The Coming Revolution in NATO Maritime Command and Control

Eric Francis Germain, The MITRE Corporation

Since the turn of the decade NATO has made major improvements in the architecture supporting maritime command and control (C2). As late as the early 1990s, shore-based NATO commanders exercized command and control over their operating forces at sea more or less as had been done during World War II: via paper signals, grease-pencil status boards, metal-backed map boards, and magnetic pucks—representing ships and aircraft—that were moved about by sailors on tall ladders.

In only the last few years—since about 1993—all this has changed. Now, maritime command and control is performed via satellites, wide-area networks, computerized tactical data processors and machine-readable messages. The Maritime Command and Control Information System (MCCIS) has emerged as the C2 tool of choice for NATO's maritime component commanders. Operations in Bosnia resulted in the development of CRONOS (Crisis Response Operations in NATO Open Systems), and the NATO Initial Data Transfer Service (NIDTS) network also has come into being.

Last spring's exercise Linked Seas 1997 was the first operational test of various MCCIS nodes carried on the NIDTS network. Linked Seas 97 was a tremendous success, though not an unqualified success. Together, MCCIS and NIDTS form the foundation for a robust architectural backbone for the conduct of maritime C2 at the operational level of command. Some important issues still must be addressed, however, before the revolution in maritime C2 becomes a reality. These include: a greater focus on integrating ships into NATO's architecture, staffing flagships and shore commands with dedicated and trained MCCIS watchstanders, and the development of standard operating procedures and supporting reference materials that provide the warfighter with the needed guidance and tools.

The Genesis of Modern-Day Maritime Command and Control

The transformation from grease pencils to computers began in the U.S. in the late 1980s with the Joint Operational Tactical System, or JOTS. But JOTS was only the tool on which the surface picture was depicted, and in fact the U.S. Navy also built a complete infrastructure of satellite communications, C2 support systems, doctrine, procedures, operators and schools.

Operation Desert Storm—the Southwest Asia War against Iraq—occurred just as this type of maritime command and control was maturing in the U.S. Navy (and just prior to its adoption by NATO). It is natural, therefore, to wonder about the success of maritime command and control in Desert Storm. In general, a common and timely picture was realized and maintained in each of four maritime operating areas: the Persian Gulf, North Arabian Sea, Red Sea and Mediterranean. While it is true mission success generally was achieved, it also may be said many problems were uncovered during the war that took considerable effort to resolve. These include:

• ***Nonstandard Operating Procedures.*** Some U.S. ships departed homeport for Desert Storm sailing under U.S. Atlantic Fleet operating procedures, but when they entered the Mediterranean they switched to the Sixth Fleet's operating procedures. Then, when they passed through Suez they changed to Central Command operating procedures, and as they sailed home via the Pacific and the Panama canal they used Pacific Fleet procedures. *Different operating procedures and track naming conventions were used in each of the U.S. Navy's theaters of operation.*

• ***Ill-Defined Duties & Responsibilities.*** There were three key C4I nodes that reported tracks in the Mediterranean: the carrier battlegroup, the theater intelligence center, and the shore-based fusion center. During Desert Storm ***two*** of these three nodes received track data, "fused" the data, and broadcast this data to the other nodes and commanders worldwide, including to the Desert Storm warfighters. *Stations were manipulating other station's data and then broadcasting it back to the originators of that data.*

Architecture & Infrastructure Building Blocks	U.S. Navy Architecture		NATO Architecture	
	Desert Storm (ca. 1990–91)	Normal Ops (present day)	**Sharp Guard (ca. 1993–95)**	**Linked Seas '97 (present day)**
Systems	JOTS I	JMCIS, GCCS-M	α CCIS, NACCIS	MCCIS
Devices	HP 9020	TAC-3, TAC-4	HP 9020, TAC-3	TAC-3, TAC-4
Exchange Media	OTCIXS, TADIXS, HIT B	SIPRNet, OTCIXS, TADIXS, HIT B	AUTODIN, HIT B, NACCIS Network	NIDTS, CRONOS, HIT B
Exchange Formats	OTHT Gold, TADIL A	OTHT Gold, TADIL A, TADIL J	OTHT Gold, Link 14	OTHT Gold, Link 14 ADatP 3, APP 4, ACP 127 (AIFS)
Processes	FOTC[1]	FOTC	RedCrown	RMP Manager
Products	FOTC Broadcast	FOTC Broadcast	NTB, HIT B	RMP Bcst, HIT B
Procedures	Theater SOPs	Navywide OPTASK	EXTAC 619	**(none)**
Naming Conventions	STAR[2]	Worldwide STAR ('95)	NATO STAR ('94)	**NATO STAR ('94)**
DBM Watchstanders	OS[3]	OS	**(home grown)**	**(home grown)**
DBM Training	JOTS School	FOTC DBM School[4]	**(none)**	**(none)**

1 - The Force Over-the-horizon Track Coordinator (FOTC) mode of operation; a capability of JOTS, MCCIS, etc.
2 - The Standard Attributes Reference (STAR), a document providing uniform identifying attribute data for warships.
3 - The Operations Specialist (OS), junior/senior ratings trained in database management and the duties of FOTC.
4 - The formal school to train OSes on JMCIS, FOTC operations, Link 11 input and track database management.

Table 1 – The Building Blocks of a C4I Architecture and Infrastcucture

• ***Non-Robust Communications.*** U.S. Navy ships relied on its Officer in Tactical Command Information Exchange Subsystem, or OTCIXS, satellite system for the delivery of track data. When this medium also was used for other high-priority traffic (e.g., Tomahawk missions) *the system almost ceased to support track reporting*.

• ***Poor Interoperability with Joint and Coalition Partners.*** Except in the sharing of Link 11 pictures between fitted NATO units, there was very limited sharing of track data between the U.S. Navy and its coalition partners. This was because in 1990–91 only a few coalition units had JOTS-compatible tactical data processors, and because there was no delivery medium other than HF at 75 baud. *A NATO C4I architecture and infrastructure simply did not exist in 1991.*

The U.S. Navy has recognized and solved many of the problems first identified in Desert Storm, but some of the problems (e.g., non-robust communications) are still being worked today.

Table 1 compares aspects of the U.S. and NATO C4I architectures and shows how these have changed over the years. Items **highlighted** in the table are issues discussed in this paper.

Operation Sharp Guard

The NATO alliance had a similar awakening, and suffered a similarly steep learning curve, during the history-making events involving the Former Yugoslavia. In July 1992, NATO Operation Maritime Monitor and Western European Union (WEU) Operation Sharp Vigilance were initiated as monitoring operations in accordance with existing U.N. Security Council resolutions. On 22 November 1992 these became known as Maritime Guard and Sharp Fence, respectively, when the U.N. added enforcement as a mission. Finally, on 15 June 1993, these two operations were merged into one, unity of command was assigned to the Commander of Allied Naval Forces Southern Europe (COMNAVSOUTH), and the name was changed to Operation Sharp Guard. This enforcement activity consumed the combined efforts of two of NATO's Standing Naval Forces (Atlantic and Mediterranean) and the WEU Task Group for 36 months until Sharp Guard was suspended on 19 June 1996.

Sharp Guard presented the Allies with the classic challenge of producing and managing an accurate and timely Recognized Maritime Picture (RMP) over a wide sea area. Its key objectives were:

- Detect all ships in the Southern Adriatic Sea and its approaches,
- Maintain the picture of which ships have been challenged and which have not,
- Take appropriate action against any ship deemed suspect, and
- Prevent blockade-runners from delivering prohibited items into a Serbian port.

These objectives lie at the very heart of what a "Recognized Maritime Picture" is all about: maintaining an unambiguous and timely database of the position and identification of all tracks, both warship and merchant, and being able to distinguish the good or cleared ships from the adversary, unchallenged, suspect or blockade-running ships.

At the tactical level—at sea in the Adriatic—RMP management initially was accomplished via UHF Link 11. One task group took up station in the Montenegro operating area near the seaports of Serbia and the other operated in the Otranto operating area through which most all Serbia-bound ships must pass (see Figure 1). The two operating areas were managed independently, and there was no full-time coverage from Maritime Patrol Aircraft (MPA) to fill in the gap between operating areas.

Figure 1 – Adriatic Sea Operating Areas

At the operational level—ashore in Naples—COMNAVSOUTH was assigned responsibility for the conduct of Maritime Monitor/Sharp Guard, but he simply could not receive the RMP data being produced by the at-sea task groups (and later by RedCrown). Nowhere in Naples was there a Link 11 receive capability, and an HF signal from the South Adriatic did not reliably cross the Apennine mountains of Italy. Unable to achieve timely situational awareness of the Sharp Guard area, COMNAVSOUTH was constrained in the ability to exercise meaningful command and control over his assigned forces.

COMNAVSOUTH himself stated his operational requirement this way (quoted):

> *NATO maritime commanders need the ability to compile and disseminate a near-real-time RMP in order to exercise effective command and control. All ships or shore stations with information on naval contact positions should be able to input data and, in return, see the total surface picture. Based on this common picture OPCON authorities and involved commanders can ensure that friendly forces are effectively coordinated and deployed to intercept all contacts of interest as per the existing ROE. Without such an ability coordination is based on information that is generally several hours time-late, mission effectiveness is degraded, and much of COMNAVSOUTH's responsibility is necessarily but incorrectly devolved to the OTC afloat. A time-late synopsis of the surface picture at regular intervals may be satisfactory for those not directly involved in operations, but it is not acceptable for decision making at the level of command responsible for task group planning.*

This predicament prompted CINCSOUTH, in December 1992, to ask some pointed questions about Operation Maritime Guard and to invite NATO's Permanent Analysis Team (PAT) to investigate the following:

- How successful was the blockade?
- Were the assigned Allied forces being used effectively?
- Was NATO command and control adequate?
- What was the likelihood of "leakers" evading the blockade?

The PAT performed its analysis in January 1993 and submitted report CHEL 3109/48E, dated 11 February 1993. It restated what this author had verified in a similar RMP compilation analysis

performed on Exercise Display Determination 1991 over a year earlier:

- RMP coverage extended out to each ship's sensor horizon, and no farther.
- RMP coverage across the Otranto strait was less than 100%.
- COMNAVSOUTH's RMP was exceedingly timelate (12-18 hours on average).
- There was a distinct chance that blockade runners might be successful.

In other words, the PAT report stated clearly that RMP management in the Adriatic was imperfect, undetected "leakers" were a definite possibility, and COMNAVSOUTH as operational commander was unable to exercise viable command and control over his assigned forces because he had no current situational awareness. Not surprisingly, this prompted some changes:

- RMP management was given a theater focus: "RedCrown" was placed in charge of an Adriatic-wide, HF Link 11 net that unified the pictures of the Montenegro and Otranto operating areas.
- The on-station task groups were given nearly full-time supporting coverage from MPA that served to fill in the surveillance gaps between ships and between the two task groups.
- The Recognized Adriatic Surface Picture (RASP) architecture was an interim solution created to provide a not-too-timelate RMP ashore in Naples.
- The NATO Tactical Intelligence Broadcast (NTIB), an intel broadcast used only during exercises, was transformed into the NATO Tactical Broadcast (NTB) and dedicated to continuous all-force reporting. The NTB commenced operation on 14 April 1993.

The RASP Architecture

The Recognized Adriatic Surface Picture (RASP) Architecture was a no-cost solution to COMNAVSOUTH's operational requirement. It was also strictly an interim solution because the architecture relied on donated U.S. equipment and U.S. Navy communications. Nineteen old and insupportable JOTS Is were given to NATO and placed in various command centers from Naples to Santa Rosa, and these were interconnected by NATO and Italy. This gave the shore-based commanders an infrastructure, albeit limited, with which to display tactical data produced by the forces at sea. The only thing missing was the RMP data itself.

Some form of long-haul communications were needed to deliver track data from the Adriatic Sea to a connected node ashore. As it turns out, this is the very reason the U.S. OTCIXS tactical data satellite network was developed. The key U.S. players at sea—RedCrown and Force Over-the-horizon Track Coordinator (TF60 FOTC)—had all the RMP data the commanders ashore needed, and they also had direct connectivity via the OTCIXS satellite to Naples, Rota and Norfolk (amongst others). Figure 2 shows the gathering of RMP data by TF60 FOTC via two methods: via Link 11 and voice from RedCrown, and via OTCIXS broadcast from the various FOTC participant ships.

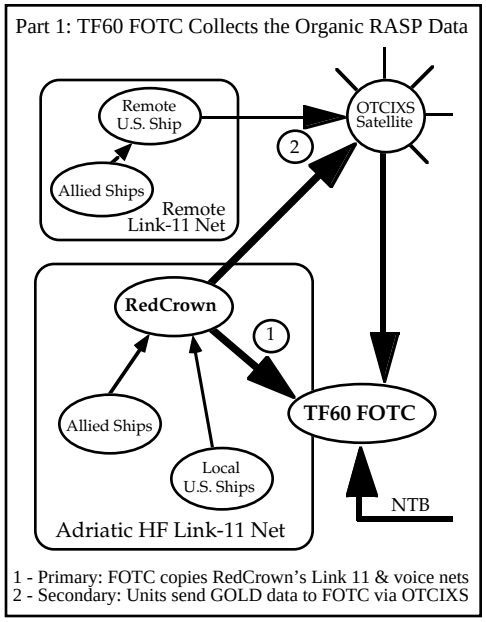

Figure 2 – Sharp Guard C4I (Part 1)

TF60 FOTC input the important organic Link data from the ships in Sharp Guard, sent its normal FOTC broadcast, and this was copied by many U.S. shore stations. For various national reasons the former Fleet Ocean Surveillance Information Facility (FOSIF) in Rota, Spain became the designated fusion point for the RASP and the producer of the NTB data stream. FOSIF provided "value added" to the RASP by adding in the non-organic intelligence data derived by FOSIF from various sources; this non-organic intelligence carried on the NTB was useful to both the operational commanders ashore and the commodores at sea. The RASP data then was sent via the U.S. AUTODIN circuit to NCTAMS

Med in Naples, the U.S. Navy's Mediterranean communications hub. NCTAMS Med keyed the NTB, and this in turn was rekeyed via a host of NATO and national comms circuits as needed. Figure 3 shows FOTC's delivery of the organic RASP data to FOSIF Rota, and FOSIF's transmission of the fused RASP sent as the NTB data stream.

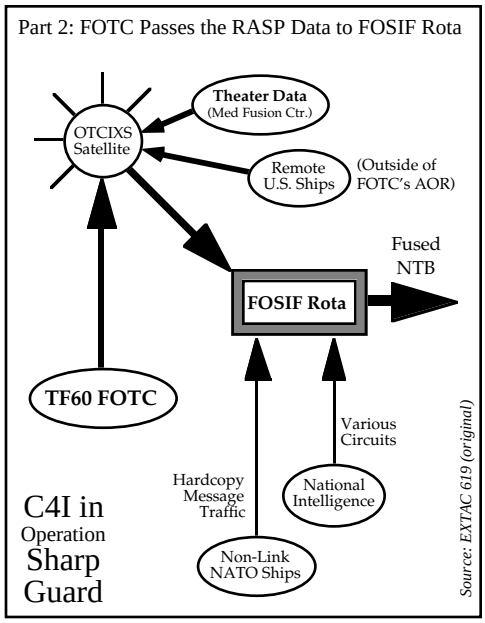

Figure 3 – Sharp Guard C4I (Part 2)

If Operation Sharp Guard provided significant impetus for a revolution in maritime C4I, then it was the scheduled live exercises that provided opportunities for more deliberate testing and analysis of the new architecture as it evolved.

NATO Live Exercises in 1995

Strong Resolve 1995 was an extremely complex exercise from a C4I perspective. The North Atlantic CCIS, or NACCIS, was the communications processor used for the passing of RMP data, and SACLANT's serial, point-to-point NACCIS network was the exercise's medium of exchange. Both the GREEN and WHITE sides had afloat RMP managers who operated their NACCIS in the FOTC mode, and each side had one or more ashore fusion centers.

USS *Deyo*, at the tactical level, was tasked as GREEN force RMP manager and operated as a FOTC. USS *Mount Whitney*, at the operational level, further fused the data and then broadcast an RMP. SACLANT, at the strategic level and not a full-time exercise participant, also operated as FOTC and sent a broadcast. To complicate matters further, CINCEASTLANT's watchstanders managed the theater picture and sent their own broadcast, and the WHITE side had a similar arrangement. Finally, multiple directing staffs (DISTAFFs) in various locations each required both the GREEN and WHITE RMPs.

Procedurally, there was little in the way of formalized direction on reporting RMP data other than the mandated use of artificial, exercise flag codes (e.g., "XG" for GREEN, rather than "BE" for Belgium). Notably, there was no guidance on using data filters to keep out-of-area or very old data from being broadcast. There also was no NATO Standard Attributes Reference, or STAR, for use in assigning names to warship contacts, and no promulgated conventions for assigning names to unknown contacts.

The exercise did not go well at all. The lack of naming conventions meant that watchstanders assigned names to their contacts any way they saw fit, and this naturally resulted in multiple names being assigned to the same ship. (The original EXTAC 619 contained the needed naming conventions, but it had not been fully promulgated as of SR95.) The use of exercise flag codes resulted in duplicate tracks—one with the real flag and one with an exercise flag—that further corrupted the track databases. Stations with no value to add mistakenly were tasked with sending both broadcasts and autoforwards of the same data—other stations' data—because this had not been properly considered prior to STARTEX, and the failure to use broadcast filters meant that days-old tracks and tracks from the East Med also were being broadcast. The multiplicity of database managers meant that everybody was *managing* everyone else's data, and the lack of unified reporting procedures meant that everybody was *broadcasting* bad data to everyone else. This resulted in rampant circular reporting and the "ping-pong" effect.

The C2 architecture used in Strong Resolve also was flawed. The use of NACCIS as the comms processor, with its limited capabilities in this area, meant that two-color support to DISTAFFs in many cases caused the compromise of one side's tactical data to the other side. Because the Radiant Mercury sanitizers located onboard *Mount Whitney* and ashore in Norfolk had not been programmed to accept and pass tracks with exercise flag codes, use of the exercise flags

resulted in an initial inability for U.S. systems to send exercise data to NATO (this was corrected). Finally, SACLANT's fragile NACCIS network as the C4I backbone resulted in repeated connectivity outages, often for 4 to 6 hours at a time. Many useful lessons were learned from exercise Strong Resolve '95. To summarize:

1. RMP operations at sea must be emphasized and should be fully integrated.*
2. An "Allied OPTASK RMP" is required to address afloat RMP operations.*
3. STAR data is required for every maritime exercise.*
4. Reporting procedures and look-up tables are required.*
5. Broadcast filters on track category, timelate and geographic area must be used.*
6. Exercise flag codes only institutionalize nonstandard reporting.
7. Exercise C4I play must be thoroughly considered in the planning process.
8. NACCIS operator training was poor; RMP management training is required.
9. The NACCIS network is inadequate; operators require more flexible and robust connectivity.

* - These items were addressed in EXTAC 619.

Linked Seas 1995 took place just a few months after Strong Resolve. The Linked Seas C4I architecture was vastly simpler than that of Strong Resolve because there was one participating node at sea, HMS *Chatham*, and one participating node ashore, CINCIBERLANT.

Simple it was, but the communications backbone was still the fragile NACCIS point-to-point network. EASTLANT was directly involved because all connectivity between *Chatham* and Iberlant went via Northwood and Oakhangar (see Figure 4). SACLANT was involved as an alternate path whenever the Iberlant-EASTLANT point-to-point line failed, but this "back door" was not available until well after STARTEX. But even with two paths available the connectivity was very poor because the lines and crypto routinely failed. The connectivity outages lasted sometimes for 12 hours; these continued until one of the staffs noticed timelates had grown surprisingly large, and the problems often could not be fixed until arrival of the day worker in Norfolk or Northwood.

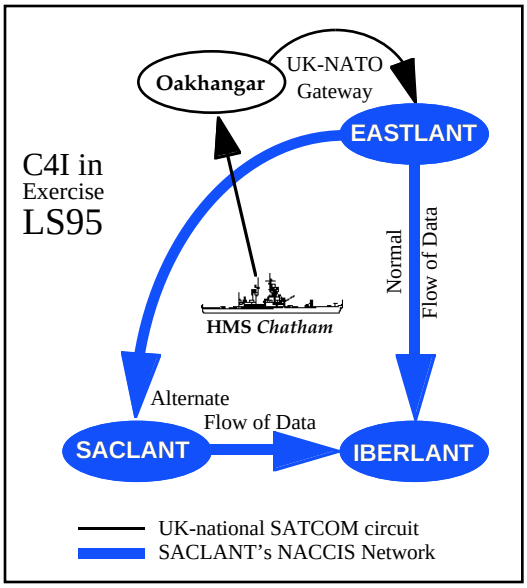

Figure 4 – Getting RMP Data ashore to the Operational Commander in Linked Seas '95

A key lesson was re-learned: the most urgent C4I improvement NATO operators require is a robust router-based wide area network (WAN) that immediately senses line or crypto failures, provides automatic routing via any available path, and guarantees a reliable delivery of traffic. Thus, the urgent operational need for some form of NIDTS-like connectivity was well established in early 1995.

A noteworthy success of Linked Seas was the first-ever demonstration of an "Allied FOTC" architecture. HMS *Chatham* operated as FOTC controller and CINCIBERLANT operated as FOTC participant, and everything worked as expected: tracks renamed, merged or deleted by *Chatham* were similarly renamed, merged and deleted at Iberlant. While the results were not surprising, one can never be sure until a function is proven to work. Allied FOTC worked.

NATO in 1995: An Interesting Revelation

This author analyzed exercises Strong Resolve '95 and Linked Seas '95 for SACLANT, wrote lessons learned reports on each, and came to a curious and somewhat surprising realization:

NATO in 1995 was in very nearly the same situation the U.S. Navy found itself during Operation Desert Storm

• ***Nonstandard Operating Procedures.*** Every regional or area RMP Manager made up his own operating procedures because there existed no guidance to help him develop procedures that were standardized with the rest of NATO.

• ***Ill-Defined Duties & Responsibilities.*** Strong Resolve was a mirror of what the U.S. Navy witnessed in 1990–91: stations received data from everyone else, manipulated the data as they saw fit, and then retransmitted the changed data to everyone. Furthermore, *strategic* commanders actively participated in the management of *tactical* data rather than leaving this function to those at the tactical or operational levels of command.

• ***Non-Robust Communications.*** SACLANT's NACCIS network routinely failed without warning. Very often the failure points were at nodes not participating in the exercise, so a fix could not be applied until the start of that staff's next working day. The fragility of this circuit was extremely frustrating to the operator: one could see how the system should work—how a wide-area RMP could provide timely situational awareness to his commander—but lines of communication simply were not up to the task.

• ***Poor Interoperability with Joint and Coalition Partners.*** Link 11 remained, for most, the one medium of tactical interoperability between ships at sea. But if data is to flow from the ships to the commanders ashore then the ships must be reliably connected to NATO tactical circuits; they were not. Furthermore, there was virtually no connectivity or interoperability with the air and land component commanders, or between the MCCIS other systems (such as Perseus).

NATO in 1997: A New Era in Allied C2

Exercise Linked Seas 1997 was a ground-breaking event in many ways. It was:

1. The first LIVEX to enjoy the benefits of robust connectivity brought about by NIDTS.
2. The first LIVEX to benefit from a clean separation of colors of data; that is, the ability to keep NATO-force exercise data separate from OPFOR and Real-World data.
3. The first time a shore-based MCCIS RMP Manager was fully supported by three sections of fully trained watchstanders.
4. The first LIVEX to promulgate an exercise standard attributes reference (STAR) and, thus, the first to benefit from common naming conventions.

The NIDTS Revolution. The NATO Initial Data Transfer System/Service (NIDTS) is the IP WAN that solved most of the recurring long-haul connectivity problems. NIDTS brings to NATO command and control the same capabilities and robustness that supports the millions of users of the worldwide commercial Internet:

- Reliable delivery of traffic,
- Automatic and transparent re-routing of traffic via any available path,
- Elimination of the need for exceedingly detailed MCCIS autoforwards,
- Line sensing to alert the CIS watches when continuity is lost, and
- Desk-to-desk (or server-to-server) electronic mail.

Long overdue but much appreciated by NATO's operators, NIDTS is a tremendous improvement as the C4I backbone for tactical connectivity between shore stations. (See Figure 5.)

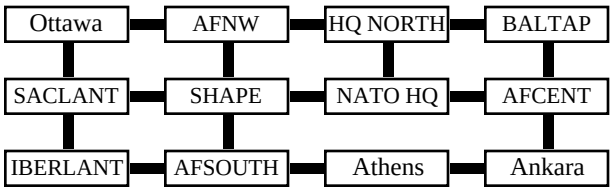

Figure 5 – The NIDTS Network

However, the current inability to extend NIDTS connectivity to ships at sea, due in part to their limited bandwidth capabilities, means that legacy national systems and connectivities are still a key part of the overall architecture (see Figure 6). These systems somehow must deliver data to a NIDTS node if the data is to be shared. Thus, until afloat units are more fully integrated, this NATO architecture will never completely fulfill the requirement for a timely RMP delivered to shore commands. NATO IP connectivity to NATO flagships must become a near-term goal.

OPSEC in a Two-Color Exercise. CINCIBER-LANT and CINCEASTLANT succeeded, for the first time, in successfully maintaining operational security (OPSEC) between two colors of data in a live exercise. This resulted from the use of dedicated servers at both sites (for Real World, GOLD and SILVER) and by having NIDTS route

all track data directly to one of these three servers. This was a noteworthy achievement, because every previous live exercise that used a CCIS for C2 suffered from an inability to properly separate colors of data, with the result being badly compromised exercise OPSEC.

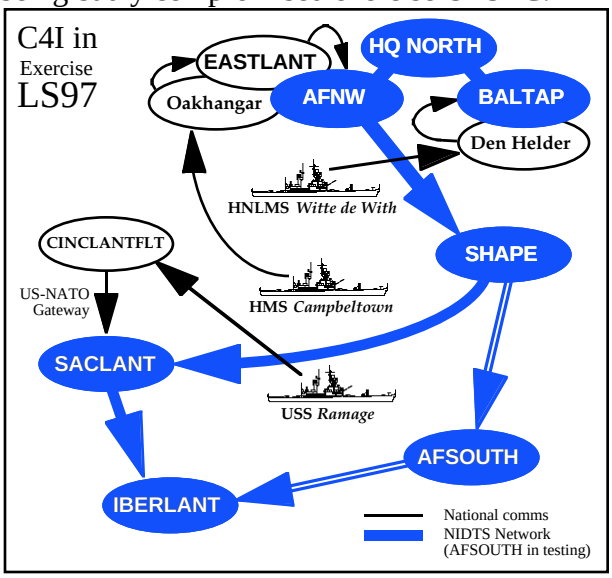

Figure 6 – Getting RMP Data ashore to the Operational Commander in LS97 (via NIDTS)

Color separation has been so difficult in the past because MCCIS and SACLANT's old NACCIS network were designed for the real world: with NATO operating on one side of crypto, and the opposition on the other side. The system and architecture were not designed to support two colors of data on the same crypto or carried on the same physical point-to-point network.

NIDTS helps divorce the tricky color-separation functionality from the CCIS and gives it instead to the routers. Whereas the communications capabilities of MCCIS are rudimentary at best, routers are devices specifically designed to manage the delivery of message traffic. Clever IP addressing is used to establish logically discrete broadcasts for data of a given color: BLUE data is sent only to BLUE servers and it never gets anywhere near an ORANGE server.

Networks prior to NIDTS were not able to carry discrete color-based broadcasts, but today NIDTS permits any number of logically discrete broadcasts over the same physical lines. This leap in architecture design, from MCCIS-based connectivity to router-based connectivity, is revolutionary and will significantly improve every future two- or multi-color NATO exercise.

Exercise STAR. For the first time in a LIVEX a Standard Attributes Reference (STAR) was prepared, approved by the nations and promulgated by signal to all participants. This gave every ship and station the exact format of the "contact" line of a MCCIS's Gold message for every participating ship in LS97. But how important is this?

Database problems and ambiguous tracks result whenever contacts are improperly named, or whenever operators pick names at random, or whenever names are assigned according to nonstandard local custom. For example, the "CTC" line for the Portuguese oiler *Berrio* reads as:

CTC/TXXX/ROVER-BERRIO//AOL/NAV/A5210/PO

If instead of "Rover" the class name is listed as "Blue Rover" or "Berrio" then an ambiguity would result, a purple track would clutter the display and the database would be degraded. The same is true if the ship's type is listed as "AO" or "AOR" instead of "AOL", or if its hull number is listed as "5210" instead of "A5210." Is the flag "PO" or "PT" or "XG"?

Non-ambiguous track naming is central to the problem of maintaining an accurate contact database on MCCIS while moderating the workload of the database managers. A primary function of an RMP database manager is to resolve ambiguities, but when ambiguities keep reappearing because of nonstandard naming conventions, or when exercise flag codes and real-world flag codes are both used and duplicate tracks result, then the RMP Manager's full-time task is to fix or eliminate this bad data. The RMP manager cannot tend to other more useful functions when he spends all his time resolving recurring ambiguities and merging endless numbers of duplicate tracks.

This poor use of a watchstander can be remedied through development of an agreed STAR and it's online integration within the MCCIS software. In the interim, this problem is easily remedied through promulgation of an exercise STAR just prior to every maritime exercise.

Trained Watchstanders. The full-up manning of three sections of trained RMP database managers was another noteworthy success first achieved in LS97. Two sailors per section managed Iberlant's RMP: one for the friendly force database and one for the intelligence (OPFOR) database.

This had the significant benefit of relieving the relatively untrained watch officers from performing these functions and permitting them to devote time to more appropriate functions (such as evaluation and assessment, the preparation of tasking directives and flag officer briefings).

The availability of sufficient numbers of fully trained watchstanders, along with the standardization of ship naming conventions, were very successful in terms of limiting the number of ambiguous contact reports and lessening the workload on the watchstanders. Together, these two achievements materially improved the headquarters' conduct of Linked Seas 1997.

The Joint Warrior Interoperability Demonstration (JWID) of August 1997 integrated all participating units and stations into a single Coalition WAN (CWAN) that shared track data with coalition partners world-wide. JWID showed that WAN connectivity can be achieved independent of path as long as all nodes have routers and all can work at the same level of classification.

The Way Ahead

MCCIS and NIDTS are remarkable successes and noteworthy achievements. Beyond evolutionary, this new architecture is truly revolutionary; but the revolution is not complet. As **highlighted** at the beginning of this paper in Table 1, there remain several holes in NATO's C4I architecture that still must be addressed. These are reviewed below as issues and recommendations.

Manning the RMP Desk

Issue: MCCIS and NIDTS are successes, and together they form two of the three necessary pillars of a viable maritime C4I architecture: the missing pillar is fully trained watchstanders. (Note Figure 7 on the next page.) Perfection will never be achieved: ambiguities and duplicate tracks always will exist, and databases will never be able to manage themselves. Because of this, trained watchstanders are always needed if RMP management is to succeed. The personnel and staffing issues are distinct from the training issues, but both are important. It is appropriate to reexamine headquarters manning in light of the new systems and architecture because, as discussed earlier, the management by computer of a track database requires a different skills set from what was required of the manual plotters of old. Further, it must be recognized that RMP management is an operational and war fighting support function, even though the term "database manager" suggests the function is clerical or one of system administration.

Recommendation: Each MCCIS command's peacetime and wartime manning documents should be revised in order to dedicate proper levels of manning to support the operational command and control requirements of the new NATO C4I architecture. RMP management should be performed by operators who have been to sea and who understand datalinks, tactical plots and the requirements for providing timely situational awareness. RMP management should not be performed by system administrators, LAN managers, UNIX experts, software troubleshooters or communicators *unless they have received the proper operational training.*

RMP Database Management Training

Issue: Each year NATO's scheduled exercises are supported by more and more C4I-fitted ships (only one in LS95, but about twelve in LS97), so the need for RMP Manager training exists and is becoming more urgent. SACLANT's MCCIS curricula do not address the operational aspects of managing a tactical database or performing the functions of RMP Manager. The existing "operator" course, and the contractor-provided on-site training (usually given just prior to and during exercises), only emphasizes the most rudimentary aspects of button-pushing and pull-down menus. They teach the simple functioning of MCCIS, but not its proper use in an operational setting. They teach how to merge and delete tracks, but not when and why to do this (or when and why ***not*** to do this). They teach the mechanics of setting up filters and broadcasts, but they fail to explain how and when to do this in an operational scenario. Moreover, they do not teach the FOTC mode of operation: when FOTC should be used, how it is used, the purpose and use of FOTC SITREPs, and the duties and relationships of FOTC and the Link 11

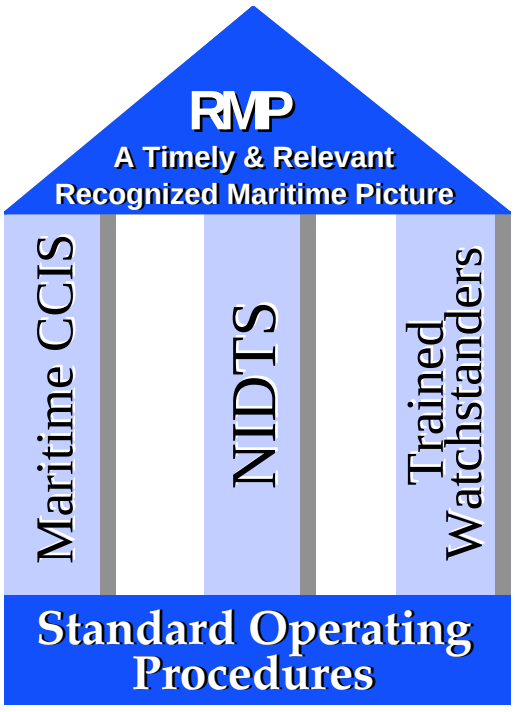

Figure 7 – Three Pillars of the Architecture supported by Standard Operating Procedures

Force Track Coordinator. (The current EXTAC 619(A) fails in all the above as well.)

Recommendation: MCCIS training programs must include a course of hands-on instruction dedicated to the operational requirements of managing a tactical track database at sea (with Link 11) and ashore (without Link 11). Clearly, this course should be developed and taught by suitably experienced people. Further, all course curricula should be available via world wide web access in order to facilitate self training by users with some previous knowledge and experience.

RMP Standing Operating Procedures

Issue: Standard operating procedures are the critical foundation for the three pillars of the new architecture (see Figure 7). Agreed procedures are the mechanism by which the architecture is made to function smoothly and efficiently. Put simply, no SOP exists at present. SACLANT's EXTAC 619(A) purports to be this SOP but it is nothing of the kind. EXTAC 619(A) contains no operationally relevant guidance or direction and, in fact, it is little more than lists of things for the operator to consider. It fails to address afloat operations, and it eliminates the useful look-up tables and naming conventions needed to report contacts and manage a database (information that was contained in its predecessor EXTAC). Unless this is corrected, the reporting chaos witnessed in 1995 will recur in 1998 because there exist no unifying procedures to orchestrate how RMP management should be performed.

Recommendation: Some form of RMP standard operating procedures is urgently required prior to exercise Strong Resolve 1998. A major revision, perhaps an EXTAC 619(B), also is required.

Extending the Architecture

Issue: NATO's primary focus to date has been to interconnect its shore commands, but now greater attention must be given to integrating the tactical forces at sea. All timely track reporting originates from the operating forces and their tactical datalink, so neglecting C4I for afloat operations dooms the shore commander to a time-late RMP. Further, the connectivity that exists today between NIDTS and ships at sea is via national C2 systems, gateways and firewalls. JWID '97 demonstrated a better way: direct router-based connectivity into a multi-national WAN that bypasses national gateways. Figure 8 attempts to predict a future architecture.

Recommendation: The nations should equip and man their ships—at least their flagships—so they are able to participate in this revolution in maritime command and control. In order for these ships to fully participate they require the same three pillars of the architecture: connectivity into NIDTS, an MCCIS or compatible device, and sufficient numbers of trained watchstanders. Whenever possible, flagships sailing under NATO OPCON should establish an unbroken IP connection directly into NIDTS (and all the various security issues also must be resolved). Future NATO operations should be conducted via a CWAN-like network rather than via today's uneven patchwork of serial national connections into various NIDTS gateways.

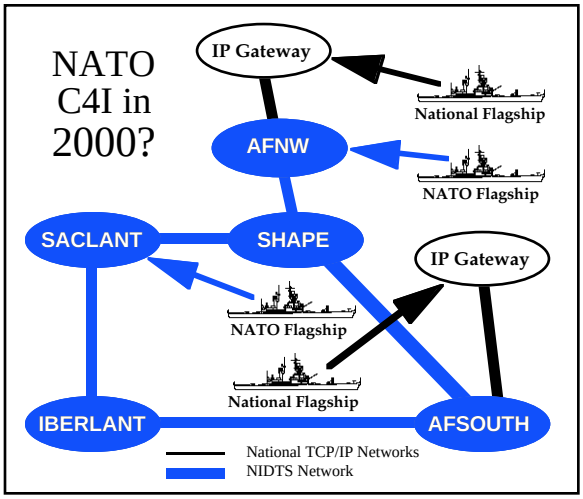

Figure 8 – Connectivity to NATO Flagships and Seamless National Gateways into NIDTS