Access all areas

A variety of technologies are currently in use for maritime and anti-piracy C2 at strategic and tactical levels in the Indian Ocean. **Giles Ebbutt** examines both ends of the spectrum.

C2 has many facets, some of which are technological and some human or cultural. Technology can provide connectivity, processing and presentation: the ability to transfer data from one place to another; manipulate and merge it; and display or present it in the most effective manner possible. But command is also about human relationships and the chemistry between individuals and organisations with very different cultural and political backgrounds.

C2 is also about scale. At the strategic end it is about policy, coalitions, a multitude of considerations and long-term planning. At the other it is about real-time situational awareness, rapid decision-making and communication over a few hundred metres. The maritime security operations, particularly anti-piracy patrols, currently being conducted in the Indian Ocean provide a good illustration of this.

PRIME EXAMPLE

Operations are being conducted over an area of the Indian Ocean comprising more than 6.7 million square kilometres, and the navies of more than 40 countries are taking part. There are three major organisations involved. Combined Maritime Forces (CMF) is based in Bahrain, with its subordinate Combined Task Force (CTF) 151 which has a specific counter-piracy role. CTF 151 is multinational in composition and command rotates between different countries.

NATO's Operation *Ocean Shield* force in April 2011 consisted of five vessels, commanded by a commodore from the Royal Netherlands Navy, subordinate to the Allied Maritime Command HQ in Northwood, just outside London. Its composition and command also change at regular intervals.

The EU Naval Force (EUNAVFOR) conducts Operation *Atalanta*, which is specifically tasked to provide protection for UN World Food Programme supplies, but also has a subsidiary counter-piracy role. This consists of between four and 12 ships from EU nations together with maritime patrol and reconnaissance aircraft (MPRA). The Operation *Atalanta* force is also commanded in-theatre on a rotational basis (in April 2011 by Spain), with an operational HQ which is also in Northwood, although in a separate facility to NATO. Here the staff is provided by elements of the Royal Navy's (RN's) Fleet Battle Staff.

In addition to these three major groupings, there are also 'independent deployers', who contribute forces to the counter-piracy operations, notably China, India, Japan and Russia. The variety of these groupings demonstrates the complexity and potential difficulties concerned with C2 on this operation.

BUILDING TRUST

According to Maj Gen Buster Howes, Royal Marines, the UK's Commander Amphibious Forces and the current Commander EUNAVFOR, a key aspect of his role is contributing to building consensus and trust. This is not only amongst the various participants, but also with many of the countries on the Indian Ocean rim through personal discussions and contact, in order to help with such things as MPRA basing. 'Building personal relationships and trust is crucial,' he said.

Information-sharing at the tactical level is important in order to achieve some unity of effort amongst the various participating forces, and there are both technological and procedural solutions to this. The Shared Awareness and Deconfliction (SHADE) group, chaired rotationally by CMF, NATO and EUNAVFOR, meets every eight to ten weeks in Bahrain. According to Howes, it focuses on 'achieving coherence of tactical action in a very pragmatic way' to avoid any political difficulties with non-aligned nations. This has resulted in some task-sharing benefits, such as China taking on a particular UN escort task from EUNAVFOR.

A French boarding party apprehends suspected pirates as part of Operation *Atalanta*. *(Photo: EUNAVFOR)*

Cobham's Marinised Data Terminal, showing WaveHawk C2 software being used with an electronic chart. *(Photo: Cobham)*

The Royal Australian Navy has equipped its RHIBs with Saab 9LV SAT terminals. *(Photo: Saab)*

In addition to the SHADE meetings, the various in-theatre force commanders 'speak every day', the three main participants all have liaison officers in each others' HQs, and plenty of use is made of video teleconference facilities.

Immediate shared situational awareness is provided by EUNAVFOR's Mercury common information-sharing system, an internet-based secure chat facility run by the Maritime Security Centre – Horn of Africa (MSC-HOA). This is an initiative established by EUNAVFOR with close co-operation from the shipping industry. The MSC-HOA provides 24-hour manned monitoring of vessels transiting through the Gulf of Aden, whilst the provision of an interactive website enables the centre to communicate the latest anti-piracy guidance to industry and for shipping companies and operators to register their movements through the region.

A further initiative is the introduction of 'group transits', where vessels are co-ordinated to pass through high-risk areas overnight, when attacks are reduced. This enables military forces to 'sanitise' the area ahead of the merchant ships. MSC-HOA will also identify particularly vulnerable shipping and coordinate appropriate protection arrangements, either from within EUNAVFOR, or other forces in the region.

CLEARER PICTURES

The Mercury chat facility is hosted on a secure website – users have to register to receive the necessary usernames and passwords for access, and potential registrants are carefully assessed before their registration is approved. It contains simple event messages to and from those who have access, and is also updated by the UK Maritime Trade Operations (UKMTO) office in Bahrain with further information which has been passed to it by merchant ships. UKMTO acts as the central counter-piracy point of contact for all merchant shipping in the area. Information provided by naval forces and MPRA is input into Mercury to add to the shared awareness picture.

The various naval forces obviously maintain their own surface pictures, which are augmented by Mercury and the Automatic Identification System (AIS), the tracking technology used by all seagoing vessels over 270t and all passenger vessels. The AIS picture is also maintained at UKMTO.

Where NATO, EUNAVFOR or coalition allies are involved, tactical information exchange can be relatively simple, with standard doctrine and protocols available. For those less accustomed to working together, it can be more difficult but not insurmountable. According to Howes, 'there are some information-sharing walls which can be a bit vexing, but pragmatically we find ways to share situational awareness when we need to'.

Another aspect of C2 that can be tested in a coalition and cooperative environment like this is the possible conflict between different national directives and rules of engagement, and the collective action being taken. According to Wg Cdr Paddy O'Kennedy, a EUNAVFOR spokesperson, in practice this is not a problem within the *Atalanta* task force. 'We are aware of all the different national considerations and caveats' he said, 'and there are rarely major hiccups. In the event that there is a divergence between EU and national policy, a ship will briefly revert to its national command authority for the duration of the particular incident.'

A screenshot from the Maritime Boarding system showing biometric information for transmission. *(Image: Systematic)*

JOINING THE PARTY

At the opposite end of the scale, the growth in maritime security operations has led to a commensurate increase in the systems being offered to support the C2 of boarding parties. Generally, these consist of a number of standard elements. There will be a communications system which provides a link between the mothership and the boarding party's vessel, and communications between different members of the team. The former has to work over longer ranges, while the latter must function within the confines of a ship, so they may not necessarily be the same. There will almost certainly be integrated GPS.

The mothership link requires sufficient bandwidth to transmit imagery, as cameras and scanners are used to copy ship and crew documentation, and to photograph crewmembers for comparison with databases. Sometimes, biometric recording devices such as fingerprint readers are also integrated. These elements have to be sufficiently accurate to provide evidential-quality information if necessary.

A key part of the system is a situational awareness display, which will include own and other track information, and possibly C2 functionality such as messaging and overlays.

The earliest example of this kind of capability is the Xeres Maritime Interdiction System from Drumgrange, which has been in fleet-wide service with the RN since 2002. It provides secure voice communications between the mothership and a boarding party embarked in a sea boat. Photographs, scanned documents and streaming video can be passed back over this link. There is also a chemical sensor which will detect explosive gases and provide an aural and visual alarm.

The system automatically tracks the position of both mothership and sea boat(s) with integrated GPS, with the positional information passed over a dedicated UHF link, and the data displayed against standard Admiralty charts. This is updated every five seconds. Xeres can also be integrated with the mothership's radar using an Automatic Radar Plotting Aid interface, which allows selected radar tracks to be transmitted to the boarding party.

SYSTEMATIC APPROACH

Since the introduction of Xeres, a number of other systems have been developed. Systematic's SitaWare Maritime Boarding is a backpack-based system which is communications-agnostic and leverages the company's SitaWare C2 software. Variants of SitaWare, which uses the Multilateral Interoperability Programme II-compliant Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) are in use in a number of tactical battle management systems and operational-level C2 systems. It was originally developed in response to a Royal Danish Navy (RDN) urgent requirement in 2008, prior to Denmark assuming command of the then Joint Task Force 150 (JTF 150) conducting the counter-piracy task off Somalia.

The system includes a ruggedised laptop or tablet computer running SitaWare, which has the standard C2 core with additional maritime functionality such as chart data and symbology. Camera, video, a scanner and a fingerprint reader are all included, enabling documentary and biometric data to be passed, as well as streaming video.

The original communications configuration was based on a WiFi solution, partly because Danish tactical doctrine expects a mothership to be within 500m of the target, negating the requirement for any sort of extended range. The solution selected was Rajant's BreadCrumb, which provides a self-forming, self-healing mesh network. It was developed for use in mines and is therefore ideal for use below decks. This was the configuration successfully used by the RDN in 2009 on HMDS *Absalon* during the JTF 150 deployment.

Since then, Systematic has expanded the communications possibilities with an eye to an export market where greater ranges between boarding party and mothership may be required, and has demonstrated two alternative solutions. One utilises ITT's SpearNet Team Member UHF data radio, which provides the same mesh characteristics as WiFi but with greater ranges, embedded GPS, secure voice, data and video with a maximum sustained data rate of 1.5Mb/s, and IP. This can be used either as a complete solution both for intra-team communications and a mothership link, or just the former. Systematic has also demonstrated a mothership link using a mobile Inmarsat maritime terminal integrated with both WiFi and SpearNet Team networks.

According to Systematic, having completed an extensive trial and evaluation period, the RDN is now independently considering how a future maritime boarding system should be configured.

ALTERNATIVE SOLUTIONS

An alternative Danish solution to support deployed sea boats and similar platforms has been developed by Terma, with its C-Raid system, although this does not include intra-boarding party communications or data collection. C-Raid is essentially a scaled-down and customised version of the C-Flex maritime combat management system (CMS), which is itself built on the company's T-Core open-architecture C2 software. C-Flex is the standard CMS for the RDN.

The Saab 9LV Situation Awareness Terminal mounted on the bridge of a frigate.
(Photo: Saab)

The default system layout consists of a ruggedised computer, a C-Raid Panel PC, for the deployed unit linked via a data link to another PC on the mothership. The Panel PC, which uses Windows XP, has integrated GPS, touchscreen functionality and a total of 12 programmable hard keys, six on each side of the screen, to make it easy to use while in a small boat. It provides a situational awareness display on electronic charts or satellite imagery, with own position and other live tracks – the latter can be injected from a mothership's C-Flex. Other functionality includes tactical overlay creation and display, message management, route management and auto-intercept calculations.

Communications, which can be HF, VHF or UHF radio, satcom or WiFi, are routed through the Tactical Access Unit (TAU), also developed by Terma. The TAU allows up to four different channels to be utilised concurrently, selecting the quickest message route, and can serve several Panel PCs.

OPERATING SYSTEM

Cobham Defence Communications (CDC) has developed a complete package called the Maritime Interdiction Operations System (MIOS), which includes integrated body-worn boarding party equipment, leveraging CDC's experience in developing individual soldier systems. This is a communications-agnostic system using CDC's WaveHawk C2 software. It can be installed on a range of maritime platforms, and could even be extended to land-based units through the interoperability of the WaveHawk and BattleHawk software.

The MIOS Boarding Party configuration has been designed to provide maximum capability and manoeuvrability with minimal weight. The system allows inflation of a life jacket without the removal of equipment, and all components are waterproof. The System Interface Unit (SIU) which integrates a number of devices into MIOS, is the central component of the assembly. Its key features include audio mixing of different radios into one headset, generation of system audio alerts, USB/Ethernet connectivity, integrated GPS and a digital magnetic compass option. The GPS allows the mothership to track and display boarding party craft locations, with updates at less than ten-second intervals

The SIU is used to integrate intra-boarding party communications and the high-data-rate link to the mothership. CDC offers its Cobham Eagle individual radio as the default for the former task. This UHF system provides full duplex voice and simultaneous data communications at up to 128Kb/s in an ad-hoc network with automatic rebroadcast and AES-128 encryption.

The boarding party commander, and optionally other members of the party, carries the Marinised Data Terminal (MDT). This is a lightweight, ergonomically designed, ruggedised computer using Windows XP and running WaveHawk. It has a touchscreen display and can be used to support a variety of other features including translation software, video cameras and CBRN sensors.

The boarding party platform is equipped with a user data terminal, a large daylight-readable touchscreen unit which runs WaveHawk and AIS information. The full Windows XP system supports RS-232/422/485, USB 2.0 and Ethernet interfaces, as well as standard National Marine Electronics Association devices such as depth sounders.

MIOS has been selected by the Royal New Zealand Navy (RNZN), which awarded a contract to Cobham in 2008 for more than 50 systems, including fitting equipment to a number of motherships and rigid hull inflatable boats (RHIBs). As a result of this contract, CDC worked closely with the RNZN to refine and develop the system, resulting in the current configuration but delaying delivery until 2010. The RNZN selected the Raytheon MicroLight-DH500 radio for the high-bandwidth data link task, retaining the Eagle radio for boarding party communications. The DH500 is a fully IP-compliant system which provides simultaneous voice, data and video communications over three frequency bands in the 225-2,000MHz range, with an ad-hoc self-healing network and a maximum data rate of 1Mb/s.

NEW ARRIVALS

The most recent arrival on the scene is from Saab, whose Australian subsidiary has developed the 9LV Situation Awareness Terminal (SAT), which is designed to provide deploying RHIBs or similar platforms with a tactical display capability. The 9LV SAT core software is a derivative of Saab's widely used 9LV Mk 3E CMS, with a specialised human-machine interface.

A 9LV SAT ruggedised terminal is fitted to the coxswain's console on the ship's boat and is linked to the mothership CMS via a high-frequency data link to enable over-the-horizon connectivity up to 55km. The SAT network can include a number of participants. The RHIB terminal shows simplified maps and target symbology, and has large on-screen commands and buttons for operator-initiated functions.

The standard system comes with interfaces to GPS, AIS, ARPA, sensors and the CMS. The tactical picture is augmented by automated probabilistic track correlation, and a tactical chat function allows communication between mothership and deployed platform. The system has data-recording facilities to enable recall of events, and the SAT network can include multiple participants.

Royal Australian Navy ships and their RHIBs deployed to overseas operational areas are equipped with the 9LV SAT. It is also fitted to vessels assigned to border protection duties. DB