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

# 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*

### Commander's information exchange requirements

Information flow has improved dramatically since NATO initially began conducting counter-piracy operations.  This improvement is largely due to the professionalism and dedication of personnel.  However, the absence of a concise list of information exchange requirements (IER) has caused information sharing to be somewhat ad-hoc and based on the perceived priorities and personalities of incumbent personnel.  In other theatres, it has been observed that formally articulating a Commander's IER List has helped to standardize and stabilize communications with external entities and it is believed that OOS would similarly benefit from such an approach.

Recommendations

Commander Maritime Command Northwood should articulate the Commander’s IERs for OOS: with the aid of the suggestions provided in Annex C to this report and the format used by International Security Assistance Force.

SHAPE and HQ SACT should collaborate to expand the direction in two Strategic Commands' (Bi-SC) Reporting Directive 80-3 for defining IERs, including recommended format and the various purposes that a consolidated list can serve.

### 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.

### Information classification and release

Although OOS largely consists of law enforcement activity, essentially conducted in a non-classified environment, a significant portion of intelligence information supporting the operation is over-classified.  Great efforts are being made to downgrade and declassify information to allow sharing, but recent NATO Security Policy changes and tools designed to support exchanging information in multinational military operations are not well known by the OOS staff and are consequently under-utilized. Additionally, even though NATO Security Policy does not require a mission classification system for OOS, implementing a mission classification system could improve the timeliness of sharing.

Recommendations

SHAPE and HQ SACT should ensure awareness and provide better training of the Bi-SC Handbook for Information and Intelligence Sharing with Non-NATO Entities. Although Allied Command Operations and Allied Command Transformation staffs have been provided with some training, training of this type needs to be provided to the intelligence, operations and planning staffs at all levels.

Commander Task Force 508 should implement a mission classification for mission generated information (NATO/OOS ____) and all classified mission information should be classified under this marking.

NATO should actively encourage nations providing information and intelligence to missions to classify it using the mission designator where possible, giving the mission commander greater authority and flexibility to share the information within the mission area.

### 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.

# Distribution

**Action**:

COS HQ SACT

COS SHAPE

COS JFC Lisbon

**Information**:

IMS

NATO Office of Security

HQ SACT CAPDEV

HQ SACT AOS

SHAPE FOR

SHAPE OPI-INT-COI

Mar Cmd HQ Northwood COS

Mar Cmd HQ Northwood DCOS OPS

Mar Cmd HQ Northwood NSC

Mar Cmd HQ Naples

SNMG1

SNMG2

CJOS COE Norfolk

NMIOTC, Chania Greece

CIMIC Fusion Centre, Norfolk

JWC

JFTC

SHAPE FOR RER

HQ SACT Deployable Forces IPT

SHAPE FOR RER FSL

SHAPE FOR RER FSL Lessons Learned

SACTREPEUR

HQ SACT DCOS SPP

HQ SACT ACOS CAP REQ

HQ SACT CAPDEV PPM LLI

National Military Representatives to SACEUR

National Liaison Representatives to SACT

NSO

C2COE

COMFRMARFOR

COMITMARFOR

COMNLMARFOR

COMSPMARFOR

COMUKMARFOR

CINCGERFLT

CINCTURNAV

DANFLEET

STRIKEFORNATO

COM US Naval Forces Europe-Africa

COM US Naval Forces Central Command

INTERPOL

UKMTO

CMF HQ, Bahrain

EU MIL HQ, Brussels

EU NAVFOR HQ, Northwood

# Contents

**TF 508 Manoeuvres at Speed**[1]

[1] Photo courtesy of Maritime Command Northwood Public Affairs

# 1
# Introduction

## *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.

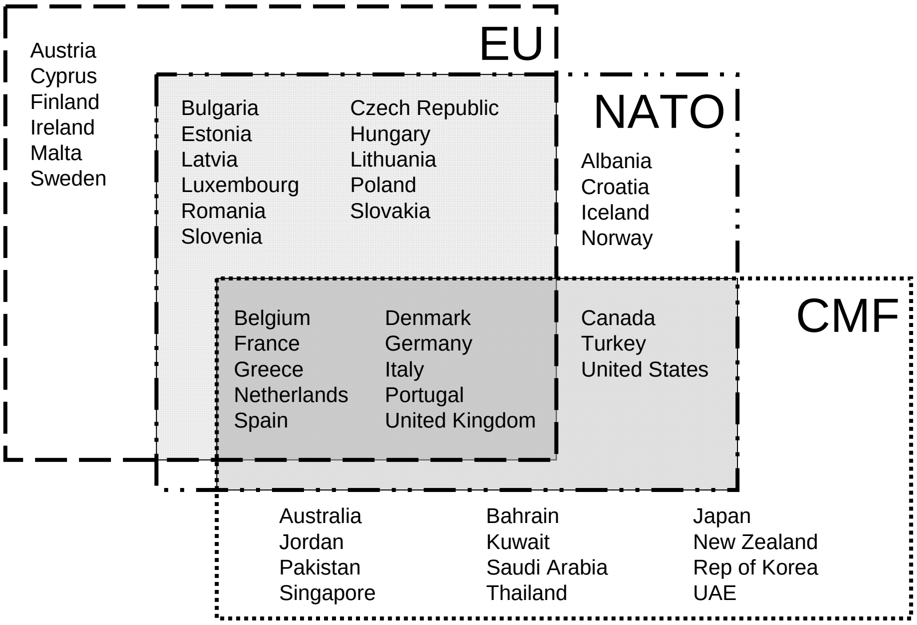


**Figure 1: Venn Diagram showing N-E-C Group membership commonality**

# 2
# Commander's Information Exchange Requirements

## *INTRODUCTION*

15. There is presently no document, or even set of documents, that articulates the full set of Information Exchange Requirements (IER) for OOS. Such a shortcoming would be significant for any military operation, but it is made even more significant for OOS by the complexity of external relationships in the CP environment. The OOS commanders' IERs should be published as soon as practical. Parallel to doing this, improvements to Bi-SC policy and procedures could help staffs articulate IERs more accurately and be more aware of their value to NATO operations.

## *DISCUSSION*

16. The necessity for maritime mission commanders to define their information exchange requirements is prescribed in MC 0195/8 (Reference C), and further articulated in Volume I of the two Strategic Commands' (Bi-SC) Directive 80-3 (Reference D). As stated in the directive, IER lists should include requirements and capabilities, as well as associated methodologies and guidelines.

17. The rationale for identifying IERs is rather straightforward, but the importance becomes amplified in a complex environment such as CP. As stated in the opening paragraph of Bi-SC Directive 80-3:

> *"Commanders are facing a formidable command and control challenge that results from the variety and dispersion of forces assigned. … A cohesive, integrated, operational information exchange structure is a fundamental prerequisite for effective employment of these Forces."*

18. As described in Bi-SC Directive 80-3, the concept of listing IERs is part of a larger concept called the Bi-SC Operational Information Exchange System encompassing orders, reports, coordination, and means used to convey information. Operationally, the concept should serve as a point of reference for those responsible for collecting and disseminating the information, those responsible for providing the capabilities, and the key leaders responsible for providing oversight and direction. Unfortunately, observations by JALLC project teams for two different analysis projects[2], as well as a significant number of interviews, suggests that the guidance for defining IERs is lacking in two respects:

a. In the first place, it does not provide a format. Without a template or any examples, the format—and more importantly, the details that need to be included in that format—is left to the discretion of commanders and operational planners. Accordingly, one operational planner might state little more than the fact that a requirement exists for military forces to exchange information with merchant mariners, whereas another planner might define the same requirement by giving much better clarity with regard to details of the requirement (e.g. what information, how often, how quickly, by what means, etc.).

b. Secondly, the guidance falls quite short in describing to commanders and operational planners what purposes IER lists could or should serve. It places

[2] This project and the JALLC Report "Sharing, Dissemination, and Release of Information in [the International Security Assistance Force] ISAF", Reference E

significant emphasis on using the list to configure the communications architecture, but other purposes are not mentioned. Indeed IER lists are an important tool for communicating guidance to technicians on the establishment and configuration of the communications infrastructure for an operation, but the lists can also contribute to other needs. For example, they can aid in maintaining staff battle rhythm; they can serve as a quasi-checklist to help staff ensure that all exchange requirements are being met; they can help ensure staffs are properly organized and trained; and, they can be used by policy makers, legal staffs, and planners to ensure the proper frameworks are in place.

19. Bi-SC Directive 80-3 includes a list of IERs that are common to most military operations. Historically, such a list might have represented the vast majority of requirements. In most of the recent NATO operations[3], however, the common list of IERs has fallen short of the full set of exchange requirements. Two examples predating OOS illustrate this observation:

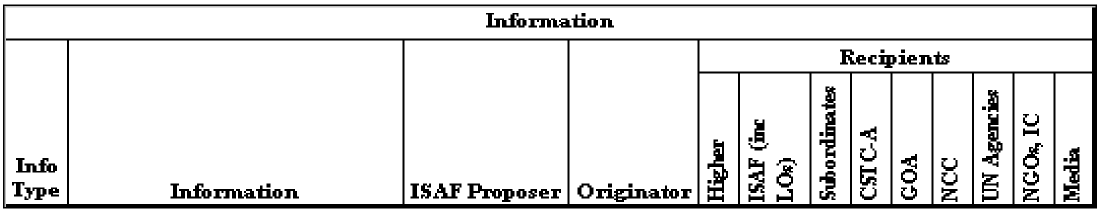
a. In Afghanistan, the Commander of the International Security Assistance Force (COMISAF) faces the necessity to share classified operations plans and daily operations orders with Afghan National Security Forces, and to share classified reconstruction plans with a vast number of Afghanistan government officials and other external entities (e.g. NGOs). Providing the capability for COMISAF and his forces to meet those requirements has gone well beyond the more traditional challenges of exchanging common military information with subordinate forces and higher headquarters.

b. During NATO's assistance to Pakistan following the 2005 earthquake, extensive exchanges of information were required with entities such as other military forces, government organizations and NGOs, local government entities, and civilians. The list of IERs fell short of the full scope of information that needed to be exchanged.

20. With regard to the ISAF example, a previous JALLC report (Reference E) credited the Allied Rapid Reaction Corps (ARRC)[4] with demonstrating the greater value of IER lists, as well as with developing a useful format that could be used for other NATO operations. Examination of COMISAF IX's list of IERs is relevant to the present study as this list is reported to have been used as a basis for significant changes to NATO policy, doctrine, and procedures.

21. The list developed by ARRC provided relevant details of each exchange requirement. Specifying those details led to a formatted list articulating approximately 100 specific types of information and reports to be exchanged by HQ ISAF with lower and higher echelons of command, and specific external entities (e.g., the government of Afghanistan, United Nations agencies, non-governmental organizations, and the media). The list of IERs was described in two tables with headers as shown below:

Table 1: Identification of IERs



| Information | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Recipients | | | | | | | | | |
| Info Type | Information | ISAF Proposer | Originator | Higher | ISAF (inc LOs) | Subordinates | CSTC-A | GOA | NCC | UN Agencies | NGOs, IC | Media |

[3] Prior to this analysis project for OOS, JALLC project teams have examined IERs for NATO operations in Bosnia and Herzegovina, Pakistan, Kosovo, and Afghanistan.

[4] Following extensive preparation, ARRC deployed to Afghanistan in 2006 to lead ISAF IX.

Table 2: Nature of IER Content

| Nature of Information | | | | | | | |
|---|---|---|---|---|---|---|---|
| Criticality | | | Timing | | Transmission | | |
| MCI | Classification | Precedence | Frequency | Time Sensitivity | Preferred Format | Alternative Format | Approx Size |

22. The value of articulating IERs to that level of detail, or even further, seems especially relevant in a complex information environment such as CP in which there are many types of entities, and where sharing the right information with those entities at the right time and in the right way offers so much synergy to the overall set of international objectives. As noted elsewhere in this report, there are legal and policy issues in some instances, similar in some respects to challenges experienced by COMISAF.

23. For the military forces, there are also differences in command structures that add to the complexity. So, in addition to knowing what information needs to be exchanged with each entity, it can be important to specify precisely where within the entity the exchange needs to take place. Figure 2, reportedly developed by a staff officer situated in Djibouti, illustrates that many different entities are involved at different command levels of the forces in theatre. The transmission delays (and potential for loss) implicit in information moving up, down or sideways in these structures underlines the need to correctly target information exchanges.

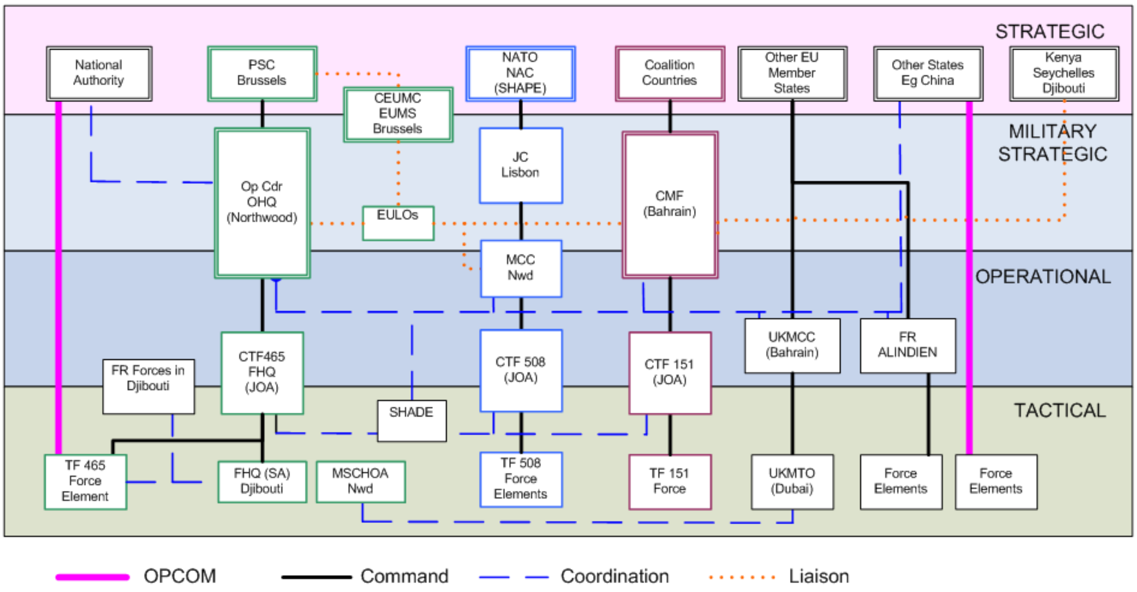


Figure 2: Notional Depiction of Organizational Relationships

24. To support the effort for OOS, staff officers should use the table of common IERs shown in Table 2-1 of MC 0195/8 (Reference C), as well as the standard requirements listed in Bi-SC Directive 80-3, as a baseline. With that baseline in place, IERs specific to OOS need to be added to complete the list. To assist in that effort, and in partial response to AO-1 of this report to "*identify what information is and should be shared, as well as how, between NATO and external entities*", the Project team has compiled a partial list of external IERs specific to OOS. The JALLC list (Annex C) was developed by interviewing people at all levels of command involved with OOS, as well as others

outside the OOS chain of command (e.g. other military forces, merchant mariners, and external organizations), and is offered for consideration[5].

## *CONCLUSIONS*

25. In accordance with the intent of Bi-SC Reporting Directive 80-3, a clear list of the Commanders IERs for OOS would provide clarity and facilitate better communication with external entities. However, the lack of clarity in Bi-SC Reporting Directive 80-3 leaves it to planners to draw their own conclusions with regard to format, intent, and potential value to operations.

26. The format used by HQ ISAF at Annex Q to COMISAF OPLAN 38302 (Reference F) appears to be a pragmatic implementation of an IER list.

## *RECOMMENDATIONS*

27. COM MCC Northwood should articulate the Commander's IERs for OOS with the aid of the suggestions provided in Annex C to this report and the format used in Reference F.

28. SHAPE and HQ SACT should collaborate to expand the direction in Bi-SC Reporting Directive 80-3 for defining IERs, including recommended format and the various purposes that a consolidated list can serve.

[5] During the final review of this report, the project team had the opportunity to review Commander JFC Naples's Operation Plan (OPLAN) 40309 for NATO Support to the Arms Embargo Against Libya. The "Liaison, Coordination and Engagement Matrix" (Annex B, Appendix 3) provides a clear description of the external engagements anticipated for the conduct of operations and the appropriate level of command for each engagement to occur.

# 3
# Sharing Situational Awareness Information and Operating Pictures

## *INTRODUCTION*

29. 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*

30. 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.

31. 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.

32. 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 report[6] to the NATO Secretary

[6] "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*

33. 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 organizations[7].

34. 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*

35. 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. Lack of Unity of Effort and Awareness of Capabilities

c. Multiple Information Networks

d. Multiple Sources of Information and Limited Capacity for Correlation of Information

e. Tools for Correlation

f. Different Communities of Interest

### Geography

36. 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

[7] 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).

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.

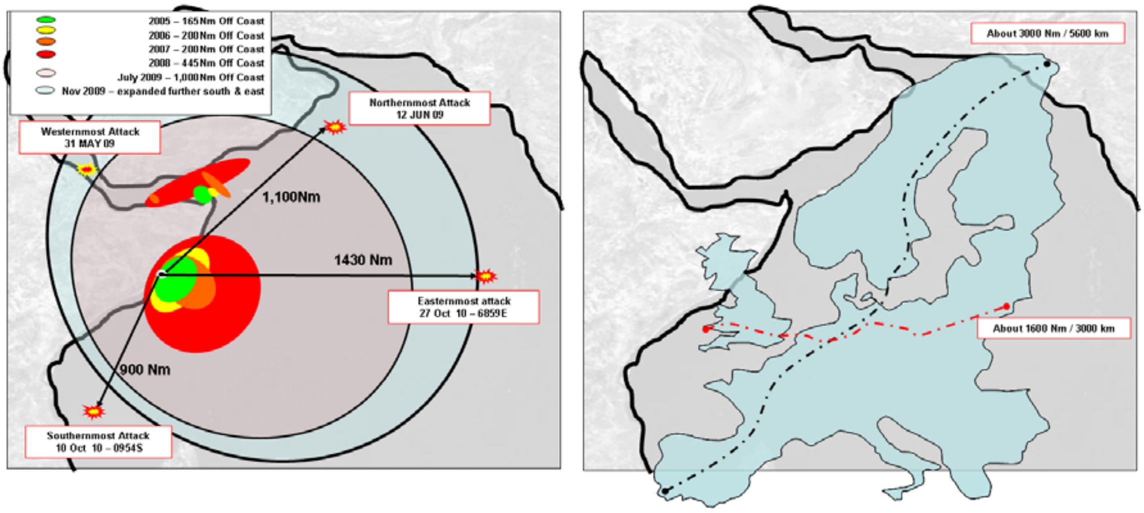

🟩 2005 – 165Nm Off Coast
🟨 2006 – 200Nm Off Coast
🟧 2007 – 200Nm Off Coast
🟥 2008 – 445Nm Off Coast
○ July 2009 – 1,000Nm Off Coast
○ Nov 2009 – expanded further south & east
Northernmost Attack 12 JUN 09
Westernmost Attack 31 MAY 09
1,100Nm
1430 Nm
Easternmost attack 27 Oct 10 – 6859E
900 Nm
Southernmost Attack 10 Oct 10 – 0954S
About 3000 Nm / 5600 km
About 1600 Nm / 3000 km

**Figure 3: Map of CP danger areas**

37. 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.

### Lack of Unity of Effort and Awareness of Capabilities

38. Military leaders are well aware of the importance of unity of command and effort. The number and variety of nations deploying forces to the region renders unity of command functionally impossible and leaders involved in CP operations have therefore stressed the need for unity of effort. As noted by one senior leader at Mar Cmd HQ Northwood; "*Unity of command is not possible in CP, so you hope for unity of effort. This means common understanding of situational awareness, OPS, and Intelligence, especially for the [N-E-C group]*".

39. The need to be aware of capabilities and intentions was expressed by many of those interviewed to be one of the more significant challenges of CP operations. In a cooperative effort among forces without unity of command, knowledge of adjacent forces' capabilities and limitations is essential to unity of effort. They noted that not having knowledge of capabilities of other CP forces present in the area can result, and has resulted, in lost opportunities and inefficient use of critical resources. In one tactical operation, two nearby forces' not being aware of each others' capabilities and intentions nearly resulted in a fratricide incident between special operations units.

40. In order to rectify these gaps there is a daily chat between the N-E-C group commanders, cited by Commander TF 508 as an essential tool in coordinating efforts. An effort has been started to build a capability matrix in OOS that could be shared with other TF commanders, recording the known capabilities and intentions for forces in the area of operation.

41. The challenges in achieving transparency might be largely political, but taking pragmatic steps toward sharing relevant information is essential. Clearly, the Capability Matrix that Commander TF 508 has begun constructing is a pragmatic step toward common situational awareness of CP forces. Articulating information about capabilities and intentions in the commander's list of IERs would be a logical part of that endeavour and would help in setting a good example for other CP forces.

**Multiple Information Networks**

42. Presently, there are three main coalition forces and several independent deployers conducting CP operations in the Gulf of Aden and off the Horn of Africa. Each of the main forces (i.e. the N-E-C group) and independent deployers has brought its own Communication and Information Systems (CIS) to the region to support requirements for command and control, situational awareness, logistics coordination, administration, etc. A common information network for sharing situational awareness information would go far in supporting establishment of common understanding of the situation in the region.

43. Ideally, if a common situational awareness capability is possible in the immediate future, the solution should be found within existing systems:

a. NATO uses the NATO Secret (NS) WAN.

b. CMF uses the "Combined Enterprise Regional Information Exchange System" for Combined Maritime Forces Central Command (CENTRIXS CMFC).

c. The EU has an EU Secret WAN; at time of writing it does not connect all EU military forces and there are non-EU forces contributing to Operation ATALANTA. ATALANTA therefore uses the EU Secret WAN when possible, otherwise using national systems or an unclassified EU internet-based system known as MERCURY.

44. In addition, most nations participating in one of the N-E-C groups have access to one or both of the other networks, mainly because nations are participating in more than one operation. According to data compiled by TF 508 in November 2010, CENTRIXS CMFC is the most commonly shared CIS:

a. 52% of all N-E-C group forces reported operational access to NS WAN.

b. 92% of all N-E-C group forces reported operational access to CENTRIXS CMFC.

c. 88% of all N-E-C group forces reported operational access to MERCURY (Unclassified only).

45. Consequently, in the absence of a common network for all forces, CENTRIXS CMFC appears to be the most pragmatic solution to fill the current gap for a common situational awareness platform.

46. Access to CENTRIXS CMFC is granted by the United States using bilateral agreements. For ships, the provision to use those agreements is relatively straightforward because ships remain under the operational command of their nations even when participating in NATO or EU operations such as OOS and ATALANTA. For static NATO HQs, the application of bilateral agreements is not so straightforward. Mar Cmd HQ Northwood has access to CENTRIXS CMFC through its host nation United Kingdom, but with the strict provision that non-CMF members of the HQ are never allowed to use it—including viewing the monitors.

47. SHAPE raised a mission critical Crisis Response Operation (CRO) Urgent Requirement (CUR) to provide a NATO point of presence for CENTRIXS. In 2010, the NATO Office of Resources (NOR) judged that it would be more appropriate for this CUR to be satisfied by the Secure Maritime Releasable CIS (SEMARCIS) Capability

Package. Furthermore, SHAPE's request for full NATO access to CENTRIXS by letter to US Naval Forces Central Command was not granted on the grounds that CMF coalition's primary mission of Counter-Terrorism could be diluted by a purely CP-related inclusion of NATO (Reference J). This position was reiterated at the Maritime Multinational IP Interoperability Conference[8] in February 2011 which concluded that the approach to exchange information between NATO and CTF 151 by NATO receiving access to the CENTRIXS CMFC enclave is not viable, US Naval Forces Central Command being unable to grant access.

48. Therefore, a pragmatic short-term approach to fulfilling the pressing requirement for a common SA network using CENTRIXS CMFC would be for NATO nations to negotiate bilateral agreements, using the existing process used by the United States to grant access to nations.

49. As recognized by the NOR, the longer term solution is SEMARCIS. SHAPE’s SEMARCIS statement of operational requirement (SOR) was endorsed by NC3B in 2009, and responsibility for which subsequently passed to HQ SACT for capability package implementation. This SOR would potentially meet the requirement for a common network for NATO and any non-NATO nation or TF willing to accept the capability and meet NATO’s security requirements.

### Multiple Sources of Information and Limited Capacity for Information Correlation

50. 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:

51. 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 UKMTO[9] or the NATO Shipping Centre as agreed or deemed necessary, and voluntary sighting reports when they see something significant[10]. Similarly, different Intelligence sources often provide slightly different information about pirate camps or mother-ship locations.

52. 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 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.

[8] As reported in the *Status Report on CENTRIXS (CUR 267)* proceedings from that conference released by the SHAPE CIS Director on 08 June 2011.

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

[10] 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.

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.

53. 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.

54. 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.

55. 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).

56. 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)[11] which meets weekly via secure video-teleconference.

57. 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.

### Tools for Correlation

58. Speedily and accurately correlating data requires appropriate tools. Such tools are currently not available. Mar Cmd HQ Naples demonstrated a set of two tools with which they have been experimenting that could help to conduct correlation, not only for OOS but for other entities involved in CP operations. As explained to the project team, Mar Cmd HQ Naples is conducting a proof of concept of these tools in their role as a designated participant in NATO Maritime Situational Awareness (MSA) concept development and demonstration (Reference G).

59. One of the tools in the set being examined by Mar Cmd HQ Naples is the Maritime Safety and Security Information System (MSSIS). This system has been developed by the US Department of Transportation's Volpe Centre in support of the US government's programme for maritime domain awareness and information integration. The United States has made MSSIS available to nations and other entities around the world; the system is low cost, and its architecture is open[12]. The MSSIS initiative has proven to be highly successful, with MSSIS emerging as an international standard for aggregating and displaying AIS data. In fact, the NATO MSA Concept Development Plan (Reference M) refers to MSSIS as the preferred software package to aggregate AIS feeds from various sources into a single AIS data stream. MSSIS is operational today in 63 nations around the world and is provided free to NATO by the United States.

60. The other tool in the set being proven by Mar Cmd HQ Naples, under the sponsorship of SACT, is actually a suite of applications comprising the Baseline for Rapid Iterative Transformational Experimentation (BRITE). As suggested by its title, BRITE is an experimental platform developed by NATO, and it is highly network enabled. It is designed to interface with MSSIS and reference databases (such as Lloyd’s database for shipping), automatically flagging anomalies and providing expert tools for resolving them.

61. Based on interviews and research, the project team believes that an ideal solution for CP operations would be the combined fusion centre previously discussed, equipped with both MSSIS and BRITE. MSSIS would aggregate AIS data and feed it

[11] 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.

[12] According to public sources, MSSIS can be implemented for approximately 2000 Euro (or 3000 USD). The term “open architecture” is assigned to architectures which are not proprietary.

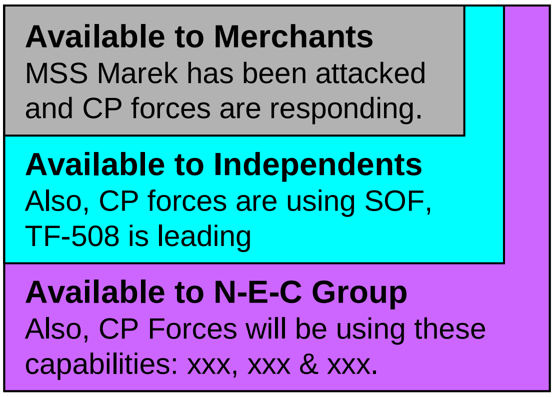
to BRITE[13]. BRITE would merge AIS data with other data, both unclassified and classified, and identify anomalies. Personnel assigned to the combined fusion centre would work together in resolving the anomalies, providing commanders and decision makers with common, accurate, non-conflicting information in a timely fashion. Architecturally, the tools might be configured as described in the NATO MSA Concept Development Plan.

### Different Communities of Interest

62. 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).

63. 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.



**Available to Merchants**
MSS Marek has been attacked and CP forces are responding.

**Available to Independents**
Also, CP forces are using SOF, TF-508 is leading

**Available to N-E-C Group**
Also, CP Forces will be using these capabilities: xxx, xxx & xxx.

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

## *CONCLUSIONS*

64. 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.

[13] HQ SACT reports that around 2016/2018, MSSIS and BRITE should merge into one product currently referred to as the TRITON project.

b. No common network being available to all CP forces; CENTRIXS CMFC is operationally available to more CP forces in theatre than any other CIS capability.

c. The lack of formal tools for tracking correlation; trials by Mar Cmd HQ Naples suggest that BRITE, used in conjunction with MSSIS as a principle source of raw information about white shipping, would be an excellent tool for correlating and sharing a CP operating picture (unclassified and/or classified) with all entities involved in CP operations and the shipping industry.

d. No current deployable capability for sharing classified information with non-NATO entities in OOS.

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

## *RECOMMENDATIONS*

66. In the near term, nations should be encouraged to pursue bilateral agreements with the United States for access to CENTRIXS CMFC.

67. HQ SACT should accelerate, where possible, the implementation of BRITE as a standard MCCIS application, and in collaboration with SHAPE and JFC Lisbon, consider offering BRITE to CMF and EU.

68. 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.

69. 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 SEMARCIS.

70. Mar Cmd HQ Northwood should sustain and promote Commander TF 508’s capability matrix initiative.

# 4
# Classification and Release

## *INTRODUCTION*

71. In any discussion of information sharing within a military organization, questions of classification, sensitivity, and releasability invariably arise. We understand the need to share within our own force structure and command, but sharing outside of that command is difficult. In CP operations we share a common goal with many other forces and that mutual goal is furthered by the sharing of information not just with the N-E-C group, but with independent deployers as well. Among this latter group are nations with whom we do not share classified data routinely or, in some cases at all.

72. This chapter examines elements of NATO security policy that deal with the ability of a commander in theatre to release information to forces on a similar mission, arguing that the tools to do so are on hand and that precedent exists for their use. These tools would benefit from the ability to release series or groups of documents, including anticipated future documents. In addition, we propose that the creation of a mission classification would speed up the sharing of information by making it clear what information is releasable.

## *IMPLEMENTATION OF NATO SECURITY POLICY CHANGES THAT CAN SUPPORT SHARING*

73. NATO has a myriad of documents and guidelines with respect to the security of information, collectively forming the NATO Security Policy and headed by the overarching document Security within the North Atlantic Treaty Organization (Reference N) and its eight corrigenda (Reference O) to date. The documents relevant to the exchange of information with external actors include the Directive on the Security of Information (Reference P) and the Supporting Document on Information and Intelligence Sharing with non-NATO Entities (Reference Q). The Bi-SC Handbook for Information and Intelligence Sharing with Non-NATO Entities (Reference R) was written to implement the Supporting Document at a user level.

74. The original Reference N in 2002 understood the need to share classified information outside of NATO within the constraints imposed by the need to protect and safeguard information. However, it maintained the authority to release information at the committee level at NATO headquarters. It has since been updated and amended, most recently in 2010, and often these amendments have been aimed at improving NATO's ability to share information. Corrigendum 3 (Reference S) in 2006 widened the scope and authority for release of NATO classified information. Of particular note, it recognized classified information related to a NATO military operation and delegated release authorities for such information to Supreme Allied Commander Europe (SACEUR) and Deputy SACEUR and even to the mission commander under defined criteria. It also allowed for the release of a “*general category of information*”, allowing one release procedure to apply to a group of related documents/information including documents yet to be created.

75. While these changes represented a significant step forward in the ability to share information, they did not fully meet the needs of operational commanders[14]. The supporting document and handbook were developed to better address ISAF’s

[14] As reported in discussions with staff involved in the ongoing drafting of NATO’s security policies and guidance.

requirements to share information more easily with non-NATO entities. While the impetus was from ISAF, these two documents were written to apply to numerous operational and training situations. These documents contain several specific provisions which can aid OOS commanders in the sharing of information but which have not been implemented.

76. 46% of those interviewed who deal with the release of classified information indicated problems in releasing information and, specifically, in the timeliness of release. The recently enacted provisions to facilitate that release, contained within the documents on Information and Intelligence Sharing, were unused and unknown. These provisions include the delegation of release authority for certain information to in-theatre leaders (Commander TF 508), the authority for commanders to conclude security assurances, and the use of a mission classification. It appears that the principal reason these provisions are not in use is that OOS staff, at operational, mission, and theatre level, are unaware of the authority they have or the value of using the provisions. It is the JALLC's contention that the application of these policy amendments and new procedures will greatly alleviate problems of sharing.

### Delegated Authority to Release Information

77. One of the most significant attributes of the documents on information and intelligence sharing is the delegation of release authority significantly lower in the chain of command and, in the case of OOS, to individuals in theatre. Yet, the project team conducted over 80 interviews with CP staff officers at all levels of the command structure of OOS and in those interviews we found only one person who knew of the supporting document and handbook and understood what they allowed. Authorities designated as release authorities (Delegated Authorities or DAs) under these documents were not aware of the authority they held.

### Security Assurances

78. The establishment of a security agreement or a security assurance with the receiving entity is a key requirement of sharing information under NATO Security Policy[15] and its subordinate documentation. With a security agreement, the entity has been certified by the NATO Office of Security (NOS) as meeting specific criteria to ensure the continued protection of NATO information. Under the supporting document and handbook a security assurance can be established between an empowered DA and a non-NATO entity to allow the sharing of NATO information for the purposes of the mission. These assurances are more limited in scope and duration, not having been scrutinized by the NOS.

79. The EU forces of Operation ATALANTA are covered by a security agreement[16]; however, there is no known agreement with CMF as a whole. NATO has security agreements with 22 of 25 CMF participating nations and CMF is led by the United States, a NATO member. As such, in consideration of the agreements that would have been signed between the United states and CMF member nations, the United States would likely fulfil the role of a NATO sponsor[17] guaranteeing the ongoing safekeeping of information released to CMF and its members. However, NATO should seek to establish an assurance with any non-NATO entity that has not already signed a NATO security agreement or assurance.

[15] See Reference N

[16] EU Operation ATALANTA falls under the EU council, with which NATO has a security agreement.

[17] Reference P, appendix 2, paragraph 4c.

80. The project team found many officers stating the need to share mission originated intelligence information with independent deployers, not part of NATO, EU, or CMF, but thought it impossible. A security assurance signed with these nations' mission would legally enable the release of appropriate classified information to them. While there are limitations imposed on the releasing DA related to balancing the risk and need to know, it is assessed that if these authorities and policies were understood, the needed reciprocal information exchange could be established for the benefit of the mission.

**Mission Classification**

81. OOS does not use a mission classification. Appendix 6 of the Directive on the Security of Information authorizes and directs Combined Joint Task Forces (CJTF) to identify mission generated information as NATO/CJTF. This appendix is cited and used by JFC HQ Lisbon as a basis for guidance to share information in OOS, (Reference T). However this appendix is about non-NATO nations participating in a NATO-led CJTF or similar formation.[18] This authority is very useful in a mission such as ISAF, which is NATO-led, in that it allows information to be classified such that it is accessible to all members of the CJTF, regardless of their NATO membership. OOS has been established with the potential to be a NATO-led CJTF (annex GG to SACEUR's OPLAN, Reference U); though to date no non-NATO nations have made contributions to OOS directly.

82. Whether the "CJTF or similar formation" is considered to be OOS/TF 508, in which case it does not contain non-NATO Entities (NNE), or the "similar formation" to be the amassed CP forces coordinating their efforts, in which case it is clearly not "NATO-led", a mission classification is not required. However, it is permitted and implementation of such a mission classification would offer significant benefits, allowing for a clear differentiation between NATO classified material and mission material for which there is generally a need to share with "like minded missions". This classification allows SACEUR, a Mission Commander, or a DA to release information marked as generated in or as releasable to the operation (NATO ___, releasable to CJTF) to non-NATO elements participating in the CJTF, to their nations and even *to "individuals or organizations beyond the CJTF"*[19].

83. NATO information not suitable for release to the NNE in the mission would not be marked with the mission classification, and hence would require more stringent procedures prior to its release. As such, use of this classification would also permit NATO Nations contributing information to OOS to decide in advance which material it was willing to see passed on and which it genuinely wishes retained within NATO. Its use would also reduce instances where information is inappropriately shared. For example, the project team found numerous examples where people were under the impression that, as the originator, they could release mission related NATO classified information to CMF or EU by labelling the document "NATO ___/releasable to ___".

[18] This appendix if fully titled "Security Arrangements for the Release and Protection of NATO Classified Information to a NATO-led Combined Joint Task Force (CJTF) or Similar Formation and the Exchange and Protection of Classified Information with non-NATO Nations/Organizations Participating in a NATO-led CJTF or Similar Formation".

[19] Reference P, para 12c.

## *OTHER FACTORS THAT IMPOSE LIMITS ON SHARING*

### Generic Release Authority

84. The project team has reviewed the shortfalls in NATO's ability to share information, and determined that most objections can be alleviated by the implementation of provisions in the Supporting Document (Reference Q). However, there is one remaining problem that should be addressed. The Supporting Document Reference Q does not allow for "generic release" which the Bi-SC Handbook (Reference R) defines as "*general documents such as [Standardization Agreements] and Manuals*". In most of the release tables, release authorities must detail specific documents or parts of documents that have been authorized for release. The Directive on the Security of Information (Reference P, however, allows for "a request for generic release", which it defines as "*specific subject areas, defined series of documents, anticipated future documents or series of documents …*"[20], meaning that if (for example) a series of previous Intel Summary was authorized for release then subsequent Intel Summaries in that series could be released under the same authorization.

85. There is a need for DAs to be able to release documents of specific subject areas, defined series of documents and anticipated future documents under the Supporting Document and Handbook. This type of release was authorized under Operation ACTIVE ENDEAVOUR[21] so there is precedent for its use to release OOS data to other CP forces. The bulk of the information to be shared by OOS with other CP forces would fall under this category of release (intelligence summaries and assessments, COP details in particular), which have a very short lifespan.

### Blanket Classification and Over-Classification

86. Throughout OOS, there is strong and frequent guidance to "write for release", a concept included in many NATO policy documents. Considerable effort is made to write intelligence and situation reports for OOS at an unclassified level, allowing them to be shared with all CP forces. Classified information was written to be releasable to EU/CMF whenever possible and shared through CMF's CENTRIXS-CFMC system.

87. There is nonetheless an issue with the use of blanket classifications, especially with intelligence data—namely the application of a classification based on the asset generating the information, rather than the information itself. This is usually, and legitimately, done in order to conceal the presence or capabilities of intelligence collecting assets, but when done instinctively it can lead to simple data possessing an unnecessarily high classification even after any indication of source is removed, resulting in delays in sharing.

88. A significant portion of blanket classification originated from national sources. NATO does not have many intelligence collection assets and therefore relies on member nations to provide their intelligence to NATO; MC 0128/7 Policy for NATO Intelligence (Reference V) provides guidance, which again emphasizes the need to write for release, allowing the intelligence to be given the widest audience necessary to meet NATO's requirements. The clear marking of which data elements are classified would make it easier for CP forces to sanitize data, allowing earlier release of the unclassified elements and, as discussed above, a mission classification would enable Nations to better describe their wishes when classifying data.

[20] Reference P, appendix 2, paragraph 3(a)(v)

[21] Reference W.

## *CONCLUSIONS*

89. Recent changes to NATO Security Policy have not been fully implemented and used within OOS. These changes would seem to address most of the issues expressed by operators in theatre, though their effectiveness cannot be assessed until they are actually used.

90. OOS commanders appear to be unaware of their authority to establish a security assurance with entities involved in the CP effort or their ability to release classification information to these entities once an assurance has been signed.

91. The lack of a mission classification system in OOS limits the ability to differentiate between mission related classified information which should generally be shared with aligned CP forces and NATO specific information that generally does not need to be shared with other CP forces.

92. There is a discrepancy in the definition of the term "generic release" between two NATO Security Policy documents. There is a need for DAs to be able to authorize the release of series documents, including anticipated future documents.

93. There is a need to look at the classification assigned to documents, ensuring that they are assigned the minimum classification truly needed by the content itself, emphasizing the “write for release” principle. This should be emphasized to member nations providing information and intelligence to NATO/OOS.

## *RECOMMENDATIONS*

94. SHAPE and HQ SACT should ensure awareness and provide better training of the Bi-SC Handbook for Information and Intelligence Sharing with Non-NATO Entities. Allied Command Operations (ACO) and Allied Command Transformation (ACT) have provided training[22]; however, training of this type needs to be provided to the intelligence, operations and planning staffs at all levels.

95. Where appropriate, Commander TF 508 should develop security assurances with independent deployers to allow for the timely sharing of information.

96. The NATO Security Committee should examine feedback from OOS with respect to the utility of the Supporting Document and in particular the annex for non-NATO multinational forces, making amendments as required. The inclusion of generic or categorical release of groups of documents should be included in the next revision.

97. Commander JFC Lisbon should implement a mission classification for mission generated information (NATO/OOS ____). All classified mission information should be classified under this marking.

98. NATO should actively encourage nations providing information and intelligence to missions to classify it using the mission designator where possible and as appropriate, giving the mission commander greater authority and flexibility to share the information within the mission area.

[22] ACO and ACT have provided training via the Bi-SC Conferences on Intelligence and Information Sharing with NNEs which have been sponsored by the SHAPE and HQ SACT Security Offices

# 5
# Sharing with Interpol

## *INTRODUCTION*

99. NATO counter-piracy forces will sometimes collect information[23] 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).[24]

100. 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*

101. Interviews with many senior leaders and staff officers responsible for conducting OOS[25] 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.

102. 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.

103. 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.

104. 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.

[23] 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.

[24] 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.

[25] 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*

105. 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.[26]

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.

106. 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 commander[27], and a set of NATO guidelines for handling biometric data[28]. 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*

107. 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

[26] 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.

[27] Security Assurances are discussed in Chapter 4 of this report.

[28] 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.

unique to that country, but Interpol's constitution and core functions accommodate these differences.

108. 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.

109. 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 responsibility[29] 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.

110. 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*

111. 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.

112. 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.

113. 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.

114. 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:

[29] Use of the word “responsibility” is based on national agreements to UNSCR 1950.

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

115. 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*

116. 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.[30]

117. 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 training[31] 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*

118. 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.

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

[31] 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.

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.

## *CONCLUSIONS*

119. 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.

120. 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.[32] 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.

121. 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.

122. 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*

123. 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.

124. 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.

125. 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.

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

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

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

# 6
# Sharing with Merchants

## *INTRODUCTION*

128. 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.

129. 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.

130. 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.

131. 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*

132. 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.

133. 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*

134. 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 indentify pirates at sea, where suspect vessels are located, and how to avoid them.

135. 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.

136. 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 Africa[33] (MSCHOA), UKMTO, The Maritime Liaison Office[34], etc, as well as contact points within the independent deployers' nations.

137. 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.

138. 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*

139. 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. <u>Location of ships</u>: 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. <u>Piracy risk factors</u>: 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).

[33] An office within EU NAVFOR

[34] 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*

140. 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.

141. 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.

142. 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*

143. 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.[35]

144. 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.

145. 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.

[35] 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.

# 7
# Best Practices

146. 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*

147. 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*

148. BMP3 is the third version of the BMP booklet[36] 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 aggressive 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*

149. 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*

150. 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.

[36] 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.

### *COALITION NETWORK – CENTRIXS CMFC*

151. The CMF, including CTF 151, have established a classified coalition network to interconnect all CMF assets. The network, CENTRIXS CMFC, uses virtual private network technologies to provide an acceptable level of assurance against security risks. Certain NATO and EU countries have extended CENTRIXS access to key offices responsible for conducting OOS and ATALANTA, respectively. Although a multi-mission network of this nature is not deemed suitable for meeting NATO command and control requirements[37] and the bilateral approach that has been necessary to extend network access into NATO work spaces has shortcomings[38], the demonstrated concept of interconnecting multiple missions in this fashion is deemed a Best Practice. As recommended in Chapter 3 of this analysis report, this should be considered for a deployable NATO collaboration system.

### *TRI-LATERAL COMMANDERS' DAILY CHAT*

152. The commanders of TF 508, TF 465, and CTF 151 hold a daily discussion. The meetings are brief, normally conducted via network "chat" on CENTRIXS CMFC. They function similarly to the SHADE meetings in that they are tactical-level and non-political. The commanders use the forum to increase and synchronize their overall awareness of the situation in the region, deconflict operations when necessary, seek synergy in working together toward common objectives, and share advice. The daily chats help to enable the commanders to optimize their collective efforts.

### *TRILATERAL JOINT COORDINATION MANAGEMENT BOARD*

153. The trilateral JCMB is an informal body comprising senior Operations and Intelligence representatives of the N-E-C group. Its purpose is to review the Intelligence requirements of each member and, where agreed, combine those requirements into a single prioritized list. Consequently, Intelligence collection can be optimized. The JCMB meets as often as required, but typically two times each week. The forum for each meeting is a combination of physical presence and encrypted video teleconference.

### *MAR CMD HQ NORTHWOOD ENGAGEMENT TEAM*

154. The Mar Cmd HQ Northwood Engagement Team is chaired by Mar Cmd HQ Northwood Chief of Staff and is comprised of selected staff members representing most of the HQ staff. Its purpose is to focus on forthcoming engagements (e.g., meetings) in order to optimize each outcome. The JALLC team observed it to be a rather simple concept, functioning in most respects as a normal staff meeting. The key differences, though, are that the attendees are carefully chosen, and they come to each meeting with a single focus. The spectrum of engagements range from political to tactical within a time-frame of the immediate future to approximately three months out. Collectively, the team identifies engagement opportunities and examines each with respect to intention and possible secondary purpose(s). The team identifies what, if anything, the Mar Cmd HQ Northwood staff might need to do to optimize the outcome of the meeting, especially with regard to fulfilling the Commanders intentions.

[37] As noted in Chapter 3 of this analysis report, NATO command and control requirements for OOS should continue to be met by NS WAN. Attempting to use a non-NATO system for these requirements would introduce risks to security and unity of command.

[38] These shortcomings, as well as recommendations to mitigate those shortcomings, are addressed in detail in Chapter 3 of this analysis report.

### *PROFESSIONALISM*

155. 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 a 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[39] |
| 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 |

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

| | |
|---|---|
| JCMB | Joint Coordination Management Board |
| 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 |

# Annex B
# Entries to NATO Lessons Learned Database

1. The following *Lessons* will be entered into the JALLC-managed NATO LLDb. Although these are the lessons JALLC considers to meet the requirements for LLDb entry in accordance with the Bi-SC Lessons Learned Directive, they in no way represent the only important findings of this report. Therefore, readers are encouraged to read the main body of this report in its entirety to ensure all findings are fully taken into consideration.

## Lesson 1
## Articulating Information Exchange Requirements

Observation

There is presently no document, or even set of documents, that articulates the full set of information exchange requirements (IER) for Operation Ocean Shield (OOS). Such a shortcoming would be significant for any military operation, but it is made even more significant for OOS by the complexity of external relationships in the counter-piracy (CP) environment.

Discussion

The necessity for maritime mission commanders to define their information exchange requirements is articulated in MC 0195/8, and further prescribed in Volume I of Bi-SC Directive 80-3. As stated in the directive, IER lists should include requirements and capabilities, as well as associated methodologies and guidelines.

As described in Bi-SC Directive 80-3, the concept of listing IERs is part of a larger concept called the Bi-SC Operational Information Exchange System encompassing orders, reports, coordination, and means used to convey information. Operationally, the concept should serve as a point of reference for those responsible for collecting and disseminating the information, those responsible for providing the capabilities, and the key leaders responsible for providing oversight and direction

Unfortunately, observations by JALLC project teams for different analysis projects, as well as a significant number of interviews, suggests that the guidance for defining IERs is lacking in two respects:

a. In the first place, it does not provide a format. Without a template or any examples, the format—and more importantly, the details that need to be included in that format—is left to the discretion of commanders and operational planners. Accordingly, one operational planner might state little more than the fact that a requirement exists for military forces to exchange information with merchant mariners, whereas another planner might define the same requirement by giving much better clarity with regard to details of the requirement (e.g., what information, how often, how quickly, by what means, etc.).

b. Secondly, the guidance falls quite short in describing to commanders and operational planners what purposes IERs lists could or should serve. It places significant emphasis on using the list to configure the communications architecture, but other purposes are not mentioned. Indeed IER lists are an important tool for communicating guidance to technicians to establish and configure the communications infrastructure for an operation, but the lists can also contribute to other needs. For example, they can aid in maintaining staff battle rhythm; they can serve as a quasi-checklist to help staff ensure that all exchange requirements are being met; they can help ensure staffs are properly organized and trained; and, they can be used by policy makers, legal staffs, and planners to ensure the proper frameworks are in place.

Bi-SC Directive 80-3 includes a list of IERs that are common to most military operations. Historically, such a list might have represented the vast majority of requirements. In most of the recent NATO operations, however, the common list of IERs has fallen short of the full set of exchange requirements. Two examples pre-dating OOS illustrate this observation:

a. In Afghanistan, the Commander of the International Security Assistance Force (COMISAF) faces the necessity to share classified operations plans and daily operations orders with Afghan National Security Forces, and to share classified reconstruction plans with a vast number of Afghanistan government officials and other external entities (e.g., non-governmental organizations). Providing the capability for COMISAF and his forces to meet those requirements has gone well beyond the more traditional challenges of exchanging common military information with subordinate forces and higher headquarters.

b. During NATO's assistance to Pakistan following the deadly earthquake in 2005 (including airlift, engineering and medical support) extensive exchanges of information were required with entities such as other military forces, government and non-governmental organizations, local government entities, and civilians. The predicted list of IERs fell short of the full scope of information that needed to be exchanged.

Previously, best practice has been identified in the method used by the Allied Rapid Reaction Corps (ARRC) to specify IERs which demonstrated the greater value of IER lists, as well as with developing a useful format that could be used for other NATO operations. The entire list of IERs was described in two tables containing the following headers:

a. Table 1. Identification of IERs:

- Information Type
- Information Description
- Proposer
- Originator
- Recipients (including higher and lower commands, UN Agencies, NGOs, Media, etc)

b. Table 2. Nature of IER Content

- Criticality: Classification
- Criticality: Precedence
- Timing: Frequency
- Timing Time Sensitivity
- Transmission: Preferred Format
- Transmission: Alternative Format
- Transmission: Approximate Size

The value of articulating IERs to this level of detail, or even further, seems especially relevant in a complex information environment such as CP in which there are many types of entities, and where sharing the right information with those entities at the right time and in the right way offers so much synergy to the overall set of international objectives.

Conclusion

In accordance with the intent of Bi-SC Reporting Directive 80-3, a clear list of the Commanders IERs for OOS would provide clarity and facilitate better communication with external entities. However, the lack of clarity in Bi-SC Reporting Directive 80-3 leaves it to planners to draw their own conclusions with regard to format, intent, and potential value to operations.

Recommendation

SHAPE and HQ SACT should collaborate to expand the direction in Bi-SC Reporting Directive 80-3 for defining IERs, including a recommended format and the various purposes that a consolidated list can serve.

## Lesson 2
## Information and Intelligence Sharing with Non-NATO Entities

Observation

Many staff officers participating in Operation Ocean Shield (OOS) stated the need to share mission originated intelligence information with entities from non-NATO nations, but thought it impossible to do so.

Additionally, 46% of those people interviewed who deal with the release of classified information indicated problems in releasing information and specifically in the timeliness of release.

Discussion

NATO has a myriad of documents and guidelines with respect to the security of information, collectively forming the NATO Security Policy and headed by the Security within the North Atlantic Treaty Organization and its eight corrigenda. The documents relevant to the exchange of information with external actors include the Directive on the Security of Information and the Supporting Document on Information and Intelligence Sharing with non-NATO Entities. The Bi-SC Handbook for Information and Intelligence Sharing with Non-NATO Entities was written to implement the Supporting Document at a user level.

One of the most significant attributes of the documents on information and intelligence sharing is the delegation of release authority significantly lower in the chain of command and, in the case of OOS, to individuals in theatre. The project team conducted over 80 interviews with staff officers at all levels of the command structure of OOS and in those interviews only one person knew of the supporting document and handbook and understood what they allowed. Authorities designated as release authorities (Delegated Authorities) under these documents were not aware of the authority they held.

The establishment of a security agreement or a security assurance with the receiving entity is a key requirement of sharing information under NATO Security Policy and its subordinate documentation. With a security agreement, the entity has been certified by the NATO Office of Security (NOS) as meeting specific criteria to ensure the continued protection of NATO information.

Under the supporting document and as articulated in the Bi-SC Handbook for Information and Intelligence Sharing with Non-NATO Entities, a security assurance can be established between an empowered delegated authority and a non-NATO entity to allow the sharing of NATO information for the purposes of the mission.

Conclusion

The recently enacted provisions in NOS documents to facilitate the release of classified information—as articulated by the Bi-SC Handbook for Information and Intelligence Sharing with Non-NATO Entities—were unused and unknown by OOS staff officers; the changes made would seem to address most of the issues expressed by operators in theatre, though their effectiveness cannot be assessed until they are actually used. In particular, OOS commanders appear to be unaware of their authority to establish a security assurance with entities involved in the counter-piracy effort or their ability to release classification information to these entities once an assurance has been signed.

Recommendation

SHAPE and HQ SACT should ensure awareness and provide better training of the Bi-SC Handbook for Information and Intelligence Sharing with Non-NATO Entities. Although some training has been carried out, training of this type needs to be provided to the intelligence, operations and planning staffs at all levels within the ACO command structure.

## Lesson 3
## Sharing evidence with Interpol

Observation

NATO forces participating in Operation Ocean Shield (OOS) 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.

Discussion

Interviews with many senior leaders and staff officers responsible for conducting OOS revealed strong agreement that NATO counter-piracy forces need to provide information about suspected pirates and pirate activities to Interpol. In fact, there was 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.

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

Interpol is already working with a variety of UN agencies including the Political Office for Somalia, Development Programme, Department for Peacekeeping Operations and Contact Group on Piracy off the Coast of Somalia (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.

The issues with regard to sharing information with Interpol are not 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.

b. Closely related are concerns regarding 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.

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. Other key component of that course of action would be a Security Assurance negotiated between Interpol and an appropriate NATO commander, and a set of NATO guidelines for handling biometric data.

A pragmatic, near-term solution to share information with Interpol has been proposed in the HQ SACT Maritime Situational Awareness, Phase 1 Legal Study Report: put in place mechanisms necessary to encourage, and explicitly permit, NATO counter-piracy forces to share information with Interpol through National Central Bureaus.

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.

The NATO Maritime Interdiction Operational Training Centre (NMIOTC) located at the Souda Bay Naval Base near Chania, Crete, Greece provides training for disrupting illegal activities such as suspected pirate activities, including also 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.

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 training 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.

## Conclusion

NATO has not established a single, overarching legal framework tailored to counter-piracy operations which would establish a single legal framework for sharing information with law enforcement authorities such as Interpol. However, each NATO Nation has an established legal arrangement for cooperating with Interpol —to include sharing information—through their National Central Bureau, and maritime forces assigned to NATO can use their respective national arrangements for sharing information with Interpol.

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.

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.

## Recommendation

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.

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.

# Annex C
# Partial Information Exchange Requirements

## Partial IERs – Operational & Tactical Levels of Command

### Military Information

### From NATO to External Entities

The tables in this annex, which are supplemental to the analysis described in Chapter 2, reflect partial lists of IERs specific to OOS. The IERs have been identified based on interviews with personnel involved in CP operations, including not only personnel assigned to TF 508 and higher headquarters, but also military and civilian personnel external to NATO.

| | | FROM NATO - TO EXTERNAL ENTITIES | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | NMF | | | | | Nations | | | | GOs | | | NGOs | | | Others | | |
| | INFORMATION | CMF | EU (Operation ATALANTA) | Independent Deployers | MPRA Forces | National NCAGS Entites | NATO-Member Law Enforcement Authorities | Regional Authorities | Port Authorities | National Casualty Reporting Centres | Interpol | IMO | United Nations | IMB (Including IMB Piracy Reporting Centre) | NGA WWMS | Jt War Committee & OCIMF | Merchant Mariners | AIS Satellite Contractors | Media |
| Military Information | Ad-hoc analytical assessments of counter-piracy operations | X | X | X | | | | | | | | | | | | | | | |
| | Capabilities, intentions, and national caveats | X | X | X | | | | | | | | | | | | | | | |
| | Availability of MPRA and helicopter assets | X | X | X | X | | | | | | | | | | | | | | |
| | Classified boarding team reports | X | X | | | | | | | | | | | | | | | | |
| | Classified interview reports | X | X | | | | | | | | | | | | | | | | |
| | COP and "battlefield" SA | X | X | X | | | | | | | | | | | | | | | |
| | Counter-Piracy lessons learned | X | X | X | | | | | | | | | | | | | | | |
| | Force Generation plans | X | X | | | | | | | | | | | | | | | | |
| | Fused Intelligence products | X | X | | | | | | | | | | | | | | | | |
| | In-chop & out-chop plans | X | X | X | | | | | | | | | | | | | | | |
| | Information about how counter-piracy forces coordinate with each other | X | X | X | | | | | | | | | | | | | | | |
| | Information about military convoys & escort operations | X | X | X | X | X | | | | | | | | | | | X | | |
| | Information about ongoing counter-piracy operations | X | X | X | X | X | | | | | | | | | | | | | |
| | Information necessary to coordinate port visits | X | X | X | | | | | X | | | | | | | | | | |
| | Counter-piracy information that is available on CENTRIXS | X | | | | | | | | | | | | | | | | | |
| | Counter-piracy information that is available on MERCURY | | X | | | | | | | | | | | | | | | | |
| | Actionable Intelligence | X | X | X | | | | | | | | | | | | | | | |
| | Intelligence Advisories | X | X | | | | | | | | | | | | | | | | |
| | Intelligence assessments | X | X | | | | | | | | | | | | | | | | |
| | Intelligence procedures | X | X | | | | | | | | | | | | | | | | |
| | Intelligence requirements | X | X | | | | | | | | | | | | | | | | |
| | Intelligence Summaries | X | X | | | | | | | | | | | | | | | | |
| | Link-11 data (to forces capable of receiving it) | X | X | | | | | | | | | | | | | | | | |
| | Logistics coordination, especially in employment of RAS & medical assets | X | X | X | | | | | | | | | | | | | | | |
| | Media reports about piracy and counter-piracy activities | | | | | | | | | | | | | | | | | | X |
| | Mission analysis & preliminary planning | X | X | | | | | | | | | | | | | | | | |
| | NATO-designated contacts of interest/vessels of collection interest | X | X | X | X | X | | | | | | | | | | | | | |
| | Operation OCEAN SHIELD Standing OPTASK INTEL | X | X | | | | | | | | | | | | | | | | |
| | Operational Lessons | X | X | X | | | | | | | | | | | | | | | |
| | Planning information | X | X | X | | | | | | | | | | | | | | | |
| | Planning/location about military ships | X | X | X | | X | | | | | | | | | | | | | |
| | Plans and results from key leader engagements | X | X | X | | | | | | | | | | | | | | | |
| | Relevant Casualty Reports | | | | | | | | | X | | | | | | | | | |
| | Rules of Engagement | X | X | X | | | | | | | | | | | | | | | |
| | Situational updates & data (including that provided by Intelligence capabilities) | X | X | X | | | | | | | | | | | | | | | |
| | Tactical Imagery Summaries | X | X | | | | | | | | | | | | | | | | |
| | Unclassified boarding team reports | X | X | X | | | | | | | | | | | | | | | |
| | Unclassified interview reports | X | X | X | | | | | | | | | | | | | | | |
| | Updated IPB (Intelligence Preparation of the Battlefield) Products | X | X | | | | | | | | | | | | | | | | |
| | Weekly Intelligence Summaries | X | X | | | | | | | | | | | | | | | | |
| | What assets are available (including submarines) ? | X | X | X | | | | | | | | | | | | | | | |
| | What capabilities are in the area ? | X | X | X | | | | | | | | | | | | | | | |
| | What military response is planned against pirate activity? | X | X | X | | X | | | | | | | | | | | | | |
| | Where are the helicopter capabilites ? | X | X | X | | | | | | | | | | | | | | | |
| | Where is (are) Role-2 medical capabilities ? | X | X | X | | | | | | | | | | | | | | | |

# Partial IERs - Operational & Tactical Levels of Command

## Other Information and Information about Pirates

## From NATO to External Entities

| | | FROM NATO - TO EXTERNAL ENTITIES | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | NMF | | | | | Nations | | | | GOs | | | NGOs | | | Others | | |
| | INFORMATION | CMF | EU (Operation ATALANTA) | Independent Deployers | MPRA Forces | National NCAGS Entites | NATO-Member Law Enforcement Authorities | Regional Authorities | Port Authorities | National Casualty Reporting Centres | Interpol | IMO | United Nations | IMB (Including IMB Piracy Reporting Centre) | NGA WWMS | Jt War Committee & OCIMF | Merchant Mariners | AIS Satellite Contractors | Media |
| Other Information | Fishing areas and movements of fishing vessels | X | X | X | | | | | | | | | | | | | | | |
| | Extraordinary information about other ships | | | | | | | | | | | | | | | | | | |
| | UN Working Group & Committee reports | | | | | | | | | | | | | | | | | | |
| | Information about ports | X | X | X | | X | | | | | | | | | | | | | |
| | Information about weather and sea conditions | | | | | | | | | | | | | | | | | | |
| | Format Alpha messages | | | | | | | | | | | | | | | | | | |
| | Technical data about hijacked ships | | | | | | | | | | | | | | | | | | |
| | MIEVOM agenda and minutes (and similar events involving merchants) | | | | | | | | | | | | | | | | | | |
| | Vessel position & status reports | | | | | | | | | | | | | | | | | | |
| | Information about BMP3 compliance | X | X | X | | X | | | | | | | | | | | | | |
| | LRIT (Long-Range Idendification and Tracking) data | | | | | | | | | | | | | | | | | | |
| | AIS data | | | | | X | | | | | | | | | | | | | |
| | Information about national means & capabilities to hold & prosecute pirates | X | X | X | | | | | | | | | | | | | | | |
| | Information to help identify foreign merchant ships | | | X | | | | | | | | | | | | | | | |
| Information about Pirates | Alerts about pirate events:<br>- An event has occurred.<br>- Counter-piracy forces are engaged.<br>- Military assessment of event. | | | | | | | X | | | | | | | | X | | | |
| | Any classified information about pirates | X | X | | | X | | | | | | | | | | | | | |
| | Information about mother ships (including suspect mother ships):<br>- Location<br>- Imagery, if available<br>- Crew size, if known | | | X | X | | | | | | | | | | | | | | |
| | Information about pirate activity:<br>- Where are they?<br>- What are they doing?<br>- What capabilities do they have?<br>- What attacks have been conducted, and what was the result?<br>- What is current situation of pirated vessels? | X | X | X | | | | | | | | | | | | | X | | |
| | Intelligence predictions regarding intentions of pirates | | | | | | | | | | | | | | | | X | | |
| | Situational information about pirates & Pirate Action Groups (PAGs):<br>- Where are the pirates?<br>- What direction are they moving, and how fast?<br>- What capabilities do they have? | X | X | X | | | | | | | | | | | | | X | | |
| | Personal information about pirates to support prosecution:<br>- Photographs<br>- Biometrics<br>- Cell phone data<br>- Name & Surname<br>- Year of birth<br>- Country of origin<br>- Country of piracy operation<br>- INTERPOL Reference (ID)<br>- Photo<br>- Phone number(s)<br>- Mother's name | | | | | | X | | | | X | | | | | | | | |
| | NAV WARNINGS and IMB ALERTS about pirates and pirate activity | X | X | | | | | | | | | | | X | X | | X | | |
| | Pirate "de-briefs" following pirate encounters | | | | | X | | | | | | | | | | | | | |
| | Recognized and probable piracy mother-ships, including electronic parametric details of all recognized and probable piracy mother-ships | X | X | X | | | | | | | | | | | | | | | |
| | Counter-piracy feedback from judicial authorities, such as:<br>- Confirmation of evidence<br>- Confirmation that captured pirates are in database<br>- Charactreristics of pirates with regard to importance or level of threat<br>- Information about piracy networks<br>- Information about who is behind piracy (i.e., funding it, overseeing it, etc.)<br>- Verification that captured pirates are (or are not) previously known criminals<br>- Feedback on counter-piracy contributions to prosecution of criminals | | | | | | | | | | | | | | | | | | |
| | Suspicious vessels and/or maritime activity | X | X | X | | | | | | | | | | | | | | | |

# Partial IERs - Operational & Tactical Levels of Command

## Military Information

## To NATO from External Entities

| | | TO NATO - FROM EXTERNAL ENTITIES | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | NMF | | | | | Nations | | | | GOs | | | NGOs | | | Others | | |
| | INFORMATION | CMF | EU (Operation ATALANTA) | Independent Deployers | MPRA Forces | National NCAGS Entites | NATO-Member Law Enforcement Authorities | Regional Authorities | Port Authorities | National Casualty Reporting Centres | Interpol | IMO | United Nations | IMB (Including IMB Piracy Reporting Centre) | NGA WWMS | Jt War Committee & OCIMF | Merchant Mariners | AIS Satellite Contractors | Media |
| Military Information | Ad-hoc analytical assessments of counter-piracy operations | X | X | X | | | | | | | | | | | | | | | |
| | Capabilities, intentions, and national caveats | X | X | X | | | | | | | | | | | | | | | |
| | Availability of MPRA and helicopter assets | X | X | X | X | | | | | | | | | | | | | | |
| | Classified boarding team reports | X | X | | | | | | | | | | | | | | | | |
| | Classified interview reports | X | X | | | | | | | | | | | | | | | | |
| | COP and "battlefield" SA | X | X | X | | X | | | | | | | | | | | | | |
| | Counter-Piracy lessons learned | X | X | X | | | | | | | | | | | | | | | |
| | Force Generation plans | X | X | | | | | | | | | | | | | | | | |
| | Fused Intelligence products | X | X | | | | | | | | | | | | | | | | |
| | In-chop & out-chop plans | X | X | X | | | | | | | | | | | | | | | |
| | Information about how counter-piracy forces coordinate with each other | X | X | X | | | | | | | | | | | | | | | |
| | Information about military convoys & escort operations | X | X | X | | X | | | | | | | | | | | | | |
| | Information about ongoing counter-piracy operations | X | X | X | X | X | | | | | | | | | | | | | |
| | Information necessary to coordinate port visits | X | X | X | | | | | X | | | | | | | | | | |
| | Counter-piracy information that is available on CENTRIXS | X | | | | | | | | | | | | | | | | | |
| | Counter-piracy information that is available on MERCURY | | X | | | | | | | | | | | | | | | | |
| | Actionable Intelligence | X | X | X | | | | | | | | | | | | | | | |
| | Intelligence Advisories | X | X | | | | | | | | | | | | | | | | |
| | Intelligence assessments | X | X | | | | | | | | | | | | | | | | |
| | Intelligence procedures | X | X | | | | | | | | | | | | | | | | |
| | Intelligence requirements | X | X | X | | | | | | | | | | | | | | | |
| | Intelligence Summaries | X | X | | | | | | | | | | | | | | | | |
| | Link-11 data (to forces capable of receiving it) | X | X | | | | | | | | | | | | | | | | |
| | Logistics coordination, especially in employment of RAS & medical assets | X | X | X | | | | | | | | | | | | | | | |
| | Media reports about piracy and counter-piracy activities | | | | | | | | | | | | | | | | | | X |
| | Mission analysis & preliminary planning | X | X | | | | | | | | | | | | | | | | |
| | NATO-designated contacts of interest/vessels of collection interest | | | | | | | | | | | | | | | | | | |
| | Operation OCEAN SHIELD Standing OPTASK INTEL | | | | | | | | | | | | | | | | | | |
| | Operational Lessons | X | X | X | | | | | | | | | | | | | | | |
| | Planning information | X | X | X | | | | | | | | | | | | | | | |
| | Planning/location about military ships | X | X | X | | | | | | | | | | | | | | | |
| | Plans and results from key leader engagements | X | X | X | | | | | | | | | | | | | | | |
| | Relevant Casualty Reports | | | | | | | | | | | | | | | | | | |
| | Rules of Engagement | X | X | X | X | X | | | | | | | | | | | | | |
| | Situational updates & data (including that provided by Intelligence capabilities) | X | X | X | | | | | | | | | | | | | | | |
| | Tactical Imagery Summaries | X | X | | X | | | | | | | | | | | | | | |
| | Unclassified boarding team reports | X | X | X | | | | | | | | | | | | | | | |
| | Unclassified interview reports | X | X | X | | | | | | | | | | | | | | | |
| | Updated IPB (Intelligence Preparation of the Battlefield) Products | X | X | | | | | | | | | | | | | | | | |
| | Weekly Intelligence Summaries | X | X | | | | | | | | | | | | | | | | |
| | What assets are available (including submarines) ? | X | X | X | X | | | | | | | | | | | | | | |
| | What capabilities are in the area ? | X | X | X | | | | | | | | | | | | | | | |
| | What military response is planned against pirate activity? | X | X | X | | | | | | | | | | | | | | | |
| | Where are the helicopter capabilites ? | X | X | X | | | | | | | | | | | | | | | |
| | Where is (are) Role-2 medical capabilities ? | X | X | X | | | | | | | | | | | | | | | |

# Partial IERs - Operational & Tactical Levels of Command

## Other Information and Information about Pirates

## To NATO from External Entities

| | | TO NATO - FROM EXTERNAL ENTITIES | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | NMF | | | | | Nations | | | | GOs | | | NGOs | | | Others | | |
| | INFORMATION | CMF | EU (Operation ATALANTA) | Independent Deployers | MPRA Forces | National NCAGS Entites | NATO-Member Law Enforcement Authorities | Regional Authorities | Port Authorities | National Casualty Reporting Centres | Interpol | IMO | United Nations | IMB (Including IMB Piracy Reporting Centre) | NGA WWMS | Jt War Committee & OCIMF | Merchant Mariners | AIS Satellite Contractors | Media |
| Other Information | Fishing areas and movements of fishing vessels | X | X | X | | | | | | | | | | | | | | | |
| | Extraordinary information about other ships | | | | | | | | | | | | | | | | X | | |
| | UN Working Group & Committee reports | | | | | | | | | | | | X | | | | | | |
| | Information about ports | X | X | X | | X | | | X | | | | | X | | | X | | |
| | Information about weather and sea conditions | | | | | | | | | | | | | | | | X | | |
| | Format Alpha messages | | | | | | | | | | | | | | | | X | | |
| | Technical data about hijacked ships | | | | | | | | | | | | | | | | X | | |
| | MIEVOM agenda and minutes (and similar events involving merchants) | | | | | X | | | | | | | | | | | | | |
| | Vessel position & status reports | X | X | X | X | X | | | | | | | | X | | | X | X | |
| | Information about BMP3 compliance | X | X | X | | X | | | | | | | | | | | X | | |
| | LRIT (Long-Range Idendification and Tracking) data | | | | | | | | | | | X | | | | | | | |
| | AIS data | X | | | | | | | | | | | | | | | | X | |
| | Information about national means & capabilities to hold & prosecute pirates | X | X | X | | | X | | | | X | | | | | | | | |
| | Information to help identify foreign merchant ships | | | | | | | | | | | | | | | | | | |
| Information about Pirates | Alerts about pirate events:<br>- An event has occurred.<br>- Counter-piracy forces are engaged.<br>- Military assessment of event. | X | X | X | | X | | | | | | | | X | | | | | |
| | Any classified information about pirates | X | X | | X | | | | | | | | | | | | | | |
| | Information about mother ships (including suspect mother ships):<br>- Location<br>- Imagery, if available<br>- Crew size, if known | X | X | X | X | | | X | | | | | | X | | | X | | |
| | Information about pirate activity:<br>- Where are they?<br>- What are they doing?<br>- What capabilities do they have?<br>- What attacks have been conducted, and what was the result?<br>- What is current situation of pirated vessels? | X | X | X | X | X | | X | | | | | | X | | | X | | |
| | Intelligence predictions regarding intentions of pirates | X | X | X | X | | | | | | | | | | | | | | |
| | Situational information about pirates & Pirate Action Groups (PAGs):<br>- Where are the pirates?<br>- What direction are they moving, and how fast?<br>- What capabilities do they have? | X | X | X | X | X | | X | | | | | | X | | | X | | |
| | Personal information about pirates to support prosecution:<br>- Photographs<br>- Biometrics<br>- Cell phone data<br>- Name & Surname<br>- Year of birth<br>- Country of origin<br>- Country of piracy operation<br>- INTERPOL Reference (ID)<br>- Photo<br>- Phone number(s)<br>- Mother's name | | | | | | | | | | | | | | | | | | |
| | NAV WARNINGS and IMB ALERTS about pirates and pirate activity | X | X | | | X | | | | | | | | X | | | | | |
| | Pirate "de-briefs" following pirate encounters | X | X | X | | | | | | | | | | | | | | | |
| | Recognized and probable piracy mother-ships, including electronic parametric details of all recognized and probable piracy mother-ships | X | X | X | X | X | | X | | | | | | X | | | X | | |
| | Counter-piracy feedback from judicial authorities, such as:<br>- Confirmation of evidence<br>- Confirmation that captured pirates are in database<br>- Charactreristics of pirates with regard to importance or level of threat<br>- Information about piracy networks<br>- Information about who is behind piracy (i.e., funding it, overseeing it, etc.)<br>- Verification that captured pirates are (or are not) previously known criminals<br>- Feedback on counter-piracy contributions to prosecution of criminals | | | | | | X | | | | X | | | | | | | | |
| | Suspicious vessels and/or maritime activity | X | X | X | X | X | | X | | | | | | X | | | X | | |