10th International Command and Control Research and Technology Symposium
The Future of C2

Net Centric Maritime Warfare – Countering a 'Swarm' of Fast Inshore Attack Craft

Authors:

David Galligan
Defence Technology Agency
NZ Defence Force
Naval Base Private Bag
32901, Devonport,
Auckland, New Zealand
☎ IDD 64 9 445 5847
Fax IDD 64 9 445 5890
d.galligan@dta.mil.nz

George Galdorisi
Office of Science,
Technology and Engineering
SPAWAR Systems Center,
53560 Hull Street
San Diego CA 92152-5001
United States of America
☎ IDD 01 619 553-2104
george.galdorisi@navy.mil

Peter Marland
Defence and Science
Technology Laboratory
Dstl Portsdown West
Fareham, Hampshire,
PO17 6AD, United Kingdom
☎ IDD 44 2392 21 7734
Fax IDD 2392 21 7900
Pmarland@dstl.gov.uk

All the authors are affiliated to TTCP MAR AG-1. Peter Marland is the nominated single point of contact for ICCRTS.

Abstract

This paper reports the experience of TTCP MAR Action Group 1 on Net-centric Maritime Warfare, where one study addressed defence of a maritime force against swarm attack. A significant and emergent threat in the Littoral is from Fast Inshore Attack Craft (FIAC). These range from leisure craft (like 'Jetski's'), up to small Fast Patrol Boats. Their armament ranges from suicide bombs, through crew served weapons, up to larger anti-tank missiles. These all pose a significant threat to Coalition units. The innovative aspect of the FIAC's operations are the potential use of swarming tactics, where larger numbers of vessels carry out an attack which 'mobs' the target. This asymmetric warfare uses a low technology approach to overcome higher level Coalition technology, by saturating the defences.

The study used New Zealand's MANA agent based distillation model to represent the C2 and sensor interactions between Allied units, and separately between the units of the attacking force. This has shown the degree of improvement possible via surveillance and targeting, indicated the point at which the battle must be moved 'offshore' using either a helicopter or UCAV, and has provided guidance on tactics and procedures. The work has been acclaimed, and the Action Group members are the recipients of an outstanding achievement award from TTCP.

Release Statement. This document contains information that was originally provided to the Governments of Australia, Canada, New Zealand, the United Kingdom and the United States under The Technical Co-operation Programme (TTCP).

This paper contains (UK) Crown Copyright material. The paper is open releasable, and may be reproduced without further enquiry, provided the source is acknowledged. However the views expressed are those of the authors and do not necessarily represent their National governments or Departments/Ministries of Defence.

The contribution made by all the authors of the original TTCP paper should be also acknowledged, in particular to: Ian Grivell and Mathew Fewell of DSTO Australia, Bob Burton of DRDC Canada, and Ralph Klingbeil of NUWC Rhode Island.

Overview

1. Battlespace control near land is essential to ensure prompt access and freedom of manoeuvre for coalition forces moving from the sea to objectives in the near shore area of deep inland [*]. As naval forces from nations committed to the rule of law operate in littoral areas, potential adversaries are responding with innovative, often asymmetric approaches to coastal naval warfare [†]. A number of coastal nations – several of which sit astride strategically important waterways – are exploiting small boat warfare and integrated coastal defences to blunt, neutralise or defeat larger navies operating in the near shore area.

2. The tactic that appears to have the most traction with these nations is that of 'swarming' attacks by large numbers of inshore attack craft. There is no readily definable criteria for these craft – they can be as small as recreational vehicles such Jetski's and as large as a naval or coastal patrol fast patrol boats. Nor is there just one type of 'swarming' attack. Attacks can come from multiple axes. The navies of coalition nations have conducted numerous studies and analyses to begin to come to grips with dealing with the threat of swarming small boat attacks. In one study for the US Navy, an industry team found that different types of threat platforms had different effective weapons ranges. The study grouped these into two general categories; small threat platforms (cigarette boats, Boghammars and others) with a maximum effective weapon range from 0.1 to 0.5 nm and larger naval vessels such as advanced patrol boats carrying short-range guided missiles.

3. While a number of studies did not discount swarming attacks by larger vessels such as advanced patrol boats, they focused heavily on swarming attacks by very small craft as the predominant scenario that coalition navies operating in littoral waters would have to deal with. The consensus of a number of studies and the opinions of serving naval officers appear to converge and focus on primary threat of massed, small boat threat; that consists of 10 to 20 high-speed manoeuvring boats attacking over a 20-degree to 60-degree azimuth sector. The boats have a simultaneous arrival time with closing speeds of 35 knots. Their manoeuvre is typically in a sinusoidal path. The small boats are considered to be commercial types with no real distinguishing feature to support easy classification. Identification of the attack results from the characteristic behaviour of a large number of high speed, radially inbound boats.

4. The threat of swarming small boats is not a new one. For a number of years, work in Naval laboratories focused on the small, fast, manoeuvrable boats as the primary threat elements. These reports indicated that forces must be capable of engaging small coastal naval combatants such as patrol boats and guided missile corvettes or other smaller boats. Reports noted that boats could be operated in an unpredictable manner and under unexpected conditions. These reports concluded that these craft may appear as part of the normal friendly or neutral traffic in the area, which makes them all the more difficult to counter. Industry reports provides numerous examples of observed and reported naval exercises by rogue nations that demonstrate their willingness and ability to surreptitiously get inside the effective maximum range of a larger naval force's surface weapon systems.

5. The nature and the magnitude of this threat has riveted the attention of coalition navies who recognise, in general, that a co-ordinated response from networked coalition naval assets is the optimal way to defeat this threat. In an article in the *US Naval Institute Proceedings*, the incoming US Chief of Naval Operations opined:

> "Small, fast enemy surface combatants represent another threat to operations in geographically confined areas, where their size and the surrounding clutter of geography and traffic make long-range detection difficult … A diverse force, networked with distributed

* Sea Power 21: Projecting Decisive Joint Capabilities (Washington DC, Department of the Navy, January 2005).

† Owens Sirrs, Operational Art Can Neutralize the Asymmetric Small Boat Threat in Major Operations (Newport, Rhode Island, Naval War College, February 2, 2002).

sensors, offers promising response capabilities once enemy vessels are under way" [‡]

While this swarming small boat attack threat has been discussed in professional journals and discussed in depth in various studies, to date, there has been little quantitative analysis to determine the extent to which networking coalition naval platforms can begin to deal with such a threat. Further, we believe that there is no extant, standing, *international* team of likely coalition partners that has begun to analyse this threat, identify potential solutions, and quantitatively define the benefits that would accrue in various scenarios when coalition naval ships, operating in a robustly-networked environment, take on this threat.

Introduction

6. This paper reports on the experience of TTCP MAR Action Group 1 (TTCP MAR AG-1) which covered the topic of Net-centric Maritime Warfare, specifically the workstrand addressing analysis of the defence of a maritime force against swarm attack. The work has been recognised in multiple fora. The study characterises the degree of networking between members of a Maritime force, and used the MANA intelligent agent based distillation model to represent the C2 and sensor interactions between Allied units, and separately between the units of the attacking force. This has shown the degree of improvement possible via surveillance and targeting, and indicated the point at which the battle must be moved 'offshore' using either helicopter or UCAV.

7. **Background.** A significant and emergent threat in the Littoral is from Fast Inshore Attack Craft (FIAC). These range from leisure craft (like 'Jetski's') with a single crewmember, up to small Fast Patrol Boats that have sensor and weapon suites, with sufficient crew to remain at sea overnight. Their armament ranges from suicide blast bombs, through crew served weapons, up to bombardment rockets and the longer-range anti-tank guided missiles. These all pose a significant threat to Coalition units, illustrated by the damage to the USS COLE shown in Figure 1:

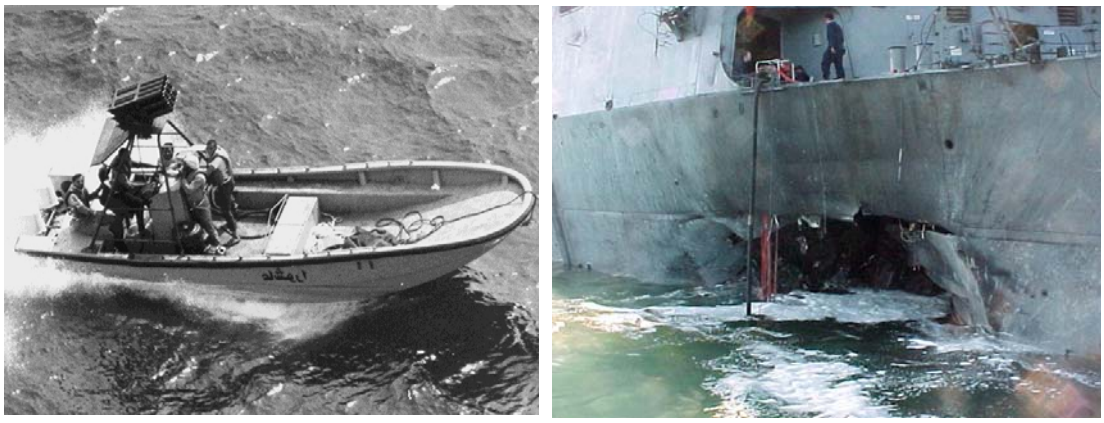


Figure 1 – Example of FIAC and of the damage caused to USS COLE

The innovative aspect of the FIAC's operational concept is the potential use of swarming tactics, where larger numbers of vessels carry out an attack which 'mobs' the target. This asymmetric warfare uses a low technology approach to overcome higher level Coalition technology by saturating the defences

‡ Vice Admiral Mike Bucchi and Vice Admiral Mike Mullen, "Sea Shield: Projecting Global Defensive Assurance," *US Naval Institute Proceedings*, November 2002, pp56-59.

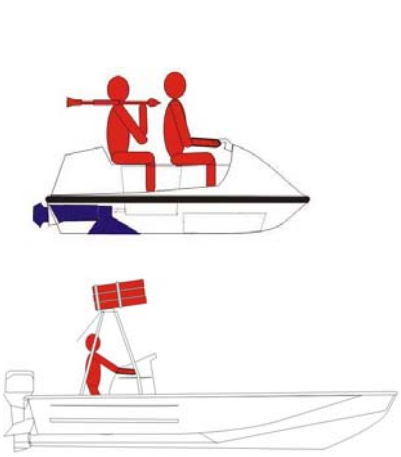


Figure 2 - Artists Impression of FIAC, and of a 'Swarm'

8. The FIAC target classes fall into three broad groups:

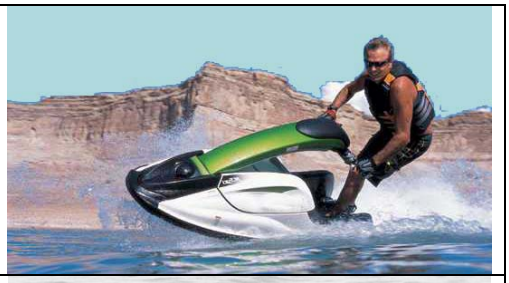
Type 1	Jetski or Boston Whaler with Rocket Propelled Grenade (RPG) weapons or a large blast bomb used in a suicide attack. Credited with a firing range of 3-500m, at which point the enemy is assessed as a 'leaker', who has achieved their mission objectives by inflicting damage on the Coalition force.	
Type 2	Larger 'Boghammer' class boat with an unguided multiple launch bombardment rocket, or a larger anti-tank guided weapon with a launch range of 8km, at which point it then becomes a 'leaker'. The craft has weather protection and accommodation. The small crew allow it to remain at sea overnight.	
Type 3	Small Fast Patrol Boat (FPB) typified by Super Dvora, with smaller anti-ship missile or torpedo armament, and degree of sensor and Command and Control (C2) fit. Weapon ranges of 4 km (torpedo) out to 15 km (ASM) The vessel has more endurance than Type 2, allowing mission duration's of several days.	

Table 1 - FIAC Classes

These characteristics also affect the number of targets present in an encounter, ranging from 10-50 of the smallest class, through 5-10 of the medium type, and only 1-5 of the smaller FPB which represent small warships.

Early Work

9. The AG-1 remit was to investigate possible Network-Centric measures to overcome the

challenge, using operational analysis to quantify the outcome. The problem was defined by very short surveillance (detection) ranges due to the small size of Type 1 FIAC, and even shorter identification (ID)/classification range. These are very scenario/environment dependent, and ducting conditions may hamper ship-mounted sensors. These factors, plus current Rules of Engagement (RoE), ensure that engagements are now conducted at 'whites of the eyes' ranges well inside potential enemy weapon launch range.

10. The FIAC/SWARM study was initiated in April 2003, and AG-1 took the decision for a broad three-level modelling approach using the following tools:

- Canadian 'simple' spreadsheet, plus the US Queuing Theory (QT) models
- New Zealand MANA model
- UK Threedim model

The platforms likely to be involved in the modelling include some high value units, their escorts (one or two destroyers or frigates (DD/FF)), some airborne assets (helicopter or UAV) the opposing forces, and background or neutral shipping. The 'three-tier' approach was to provide depth and a degree of validation & verification; it was not clear at the outset whether the spreadsheet and QT models might (through meta-modelling) over simplify the problem. However there was some confidence in MANA's strengths as an intelligent agent model to represent swarming aspects, whilst Threedim (as a fully featured battlemodel) had the ability to model at greater fidelity, including weapon system arcs, but with a simpler (i.e. dumb) target set. The strengths and weakness are shown in Figure 3 below:

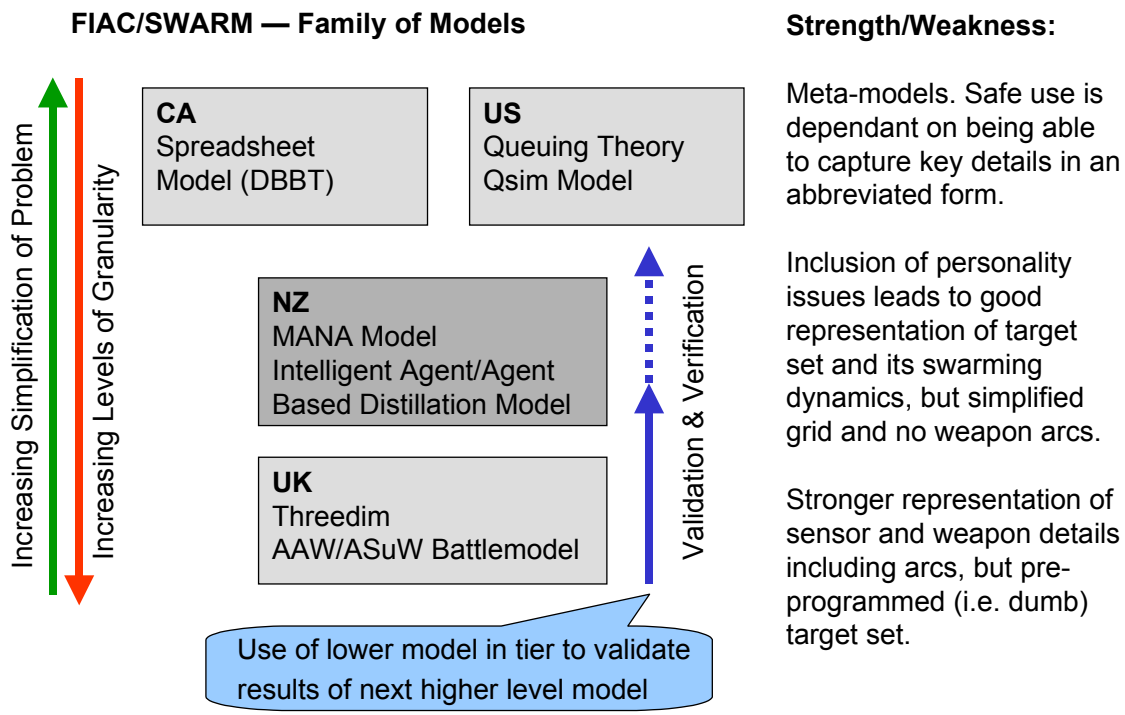


Figure 3 - FIAC/SWARM Modelling Strategy

11. The UK modelling workshop was held in the fall of 2003 with representatives from all five TTCP member nations. The characteristics of FIAC and defensive systems were presented and discussed along with the operational realities of swarm engagement, using experts from the UK Maritime Warfare Centre at HMS DRYAD. The study hypothesis was reviewed and it was agreed that it captured the essence of the analysis problem:

> "In an ASuW swarm attack, Blue shared situational awareness and an associated sensor-to-effector capability reduces the number of leakers against Blue assets."

Four concepts were developed based on discussion and analysis conducted during the workshop:

(1) Current capabilities, (2) Improved target indication using third party information and network linkage back to the shooter, (3) Improved helicopter ISR, weapons and network, and (4) Distributed networked mobile sensors and weapons. These were then mapped onto increasing levels of 'networking.'

12. **Structuring the Problem Space.** The Network Centric Maritime Warfare (NCMW) options for the FIAC/SWARM study include the following cases, with varying degrees of 'networking':

- **Baseline.** No communications or networking between units. This is not realistic, but sets the basecase for proper comparison between options, by reducing the force to a collection of 'singleton' ships that cannot act in a co-ordinated manner.
- **Low.** Shared situational Awareness (SA) but with organic targeting
- **Intermediate.** Shared situational awareness and organic targeting (as Low case), plus reachback to Intelligence information
- **High.** Shared situational awareness, organic targeting and reachback to intelligence information (as Intermediate case) plus inorganic (i.e. offboard) targeting.

The problem space for the modelling is defined as a matrix, shown in Figure 4 below:

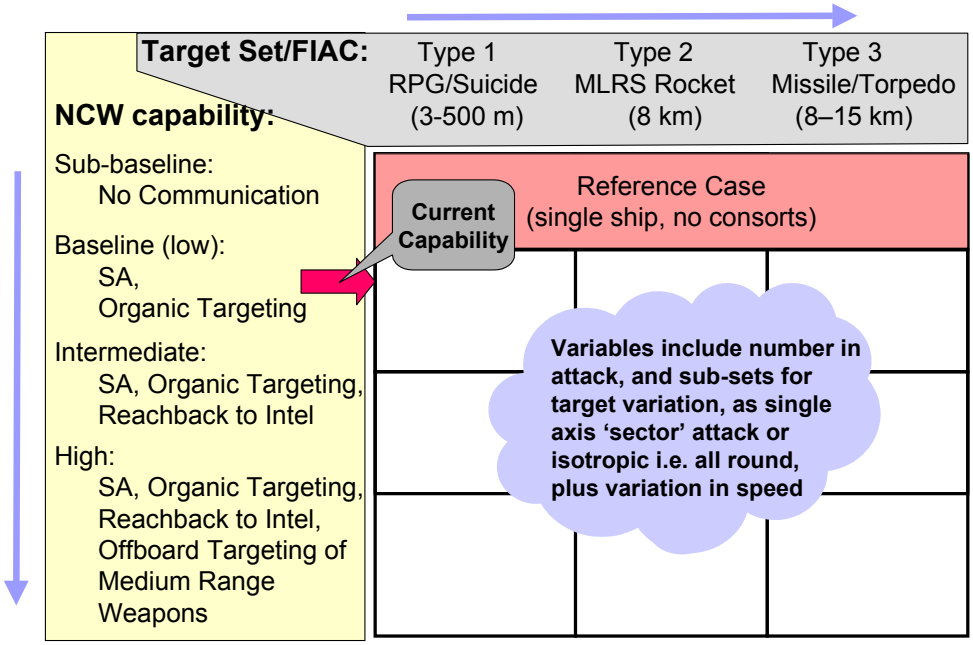


Figure 4 - Problem Space and Structuring

13. **Metrics and Presentation of Results.** It is important to define suitable measures of effectiveness (MOE) for the purpose of determining the effect NCW has when it is used in the swarm attack scenarios. The following MoE's were adopted:

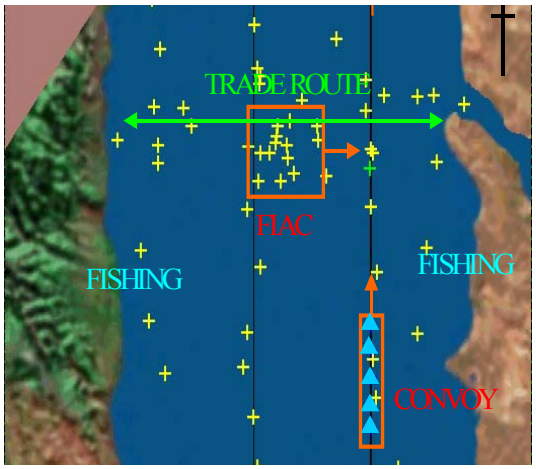
- The fraction of Red threats that come within their weapons range of the HVU.
- The probability of at least one Red threat reaching its leaker range of the HVU.
- The number of naval vessels that suffer defence capability-kill [§] ('soft-kill') while defending the force.
- The number of neutrals inadvertently destroyed, i.e. 'collateral damage' (only relevant when inorganic weapons targeting is used).

The results were generally presented as graphs of the probability or number of leakers, versus the weight of attack. Where available, the standard errors in the average MOE value were used to

§ A naval vessel is defined here as being defence capability-killed if it has sustained sufficient damage so that it cannot continue to defend the HVU. Examples of such damage could include disabled sensor and/or weapons systems.

provide uncertainty estimates for them. Error bars were used to display these uncertainties, but in many cases the uncertainties were sufficiently small that the error bars may appear not be present. It should be noted that the particular setup of a scenario might be a source of a higher level of uncertainty than is implied by the error bars.

14. Initially, comparison data was computed using both MANA and Threedim to obtain a baseline estimate of defensive capability. An example of the MANA model is shown below. MANA's strengths are in representing the personality that drives the swarm's dynamic tactics, rather than as a rigid target set. The agent based distillation model is suitable for this type of Net-Centric warfare analysis, in that it represents complexity and emergent properties.



Tacsit: Blue force in confined sea room is attacked by a swarm of FIAC.

Metrics:

- Probability of one or more FIAC reaching firing position against HVU.
- Fractions of FIAC leaking, and of Blue escorts damaged.
- Collateral damage.

The study has represented four levels of Blue networking capability.

Overall, Intermediate and High levels of networking considerable increase Force survivability.

Figure 5 – MANA ASuW/SWARM Tacsit

The results between MANA and Threedim were generally consistent for the single ship, sector attack comparison case show above. Where there are small discrepancies, these are explainable by the differences in granularity of both models. MANA is more optimistic than Threedim due to lack of weapon arc constraints and coarser definitions; as an example, Threedim has variable slew time for Blue units, versus MANA's use of a single figure.

15. **Summary.** During the initial modeling work, the basecase results with Point Defence and Improved Target Indication (TI) for a single-sector attack (using close range guns and various permutations of gun range and slew times), show that:

- Current point defence systems can be overwhelmed by a relatively small number of FIAC.
- The key drivers are FIAC speed, rate of Blue weapon fire determining the number of shots before Red fires, and the effective range difference of Red and Blue weapons.

The results were sufficiently in agreement, such that we decided to use MANA as the principal model to analyse swarm attacks for the remainder of the study, which was carried out in Australia in Spring 04. This is described in more detail below.

The MANA Model

16. MANA is an agent-based distillation model (ABDM) in which each agent is endowed with particular properties and with personality traits that guide its actions. These properties and traits change depending on events that occur while the model is running. MANA is a time and space based model. It performs appropriate moves and other actions, such as firing weapons, at each time step for each agent. Scenarios are modelled on a two-dimensional model grid. The aim of the MANA approach is to distil a scenario down to its essential parts and then to only attempt to model these. MANA is not a detailed physics based model. Instead, it relies on performing a large number of model iterations of each scenario to determine average values for output parameters of interest. Because MANA relies on relatively simple algorithms, it is computationally fast to run and therefore a large number of iterations can be made on a scenario. This speed also allows the

user to pose 'what if' questions to help investigate the influence different parameter-value assumptions have on the outcome.

17. **Key Features.** Version 3 of MANA was used, and included a number of improvements that made it particularly useful for modelling situations involving Network Centric Warfare:

- **Event-Driven State Changes.** Agents have greater than 50 user-selected states available that they can change into depending on events that occur. Events include taking a shot, being shot at, refueling, being refueled, reaching a goal and contacting an enemy, either directly, or on a situational awareness map. When agents change states, all of their properties and personality traits can change. Typical changes include a variation in the agent's speed, their affinity for movement towards enemy contacts, and the lethality of their weapons. Agents begin in a default state and they return to this in the absence of an alternative after they leave their current state. It is possible to prioritise the state that the agent changes into on a given step. This allows the analyst to specify a preferred choice of state when there are several possibilities in a single model step.
- **Situational Awareness.** Squads in MANA are used to group agents with homogeneous characteristics. MANA maintains two situational awareness (SA) maps for each squad. A local squad map retains a memory of all contacts seen by the squad members. Similarly, an inorganic map holds a memory of contacts passed on from other squads. Contacts stored on each map are labeled as unknown, friend, enemy or neutral, as appropriate. Contacts persist on each map until a preset time has passed. Addition of particular contact types onto an SA map can be used to trigger a state change. An agent can have personality traits that cause it to move toward, or away from, specified SA map contact types. Weapons fire can be targeted based upon SA map information. When an agent's sensor detects a new contact it is added to the squad's local situational awareness map if a contact of the same type is not already within fusion radius of its position. Adding a contact to the local map causes it to also be added to relevant communications links attached to that squad. Such information is communicated to the squads on the other end of the communications link.
- **Communications.** Each squad can maintain a number of communications links with other squads. Such links provide conduits for the sending of contact information between squads. Figure 6 shows the communications link set up window for a typical link specification. It is clear that the parameters of the link can be intricately specified.

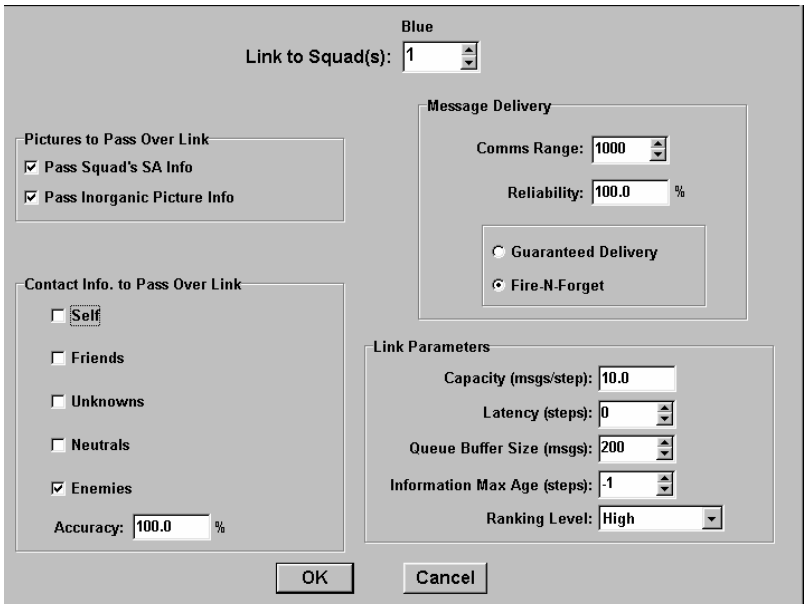


Figure 6 - Communications link editing window.

Bandwidth capacity and latency are key parameters that are often varied in communications studies. The accuracy parameter can be used to control the likelihood that the correct contact

type is sent. Messages can be passed off the squads local SA map or they can be derived from information that has been sent from other squads. The sending of information can be either via a 'fire and forget' mechanism or by guaranteed delivery; if a destination squad does not have an agent within the specified communications range then messages destined for that squad are lost unless guaranteed delivery is selected

- Figure 7 shows a simple example of using communications in a MANA scenario. The main MANA window is shown in the background. The scenario is set at sea and it shows a number of friendly vessels situated in the middle of the screen. A ship is waiting at the bottom to meet these ships, but it does not know where they will arrive from, or when; it has only very short-range sensors to assist it to find the fleet and these are inadequate in the sea area represented in the model. The vessel calls upon a reconnaissance aircraft to assist in its search:

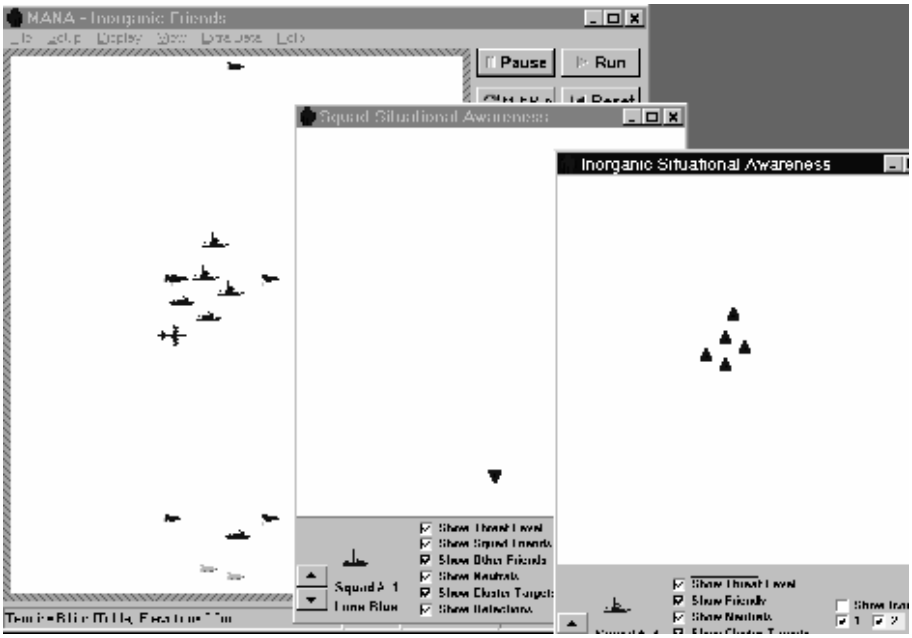


Figure 7: Guidance of a ship to friendly vessels based upon information supplied by reconnaissance aircraft. The three windows shown from left to right are: the main MANA window, the squad SA map and the inorganic SA map.

The aircraft flies a rectangular search pattern marked at the four corners by flags (only three flags are visible above). The aircraft has picked up all of the incoming ships at the time-step this snapshot was taken. The two foreground panels show the situational awareness maps of the search ship. It is clear from the ship's squad level map (labelled 'Squad Situational Awareness') that the only vessel it can see is itself (upside-down triangle). The 'Inorganic Situational Awareness' map containing data provided by communications link from the reconnaissance asset, tells a different story – there, the positions of all of the incoming ships are clearly marked. At the time shown, the search ship has just made a state change based upon the appearance of this inorganic contact information. The model continued to run after this snapshot, with the search vessel moving towards, and then remaining with, the incoming vessels.

- **Weapons Suite.** MANA provides a number of generic weapons for use in military modeling. There are two main types of weapons: kinetic energy and high explosive weapons. Kinetic energy (KE) weapons have a range-probability kill profile based on range measured from the shooter. Conversely, high explosive (HE) weapons measure their range for this profile from the target. Targeting can be off the agent's immediate situational awareness, or off either of the situational awareness maps. The location of targets obtained from the former is exact, while that obtained from the latter may suffer from map resolution aggregation issues, or from the movement of fast targets. Target prioritisation and Rules of Engagement (RoE) can be

represented.

- **Sensor Modelling.** Each agent has an ability to sense its environment. It has a specified detection range, within which other agents are detected, but not classified or identified. It also has a specified classification range-probability profile. On each time-step, detected agents are classified (as enemy, neutral or friendly contacts) if the probability of classification at their range allows them to be classified on that step. Classification range can be specified in a 'cookie-cutter' style as for detection range, if this is appropriate. Agents that are detected but not classified are recorded as contacts of unknown type.
- **Data Farming.** MANA includes the ability to perform simple data farming. This allows up to two parameters to be varied over a range of values for a squad, or a set of squads, in order to explore the sensitivity of the model to the particular value assigned to a parameter. This can be used to quickly explore the robustness of a particular scenario model, or to look for high-payoff areas for future optimization in the systems being modeled.
- **Terrain Features.** A wide variety of terrain's can be modelled in MANA. Terrain maps are used to control movement, sensing and shooting. Figure 8 shows the terrain map that is used in the current study. The black area represents 'billiard table' terrain, which allows complete freedom of movement, sensing and shooting. The grey area represents 'wall' terrain. Surface vessel agents cannot move through that terrain, neither can they sense or shoot through it, whilst airborne agents are free to move at will.

18. **Master Scenario.** The ASuW master scenario used as a basis throughout this report involves five ships (two naval and three high value units (HVU)) transiting in close formation through a narrow strait where a threat of unknown type is assumed. Each ship in the force is separated by 1.5 km and ships transit in a line-astern configuration [**]. The naval ships are located at opposing ends of the line of HVU and their primary duty is defence of the HVU. Type 1 FIAC are represented, and Figure 8 shows a screen shot from the MANA model:

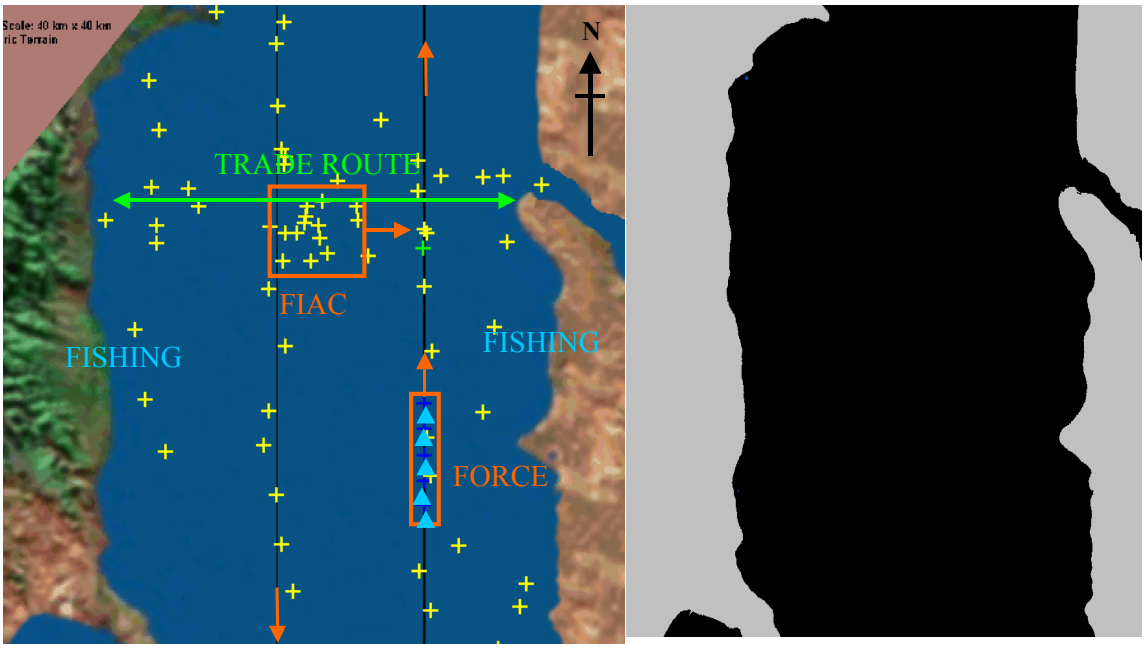


Figure 8 - MANA screenshots of master scenario (left) and terrain map (right).

The force travels in the Northbound shipping lane; blue triangles in the figure denote these. Neutral ships are shown as yellow crosses. These compromise coastal fishing vessels, cross-

** It is likely that closer formation (e.g. 750 m) of the force would lead to better outcomes for defence of the HVU at all levels of networking. However, owing to the difficulties in manoeuvring large civilian vessels, and the lack of training in military formation sailing, it is suggested that it would be problematic to allow these vessels to travel much closer than the 1.5 km used here.

channel fishing and trade vessels, and vessels transiting Southwards and Northwards in shipping lanes (left and right respectively). Type 1 FIAC are located as shown. Initially the FIAC appear as neutral vessels: this models their attempt to hide within the regular fishing and shipping traffic until they are triggered by the first HVU crossing the green trigger marker. Once triggered the FIAC form up into a tight swarm, at which point they move quickly to attack the force. When the attack begins their disposition becomes suicidal. A number of variations on this master scenario were explored. In particular: the tactical positioning of the naval ships was varied to simulate knowledge of the likely threat axis (or axes), consequences of such positioning based upon incorrect information were explored and the value-added obtained from adding information obtained from external ISR sensor platforms to the network was studied. Sensitivity analysis was performed to help understand how important the key parameter value assumptions are to the results obtained.

19. **Agent Settings.** A number of assumptions have been adopted for each of the active agent types in the scenario (neutral vessels, which are all set to travel on appropriate paths at 6 knots, are not detailed here). The active agents change state depending on events that occur. They remain in the default state until they are made aware of enemy contact, either through their own organic sensors or from inorganic information provided by friendlies over communications link. A 20 second pause has been set in the model between the time a naval vessel is made aware of enemy contact and when it enters the 'Enemy Contact' state: this allows for the necessary time-lag in communicating decisions on board a ship. Type-1 FIAC move about their initial positions with the same speed as the background vessels around them. They enter attack mode when they are triggered by actions of the force. Mainly they are triggered when the first HVU in the force crosses a designated point (the green trigger marker agent shown in Figure 8 in the shipping lane. Being shot at by the naval vessels in the force can also trigger the swarm – the naval vessels do not recognise FIAC as targets for this purpose unless aerial ISR assets have revealed their presence.

20. **NCW Capability Levels.** Four capability options were explored. These are:

- Sub-Baseline: Organic self defence (with no shared situational awareness).
- Baseline (Low): Limited shared situational awareness between platforms sufficient to enable co-ordinated action.
- Intermediate: Shared situational awareness sufficient to enable co-ordinated action at the unit level. Reachback capability available [††].
- High: Shared situational awareness sufficient to enable weapons targeting based solely on inorganic contact information.

While these capabilities are generic they can be linked with current and future networking systems. We attempt to relate some contemporary systems to these capability options. The sub-baseline case represents an instance where there is no communications capability at all; this provides a reference to measure the change in the effectiveness of the navy as networking capability is increased.

- **Baseline** NCW capability corresponds to a limited shared situational picture. Examples of the technology available at this level include secure voice, and HF/UHF radio. Baseline level NCW capability is the minimum likely in a network compatible coalition force.
- **Intermediate** level capability corresponds to the shared situational awareness available with the US's Joint Data Network (JDN), identified with force-wide tactical data links usually based on Link 16 [‡‡]. These networks have latencies measured in seconds and are used for tactical force control. The timeliness and accuracy of the situational awareness shared by an intermediate level capability system may in some cases be good enough to support targeting, where the weapon has target re-acquisition capability.

†† Reachback is the ability to access resources that are not locally available. This could include intelligence information obtained by communication with data sources located outside of the battlefield.

‡‡ Arthur K. Cebrowski and John J. Gartska (1998) 'Network Centric Warfare: Its Origin and Future', Proceedings. US Naval Institute. 124(1) 28–35.

- **High-level** capability option equates to that provided by the US Navy's Co-operative Engagement Capability (CEC). CEC produces a single multi-platform situational awareness picture fused from radar data obtained from each platform. The picture has latency at the sub-second level and sufficient accuracy to permit targeting and control of weapons. In the absence of a CEC-like capability, weapons can only be operated in a platform-centric mode, where weapon firing and guidance is only possible if the firing platform is tracking the target on its organic radar.

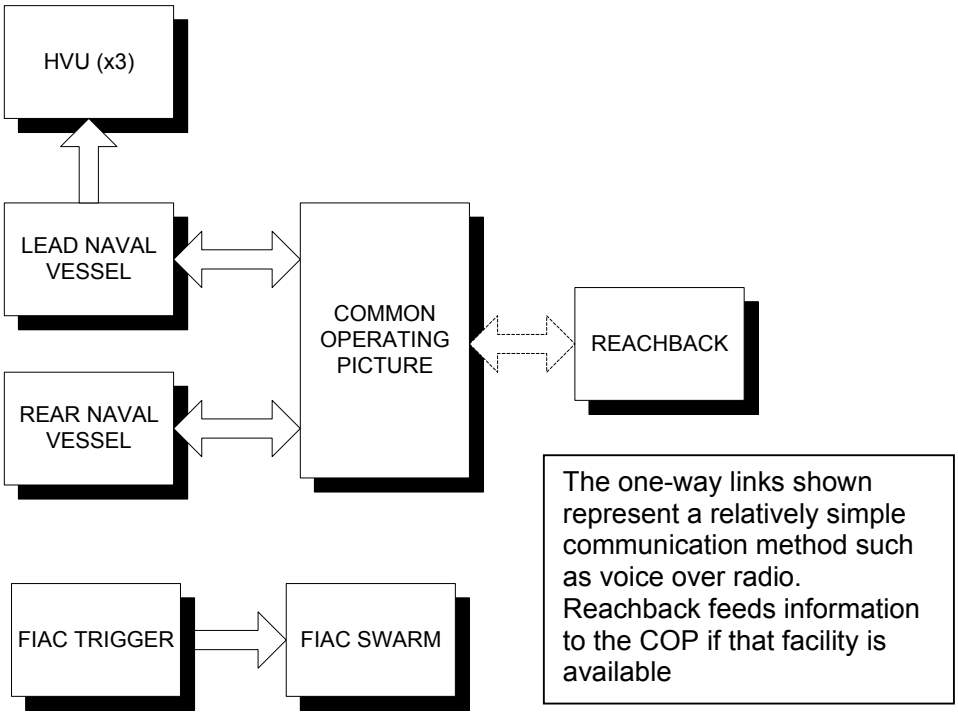


Figure 9 - Representation of the network.

21. **Networking.** The implementation of networking will vary from voice (plain or secure speech), to data exchange (via tactical data link), and transfer of digital files including imagery. The exchange could include record message (i.e. teleprinter traffic), but this has relatively little impact on this type of operation. In the FIAC scenario, the older tactical data links typically have net cycle times of 10-12 seconds, and defined message granularity with target positions from 10 to 500 m. It is possible to improve latency/accuracy by using a low latency link typified by CEC, however this system is optimised for AAW, and is relatively expensive. It would be possible to implement a Maritime Tactical Wide Area Network (TacWAN) using UHF line of sight communications that would provide latency of around one second for IP products. This performance is not in the CEC class (nor would it provide the same degree of ECM protection), however it is significantly more cost-effective; an exemplar would be the Tactical Component Network.

Results and Discussion

22. **Type 1 FIAC - Concentrated 'Sector' Attack.** The study has used the MANA model to represent the swarm's dynamic tactics, with four levels of Blue networking capability. The MoE is the probability of one or more FIAC reaching a firing position against the HVU, the fractions of FIAC leaking, and of Blue escorts damaged, and collateral damage. Sample results are shown below, with the 'gain' from higher levels of NCW highlighted:

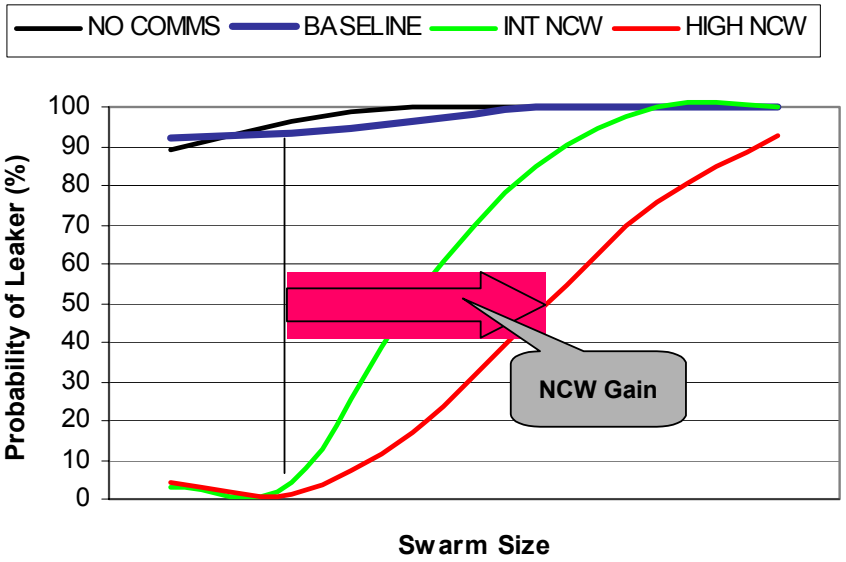
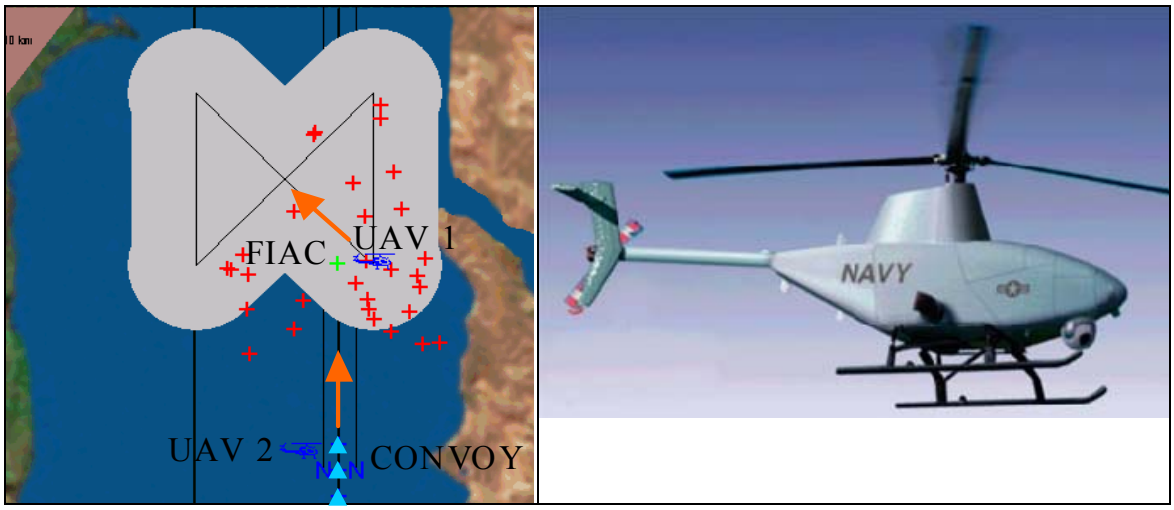


Figure 10 - Probability of at least one FIAC 'leaking' as a function of swarm size.

23. **Type 1 FIAC – Widely Dispersed.** For an 'isotropic' (i.e. a dispersed) attack, Blue relies on networking improvements and airborne ISR to allow use of existing weapons to medium range bracket to attack FIAC. With a very highly dispersed swarm, some FIAC fall outside the surveillance footprint. The trade-off between helo and UAV depends on size of threat surveillance area, driving the number of airframes required. The UAV capabilities were based on the USN *Firescout*, shown below. The results for the isotropic attack use both Green (intermediate level networking - surveillance ISR only), and Red (High-level networking - adds offboard targeting). The Blue curve shown below is a very highly dispersed swarm (over four times the previous area):



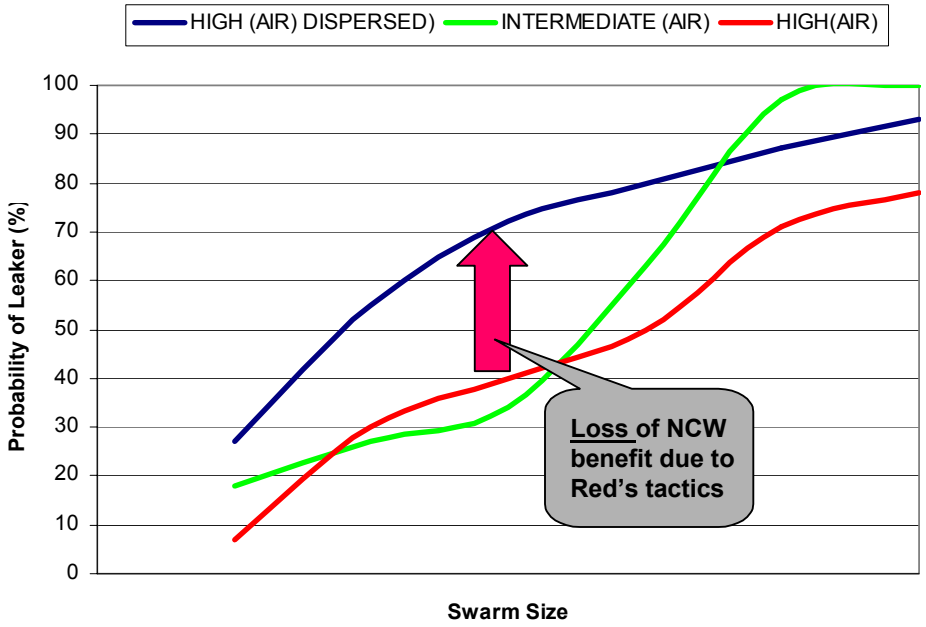


Figure 11 - Widely Dispersed FIAC scenario, Exemplar UAV and Results

24. **Type 2-3 FIAC.** Current defences are ineffective against Type 2 or 3 FIAC (whose 8-15km weapons outrange Blue CR guns). The force is assumed to face numerically fewer Type 2-3 FIAC, and the results are shown below. With networked Air ISR, if surveillance and weapon range exceed Red's launch range, the scenario is fully survivable (the blue curve), otherwise leakers are assured (the red line). The green curve is the marginal case, where ranges are equal. Networking improvements between Blue assets allow:

- use of existing MR guns to medium range bracket to attack Type 2 FIAC, plus smart rounds to maximum range, to provide cover against closer Type 3 FIAC.
- maximum use of armed helicopters/UCAV to attrite raids further out. This is the only counter to longer-range Type 3 attack.

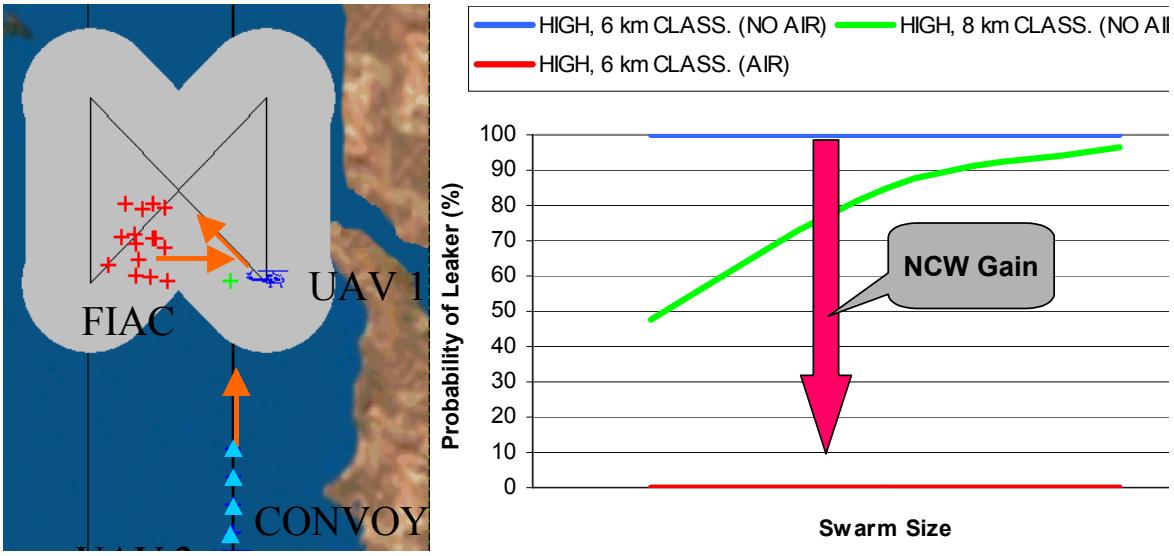


Figure 12 - Type 2-3 FIAC Scenario and Results

25. **Discussion.** The Type 3 FIAC armament was defined with a range of 8-15 km covering small torpedo, through to small anti-ship missile. These ranges were specified against particular specific threat weapons. In practice, there is a seamless transition from Type 3 into the smaller fast patrol boats with longer range weaponry, noting that this move away from 'visual' range

weapons, brings the Red forces all the problems of conventional naval warfare in terms of C2, surveillance and Over The Horizon Targeting (OTHT). For this region, the attack weapons can be handled by conventional ASMD or torpedo defence using countermeasures and decoys. Some authorities recognise this by defining a Type 4 classic Fast Attack Craft (FAC), also a Type 5 Light Corvette, through to a Type 6 Light Frigate.

26. **Operational Benefit.** The broad classes of operational gain from 'network enabling' forces, when compared to the baseline 'singleton' case are:

- **Better use of close range guns.** By meeting the RoE criteria for opening fire at the maximum useful weapon range, rather than a shorter range, once decisions have made by each weapon crew and ships command team. This would cover manually aimed ('crew served') weapons like the M-60 machine gun or 40mm grenade launcher, and 20mm and 30mm cannon, plus autonomous weapons like Phalanx Block 1B (with surface mode (PSUM), using an added electro-optic tracker). This gain is delivered by the locally networked common operational picture (COP) or recognised maritime picture (RMP)

  Note that these titles normally cover non or near-real time broadcasts, with significant latency, rather than the essentially real time tactical data link (Link 11-16) with a 10-12 second network cycle time. The solution would require a relatively high fidelity local picture, and that the defended group took a single corporate 'engage' decision, communicated to all units, removing individual sequential delays. These benefits expire at maximum Phalanx range, and there is no increase outside this range.

- **Use of Medium Calibre Gun to max range.** The escorts' medium calibre gun (a US 5"/54 or the UK 4.5" Mk 8) will typically fire 20-25 rounds per minute out to about 26km, with either direct action (DA) fusing (exploding on impact with the sea or a target), or via a Variable Time (VT) proximity fuse for airburst over the target, which is attacked by the shell fragments. These medium calibre guns cannot generally be used against single FIAC targets, due to shortcomings in the ships detection and ID sensors, which are optimised against larger targets. Current counter-FIAC tactical procedures do use medium calibre gunfire for harassment, but do not expect significant target kills, however the improvements noted above, also apply to the medium calibre gun case, and it would the theoretically possible to achieve some kills at long range, this attenuating an attack well outside the Phalanx/CR gun range. Additional benefit is possible through the use of real-time TI from offboard sensors closer to the target, or through offboard (laser) designation for course corrected shells. This class of benefits would help against Type 1 and 2 FIAC targets, but not at all in the case of Type 3.

- **Move the battle outwards.** By using helo, UAV or UCAV. This class of benefit applies to all classes of FIAC, and provide either ISR/ID information about the target, thus achieving engagement criteria for ship mounted weapons, or the helo or UCAV can also be armed, and then be used to attrite the incoming FIAC raid. The differences are that the crewed helicopter can be autonomous, whilst the UCAV relies on good networking back to the controlling ship. The DD/FF escorts in the scenario normally carry one or two helicopters, though smaller UCAV could be carried in rather larger numbers. This is less important in a narrow sector attack, but could become essential in the case of an isotropic distributed threat, where volumetric coverage then becomes important.

27. The hypothesis is that better (networked) ISR allows the full range of the current weapon systems to be exploited, firstly Phalanx 1B to its maximum envelope, and then taking the medium calibre gun (5"/54 or 4.5"Mk 8) out to maximum range. In the event that 'leakers' still occur, the battle has to be taken offshore, using a helicopter or UCAV. In the previous cases, helicopters or UAV can provide surveillance, but the offshore battle requires armed helicopter or UAV (hence UCAV). There are two other examples of potential technical developments under NEC that might improve FIAC defence:

- The first is an Electro-Optic (EO) equivalent to CEC, able to share imagery seamlessly, and giving the short range EO picture so that all vessels are able to 'see' composite imagery associated with all the surface tracks. The command could therefore associate and use

images from several directions to classify a target and reach ID criteria. This would extend to use of NEC to carry out fire co-ordination, similar to the AAW TEWA process.

- The second development worth considering is a 'swarm potential' detector that monitors the closest point of approach (CPA) criteria of all contacts via individual filters, and tracks the aggregate total. This would monitor any association or correlation 'peak' that indicated the potential for the latent swarm to coalesce into a real attack. This counters swarm tactics based on a slow approach, preceding the fast attack phase. It is easier to reach ID criteria during the attack, but it would be harder to characterise a SWARM when isotropically scattered over a wide area, due to the need to visit and ID each target.

28. All solutions require progressive networking enhancements, matched to improvements in weapons systems, and complementary doctrine like RoE; this covers all aspects of the US DOTMLP spectrum. Whilst the study considered some changes to process – typified by chat rooms, it did not explore the full impact on all the Coalition partners potential Lines of Development. These will be addressed by follow-on work, via TTCP MAR AG-6:

US – DOTMLP	**UK – TEPIDOIL**	**CA – PRICIE**
Doctrine	Training	Personnel
Organization	Equipment	Research and Development/OR
Training	Personnel	Infrastructure and Organisation
Materiel	Information	Concepts, Doctrine & Collective Training
Leadership	Doctrine & Concepts	Information Management
People	Organisation	Equipment, Supplies & Services
	Infrastructure	
	Logistics	

Table 2 – Coalition Lines of Development [Grey areas tackled by AG-1]

29. **Driving Factors.** The discussion above outlines the 'trade-space' in terms of likely solutions and their applicability to the operational problem. This is summarised in Figure 13:

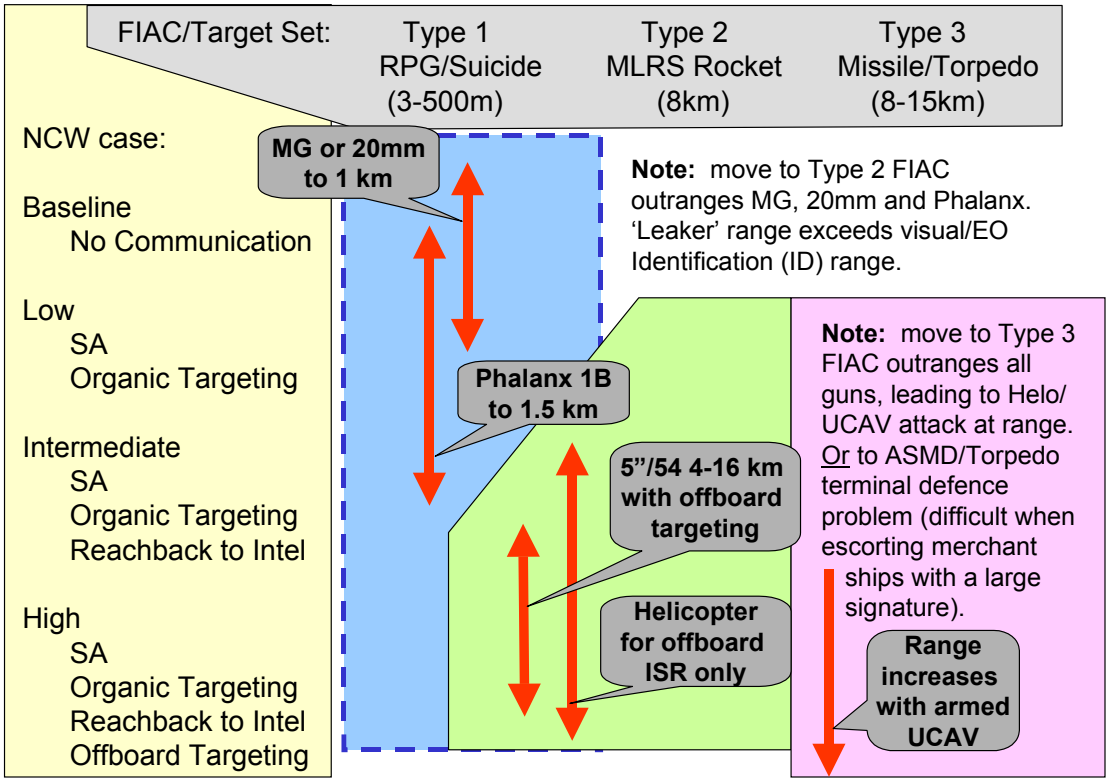


Figure 13 - Driving Factors for NCW FIAC Problem

Conclusions

30. **ASuW Swarm Implications:**

- Results show the clear need to 'do something.' Present ships defences are sensor-limited by short detection and ID ranges, and are hampered by restrictive Rules of Engagement (RoE). Saturation therefore occurs at relatively low weights of attack by Type 1 FIAC with kills made well inside Red's potential weapon launch range of 3-500m for heavy machine gun or RPG. This performance is speed dependent and reduces with increasing FIAC speed. Force defence figures are lower than single ship case, since any leaker could hit the HVU(s).
- An ASuW swarm could be countered by networking between escorts, helicopters/UAV/ UCAV and the merchant ships. Improvements come in three broad bands:
  - Use of existing Close Range (CR) guns (MG, 20/30mm, Phalanx 1B) to maximum range, to defeat Type 1 threats.
  - Use of existing Medium Range weapons to medium range bracket to attack Type 2 FIAC, plus use of smart rounds (laser designator in helo/UAV) to maximum range. This also provides some cover against Type 3 FIAC, but needs to be subject to Analysis of Alternatives (AoA).
  - Maximum use of armed helicopters/UCAV to attrite raids further out. This is the only counter to longer range Type 3 attack, but trade-off between helo and UAV/UCAV depends on detailed scenario.
- For the smallest Type 1 FIAC, intermediate and high levels of networking increase Force survivability by close to an order of magnitude.
- If the Type 1 FIAC swarm dispersed widely, some targets fall outside surveillance footprint. Potential doubling of leakers, shows Red's ability to compromise force defences, by outflanking limited ISR assets; demonstrates need for additional performance margin over previous slide.
- Countering the larger Type 2-3 FIAC could be achieved by the use of networked Air ISR. A scenario is fully survivable If Blue surveillance and weapons range exceed Red launch range, otherwise leakers are assured. A high level of networking is always necessary, but due to the outcomes, % improvement is not relevant.
- The trade-off between helo and UAV/UCAV depends on whether the threat adopts a single sector or widespread (i.e. isotropic) attack. Armed airborne assets will always improve a forces survivability, but the finite weapon payload and space/time considerations caused by the target spread, drive the number of airframes required.

31. **Systems Functionality.** All solutions require progressive networking enhancements, matched improvements to weapons systems (requiring further Analysis of Alternatives), and complementary doctrine like RoE. This covers all aspects of the DOTMLP spectrum. Potential technology requirements include networked sensor units, low latency communications, reachback, potentially an EO 'CEC style' net, a swarm warner, co-ordinated RoE/Weapons free/Fire co-ordination software, and smart gun rounds.

32. **Modelling.** The study has used MANA agent based modelling of the FIAC problem, with some validation & verification from a more detailed Battlemodel.

- MANA's strengths include representing the personality that drives the swarm's dynamic tactics, rather than merely a rigid target set. The agent based model is suitable for this type of NCW analysis, in that it represents complexity including emergent behaviour.
- Although the ASuW swarm has 'demand for service' characteristics:
  - there is insufficient knowledge of swarming characteristics to safely determine the input parameters needed by queuing theory (QT).
  - the assumptions of QT applying to analytic solutions do no hold e.g. there is no arrival

pattern, and only a finite pool of customers.
  - some of the normal metrics of QT e.g. mean-time in the queue, are not relevant.
- MANA does not address some issues such as weapon arcs that are important. Agent based models would allow results to be abstracted upwards into simplified or meta-models of the ASuW 'terminal end game' like spreadsheet or QT models.

33. There is a wide range of potential analytic techniques available for NCW problems, but in practice each country has a preferred set. One of the great benefits of the international collaborative work within TTCP has been the exposure to each other's methods and tools, plus the peer-to-peer exchange involved. The direct gain has included increased cross-visibility of: SIAP metrics, Queuing Theory, Petri and Bayesian networks, and Intelligent Agent models.

34. Intelligent Agent models can represent swarming, but require a degree of tuning to mimic real life, leading some to doubt whether their rule sets can be extrapolated. The TTCP MAR AG-1 experience with the New Zealand MANA model has been uniformly positive, and has also shown that meta-modelling (using both MANA and Queuing Theory) can integrate more detailed work by nations without needing direct access to sensitive data. This allows a broad-order comparison of alternative options, and has shown that combining nations' individual OA expertise can strengthen the likelihood of the Coalition successfully acquiring a NCW capability.

Lessons Learned

35. **Modelling Methodology.** This is the third quantitative study conducted by TTCP MAR AG-1. The two previous studies (of maritime interception operations and anti-submarine warfare), employed queuing theory. Despite the relatively few parameters, queuing theory describes a rich diversity of behaviour, and is an attractive method, provided that one is confident that the parameters selected fully capture the essential detail of the scenario. Queuing theory is often cast as a 'demand for service', typically modelling defence of military targets against multiple attackers. However, the range of 'customer' (i.e. Red) behaviour is relatively circumscribed. The sort of swarming tactic of interest in the present work, requires a rather more detailed description of Red behaviour than seems possible with queuing theory. Also, we require a much more detailed representation of the flow of information around the Blue force. The results reported herein indicate that agent based modelling can provide the representations with a sufficient level of detail, and so is a useful tool for analysing this type of military tactical situation.

36. The price paid in moving to agent-based modelling is a very substantial increase in the dimensionality of the parameter space. However, all parameters have clear interpretations in terms of agents' behaviour and warfighting capabilities, so it is possible to construct conceptually well-justified strategies for exploring the parameter space. Nevertheless, the key to successful agent-based modelling is careful implementation of the scenario so as to facilitate interpretation - in two of the study cases, insights were revealed by the modelling only because of an appropriate choice of one or two particularly sensitive parameters. The power of agent-based distillations as a modelling tool depends on the credibility with which such parameter choices can be made, explained and justified. In reality, much the same can be said of any method of military modelling or experimentation.

37. A great benefit of agent-based modelling lies in the description of Red capabilities. It is not unusual for military modelling to concentrate unduly on the description of Blue capabilities and tactics, with the depiction of the Red force being no more than an array of 'dumb' targets. Agent-based modelling, on the other hand, is symmetric between the sides; Red agents have the same potential properties as Blue agents and these must be deliberately chosen. In the present scenarios, it may seem that our choice has a certain unreality: the initial disposition of the Red force in its form-up region is chosen at random and the tactic of converging to a predesignated point before rushing the Blue force is somewhat artificial. However, any unrealistic vulnerability that these features may impart to Red is counterbalanced by some potent capabilities. In particular, it is posited that Red knows that the Blue force is coming, has complete freedom to select a favourable killing ground and can remain on station in its form-up area, undetectably

covert (in the absence of Blue air assets), for as long as it takes the Blue force to arrive. This type of detailed balancing of capability constitutes a real strength of agent-based modelling.

38. An agent based model like MANA allows the flow of situational awareness information to be measured and constrained by the modeller. Each squad maintains a log of all messages sent on each of its communications links. Each message consists of the time of contact detection and that of addition of the contact to the queue, the contact type (enemy, friendly etc.) and position, and the identification numbers of the informing agent and the detected agent. This important information allows the modeller to explore information flow at any level of interest. Owing to time constraints this facility was not able to explored here, but it should be of interest to future modellers.

39. **Robustness of Data Assumptions.** The study has used open-source information about the range and effectiveness of weapon systems. Military advice was always taken, in order to use this data intelligently. There is no reason that each nation could not re-run the work using their own classified parameters, and whilst the real numbers may be lower than the open source figures used, the overall shape of the results and broad-order conclusions are unlikely to change significantly.

- The emphasis on linked improvements in both networked sensing, and in weapon systems, plus the need to extend the weapon envelope to counter Type 2 FIAC, and that only airborne assets can counter the Type 3 are immutable truths, that would not be modified by more detailed work.
- Rules of engagement are a critical element. More definite knowledge of hostile intent needs to be gained at greater range for the force to defend itself optimally. This is particularly important for Type 2 and 3 FIAC, which have medium to long weapon ranges.

40. This analysis has provided evidence generally in support of the hypothesis, for the focussed tactical situations explored herein. We must point out however that there were also tactical situations where additional information led to *increased* danger to naval assets. Specific recommendations are:

- Efforts should be made to increase the range at which hostile intent can be discerned.
- Rules of engagement should be reviewed to determine whether threats could be engaged at greater range from Blue force.
- Inorganic targeting of medium-range weapons should be considered, and appropriate ammunition technology needs to be developed for engaging FIAC with those weapons.
- Security and technology issues involved in coalition shared situational awareness need to be resolved. Trust, accuracy, latency and bandwidth are some of the important communications and interoperability aspects to consider.

41. **Pointers towards the benefits of NCW.** Finally, it is appropriate to ask whether the modelling reported here addresses ‘true’ NCW. The nature of NCW has proven particularly elusive, even to describe theoretically, let alone to model. The key source of advantage of NCW clearly lies in the properties of the network. Some hold that this depends on the richness of network connectivity (i.e. numbers of nodes and patterns of connections). We do not explicitly model a rich network in the present study; rather we view the Blue force as recipients of the benefits of being part of such a network and we model its response to those benefits. Thus, we model an aspect of reachback as providing timely information on Red intentions. How the information may be gathered, verified and disseminated is outside of the scope of this model; we focus only on the consequences of the information being available to the Blue force.

42. A method that has been used to characterise NCW uses the emergent properties that attend ‘true’ NCW. These include enhanced speed of command, force agility, shared situational awareness, information superiority, etc. It has been argued that none of these properties, except perhaps the provision of high-capability reach back, are really diagnostic of NCW but they

nevertheless provide a means of assessing the level of advantage obtained from a network. The following comments stem from this point of view:

- The value of intelligence in greatly increasing the effectiveness of Blue's response is clear in most of the scenario variants. This can be seen as an NCW benefit inasmuch as the network facilitates gathering the information and enables timely dissemination of intelligence products. The effect of the heightened level of information superiority provided by aerial reconnaissance assets is also clear.
- The scenario in which intelligence provides incorrect information is particularly interesting from the point of view of force agility. Blue performs quite poorly with lower than intermediate NCW capability, even against small swarms. This points to one of the most significant capability enhancements identified in this study: timely recognition of a mistake and effective adjustment of force posture. If it is true that no plan survives first contact with the enemy, then this is a real benefit of NCW.
- It is clear that the improvement in MOE due to the network depends critically on the timeliness of the information delivered. This addresses the emergent properties 'ability to amass effects' and 'information superiority.' The network is only as useful as the information available for it to transmit. This rather obvious point is emphasised by the scenario involving an incorrectly predicted threat axis.
- Finally, perhaps the most important point from this study: improvements in sensor capability must be matched with improved weaponry and the RoE that allow it to be employed. The key assumption of this study that allows for any significant level of effective response to a large swarm of Type 1 FIAC, or any sized swarm of Type 2 FIAC, is the existence of a stand-off weapon with characteristics similar to a current 5" gun, but considerably enhanced lethality at many kilometres distance, and a matching development of RoE so that the weapon may be used with inorganic-sensor targeting.
- This completes the chain of cause and effect started by the previous bullet point. Not only is a network only as valuable as the information available for it to disseminate, but also it is only as effective as the response(s) available to the warfighter once in possession of the information.

43. The Technical Co-operation Program (TTCP) Maritime Systems (MAR) Action Group One has conducted this analysis over the course of a three-year effort. This five-nation effort has produced groundbreaking results that are presented in this paper. Further research and analysis is warranted.

Biographies:

David Galligan is an operations analyst with the Defence Technology Agency in New Zealand. He has a particular interest in determining the operational effect of moving forces to a networked environment. He recently completed a study on the effect of using CENTRIXS for task group collaboration and knowledge sharing during the Tasmanex '05 exercise, which involved a range of RNZN and RAN ships. He has also authored a number of studies on maritime patrol platform and sensor optimisation and has developed evidence to support acquisition decisions. He is the principal developer of the MANA model, an agent based distillation model that is extensively used throughout the global defence science community. He holds a PhD in radar meteor physics and, prior to working for defence, he was employed for several years on European Space Agency and New Zealand Marsden funded studies involving the observation and modelling of the dust cloud in outer space.

George Galdorisi is Director of the Decision Support Group at SPAWAR Systems Center San Diego where he helps direct the Center's efforts in strategic planning and corporate communications. Prior to joining SSC San Diego, he completed a 30-year career as a naval aviator, culminating in 14 years of consecutive experience as executive officer, commanding officer, commodore, and chief of staff. He is a 1970 graduate of the United States Naval Academy and holds a Masters Degree in Oceanography from the Naval Postgraduate School and a Masters Degree in International Relations from the University of San Diego. He graduated from both the Naval War College's College of Command and Staff and the College of Naval Warfare, and in 1994 he received the Naval War College's Admiral John Hayward Award for Academic Achievement. Additionally, he is a graduate of MIT Sloan School's Program for Senior Executives.

Peter Marland is a Principal Scientist with the Defence and Science Technology Laboratory, working on the effectiveness of Maritime C2 and ISTAR systems, and the associated business cases for new projects. He is a former Royal Navy engineer officer with a wide range of seagoing experience including a Head of Department tour in an ASW frigate, and service in an AAW destroyer during the Falklands conflict. This was complemented by appointments ashore, both in the Operational Analysis and the Materiel Professional fields (where he was responsible for navigation equipment and the UK retrofit of NATO SINS). His Naval career also included the RN staff course at Greenwich, and a final tour in a 4* HQ tackling post-Cold War naval base realignment and closure. He has a BSc in Electrical Engineering, a MSc in Project Management, and has been doing postgraduate work on the application of multimedia to technical documentation and CALS.