be part of a legal framework for the mission. Such a framework was indeed addressed in the NAC Initiating Directive for OOS, which advised that the NATO International Staff would make every effort to create an overarching legal framework. Prior to that advice, the CGPCS had tasked its Working Group 2 to develop legal proposals of a similar nature. To date, though, there is no such overarching framework.¹⁰

b. The next factor regards concerns on the handling of biometric data. Global security issues have led to an ongoing search for reliable methods of identification and verification using intrinsic human features such as fingerprints, retina, DNA, voice or, more recently, body scans (referred to as biometric data). Concerns have been raised regarding the protection of human rights and fundamental freedoms and in response many nations have established strict policies and legal restrictions with regard to the handling of such data.

c. Finally, the specific information to be provided to Interpol has not been articulated to the forces—not by a legal framework, OPLAN, policy, doctrine, or tactical procedures.

44. One course of action for resolving the issues with regard to sharing information with Interpol is to continue the endeavour to establish a specific legal framework (either by the UN, by NATO, or by both) that is supported and built upon NATO and national policies and, based on that framework, define what information should be collected and provided to Interpol. Another key component of that course of action would be a Security Assurance negotiated between Interpol and an appropriate NATO commander¹¹, and a set of NATO guidelines for handling biometric data¹². But that approach will take time, and key leaders have expressed concerns about further delay. So, the JALLC sought to identify a pragmatic, near-term solution. The solution was found in the structure of Interpol and is consistent with that proposed in the HQ SACT Maritime Situational Awareness, Phase 1 Legal Study Report (Reference X).

NATIONAL DEALINGS WITH INTERPOL

45. Interpol's structure includes one National Central Bureau for each member country, the key function of which is to facilitate the exchange of information between that member country and Interpol. Every member of NATO, even every country in the vicinity of the OOS Area of Operation (including Somalia), is a member of Interpol. Each of these countries has both an existing legal arrangement defining its relationship with Interpol and a National Central Bureau making it part of the Interpol structure. Of course, each member of Interpol has its own internal legal framework which is fully unique to that country, but Interpol's constitution and core functions accommodate these differences.

¹⁰ Preamble VII of the United Nations Convention on the Law of the Sea establishes a legal framework for counter-piracy activity. The fact that both the NAC and UN CGPCS have called for a more specific framework suggests that a more specific framework would be beneficial. The JALLC did not examine that suggestion.

¹¹ Security Assurances are discussed in Chapter 4 of this report.

¹² Per a SHAPE memo to the Nations in March 2011 (Reference Y), SHAPE has already undertaken the task of developing a Biometrics Concept of Operations.

46. The immediate solution identified by HQ SACT, Interpol, and the JALLC is to put in place mechanisms necessary to encourage, and explicitly permit, NATO counter-piracy forces to share information with Interpol through their National Central Bureaus. The first step should be to define the information that should be exchanged. Ideally SHAPE would work with Interpol to define information that NATO forces might acquire and which Interpol might need. The information actually passed will be affected by national factors, but these should not limit the aspirations expressed.

47. A NATO policy should then be established encouraging NATO counter-piracy forces to share information with Interpol via their National Central Bureaus. As OOS is based on decisions agreed by the UN Security Council; such a policy should be based on UNSCR 1950, to which all NATO nations have already agreed. Recognizing that Nations contributing forces to OOS delegate operational control to SACEUR, the policy should clearly state that OOS forces are allowed to fully exercise their national responsibility¹³ in providing piracy-related information to Interpol while under the operational control of SACEUR. Essentially, the NATO policy would be one encouraging Nations to abide by the UNSCR to which they have already agreed, and to exercise the arrangements with Interpol they have already established.

48. This policy should then be established at the tactical level; articulating the information that should be shared with Interpol and ensuring that national forces are encouraged to, and certainly not impeded from, sharing piracy-related information with Interpol. National forces should be encouraged to inform Commander TF 508 of their exchanges with Interpol to assist Commander TF 508 in mission planning, operations, and assessment, to the full extent permitted by their national laws and regulations.

NATO-INTERPOL RELATIONS

49. Ideally, under either an interim or final arrangement for counter-piracy forces to provide information to Interpol, the process would include a two-way exchange that is predefined in terms of content, format, and timing. Any other arrangement would have ad-hoc characteristics, leaving each entity to guess or assume the existence of pertinent information.

50. The information NATO might have that would be pertinent to the objectives of Interpol is detailed information about suspected pirates to enable prosecution. When the JALLC team visited Interpol offices in Lyon, France, experts there were working to create a reporting format that might be helpful to military forces. Interpol is quite aware that different nations have different rules about what criminal information can be obtained, how it can be obtained, and how it must be handled. In every situation, Interpol respects those rules.

51. Some specific elements of information Interpol would like to receive from military forces is listed in the table of Partial Information Exchange Requirements at Annex C to this report. It is important to note, though, that Interpol has no interest in classified information. Even if Interpol could protect classified information, it cannot use it.

52. Information that Interpol might have that would be pertinent to NATO's objectives would include verification of data and feedback on the value that NATO is providing to Interpol's efforts in fighting crime and building capacity in the region. Generally, representatives of Interpol have indicated that they are prepared to provide the following:

- Training for the collection and preservation of evidence (either ad-hoc or permanent);

¹³ Use of the word "responsibility" is based on national agreements to UNSCR 1950.

- Assistance in drafting policy or an operational framework;
- Assistance in collecting information needed to prosecute criminals (if deemed beneficial, this assistance might include the provision of a liaison officer to Commander TF 508 or an any NATO headquarters facility);
- Verification of data;
- Feedback to counter-piracy forces on their contributions to fighting international crime;
- Access to their facilities to allow representatives of NATO to verify that information is properly protected.

53. During interviews, representatives of Interpol assured the JALLC team that they stand ready to assist NATO in any way possible. For example, Interpol could partner with NATO to establish an information exchange “pilot effort” during which both entities could observe progress and assess the best way ahead.

TRAINING

54. Concerning the subject of the possibility for Interpol to establish a permanent training arrangement for NATO forces, the JALLC team visited the NATO Maritime Interdiction Operational Training Centre (NMIOTC) located at the Souda Bay Naval Base near Chania, Greece. NMIOTC provides training for disrupting illegal activities such as suspected pirate activities, including the legal basis and policies associated with approaching and boarding suspected pirate and pirated vessels, but does not have the capacity to provide comprehensive training on the collection and preservation of evidence for international courts.¹⁴

55. At present, many ships pass through the Souda Bay Naval Base for training en-route to participation in OOS. Adding (or joining) Interpol training to existing NMIOTC courses could have the inherent advantage of enhancing the scope of the training¹⁵ while minimizing the impact to national costs and crew schedules. This could be achieved with periodic trainers' support or with train-the-trainers sessions, so that training capacity could be achieved to deliver appropriate training with NMIOTC staff.

NOTES

56. Before concluding this chapter of the report, it is significant to note that there have been two developments, based in part on UNSCR 1950 (Reference Y), that demonstrate international resolve with regard to cooperating with Interpol in bringing suspected pirates to justice:

- a. On 07 December 2010, the EU adopted a decision calling for forces participating in Operation ATALANTA to transmit information about suspected pirates to Interpol.
- b. As previously noted Interpol announced its intention on 15 February 2011 to provide essential equipment and training to law enforcement to African countries tackling maritime piracy.

¹⁴ NMIOTC seeks to improve training on this subject with trainer augmentees from Law Enforcement Agencies.

¹⁵ It has been argued that evidence collection training should be provided nationally in order to meet national court requirements. However, few NATO nations are conducting prosecutions within their own nations, preferring to seek jurisdiction agreements in the region, such as with Kenya or the Seychelles. Additionally, a key use of this evidence is for analysis allowing identification of support networks and financiers of piracy, in which Interpol is intimately involved. Here, the minimum criteria and advice of Interpol is clearly applicable.

CONCLUSIONS

57. All countries and agencies involved in the CP missions have endorsed Interpol's involvement; however few mechanisms have been established for military forces to coordinate with them directly.

58. Neither the UN nor NATO have established a single, overarching legal framework tailored to CP operations, which would establish a single legal framework for sharing information with law enforcement authorities such as Interpol.¹⁶ However, each NATO Nation has an established legal arrangement for cooperating with Interpol, to include sharing information, and maritime forces assigned to NATO can use their respective national arrangements for sharing information with Interpol.

59. NATO does not provide comprehensive training in law enforcement activities to its maritime forces. Training is needed, especially on the collection and preservation of evidence needed by foreign or international courts for the prosecution of suspected pirates.

60. There is presently no NATO concept of operations for the handling of biometric data, leading to uncertainty and inconsistency in dealing with information that could be used by Interpol.

RECOMMENDATIONS

61. JFC HQ Lisbon should propose a policy encouraging Nations participating in OOS to use national frameworks to provide information about suspected pirates to Interpol, either directly or via their National Central Bureaus.

62. To enable OOS tactical and operational commanders to determine the value of exchanging information with Interpol, SHAPE should encourage Nations to inform Commander TF 508 of the details of all information exchanges, including national information exchanges, with Interpol regarding piracy and CP activities.

63. In coordination with the International Military Staff, SHAPE should consider inviting and enabling Interpol to provide maritime law enforcement training, possibly by enhancing NMOTC curriculum.

64. Once a law enforcement training capability is established, SHAPE should encourage Nations to route contributions to OOS through that training prior to in-chop.

65. SHAPE should continue its endeavour to establish an ACO Concept of Operations for Biometrics in Support of Operations.

¹⁶ Many identify this as a lack of political will or policy. Regardless of the cause, there is no legal framework.

INTRODUCTION

66. Sharing information is an essential part of OOS and this must include sharing with merchant mariners. The very raison d'être of OOS is to provide a safe and secure environment for merchant mariners in the Gulf of Aden and Somali Basin. If we are unable to communicate with them, give them the information that they need to conduct their business and derive from them what we need to support them, then we are inviting failure.

67. There is a general will and intent to share appropriate information between merchant mariners and CP forces. However, it became clear over time that almost every issue raised by merchant mariners could be traced back to misunderstandings between CP forces and merchant mariners related to needs, methods, and capabilities. This chapter will look at these misunderstandings and how they can be resolved.

68. The project team had the opportunity to interview several merchant mariners during the data collection period. While not an extensive or definitive sample size for valid statistical analysis, the broad nature of backgrounds and activities they undertook, along with the virtually unanimous nature of their commentary gives the project team confidence to discuss the findings generated from these interviews.

69. Interaction between CP forces and merchant mariners happens at two levels: that between organizations and that between vessels at sea. NATO has established significant contact and interaction with mariner organizations, trade groups, and shipping company offices: these interactions appear to be going well, and the JALLC could not find significant areas for improvement in this area. At sea, however, there appears to be a significant divide between what the merchant masters are advocating and the naval forces are providing.

LIMITATIONS OF THE MERCHANT MARINER

70. Most masters interviewed by the team indicated that they lacked spare manpower and resources at sea. A typical merchant ship might carry a crew of 10 to 30, compared to over 200 for a typical warship involved in CP. Merchant crews are as small as safely possible to maximize the profit to the shipping firm and hence have little free capacity to actively collect information about pirate activities. With this in mind, most mariners interviewed indicated that the quantity of information coming to them by the limited means available quickly overcame their available time and often went far beyond their need. Long teletype messages were quickly discarded if the first few lines did not indicate immediate value.

71. NATO and many NATO member nations have developed information management processes with a pull system from web-based information centres. Most merchant ships do not have reliable, inexpensive internet connections to pull information from websites and lack the free time to browse for information. Few shipping companies have operations centres which can seek out information and push it to their ships and so CP forces must adapt their own processes to push the necessary information to the master at sea.

WHAT MERCHANTS NEED FROM CP FORCES

72. Merchant mariners interviewed by JALLC expressed their needs in very simple terms. They indicated that they neither needed nor wanted classified intelligence information, but were concerned simply for the safety of their ships, crews, and cargos. They were looking for information about how to identify pirates at sea, where suspect vessels are located, and how to avoid them.

73. This concern was raised with COM MCC Northwood and Commander TF 508 staff, who indicated that a significant portion of pirate information was derived from classified sources, and was therefore unreleasable. When briefed on the needs and limitations as described here, Mar Cmd HQ Northwood N2 adapted to provide this information, indicating that it would consider an INMARSAT broadcast. This would allow masters to prepare and manoeuvre their ships to ensure its best protection.

74. Additionally, merchant mariners expressed concern and reservation over “who is in charge” of the CP effort, and whom they should call. They indicated a need for a single point of contact for all interactions with CP forces. They cited the myriad of organizations involved, from NATO, EU NAVFOR, CMF, NATO Shipping Centre (NSC), Maritime Security Centre Horn of Africa¹⁷ (MSCHOA), UKMTO, The Maritime Liaison Office¹⁸, etc, as well as contact points within the independent deployers' nations.

75. It is believed that establishing a single point of contact for all CP forces will not be possible until a single command or coordination structure can be established, which is not envisioned in the foreseeable future. The merchant liaison organizations within the N-E-C group have made efforts to coordinate their efforts, a particular organization being assigned specific functions and the other organizations referring merchants to them. While this is a good start, appropriate contact points and requirements are still not clear to the merchant masters. Regrettably, this area will continue to be a cooperative effort between many military and governmental entities working together and there needs continued effort to avoid duplication and ensure a simple common face is presented to merchant mariners.

76. A consolidated effort by several shipping associations and naval/merchant liaison organizations has resulted in the publication and distribution of BMP3 (Reference K), which has been cited as very beneficial in providing clear, simple guidance to mariners entering the region.

WHAT CP FORCES NEED FROM MERCHANTS

77. CP forces do not have significant demands from the merchant community, beyond those normally asked of merchants upon the high seas. CP forces need situational awareness as described in chapter 3 and their needs can be broken down into three categories

- a. Location of ships: provided by AIS data transmitted automatically and acquired by military organizations, vessel voluntary reporting through UKMTO, and warship observations and reporting/exchange. The project team found little indication of a lack of information in this regard, but only a lack of compilation and coordination of this information (as addressed in Chapter 3).
- b. Piracy risk factors: CP forces need to be aware of the piracy risk level for vessels transiting the region (risk factors and preventative measures as detailed in BMP3).

¹⁷ An office within EU NAVFOR

¹⁸ An office within US Naval Forces Central Command

This information is requested and generally provided through arrival messages sent to MSCHOA, UKMTO, and/or NSC.

c. Piracy incident observations: CP Forces need awareness of potential pirate sightings, attacks, etc. Merchant mariners have generally been very forthcoming with this information when required, which is usually passed through UKMTO.

All of this information is generally forthcoming from the larger ships and from well established companies. Smaller or independent ships tend to be less compliant, likely due to time and communications limitations.

CONCLUSIONS

78. CP forces have been placing useful information in a number of locations with the expectation that the merchant mariner would pull it when required, however merchant vessels at sea lack the time, resources, and manpower to actively pursue this search. Therefore CP forces need to adapt to a push format, actively distributing the relevant information and no more.

79. Unless unity of command is achieved, there will continue to be many organizations that deal with merchant mariners about the dangers of piracy. There exists a unity of purpose between these organizations and they are making every effort to cooperate and coordinate in this matter, however, unless a division of roles and responsibilities is made clear to the merchant mariner, confusion will still exist.

80. Merchant vessels are the primary targets of pirate attacks and knowing where merchants are located permits the CP forces to offer protection, in addition to which each merchant ship represents an additional observer that can report on suspicious activity. Therefore information provided to CP by merchant mariners forms an important part of the CP forces' situational awareness.

RECOMMENDATIONS

81. Mar Cmd HQ Northwood should provide a periodic (daily) summary of pirate group locations and movements/intentions. This needs to be broadcast (pushed) to ships at sea in a short, concise teletype message.¹⁹

82. It is recommended that Mar Cmd HQ Northwood/NSC continue efforts to coordinate their work with other merchant liaison offices and simplify the requirements and points of contact for merchant mariners.

83. It is recommended that Mar Cmd HQ Northwood/NSC encourage merchant vessels to continue providing information to CP forces in order to improve situational awareness and the protective ability of the CP effort.

¹⁹ During the post data collection phase brief at Mar Cmd HQ Northwood, that HQ indicated that they were already producing and posting the message, and would endeavour to ensure that it was broadcast as well.

84. During data collection, the Project team discovered a number of efforts that were deemed to be worthy of consideration for future NATO operations. In some respects, these might be considered “Best Practices”.

MULTILATERAL SHARED AWARENESS AND DECONFLICTION

85. The SHADE meetings were established in 2009 to provide a tactical-level, non-political forum in which all military elements engaged in CP operations in the Gulf of Aden and off the Horn of Africa can discuss successes and challenges, share best practices, and coordinate forthcoming activities. The 18th meeting in January 2011 was attended by representatives of 32 countries and numerous organizations. SHADE meetings are held in Bahrain, normally on a monthly basis, with every country engaged in CP activities being eligible to chair or co-chair a meeting.

“BEST MANAGEMENT PRACTICES” BOOKLET

86. BMP3 is the third version of the BMP booklet²⁰ that is being distributed to the shipping industry, including ship crews, to publicize what the shipping industry believes to be best practices to avoid and disrupt pirate attacks. The publication of the BMP3 booklet is a combined effort of several entities—government, non-government, and military. Those involved in identifying and publishing best practices collaborate to aggressively distribute the booklet to as many recipients as possible. BMP3 lists 21 entities, including both the NSC and OOS, as those cooperating in the effort.

MULTILATERAL AIR COORDINATION ELEMENT

87. The multilateral ACE, which is collocated with CMF in Bahrain, is responsible for coordinating the schedules and flying missions of all military air assets supporting CP activities. It includes representatives of the N-E-C group, as well as each of the independent deployers providing air assets to support the effort. Its existence helps tremendously in mitigating challenges resulting from there being too few air assets to meet all demands and there being no unity of command.

EUROPEAN UNION “MERCURY” SYSTEM

88. MERCURY is a website established by the EU MSCHOA to enable trusted users having internet access to collaborate and maintain awareness of the situation regarding pirate activities, including suspected pirate activities, and military actions to disrupt those activities. The site provides online awareness, 24-hour chat (including private chat forums), relevant documents, and a graphical representation of white shipping, as well as detailed information (including photographs, when available) of actual and suspected pirates and pirate activity. Recognizing the need to collaborate with entities without access to classified network (e.g. shipping industry, shipping organizations, and independent deployers), the EU established MERCURY very early in its operation. Although the website exists in the unclassified internet domain, there are several security measures in place to protect information.

²⁰ It is a 12cm x 18 cm (5”x 7”) booklet having 80 pages, including a two-page map and five pages for notes at the back. It is also distributed electronically at different levels of resolution.

PROFESSIONALISM

89. Finally, the determination and professionalism observed at all levels of command in cooperating with other entities and adapting NATO policies and procedures to the CP environment are cited as a collective set of good practices.

- a. One of the most prevalent examples observed at the levels of JFC, COM MCC, and Commander TF was the relentless challenging of Intelligence characteristics. What classification should be assigned to Intelligence information? To whom should Intelligence be provided? The observed consensus at all levels of command was that CP Intelligence needs to be given to those who need it, including independent deployers and merchant mariners; and meeting that need infers that those who hold the information must do whatever is necessary to share it.
- b. Another demonstration of this professionalism was the conviction at all levels that every entity involved in CP has an important part to play, and that the effort each entity contributes is worthy. Whether considering differences in mission approach, levels of effort, capabilities, political will, legal limitations, or various other seemingly significant factors, the NATO personnel interviewed during this analysis displayed tremendous respect for every effort. One of the more significant examples of this professionalism is the tremendous respect consistently rendered to each of the independent deployers, regardless of the capabilities of any country or the manner in which that country decided to use those capabilities.
- c. A third form of this determination and professionalism can be seen in the efforts to cooperate. Most of the "Good Practices" already listed in this chapter serve as examples. Another example, though, that was interesting to the JALLC team regarded credit for identifying best practices and publishing BMP3. As previously noted, the "BMP3" booklet lists 21 entities that cooperated in those efforts. The project team concluded that it was indeed a cooperative effort, with each of the 21 entities contributing. If any entity did contribute more than any other, the NATO Shipping Centre and others involved in BMP3 clearly see the greater value of equal credit to all.

References

- A. HQ SACT, 2010 JALLC POW, 7 December 09, TI-3592/Ser:NU:0804, NATO UNCLASSIFIED
- B. HQ SACT, 2011 JALLC Programme of Work, 1 December 10, 5000 FPK-0050/TT-6843/Ser: NU0656, NATO UNCLASSIFIED
- C. MC 0195/8, NATO Minimum Interoperability Fitting Standards for Communications and Information Systems (CIS) Equipment Onboard Ships, Submarines and Maritime Aircraft, 09 October 2008, NATO Restricted
- D. Bi-SC Reporting Directive 80-3, Volume I, Concept and General Instructions, 01 January 2000, NATO Unclassified Releasable to PfP
- E. JALLC, Sharing, Dissemination, and Release of Information in ISAF, 17 February 2009, JALLCCG/09/021, NATO Restricted Releasable to ISAF
- F. COMISAF IX, Annex Q to OPLAN 38302 (Revise 1), International Security Assistance Force (ISAF) Operations in Afghanistan, 08 January 2007, NATO/ISAF Confidential Releasable to GCTF
- G. MC; NATO Concept for Maritime Situational Awareness, 14 January 2008, MCM-0140-2007, NATO Restricted
- H. MC 0401; NATO Policy for Defence and Protection of Off-Shore Infrastructure in the North-western European and Eastern Atlantic Region; 2 June, 1998; NATO Restricted,
- I. MC; Operation OCEAN SHIELD Periodic Mission Review (PMR) 2010, 13 August 2010; MCM-0095-2010,; and Office of the Secretary General,; NAC Approval - 2010 Periodic Mission Review (PMR) of Operation OCEAN SHIELD, 11 October 2010; DSG(2010)0669; NATO Confidential
- J. Commander Combined Maritime Forces; Letter to SHAPE; 18 April 2010
- K. Best Management Practices to Deter Piracy off the Coast of Somalia and in the Arabian Sea, 3rd edition; Witherby Seamanship Intl Ltd; 2010
- L. COM MC Northwood; OPLAN 27704 Operation OCEAN SHIELD for Enhanced NATO Counter Piracy Engagement Off The Horn Of Africa (Annex D), 14 August 2009, 1700/NWNOI /180109, NATO RESTRICTED Releasable to EU/PfP/MD/ICI/CC
- M. MSA (Maritime Situational Awareness) CD Plan (Concept Development Plan), 15 August 2008; Enclosure 2 TO 5000 C-210/TT-4322/Ser: NU DATED: 17 MAR 09; Unclassified
- N. NAC; Security within the North Atlantic Treaty Organization (NATO) 17 June, 2002; Document C-M(2002)49; NATO unclassified
- O. NAC; Security within the North Atlantic Treaty Organization (NATO) Corrigendum 8, 09 April, 2010; Document C-M(2002)49-COR 8; NATO unclassified
- P. NATO Security Committee, NATO Security Committee Directive on the Security of Information, 6 December, 2006 AC/35-D2002-Rev 3; NATO Unclassified
- Q. NATO Security Committee; NATO Security Committee Supporting Document on Information and Intelligence Sharing with Non-NATO Entities, 20 December 2010. AC/35-D/1040-Rev 2, NATO Unclassified

- R. Bi-SC Handbook for Information and Intelligence Sharing with Non-NATO Entities Version 4.0, April 2010; NATO Unclassified
- S. NAC; Security within the North Atlantic Treaty Organization (NATO) Corrigendum 3, 05 December 2006; Document C-M(2002)49-COR 3; NATO unclassified
- T. JHQ Lisbon; Staff Notice, Release of Information to Non-NATO Entities; 02 June 2010; SN:080/10; NATO Unclassified
- U. SHAPE, SACEUR Operations Plan 10710 OCEAN SHIELD for an Enhanced NATO Role in Countering Piracy at Sea Off the Horn of Africa, 13 August 2009, SHJ5Plans/7340-59/09 - 207311; NATO Restricted Releasable to EU/PfP/MD/ICI/CC
- V. MC 0128/07; Policy Guidance for NATO Intelligence; 11 May 2009; NATO Restricted,
- W. SHAPE; Information and Intelligence Sharing Between CC-Mar Naples and Non-NATO Op ACTIVE ENDEAVOUR Contributing Nations, 23 February, 2007; 3050/SHIXX/060/07-201877; NATO Restricted
- X. HQ SACT; Maritime Situational Awareness, Phase I Legal Study Report, 01 Sep 2010; 1000 TSC GLX 0030/TT-66261Ser: NU0518, NATO Unclassified.
- Y. United Nations, UNSCR 1950(2010), The Situation in Somalia, 23 November 2010

Annex A

Glossary of Acronyms

ACE	Air Coordination Element
ACO	Allied Command Operations
ACT	Allied Command Transformation
AIS	Automatic Identification System
AO	Analysis Objective
Bi-SC	of the two Strategic Commands
BMP3	Best Management Practices, third edition.
BRITE	Baseline for Rapid Iterative Transformational Experimentation
CENTRIXS CMFC	Combined Enterprise Regional Information Exchange System for Combined Maritime Forces Central Command
CGPCS	UN Contact Group on Piracy off the Coast of Somalia
CIS	Communication and Information Systems
CJOS	Combined Joint Operations from the Sea
CJTF	Combined Joint Task Force
CMF	Combined Maritime Forces
COE	Centre of Excellence
COMISAF	Commander, International Security Assistance Force
COM MCC	Commander Maritime Command ²¹
COP	Common Operating Picture
CP	Counter-Piracy
CTF	Combined Task Force
CUR	Crisis Response Operation Urgent Requirement
DA	Delegated Authority
DSACT	Deputy Supreme Allied Commander Transformation
IER	Information Exchange Requirements
Interpol	International Criminal Police Organization
ISAF	International Security Assistance Force
JALLC	Joint Analysis and Lessons Learned Centre
JCMB	Joint Coordination Management Board

²¹ In accordance with MC 0324/2, The NATO Command Structure, Annex A, 09 November 2009, NATO Restricted

JFC	Joint Force Command
Mar Cmd	Maritime Command
MC	Military Committee
MCCIS	Maritime Command and Control Information System
MIEVOM	Maritime Information Exchange Vessel Operators Meeting
MSA	Maritime Situational Awareness
MSCHOA	Maritime Security Centre – Horn of Africa
MSSIS	Maritime Safety and Security Information System
NAC	North Atlantic Council
NAVFOR	Naval Force
N-E-C group	NATO, EU, CMF Counter-Piracy Forces
NMIOTC	NATO Maritime Interdiction Operational Training Centre
NNE	Non-NATO Entity
NOR	NATO Office of Resources
NOS	NATO Office of Security
NS	NATO Secret
NSC	NATO Shipping Centre
OOS	Operation OCEAN SHIELD
OPLAN	Operation Plan
SACEUR	Supreme Allied Commander Europe
SACT	Supreme Allied Commander Transformation
SEMARCIS	Secure Maritime Releasable CIS
SHADE	Shared Awareness and Deconfliction
SOR	Statement of Requirement
TF	Task Force
UKMTO	UK Maritime Trade Organization
UNSCR	United Nations Security Council Resolution