# SMALL NAVIES AND NETWORK CENTRIC WARFARE: IS THERE A ROLE?

**Canada and US Carrier Battlegroup Deployments**

**Dr. Paul T. Mitchell**
Director of Academics
Canadian Forces College
215 Yonge Blvd.
Toronto, ON
M5M 3H9

mitchell@cfc.dnd.ca
(416)482-6800

**Abstract**

Is there a place for small navies in network centric warfare (NCW)? Will they be able to make any sort of contribution in multinational naval operations of the future? Or will they be relegated to the sidelines, undertaking the most menial of tasks, encouraged to stay out of the way or stay at home? If the recent experience of the Canadian navy is any guide, small navies may have every right to be concerned about their future in NCW operations. For while the Canadian navy has achieved a high degree of success within US naval formations, it has done so only through highly privileged access. To date, the challenges posed by the revolution in military affairs in general and NCW in specific have been framed in terms of technology and investment. US allies and partners are lagging in technology and investment therein and need to make significant capital investments in order to catch up. Worse, "dynamic coalitions", or those developed rapidly to deal with crisis situations may be the most common form of military co-operation. In such coalitions, detailed, prearranged plans and doctrine are likely to be entirely absent. Partners will have had little in depth operational experience or knowledge of their own capabilities. Technical standardisation will be low; logistical support may be limited or entirely absent. Significantly, there may be serious questions regarding the professionalism of personnel participating in these coalitions.

This paper, then examines the nature of NCW and the challenges it presents to coalition operations, and some recent developments that seek to overcome these challenges. Furthermore, it uses the Canadian navy's recent and ongoing experience in directly integrating into US carrier battle group (CVBG) operations as a test case. The paper finds that the principal challenges that will be raised by NCW are not likely to be technical ones, although undoubtedly these will be formidable. Rather, the challenges NCW presents to all navies, and small ones in particular, stem from policy oriented areas. If Canada's example is typical, then navies which have a less well developed relationship with the USN are likely to confront such crippling difficulties in integrating into NCW dominated operations as to be automatically excluded from any sort of consideration.

## Introduction

Is there a place for small navies in network centric warfare (NCW)? Will they be able to make any sort of contribution in multinational naval operations of the future? Or will they be relegated to the sidelines, undertaking the most menial of tasks, encouraged to stay out of the way or stay at home? If the recent experience of the Canadian navy is any guide, small navies may have every right to be concerned about their future in NCW operations. For while the Canadian navy has achieved a high degree of success within US naval formations, it has done so only through highly privileged access. To date, the challenges posed by the revolution in military affairs in general and NCW in specific have been framed in terms of technology and investment.[1] US allies and partners are lagging in technology and investment therein and need to make significant capital investments in order to catch up. Worse, "dynamic coalitions", or those developed rapidly to deal with crisis situations may be the most common form of military co-

[1] Gompert, ., Mind the Gap
Defense University Press, 1999).

operation. In such coalitions, detailed, prearranged plans and doctrine are likely to be entirely absent. Partners will have had little in depth operational experience or knowledge of their own capabilities. Technical standardisation will be low; logistical support may be limited or entirely absent. Significantly, there may be serious questions regarding the professionalism of personnel participating in these coalitions.[2]

How dynamic coalitions will function in a network centric warfare (NCW) is undoubtedly problematic. One commentator has recently raised, the nature of network centric warfare may ultimately result in more unilateral US operations (or ones that are virtually unilateral), such as that recently conducted in Afghanistan. In effect, the risk of "clueless coalitions"[3] may drive the US, however unwillingly, towards a more unilateralist military policy, irrespective of that enunciated in its National Security Strategy. The JCS has called for a more "tailored approach to interoperability that accommodates a wide range of needs and capabilities" without implying "access without restraint".[4] In the unstructured environment implied by the concept of dynamic coalitions, however, the policy restraints on information sharing, surely the heart of network centric warfare, may be considerable. As Thomas Barnett has pointed out, "Not only will our allies have little to contribute to the come-as-you-are party, they won't be able to track the course of the conversation."[5]

This paper, then, examines the nature of NCW and the challenges it presents to coalition operations, and some recent developments that seek to overcome these challenges. Furthermore, it uses the Canadian navy's recent and ongoing experience in directly integrating into US carrier battle group (CVBG) operations as a test case. The paper finds that the principal challenges that will be raised by NCW are not likely to be technical ones, although undoubtedly these will be formidable. Rather, the challenges NCW presents to all navies, and small ones in particular, stem from policy oriented areas. If Canada's example is typical, then navies which have a less well developed relationship with the USN are likely to confront such crippling difficulties in integrating into NCW dominated operations as to be automatically excluded from any sort of consideration.

**The Nature of NCW**

Much of what has been revolutionary in the revolution in military affairs is not so from a naval perspective.[6] Navies have been working with information technology since 1957 when the CANUKUS Naval Data Transmission Working Group ratified the technical standard for data exchange, developed after three years of deliberations.[7]

---

[2]S.C. Spring; Dennis M. Gormley; K. Scott McMahon; Kenneth Smith; Daniel Hobbs, "Information Sharing for Dynamic Coalitions", Unpublished Paper accessed at, (Arlington VA: Pacific Sierra Research, VPSR Report 2836, Dec. 2000), pp. 5-6.

[3] Col. Robert Chekan (CF), “The Future Of Warfare: Clueless Coalitions?” unpublished paper, (Toronto: Canadian Forces College, October 2001).

[4] Spring, *et al.* p. 6.

[5] Thomas B. Barnett, "The Seven Deadly Sins of Network Centric Warfare", *Proceedings*, January 1999, p. 37.

[6] James Tritten , “Revolutions in Military Affairs: Paradigm Shifts and Doctrine”, *A Doctrine Reader, Newport Paper #9,* (Newport RI: Center for Naval Warfare Studies, 1995).

[7] Originally named the Tactical International Data Exchange, (or TIDE “good for cleaning up messy tactical pictures”) it later became known as Link 2 (II in roman numerals) in the Royal Navy which was already using forms of data

Link 11 is relatively standard within most Western navies. Primarily used to share tactical information so as to assist in the development of a common operational picture (COP) amongst a task group, Link 11 data is also used by the USN to transmit some engagement orders. However, for many reasons, Link 11 is a relatively slow system for obtaining tactical information. As such, the information received is not of fire control quality given the significant lag times between target detection and the posting of data onto the Link network. Further, it only passes data that has already been processed on board each contributing ship. This occasionally leads to duplicate tracks and/or conflicting information about the same target. Link 11 demands a high degree of professional competency on the part of track co-ordinators in order to keep the COP clean and free from extraneous data.[8]

NCW aims at increasing the efficiency of the transfer of maritime information amongst participating units (or nodes). By optimising the efficiency of operations through information exchange, even small naval formations can generate additional combat power.[9] Data is manipulated by a series of dynamic and interlinked grids, sensor grids gather the data, information grids fuse and process it, and engagement grids manage the operations generated.[10] Improved operational efficiency results not only from the increased speed at which operations can place, but also from the resulting "self synchronisation" that is generated between units.[11] This speed and synchronisation will ultimately merge the strategic “recognised maritime picture” (RMP) with the operational COP and the tactical “common tactical picture” (CTP).[12] For example, in Canadian ships, the RMP is provided to ships at sea by shore based facilities. Ship-based sensors and tactical data links generate local area information. At the moment, neither informs the other which can often lead to discrepancies between the RMP and the COP or CTP. With the merging of information into a common pool distributed by linked systems, plans and operations will become much more dynamically oriented as they instantly are able to react to changes in the battlespace given their enhanced awareness of it. For navies with this capability, the result is a competitive advantage enabling it to "lock in success" while locking out enemy initiative.[13]

While enhancing the speed of reaction ultimately originated in the Cold War need to deal with hypothesised regimental sized air attacks on surface ships, the continuing impetus for speed and synchronisation is driven by the return of fleet operations to their traditional location in and around the littorals. The sheer density of maritime and air traffic, the presence of naval, commercial and recreational maritime vehicles results in a

---

sharing technology to distribute tactical information amongst its ships. As other NATO links became established, Link II became known as Link 11. Norman Friedman, *World Naval Weapons Systems 1997-1998*, (Annapolis: United States Naval Institute Press, 1997), p. 28

[8] Norman Friedman, “CEC and Fleet Defence”, *RUSI Journal*, Oct. 2000.

[9] Edward Smith, "Network Centric Warfare: What's the Point?", *Naval War College Review*, Vol. 54, No. 1, Winter 2001, p. 3

[10] *The Canadian Navy’s Command and Control Blueprint to 2010,* (Ottawa: NDHQ, June 2001), p.12.

[11] Elias Oxendine IV, "Managing Knowledge in the Battle Group Theatre Transition Process", Student Thesis, (Monterey CA: Naval Postgraduate School, Sept. 2000), p. 18.

[12] *The Canadian Navy’s Command and Control Blueprint to 2010,* pp. 11-12.

[13] Oxendine, p.18.

level of complexity that blue water operations rarely encounter. This web of activity is made all the worse by the influence of micro-climates, complex oceanography, and unique geographical features. Finally, in the littoral, there are few places where a warship does not stand out, whereas enemy forces are afforded a multitude of opportunities to hide their forces, whether that be geographically or through concealing their identity by basing them on non-naval platforms.[14] In effect, naval forces are forced onto an "asymmetrical" battlefield in the littorals.[15]

Networked operations permit enhanced speed and synchronisation which in turn generate:

- Predictive planning and pre-emption - resulting in proactive, manoeuvrist, effects based operations;
- Integrated force management - allowing synchronisation of missions and resources; and
- Execution of time critical missions - permitting "near optimal weapons pairings".[16]

The most explicit technological development stemming from these conceptual developments has been the creation of the "Co-operative Engagement Capability" (CEC) which successfully passed its operational evaluation trials in September 2001[17]. CEC has three related aspects to it. Like Link 11, it seeks to develop the COP. Unlike Link 11, however, it also seeks to co-ordinate threat decisions in real time. Further, it also seeks to distribute fire control quality information to participating nodes on the CEC network.[18] CEC enhances the ability to share data, even that of a fragmentary nature. For example, because of stealth technology or terrain masking effects, a ship may be able to collect only fragmentary information from its sensors on a particular target. In a CEC formation, sensors receiving fragmentary data will cue others within a formation, thus allowing a more detailed picture to be developed on a specific contact. All this information would be pooled with other data collected on that target from the sensors of other ships in order to reveal it in a fashion that any one single ship would be unable to do. *A fortiori*, other units might relay information on targets outside the sensor horizon of a particular ship. Given the fire control quality of the information provided by CEC, this would permit weapons to be fired before the incoming threat appears above the horizon, allowing the engagement to take place at maximum distance from the targeted ship.[19] The end result of all this is that the time to make decisions is greatly increased. This permits more time to assess threats as well as allowing engaging forces to operate within their opponent's OODA loop.

---

[14] Richard Scott, "Survival of the Fittest", *Jane's Defence Weekly*. January 23, 2002.
[15] LCol. William R. Pope, "U.S. and Coalition command and Control Interoperability for the Future", Student Thesis, (Carlisle PA: US Army War College, April 2001), p. 10.
[16] Anonymous, *Observations on Network Centric Warfare*, accessed at http://www.dtic.mil/jcs/j6/education/warfare.html, Jan. 29, 2002, pp. 5-6.
[17] "CEC Passes through successful OpEval, Navy says", *Defense Daily*, Sept. 25, 2001, p. 1.
[18] Daniel Busch; Conrad J. Grant. "Changing the Face of War: The Co-operative Engagement Capability", *Sea Power*, 43, no.3, March 2000, pp. 37-39.
[19] Robert Kerno, "Co-operative Engagement Capability and the Interoperability Challenge", *Sea Power*, 42, no. 3, pp. 45-47.

Nor is CEC the only technical development speeding up the pace and efficiency of naval operations within the USN. Much as business has in the last five years, the US military has taken advantage of the opportunities offered by the internet to enhance the transmission of information. The Defense Message System, backed up by the Secret Internet Protocol Routing Network (SIPRNET), has introduced a series of web based applications such as e-mail with attachments, "chat rooms" and web pages.[20] SIPRNET in particular seems to have had a revolutionary impact on the planning and conduct of operations within the US military. It has transformed laborious manual procedures into rapid electronic ones. This became most evident during operation "Allied Force" when the hard copy format of planning threatened the rapid operational tempo of the bombing campaign. The sheer amount of paper work literally forced planners into electronic formats "which were substantially easier to create, pass via e-mail, and maintain visibility on." As Stuart points out, as superiors appended their comments on forwarded messages, it became a simpler matter to track the evolution of commanders' intents as well.[21] Mundane features such as "chat rooms" so ubiquitous amongst idle teenagers, have a distinctly revolutionary aspect about them as they permit the transmission of information (along with attachments of imagery and other intelligence) without radio communication, thus preserving communications security within theatre.[22]

Video teleconferencing (VTC) has also lead to "compressed command and control processes" through its ability to span the strategic, operational, and tactical levels. Such a feature is particularly useful for staffs widely dispersed geographically, permitting enhanced direction of operations.[23] One Sixth Fleet commander, VAdm. Dan Murphy has called VTC "the wave of the future". VTC obviates the need to collocate staffs and reduces any ambiguity in commanders' intents amongst dispersed staffs.[24] VTC together with chat functions permit "distributed collaborative planning" (DMP). DMP seeks to:

- Assemble problem solvers for rapid response to time critical situations;
- Provide access to and ensure availability of appropriate information resources; and
- Enhance the effectiveness of problem solvers despite their dispersion across both time and space.[25]

[20] Pope, pp. 9-10.
[21] Capt. Robert M. Stuart, "Network Centric Warfare in Operation Allied Force: Future Promise or Future Peril?", Student Thesis, (Newport RI: Naval War College, 16 May 2000), p. 8.
[22] "Center Outlives Network Centric Warfare Concept's Challenges, *Defense Daily*, March 23, 2001.
[23] Stuart, p.7.
[24] "Defense Watch", *Defense Daily*, Oct. 18, 1999.
[25] *The Canadian Navy's Command and Control Blueprint to 2010*, pp. 20-21.

These conceptual and technical developments will enhance the already dynamic organisations of American naval operations. As Morua describes, CVBGs are unavoidably dynamic given the constant flow of ships, personnel, and new technology through them. In order to control this dynamism, rather than be overwhelmed by it, the deployment of a CVBG involves a meticulous process of training and planning through which all participating units and individuals undergo in order to familiarise them with the synergies between processes, procedures, and systems. The end product is the development of a specified "battle rhythm" (see figure one). In order to support this battle rhythm, it is important that everything within the CVBG, whether technological system, individual operator, or ship unit, "not have an adverse effect on communications or information flow. To this end, the battlegroup proceeds through a series of sub-unit and unit training exercises. These culminate in the "Comprehensive Task Unit Exercise" which certifies the battlegroup for basic CVBG duties, and a final "Joint Task Force Exercise" which combines the CVBG with other task groups such as amphibious groups and allied formations.[26]

While Allied Force and subsequent operations in Kosovo are widely hailed as beginning the introduction of NCW operations, clearly "Enduring Freedom" in Afghanistan has laid to rest many of the criticisms aimed at the Pentagon's RMA crusade. This is especially so since it has seen the confrontation of a high tech military against a rag tag guerrilla type army:

| **Time** | **Event** |
|---|---|
| 05:00 | Receive Unit Operational Reports |
| 08:00 | Brief Battlegroup Commander |
| 09:00 | Brief JTF Commander |
| 10:00 | Warfare Commander's Co-ordination Board |
| 13:00 | Planning Cell Meetings |
| 18:00 | Release Commander's Intentions and Situational Report Messages |
| 20:00 | Units Receive Commander's Intentions Messages |
| 00:00 | Units Release Operational Reports |

Figure One

> The Afghanistan operation may ultimately prove to be a boon to the Department of Defense's revolution in military affairs, in which the prize is not territory but information. Only after a clear picture of the battlefield is assured - and that shared with as many weapons platforms as possible - can the maximum potential

[26] LCdr. Michael L. Morua, "The Carrier Battle Group Force: An Operator's Perspective", Paper Delivered at "Engineering the Total Ship (ETS) 2000 Symposium, March 21-23, 2000, Gaitherburg MD; Gordon I Peterson, "Ready to Go on Game Day: At Sea with the *USS Theodore Roosevelt* Battle Group", *Seapower*, Sept. 2001. Accessed at http://www.navyleague.org/seapower_mag/sept2001/ready_gameday.htm, Feb. 12, 2002, p. 5.

of PGMs and other high tech weaponry be unleashed both militarily and politically.

Particularly impressive has been the manner in which information from a wide variety of sources has been processed and fused for both air and ground based forces, thus permitting mid course updates, engagement zones and "moving target options", and cockpit target imaging.[27] What has also been evident was the initial lack of allied participation in the most secret and demanding operations. While this might have stemmed from a general lack of allied lift, the desire to avoid a "clueless coalition" as Chekan has suggested, must also be considered. As the godfather of NCW, VAdm. Cebrowski noted, while the US wants its partners to be as interoperable as possible, "not being interoperable means that you are not on the net; so you are not in a position to derive power from the information age."[28]

**NCW and Information Voids**

Despite the desires of Admiral Cebrowski or, indeed, that of the United States, getting on the net may not be a simple process at all for allied nations and coalition partners. Essentially, these nations face two separate and distinct challenges: network access may be hampered by technical incompatibilities inherent in their own force structure, or by the design of the network's administrators.[29]

Recent operations in the Balkans have underscored the difficulties in meeting American expectations for rapid, information dense operations. During operation Sharp Guard conducted by NATO and WEU units in the mid 1990s, at times the ability to compile a COP was limited to a ship's individual horizon. Further, COMNAVSOUTH in Naples initially had no timely access to information being collected by units under his command.[30] During Allied Force, "existing data networks were not adequate to support the flow of information of … data among key nodes of the NATO information grid." Further, because the US was unable to pass along "high fidelity data", the alliance experienced difficulties attacking time sensitive targets "because of the need for rapid exchange of precision targeting data and continuous precision updates from sensor to shooter until the target is destroyed."[31]

While, some of these issues were later addressed through technical solutions (Sharp Guard units and command centres eventually received old USN JOTS terminals for example), according to Kiszely and others, "the need for speed" in NCW operations places the whole notion of multinational operations at risk. Because connectivity problems are the "equivalent of changing to a different railway gauge at each national

---

[27] Bryan Bender; Kim Berger; Andrew Koch, "Afghanistan's First Lessons", *Jane's Defence Weekly*, Dec. 19, 2001.
[28] Peter Howard, "The USN's Designer of Concepts", *Jane's Defence Weekly*, Oct. 3, 2001.
[29] Pope, p. 10.
[30] Eric Francis Germain, "The Coming Revolution in NATO Maritime Command and Control", *MITRE Technical Papers*, (Arlington VA: MITRE Corp., Oct. 24, 1997), accessed at http://www.mitre.org/support/papers/technet97/index.html, Feb. 5, 2002, pp. 3-4.
[31] Joseph M. Ladymon, "Network Centric Warfare and its Function in the Realm of Interoperability", *Acquisition Review Quarterly*, Summer 2001, p. 115.

border",[32] high tempo operations ultimately become hostage to units with the slowest cycles.[33] The difference within NCW operations is that these barriers may extend to even the closest ally. While coalition operations must always confront issues of technology differentials, lack of physical access may be just as pressing and in the long term, even more damaging. Liaison officers (LO) have traditionally been utilised by militaries to ensure the transmission of information amongst partners, particularly when there are interoperability problems.[34] Often, LOs may be physically unable to enter US command centres because of security restrictions, thus hampering their function.[35] Technology may lead to the electronic equivalent of a physical barrier.

For example, the growing use of VTC directly raises this issue given the classified information that frequently accompanies each session. As Pope points out, in order to access the VTC comlink, "all users must be on the same level of classification of network and have access to the information on the network."[36] The lack of timely written documentation and the instantaneous experiential nature of VTC hinders any participation for those not on the network.[37] This is an issue that is broader than simply VTC. As MGen John Kiszely of the British Army has pointed out:

> Full interoperability between forces would depend upon integrated collaborative planning based on the maintenance of a common operating picture and common intelligence inputs. Without appropriate digital communications, this would not be practical, and made all the more unlikely because the US SIPRNET is NOFORN."[38]

Thus, NCW operations in a coalition or alliance environment may ultimately hinge on information releaseability rules and the ability to send information between networks with different security classifications. The trouble is that NCW is primarily oriented around the guiding principle of increasing the speed and efficiency of operations. But coalition operations are rarely about combat efficiency. Coalitions are always about scarcity, whether in terms of operational resources, political legitimacy, and sometimes both. The trade off for reducing these scarce resources is always in terms of political influence over operations. Thus, in coalitions, political considerations will frequently trump efficiency. However, information releaseability policy is not oriented around the concept of efficiency but rather that of security. "Information release and control must be conducted in a manner that prevents damaging foreign disclosure, this capability must be demonstrated to information owners" before any transfer can be effected.[39] In effect,

---

[32] "General Warns Over Digitisation split", *International Defence Review*, Jan. 01, 2002; John Kiszely, "Achieving High Tempo – New challenges", *RUSI Journal,* Vol. 144, No. 6, Dec. 1999.
[33] Smith, p. 3; Oxendine, p. 19.
[34] MGen R. H. Scales, "Trust, Not Technology Sustains Coalitions", *Future Warfare*, (Carlisle PA: US Army War College, 1999).
[35] RAdm. Gary Wheatley; Diana Buck, "Multinational Command and Control – Beyond NATO, paperpresented to 1999 Command and Control research and Technology Symposium, US Naval War College, Newport RI, p. 6.
[36] Pope, p. 12.
[37] Stuart, p. 7.
[38] "General Warns Over Digitisation split", *International Defence Review*, Jan. 01, 2002.
[39] Sping, *et al.*, p. 7.

information may be too sensitive to be risked with others. Transfer may also compromise sensitive collection systems.

The lack of common clearinghouses for information and cumbersome procedures often mean that information disclosure is a tedious and cumbersome procedure.[40] Further, because the long term of effect of information disclosure is often difficult to ascertain, and because the career impact of improper disclosure is so serious, "commanders often choose stringent release rules to avoid problems."[41] The result is that releasability concerns have dictated separated networks operating at different tempos. As BGen. Gary Salisbury, Director of $C^3$ systems for USEUCOM has pointed out,

> How do they get these national communications and information needs and fit these into a coalition environment? The bottom line is we are generally operating two different at two different security levels. We run our networks at a coalition releaseability level that 's basically unclassified.[42]

It is these information security policies that is the ultimate barrier that prevents allies and partners from operating at the same speed as the American military. Black points out that many of the problems encountered by those seeking to improve interoperability between allies and coalition partners are the same encountered by efforts to improve joint interoperability. As such, lessons learned from attempts to facilitate joint efforts can be applied to those seeking to enhance coalition interoperability.[43] Nevertheless, the intervening variable that is not present in joint solutions is that of international politics. It is the trans-national element which makes coalition and alliance interoperability a whole order more difficult than joint interoperability. In particular, it is the question of information security that ultimately complicates efforts to improve interoperability.

It would be a gross overstatement to claim that the US is unconcerned by the issue of information releaseability. Throughout the 1990s and continuing today, the US has sponsored a Joint Warrior Interoperability Demonstration (JWID) the goal of which has been to find technical solutions to common and pressing interoperability problems. In the past, the JWID has identified several technical solutions aimed at improving the connectivity between the US and its alliance/coalition partners. "Radiant Mercury"[44] and SIREN[45] are decision support software which speeds up the process of sanitisation and declassification of SECRET documents. In 1996, the JWID identified the "Coalition Wide Area Network" (CWAN) as one of its "golden nuggets". CWAN permits a shared COP at a "Coalition SECRET" level. It is separated from the SIPRNET by firewalls and

---

[40] See Lt. Gary McKerow, "Multilevel security networks: An Explanation of the Problem", accessed at http://rr.sans.org/standards/multilevel.php, Feb. 5, 2001, p. 2; Spring, *et al*., pp. 29-34; Chekan, pp. 9-23.
[41] *Ibid*, p. 11.
[42] Henry S. Kenyon, "Alliance Forces Move Toward Unified Data Infrastructure", *Signal*, Vol. 56, No. 1, Sept. 2001..
[43] Mjr. Michael B. Black, "Coalition Command, Control, Communications, Computer and Intelligence Systems Interoperability: A Necessity or Wishful Thinking?", Student Thesis, (Fort Leavenworth KS: US Army Command and General Staff College, 2 June, 2000), pp. 5-6
[44] "Radiant Mercury", accessed at http://www.fas.org/irp/program/disseminate/radiant_mercury.htm, Feb. 5, 2002, p. 1.
[45] Bryan Bender, "JWID Puts Information Sharing System to the Test", *Jane's Defence Weekly*, Aug. 16, 2001.

gateways.[46] CWAN was initially introduced at RIMPAC, it is currently being used widely elsewhere. Finally, the US Assistant Secretary of Defense for Command and Control has sponsored a series of ongoing workshops and seminars amongst a six nation working group composed of Australia, Canada, Germany, Britain, and the US, with France as an observer. The MNWG seeks to identify the core needs of information exchange and establish common doctrine and procedures prior to any operation.[47]

Eisenhower famously remarked: "Allied Commands depend on mutual confidence."[48] Like the whole issue of relinquishing command and control, information security and releasability involves an act of trust between states that is hardly to be equalled elsewhere because of the risks involved. Just as placing troops under even the limited operational or tactical control of an ally ultimately risks the lives of those troops, releasing closely held intelligence places the security of sensitive technology, operations and even personnel at a similar risk.[49] "Trust involves a willingness to be vulnerable and to assume risk. Trust involves some form of dependency."[50]

Thus, we can expect that just as nations have always been unwilling to place complete control of their troops under the control of foreign nations, so too will they be willing to completely share everything they have in terms of information. As Pope notes, "as close as our Canadian and British allies are in common interests and objectives, there will always be limits to sharing the most highly classified information with these nations."[51] This has not typically placed operations at risk in the past, however, in a network centric operation, where information is the cornerstone of all action, separated networks operating at different speeds will have an undeniable impact on the battle rhythms of US naval operations. The finely tuned orchestration of procedures, systems, and operators would be challenged by the different operating speeds of US and allied networks. Unwillingness to share closely held information necessarily jeopardises any coalition.

As Pope infers, the US is certainly willing to share most of its information with certain partners. For forces not in this privileged club, integration into American networks will be increasingly difficult depending on the frequency they operate with them and the level of trust that the US extends to them. Forces not permitted to take part in the planning of operations will ultimately be restricted to simply taking orders or assigned high casualty roles (as fixed forces) or those that may be politically unacceptable.[52] The added risk is that multinational operations will become more and more circumscribed with allied participation occurring under the most tightly circumstances. It would be doubtful that the US would choose to hamstring its military forces, placing operations and lives at risk for these considerations. As Carr points out, America is unlikely to slow its

---

[46] Spring *et al.*, p. 17; Pope, p. 11; Lt. jg (USN) Nancy Hesson, "Coalition Wide Area Network Allows Rapid Communications to RIMPAC's Multinational Force", RIMPAC Combined Information Bureau, accessed at http://www.cpf.navy.mil/rimpac2000/news/rimpac028.html, Feb. 5, 2002.
[47] Wheatley and Buck, p. 9.
[48] Quoted in LCdr. Thomas Spierto, "Compromising the Priniciples of War: Technological Advancements Impact Multinational Military Operations", Student Thesis, (Newport RI:, Naval War College, Feb. 5, 1999), p. 3.
[49] See, for example, Robert W. Riscassi, "Principles for Coalition Warfare", *Joint Forces Quarterly*, Summer, 1993.
[50] Chekan, p. 4.
[51] Pope, p. 6
[52] "General Warns over Digitization Split", *International Defence Review*, Jan. 01, 2001.

implementation of NCW given its obvious benefits. While it would obviously prefer some integration, one option is to pass entirely on alliance participation.[53] In sum then, information releaseability policy would ultimately drive the shape and nature, and perhaps even the very existence of naval coalitions

**The Case of Canadian Ships in American CVBGs**

One can get a sense of the challenges facing coalition naval network centric warfare by examining the case of the integration of Canadian ships into American CVBGs. In some respects, this case represents the real crucible, for any difficulties faced by the Canadians

| | |
|---|---|
| **MARPAC Ships** | |
| 1995, HMCS *Calgary* | 50 days as independent ship in the Maritime Interdiction Force |
| 1997, HMCS *Regina* | Surface Action Group |
| 1998, HMCS *Ottawa* | *Abraham Lincoln* BG, fully integrated |
| 1999, HMCS *Regina* | *Constellation* BG, replaced US ship |
| 2000, HMCS *Calgary* | Surface Action Group, PacMEF |
| 2001, HMCS *Winnipeg* | *Constellation* BG, on scene commander, 17-24 July '01<br>- had TACON of all BG assets during this time. |
| 2001, HMCS *Vancouver* | *John C. Stennis* BG |
| **MARLANT Ships** | |
| 2001, HMCS *Charlottetown* | LANTMEF, joined *Harry S. Truman* BG in Med. |

Figure Two

are likely to considerably more intense for navies outside the bonds of trust that are shared between the Canadian and American navies.

The Canadian navy began inserting ships into CVBGs in the late 1990s in an effort to improve its interoperability with the USN (see figure two). Initially, only West Coast ships, operating out of CFB Esquimalt in British Columbia were involved. This was because the West Coast fleet did not have the same operational commitments as the East Coast fleet (such as STANAVFORLANT), and also because the West Coast fleet had a long tradition of operating with the USN. As such, it was doctrinally more compatible with the USN than the East Coast fleet was, influenced as the latter was by its long history of NATO operations.

The integration of Canadian ships into CVBGs has been a long evolutionary process. Canadian ships started first as members of the Maritime Interdiction Force in the Persian Gulf, and later gradually moved into the actual battle group as the USN's familiarity and ease with closely working with the Canadians improved. What started first as an operational initiative has later gained more explicit strategic credence through the Department of National Defence's policy to improve interoperability with its allies, particularly the United States. The department seeks to develop and maintain what it

[53] Cdr. James Carr, "Network Centric Coalitions: Pull, Pass, or Plug-in?", Student Thesis, (Newport RI: Naval War College, 15 May, 1999), pp. 15-16.

refers to as "Tactically Self Sufficient Units" which are capable of making military contributions sufficiently relevant that their Canadian identity stands out. One need only think of the role Canadian "Coyote" LAV IIIs have played in past operations in Bosnia, Kosovo, and now Afghanistan. As Cmdre. Dan McNeil, Director for Force Planning and Programme Co-ordination recently remarked, "…we will never be able to field strategic level forces. … We're not ever going to be in that game. We're going to be fielding tactical units. (However) if you properly use tactical units, you can achieve strategic effect. That is what we are trying to do."[54]

What is so revolutionary for these series of CVBG operations has been the fact that a Canadian ship has often physically replaced an American one in the CVBG order of battle. This has been an arrangement of mutual benefit between the USN and the Canadian navy in that the United States has be able to take advantage of the economies offered by the deployment of the Canadian ship and Canada has been afforded professional opportunities for its navy that it could not hope to ever obtain operating simply on its own. These include not only the obvious benefits of extended operations in task groups larger than what the Canadian navy typically puts to sea (except for brief periods), but also the ability to operate with assets not in the Canadian order of battle, such as carriers, cruisers, and nuclear submarines. By integrating its ship into the battlegroup, Canada becomes a member of a select club of one, giving it special access in terms of command and control concepts with the USN as it travels down the road of NCW, as well as access to military support not normally offered to its allies. Finally, CVBG operations enable the Canadian navy to develop hard core professional skills in the areas of littoral and interdiction operations that are unavailable in North American waters.

At the same time, such deployments stress the mutual dependencies and vulnerabilities that are central to every good coalition operation. For the Canadian navy, each frigate deployed has value out of proportion to its ultimate contribution to the CVBG given the relative scarcity of Canadian ships (Canada has only 12 *Halifax* class ships). Obviously, sending such ships into the Persian and Arabian gulfs, typical CVBG deployments with Canadian ships, is a far more dangerous mission than the standard fisheries patrol they would most likely be faced with in Canadian waters. Similarly, by replacing an American ship with a Canadian ship, rather than simply augmenting the CVBG with an additional ship, the USN is placing a extremely high degree of trust in the professionalism and competency of Canadian crews. Accepting a Canadian ship into the CVBG reflects an unwritten agreement to look after that ship. RAdm. Mark Fitzgerald CO of the *Theodore Roosevelt* battlegroup notes, “we need to be ready to go on game day – and when we play, every game is game day”.[55] As such, Canadian ships must not place any undue liability on the battlegroup. Last, the placement of a foreign ship within the battlegroup ensures that it operates within a “coalition mindset”. Canadian ships do not operate under US ROE, and there are occasions when this directly impacts on operations. What this means is that the US ships, crews, and most especially, planning staffs, must

[54] Sharon Hobson, “Canada Aims for Defence Interoperability with the US”, *International Defence Review*, Jan. 01, 2001.
[55] Peterson, p. 7.

always consider how they will operate in a multinational environment. In many ways, in the recent Afghanistan operations, the *Stennis* battlegroup was better prepared for coalition operations because of the fact that it had had to operate with *HMCS Vancouver* within its formation for over six months.

To that end, Canadian ships participate in the same series of exercises and workups that all American ships described above. Similarly, the latest revision of GCCS-M is are installed on board the ships and the navy ensures that the crews are fully trained in order to ensure that the ship can share and use the information and pictures distributed on that system.

The Canadian navy has been increasingly challenged by these upgrades due to the legacy systems onboard its ships. The CCS330 system which controls the ship displays in the operations rooms of the *Halifax* frigates and *Iroquois* destroyers is a closed architecture system based on a unique operating system and military specific software and hardware. While state of the art ten years ago, it is becoming increasingly labour intensive in its maintenance, and most seriously, has a very limited capacity to integrate new hardware and software systems. As new capabilities are added to Canadian ships, such as JMCISS initially and now GCCS-M, they must be done so on a stand-alone basis. Canadian display terminals, thus, have no ability to send and receive operational messages. Tactical networking must be done on separate consoles and the information provided by strategic systems like GCCS-M and the Canadian equivalent of the SIPRNET, MCOIN III, become effectively stovepiped. The result is a cluttered operations room where decision makers must consult several different systems in order to gather all the information necessary to perform their jobs. Obviously not the most efficient arrangement in the heat of battle.[56]

Interestingly, while the Canadian navy has tried to remain abreast of the fast moving electronics revolution in command and control technologies, Canadian naval officers point out that this agenda is not, in fact, being driven by American officers. The US is pleased that Canada strives to stay abreast of its naval technological developments so as to discourage the formation of gaps in capabilities. However, Canadian naval officers stress it is the long history of naval co-operation, and overall familiarity between the navies which has facilitated these CVBG exchanges rather than the technical kit that is installed aboard Canadian ships.[57] Nevertheless, Canadian ships typically encounter significant difficulties in seamlessly integrating their efforts in alongside American ones in the battlegroup. These difficulties largely revolve around the issue of accessibility.

In battlegroup operations, CWAN is the principle means for co-ordinating action between Canadian and American ships. As pointed out above, the USN is gradually migrating its $C^3$ functions to web and other digitally based delivery methods. As such, SIPRNET is becoming more and more important to the planning, co-ordination, and execution of

[56] *The Canadian Navy's Command and Control Blueprint to 2010,* p. 17.

[57] Reportedly, the USN would like to extend the same level of co-operation with the RAN, however, the RAN faces considerably more difficulty in freeing up a ship for the six month workup with the CVBG given the distances involved. It is a simply matter to send ships on pre-deployment training exercises given the proximity of Halifax and Esquimalt to American naval bases.

naval operations. However, CWAN and SIPRNET have limited interoperability. E-mail messages can pass between the two systems as long as the US user has been registered with a CWAN account. Nevertheless, the secure mail guard systems strips off any attachments that associated with the e-mail before it goes onto the CWAN. Thus while the Canadian recipient may be provided with the commander's direction, he is unable to see any of the supporting information that accompanies it. Furthermore, only those SIPRNET users who have registered CWAN accounts have their messages forwarded onto the CWAN system. As such, Canadian ships may miss significant portions of message traffic, some of which may have been influential in the development of command direction.

Another key feature outlined above is the growing use of chat features to plan and co-ordinate operations. CWAN supports chat, however, there is no interconnection between the SIPRNET chat and the CWAN chat. As such, in order for a Canadian ship to partake in a chat session with its American counterparts, a CWAN watch officer must simultaneously type what is being entered onto the SIPRNET system. Furthermore, any accompanying information with the chat message must be "air-gapped" onto the system by the LO. Typically, the CWAN watch officer is the Canadian LO assigned to the battlegroup staff aboard the carrier. As there is only a single LO, often this means that it is difficult to get the information onto the CWAN during the periodic absences of the Canadian LO when not on watch. While Canada urges the US to man the CWAN terminal during these times, in periods of high operational tempo, this role can be overlooked at precisely the moment when the Canadian ship needs the information.

Finally, the web features of SIPRNET are similarly limited on the CWAN system. While CWAN supports web pages, essentially it contains only the information that is placed there by the coalition partners. In a US run operation, the majority of the information will be originating from the US. Unlike e-mail, there is no direct connection between SIPRNET web pages and CWAN web pages. As such, web files must be "air-gapped" between the systems. This can be quite a complicated procedure at time involving multiple transfers of information between networks (SIPRNET – NITDS – MCOIN III). The result of these procedures often means that the information available on accessible networks (either CWAN or MCOIN III) is out of date, sometimes by a matter of days. Second, usually the carrier has the only CWAN terminal which means it becomes the sole unit capable of posting information. The lack of redundancy enhances the possibility that information will not be posted onto the system. Furthermore, what information that is posted onto the network does not have the same amount of depth to it. In other words, the ability of coalition officers to surf for more information is seriously limited. Links are not fully functional leading to what can be referred to as only a "snapshot" of the information available to SIPRNET users. As one Canadian officer remarked, "I was happy that I had enough information to operate on a day to day basis" but it was more difficult to get the larger picture of what would happen next. "It was easy to find out what the intent was for the next 24 hours, but we were never entirely sure what they would do after that. This made it difficult to position yourself for up coming operations, to get the appropriate ROE set in place, to position yourself for getting alongside and so on." Ultimately he concluded that the effectiveness of the Canadian contribution was

entirely dependant on a priori established professional relationships between the USN and the Canadian navy. "I was not confident that I could (be kept) fully informed on something other than a voluntary basis." … "(The US) has nothing other than what the US is willing to give and what he is willing to give is based on what your relationship was."

**Conclusions: Lessons of Canadian Participation in CVBG ops for NCW**

What is not clear is whether there is anything but inefficient work around solutions to these problems. The real problem is not so much technical as policy oriented. The desire to protect sensitive information is at the root of all these issues and mandates the physical separation of networks (MCOIN III is a Canada only system just as SIPRNET is a NOFORN system). Releasability software such as Radiant Mercury and [58]SIREN do assist the effort to move information onto coalition networks in a timely fashion, but they are not gateways to the information that US officers use on a day to day basis. This results in two issues for Canadian ships. First, Canadian ships often operate with out even basic operational procedure manuals because they have not be classified RELCAN or RELCWAN. Further, US officers may be extremely reluctant at releasing even what would seem innocuous data for fear of making a mistake that will ultimately impact on their careers.[59] Cases such as these illustrate the difficulty technology like Radiant Mercury or SIREN may have in ameliorating this issue. Second, the dynamic nature of CVBGs means that information-sharing protocols must be re-brokered with each deployment. Sometimes it is a question of proving one's bona fides to the battlegroup in order to gain access. Other times it is a question that the battlegroup staff is simply unaware that the information has not been passed on or is not available to the Canadian ship. Often times, such material is eventually released when the battlegroup commander becomes aware of the issue, but it highlights the impediments to network operations in a coalition environment. Nor should we expect this hesitation to disappear anytime soon; in fact, September 11 may serve to heighten such considerations.

What is instructive about the Canadian experience with US CVBGs is both positive and negative for the overall question of network centric operations in a coalition environment. It is positive in that they demonstrate that despite the technical limitations and differences between the two navies, effective co-operation can be carried out in the modern naval environment. Once a willingness to co-operate and a basis of trust between two forces has been established, technology is not a complete barrier to operational success. Here, Canada's close experience with the US may allow it to assist in the integration of other navies. In its vision document, *Leadmark*, the Canadian navy has proposed that it should seek to develop a "Gateway $C^4$ISR" function that would allow less capable navies to integrate into network centric operations.[60] The Canadian navy has performed such a function the past. During the Gulf War one of the deciding factors in choosing Canada to lead the Combat Logistics Force was the fact that our ships had excellent interoperability with the US (a proposed French ship, *Doudart de Lagrée* "lacked good communications interoperability") our multinational crews, and remaining legacy

[58]

[59] Kevin O'Brien, "Europe Weighs up Intelligence Options", *Jane's Intelligence Review*, March 01, 2001, p. 6.
[60] *Leadmark: The Navy's Strategy for 2020*, (Ottawa, Department of National Defence, 2001), p. 107.

communications systems meant that Canadian ships could talk with pretty well anybody participating in the Gulf.[61]

However, such observations are accompanied by a very large caveat. The relationship between the Canadian navy and the USN is one that has taken decades to evolve. Furthermore, as the above indicates, there are still significant impediments to the seamless integration of forces that NCW would seem to demand. While CVBGs must be prepared for all warfare eventualities in their operations, the operations Canadian ships have participated in have largely revolved around questions of maritime interdiction. In an operation dominated by strike warfare with an asymmetric surface threat emerging from the littoral environment, it is worth wondering how welcome even Canadian ships might be within the CVBG. Finally, as close as Canada is to the United States in terms of its naval interoperability, the still significant limitations imposed on Canadian ships by the security demands of US military networks raise even more troublesome issues for those navies which do not share the same privileged access as Canadian ships and crews. Indeed, while Canadian operations would seem to indicate that network centric operations can indeed take place in a coalition environment, they also indicate that the bar navies will have to jump over in order for them to occur will remain very high. Canadian ships are welcomed into US formations precisely because of the years of shared operational experience and the wealth of trust that has been established between the two navies. In a dynamic coalition environment, the depth of trust will be markedly different. The bar for such navies will be set by both technology and policy issues. Because of the crippling effect slower networks or non-networked ships may have on US battle rhythm, US information releaseability policy may be the stimulus to US unilaterlism.

[61] Mjr. Jean Morin; LCdr. Richard Gimblett, *Operation Friction*, (Toronto: Dundurn Press, 1997), pp. 181-182; Cmdre. D. Miller; Sharon Hobson, *The Persian Excursion: The Canadian Navy in the Gulf War*, (Clementsport NS : The Canadian Peacekeeping Press, 1995), p. 156.