Enhancing the Djibouti Code of Conduct – Jeddah Amendment Information Sharing Network: Strategy Roadmap

November 2021

Mission Statement: to improve regional maritime domain awareness (MDA) and maritime safety and security through dissemination of reliable information-sharing on incidents of maritime crimes like piracy and armed robbery; illegal, unreported, and unregulated (IUU) fishing; illicit trades; human smuggling; and maritime terrorism.

Vision:

- Every DCoC-Jeddah Amendment member state has established its National Maritime Security Committee structure which oversees the work of the operationalised National Maritime Information Sharing Center (NMISC) and effectively utilises the information it provides in national maritime security decision making
- DCoC members' national agencies cooperate in sharing information through NMISCs
- Friends of the DCoC cooperate in sharing information through MOUs established with NMISCs and regional centres
- Analysis of incidents by regional centres distinguishes patterns in illicit maritime activities and supports disruption of maritime crime by guiding regional policy decisions

Assumptions:

- This process will take time and require patience to achieve ideal levels of operationalisation
- Internal advocacy will be necessary to convince governments of the value of prioritising maritime security and combating sea blindness; regional governments will be at varying levels of buy-in
- Progress begets progress; even small victories are important pieces of the overall picture
- Not all information will need to be shared between partners and it is up to the states to decide the modalities for sharing information

Roadmap: The following roadmap was developed based on feedback from the Sub-Committee on Enhancing Information Sharing, as well as interviews with experts in developing information-sharing networks.

Level	Strategy	Tactics
National	Establish NMISCs (operational) in all signatory states	• Determine minimum operational capacity necessary • Identify NMISCs capabilities and gaps • Direct funding and capacity-building to non-operational NMISCs in signatory states
Regional	Maximise regional information-sharing centres by developing clear protocols for information sharing	• Establish common protocols for sharing information between NMISCs and regional ISCs; incorporate into training and orientation for centre personnel • Establish common information-sharing SOPs to promote interoperability • Implement joint trainings, workshops, conferences, TTX, meetings, reciprocal centre visits, operations at sea to build trust and rapport, and to normalise communication
International	Reports and analysis are produced and disseminated widely	• Identify what information is needed and what purpose it serves • Decide on frequency of reports/ briefings • Determine methods by which information is shared

Strategy #1: Establish and operationalise NMISCs in all signatory states, which coordinates activities of national maritime security agencies and maritime law enforcement in maritime domain awareness.

Status quo: Some NMISCs are established and operational while other states are not currently operational [or do not have NMISCs]

Roadblocks: Securing sustainable funding sources to build and maintain operational capability of NMISCs; turnover in personnel; lack of political will/maritime security not a priority to regional governments (so-called "sea blindness")

Tactics: Determine minimum capability necessary for operations; DCoC Working Group coordinates funding and capacity-building efforts to gaps in NMISCs under DCoC framework

Proposed next steps: States develop National Maritime Security Committees, who oversee the establishment, enhancement and operations of NMISCs, and information they supply is utilised to develop National Maritime Security Risk Registers, contribute to the development of National Maritime Security Strategies, and assist with national maritime security decision-making; DCoC Information Sharing Working Group determines minimum capability requirements for information sharing centres; states complete NMISC self-assessments to determine capabilities and gaps and develop individual roadmaps to full operationalisation of NMISCs; DCoC Information Sharing Committee identifies gaps and determines priorities for future capacity building efforts and funding and, in coordination with DCoC Working Group 2, communicates these to the Friends of the DCoC and seeks support to address capability gaps; States awaiting establishment of NMISCs develop clear SOPs for multi-agency information-sharing

Strategy #2: Maximise regional information-sharing centres by establishing clear protocols for sharing information.

Status quo: ISCs are at different levels of operability

Roadblocks: Lack of trust at the national, regional, and international levels limits information sharing between agencies, which in turn may impede the region from developing complete maritime security picture and identifying patterns which would help maritime enforcement authorities to prevent future threats across the region and beyond

Tactics: Establish clear and common information sharing SOPs between agencies at the national level; establish clear and common information sharing SOPs for regional centres; establish training for information sharing and standardise across all centres in the region

Proposed next steps: Engage national stakeholders in scenario-based exercises to collectively identify the types of information to be shared with regional centres and establish clear information sharing SOPs between NMISCs and regional ISCs based on the processes laid out in Articles 11 and 12 of the Jeddah Amendment; establish clear information-sharing SOPs for ISCs in the region which details what information is exchanged between centres, based on the process laid out in Article 11 of the Jeddah Amendment; implement joint trainings, workshops, table top exercises, conferences, meetings, reciprocal centre visits, and operations at sea between actors operating in the region to

build trust and rapport and to share success stories, best practices, and lessons learned, and to normalise communications; establish training specific to information sharing protocols which is standardised across all centres operating in the region; consider future SOPs for two-way information sharing with private actors

Strategy #3: Continue evolving Information Sharing Network which shares information with wide distribution list.

Status quo: Information sharing network is focused on incidents of piracy and armed robbery at sea and is not currently inclusive of other maritime threats pertinent to the region including IUU fishing, illicit trades, human smuggling, and maritime terrorism

Roadblocks: Lack of trust at national, regional, and international levels; absence of reporting requirements or agreed upon incident reporting system; difficulties with interoperability of information reporting systems

Tactics: Identify/establish trusted, independent source to sanitise/anonymise data received from multiple sources and distribute reports widely; determine methods by which information is shared; design universal incident report; build effective working relationships between colleagues at centres across the region

Proposed next steps: Stakeholders explore what information to share using collective scenario-based exercises and build clear information-sharing protocols with international partners based on the exercise as well as the processes laid out in Article 12 of the Jeddah Amendment; stakeholders incorporate information-sharing protocols into training/orientation of NMISC and regional ISC personnel; stakeholders collectively identify trusted source to anonymise, sanitise, and analyse data; based on the process laid out in Article 12 of the Jeddah Amendment, regional reports are compiled by regional centres and distributed widely within the network, allowing recipients to decide if/how to act on information received; collectively weigh the benefits of various information sharing systems and decide on best options for expanded ISN

Milestones:

- Roadmap agreed to amongst DCoC signatory states
- NMSCs are established to establish, enhance, and oversee the operations of NMISCs and the information they supply is used to develop National Maritime Security Risk Registers, contribute to the development of National Maritime Security Strategies, and assist with national maritime security decision making
- NMISCs established and operationalised coordinate the activities of national agencies engaged in maritime security and maritime law enforcement, and facilitate interagency cooperation
- Establish clear information-sharing protocols between agencies and centres, establish information-sharing MOUs with non-DCoC information-sharing centres in the region
- Data is collected from multiple sources, sanitised to remove all identifying information by a trusted source, analysed, and distributed, helping actors in the region to identify criminal patterns and risk factors
- Information is used to disrupt and prevent maritime crime in the region

Annex 1 – DcoC Capability Assessment Grid for National and Regional Information Sharing Centres (for NMISC self-assessment)

Lines Of Development		
High Level	**Medium Level**	**Low Level**
Doctrine and Concepts	National Regional Mandate/Policy *'Higher Level Linkage to all the other Lines of Development'*	National/Regional Maritime Strategy (Signed), Mandate to define Capability Requirement, Command and Control, Identify the Threats (Piracy, Smuggling, IUU, CT, Narcotics, etc.), MDA Centre Plan (2-year road-map) - including how to measure performance (through Operational Assessment Grid), Standing Operating Procedures (SOPs). Information Sharing Agreements (MOU).
Infrastructure	Building Facilities, Services	Power, Shelter, Water, Secure Environment, Dedicated IT Space (Controlled), Internet Access (Bandwidth aligned with system requirements), Telephony, Business Continuity Plan (BCP), Meeting Room, Secure Storage.
Equipment	MDA Capability	MDA System (National, Regional, International). National and/or Regional Comms, Open Systems, GMDSS, Conference Facilities (Video Tele-Conferencing),
Organisation	Internal Manning Structure	Roles and Responsibilities (IT Security, COS, Information Officer, etc.). Hours of Operation (365/24/7), Organigram.
Information	Data Available, Understanding and Exchange	SAT-AIS, Coastal AIS, LRIT, VMS, Vessel Reporting, Radar, EO, SAR/Imagery, Air and Maritime Patrol, ELINT, E-Mail, VOIP (Secure), Data Exploitation Tools, Foundation Geospatial Information, Charts (Digital and Paper). Information Sharing (iaw MOU).
Interoperability	External Organisation Exchange/Interface	National Interfaces (Fish, Defence, Coastguard, Home Office, Foreign Office, etc), Regional Interfaces (Other MDA Centres, Regional MOCs, etc.), International Interfaces (International MDA Centres, International Organisations and Maritime Component Commands) - Digital, Voice and Physical Meetings/interaction.
People	Suitably Manned for the Operation	Maritime Background, Suitably Qualified (generic), Sustainability and Manning Plan. Maritime English proficiency.
Training	Facilities, Delivery	Training cycle sustainability, Location, Provider. Generic and Operational Training. Training Performance Standard, Operational Performance Standard (align and proven through the Operational Assessment Grid).
Logistics	Access, Transport, Finance Model	Robust and sustainable finance model (iaw endorsed Mandate), Roads, Mail Service, Cleaning, Enviromental.

Annex 2 – United States Maritime Operation Centre Capabilities Survey

Clear Form

MOC Capabilities Survey

You have been identified as the Assessor responsible for completing this assessment survey. We are using this information to properly assess the Partner Nations' capacity and capabilities to conduct Maritime Operations during this exercise. This survey only needs to be completed one time per event / exercise and will take approximately 45 minutes to complete.

This questionnaire is essentially a checklist of the required MOC instructions, equipment, and support. Please complete the survey as thoroughly as possible but do not be afraid to leave areas blank if you cannot determine the information. It is recommended that you continue filling in portions of this survey throughout your time in the MOC in order to gather as much information as possible. Due to how we extract the data, it is necessary to use Adobe Acrobat Reader which can be found at https://get.adobe.com/reader/.

We are using this information to accurately assess the Partner Nations' capacity and capability to conduct Maritime Operations during this exercise and the answers to this survey are confidential and will not be shared with any other organization. If you have questions at any time about the survey or the procedures, you may contact the NAVAF Assessor using the contact information specified below. Thank you very much for your time and support. Please save using this convention: Country_SurveyTitle_DDMMYY_LastName

NAVAF Assessor
N9 Operational Assessments CNE-CNA-C6F
Email: PhoenixExpressAssessor@gmail.com

Basic Information

Last Name:

Organization:

What is your level of qualification / experience in MOC functions?

Email where you can be reached:

What day is this survey for?

Which country are you assessing? (Select from drop down or write in as necessary.)

Which MOC are you assessing? (Select from drop down or write in as necessary.)

Please provide comments on how to improve today's events.

Essential Standard Operating Procedures (SOPs)

Procedures are written, approved, familiar to watch standers, and used for all of the following:

Enduring Tasks (select all that apply)

- ☐ Daily activities schedule (battle rhythm) (reports, weather briefs, equipment status, etc.)
- ☐ Daily operations brief/report to Chain of Command
- ☐ Periodic meetings with the Chain of Command regarding current priorities, focus, interests
- ☐ Watch handover (turnover)
- ☐ Communications checks
- ☐ Watch log (with backup and alternative for power outage if needed)
- ☐ Watch bill, roster, personnel directory
- ☐ Maintenance: notify/track/report procedures
- ☐ Critical personnel and emergency numbers (short list, easily accessible)

Emergent Tasks (select all that apply)

- ☐ Communication content checklists/templates for each event
- ☐ Piracy, hijacking events
- ☐ Illegal trafficking (drugs, arms, human, …) events
- ☐ IUU Fishing events
- ☐ Biological/Ecological (pollution, …) disasters
- ☐ Natural (crisis response) disasters
- ☐ Search and rescue (SAR)
- ☐ Maritime MEDEVAC
- ☐ Hot pursuit, contact handover
- ☐ Contact Reports (surface)
- ☐ Continuity of Operations - Evacuate/Relocate

Review and Updates (select all that apply)

- ☐ Procedures are updated, signed and dated by the chain of command
- ☐ Procedures are reviewed at least annually and revised from lessons learned

Comments on this section

Critical Systems and Equipment

The MOC has the following equipment:

Communications (select all that apply)

- [ ] Telephone, radio (HF/VHF) system, and chat, email systems
- [ ] Backup radio system
- [ ] Weather report / monitoring system

Recommended additional communications equipment (select all that apply)

- [ ] VOIP between center & sites
- [ ] Satellite telephone and/or Inmarsat

Data & display systems (select all that apply)

- [ ] Maritime Global Picture system (ie: SeaVision or equivalent web-based system)
- [ ] Up/downlink/display (ie: TV32)
- [ ] Local sensor control and fusion systems (ie: RMAC/SureTrak, MTM300, FalconEye, etc)
- [ ] Data network status display (ie: SolarWinds or equivalent)

Sensors: RADAR (select one)

- ◯ No working RADAR
- ◯ 1 Site
- ◯ All critical sea space covered
- ◯ Full coastline coverage

Sensors: Other (select all that apply)

- [ ] AIS sensor (shared via MSSIS)
- [ ] Cameras at all critical sites
- [ ] LRIT sensor
- [ ] Satellite Synthetic Aperture RADAR
- [ ] EO/IR
- [ ] MF/HF Direction Finder

Administration Equipment (select all that apply)

- [ ] Computer workstation(s)
- [ ] Dedicated MOC telephone
- [ ] Printer/copier/scanner
- [ ] Networks and web access (separate from local systems & sensor networks)

Infrastructure (select all that apply)

- [ ] Power management system
- [ ] Certified grounding for systems, towers, power systems, buildings
- [ ] Back-up power system such as a generator, auto-switchover
- [ ] Back-up power system sustainable for 24 hours

Recommended Additions (select all that apply)

- [ ] Wall displays, status boards
- [ ] Charts, chart tables

Comments on this section

Personnel / Staffing Responsibilities

Defined Responsibilities (select all that apply)

- ☐ Watch Chief /OIC
- ☐ Watch officer roles and responsibilities
- ☐ Watch supervisor roles and responsibilities
- ☐ Communications watch stander (voice/radio, chat/email, record logger) role and responsibilities
- ☐ MDA system operator (system, chart, nav-plot) role and responsibilities

Manning (select if applicable)

- ☐ No less than two of the above watch positions manned 24 hours a day

Maintenance: on site or on call (select all that apply)

- ☐ IT software and systems support, troubleshooting
- ☐ Electrical and power support
- ☐ Site and systems support

Intel Access (select if applicable)

- ☐ MOC personnel have the ability to communicate / coordinate with intelligence agencies

Interagency Access (select if applicable)

- ☐ MOC personnel have the ability to communicate / coordinate with other national agencies (i.e.: fisheries, law enforcement, judicial, etc.)

Legal Access (select most appropriate response)

- ○ A Legal advisor is present in the MOC
- ○ MOC personnel have instant access to a legal advisor (via phone or email)
- ○ MOC personnel have no access to outside legal advice but have extensive training in legal matters
- ○ MOC personnel have no access to any legal advice and have limited/no legal training

Comments on this section

Personnel, Qualifications, and Training

Personnel management for MOC staffing & prerequisites (select all that apply)

☐ Officers/ratings/interagency personnel are assigned based on experience in an appropriate field; e.g., communications, information technologies (IT), electrical engineering, navigation/radar plotter

☐ MOC assignment supports career progression and promotion – the intent is to make MOC assignment appealing to the best-qualified personnel.

Training as a continual process (select all that apply)

☐ Pre-assignment training/qualifications and OJT plan documented

☐ A training program with qualification standards and process. JQR/PQS (job qualification requirements and personnel qualification standards) (or appropriate equivalent) process and documentation

☐ Watch standers qualify in multiple watch positions, responsibilities. Cross-rate training, operational capability efficiency enhancement.

Training Areas (select all that apply)

☐ MOC mission and roles (local, national, regional and international)

☐ MDA (C4I)

☐ MOC procedures and responsibilities

☐ Watch officer training

☐ Watch supervisor training

☐ Watch stander training

☐ System and equipment use and administration

☐ System and equipment technical maintenance (as part of a maintenance program)

Comments on this section

Required Support for the MOC

Budget (select all that apply)

- ☐ Basic funding for costs, supplies, power, etc.
- ☐ Annual funding plan
- ☐ Lifecycle funding plan covering continuing costs over the expected life of the system until replacement

Maintenance Staff and Skills (select all that apply)

- ☐ Basic technical skills available; e.g. electronics technician, electrician
- ☐ The specific / specialized technical skills required for each system are available no later than the next working day

Maintenance Program (select all that apply)

- ☐ Maintenance plan with priorities for timely response
- ☐ Master Maintenance Schedule – appropriate (vendor recommended) routine maintenance for every system and component. Task assignment includes checklists for reporting
- ☐ Master status board or report, updated daily
- ☐ Staff watch bill for on-call support 24/7
- ☐ Record of all maintenance events (failures, repairs, routine maintenance, replacement, new installations)
- ☐ Library: Manufacturer documentation (use, troubleshooting, repair instructions) for each component (master plus checkout copies). All maintenance documentation should be available via checkout and included in training
- ☐ Maintenance training covering all tasks, classroom, or on-the-job (OJT). Training may be managed within the branch or in a separate program
- ☐ Job qualification requirements (JQR or PQS) plan and certifications for maintenance personnel

Maintenance Program: Corrective Action Timeline (select one)

- ○ Corrective action within 24 hours
- ○ Next day corrective action
- ○ Longer delay for corrective action

Supply (select all that apply)

- ☐ Procurement and inventory; managed in response to requests
- ☐ Procurement plan based on required spares, consumption rate, lead-time
- ☐ Inventory managed with safe storage, accounting, and feedback to procurement

Comments on this section

Additional comments for this MOC

Clear Form Submit