CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
AMSC 4 / CESM 4

# THE FUTURE OF WARFARE: CLUELESS COALITIONS?

By

Colonel Robert Chekan

October 2001

*This paper was written by a student attending the Canadian Forces College in fulfillment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied except with the express permission of the Canadian Department of National Defence.*

*La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.*

# ABSTRACT

The impact of network-centric warfare on future coalitions is examined. The risks to the United States of allowing coalition partners inside the dominant information sphere are discussed. While these risks are not trivial, the paper identifies that disclosure is the most significant challenge facing coalitions in the information age. The argument is made that disclosure restrictions will exclude foreigners from U.S. networks, and this lack of access will undermine the trust within future coalitions. Where there is no trust, there is no coalition. The paper concludes that meaningful coalitions will not be possible if network-centric warfare are implemented by the United States.

# THE FUTURE OF WARFARE: CLUELESS COALITIONS?

## *Introduction*

Alliances and coalitions are the backbone of Canadian global security and defence policy. Although military coalitions have been fashioned for thousands of years, the knowledge-based warfare of the "Information Age" is challenging the very concept of coalition warfare: can meaningful coalitions be held together when some, or most, of the members will not be operating in the information age? Are clueless coalitions inevitable, and can they work?

Knowledge-based warfare is not an option for the future – it is here already. Alvin and Heidi Toffler, in War and Anti-War, argue that warfare follows the economy, and as the economy is shifting to knowledge as a source of wealth, so too is warfare shifting to being knowledge-based.[1] This view is supported by J. Carr in his work on network-centric warfare, "[network centric warfare] is based on concepts that have made American industry and American business the most competitive in the world, and its tenets are as applicable in warfare as they are in business."[2] Moreover, the Tofflers argue the shift really began in the Persian Gulf conflict: there were two air campaigns, a traditional war of attrition by massive bombing, and the precision bombing campaign that used knowledge at its core.[3]

Knowledge-based warfare is challenging coalitions because it is being implemented at different rates by nations, and most rapidly by the United States. This difference in implementation rates introduces gaps in information collection, processing

[1] Toffler, A., and H. Toffler. War and Anti-War. Boston: Little, Brown, 1993: 69.
[2] Carr, J. "Network Centric Coalitions: Pull, Pass, or Plug-In." Final Report, Naval War College, Newport, RI, May 1999: 19.

and dissemination among the coalition partners. These gaps are already evident. During the Kosovo air campaign, John Morrocco, writing for Aviation Week and Space Technology, identified significant coalition capability gaps in both information collection and dissemination, "Allied military forces rely nearly exclusively on the U.S. for strategic reconnaissance…".[4] Moreover, David C. Gompert et al. caution these gaps could develop into "information gulfs" as the United States opens the revolution in military affairs throttles in the future.[5]

Can the gaps in information capabilities among coalition partners be closed? To find the answer this paper looks at *what makes coalitions work*; the importance of *trust*; and how trust is established in coalitions. This is followed by an overview of one concept of knowledge-based warfare: *network-centric warfare*, and the *challenges* this concept will provide for coalition technological compatibility and information disclosure. With these challenges in mind, two *knowledge-based models of future warfare* are presented: a unilateral United States model, and a coalition model. The coalition model of knowledge-based warfare fails to satisfy the need for trust in coalitions, leading to the *conclusions* that coalitions are going to be clueless and ineffective in future.

While common interest may act to pull a coalition together, and this is not trivial, what makes a coalition work once they are put together is a separate challenge on its own.

*Coalitions need a common understanding of the threat they are facing.*

Robert Riscassi, in writing on the Principles for Coalition Warfare, believes that "Any multinational operation will require planning by all the participants, interoperability, shared risks and burdens, emphasis on commonalties, and diffused credit for success."[6] Further, he argues that the test of a coalition's resolve comes when it is necessary for members to compromise. Such compromises begin with a common understanding of the situation at hand, or threat. To build a common understanding of the threat requires the foundation activity of the intelligence preparation of the battlefield, without which "…it is difficult if not impossible to shape uniform perceptions of the threat or agree upon the coalition's courses of action."[7]

*Coalitions are founded on trust based on a shared situational awareness.*

Uniform perceptions of the threat help select more than courses of action, they are used to determine the contributions of coalition members, and, in part, how those contributions will fit together – or the command and control. Indeed, many authors have identified that "…a shared situational awareness of the battle space is necessary for unity of command or unity of effort."[8] Riscassi puts a finer point on the subject of coalition command and control, it comes down to trust and confidence: "Because of the severity and consequences of war, relinquishing national command and control of forces is an act

[6] Riscassi, Robert W. "Principles for Coalition Warfare." *Joint Forces Quarterly*, Summer, 1993 : 58.
[7] Ibid., 64.
[8] Gramer, G.K. "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders Have an Intelligence Dissemination Challenge." Final Report, Naval War College, Newport, RI, May 1999: 2.

of trust and confidence that is unequalled in relations between nations."[9] The fundamental need for trust is supported by Major General Robert H. Scales, Jr., the commandant of the US Army War College. In his opinion, "…the formation of any coalition hinges upon a single, intangible characteristic – trust."[10]

Although trust is intangible, it has been the subject of considerable research in the business world. While it would be absurd to expect findings on trustworthiness in business would translate exactly to the military, there are aspects of business trust that ring true for the military and coalitions. For example, there is an understanding in business that trust is an absolute necessity when people must perform autonomously but also actively cooperate to achieve common objectives.[11] Autonomous, active cooperation is very similar to coalition "unity of effort". What becomes important is how trust is built and maintained.

### ***Trust***

There is no simple, one-size-fits-all definition of trust. In fact, Larry Reynolds, in The Trust Effect, cautions that different cultures approach trust differently.[12] Pamela Shockley-Zalabak et al. have reported that a merging of several definitions provides three basic facets to trust. Trust reflects an expectation that the other party will act benevolently. Trust involves a willingness to be vulnerable and to assume risk. Trust involves some level of dependency.[13]

[9] Riscassi, 67.

[10] Scales Jr., Robert H. "In War, The U.S. Can't Go It Alone." Future Warfare. U.S. Army War College, May 1997: 204.

[11] Shaw, Robert B. Trust in the Balance. San Francisco: Jossey-Bass, 1997: 1.

[12] Reynolds, Larry. The Trust Effect. London: Nicholas Brealey, 1997: 19.

[13] Shockley-Zalabak, Pamela, Katheleen Ellis, and Gaynelle Winograd. "Organizational Trust: What it Means, Why it Matters." *Organizational Development Journal*, Winter 2000: 36.

Trust is not built by words, but by action. “We don’t build trust by asking people to trust us. Those who say “trust me” are inviting suspicion.”[14] Reynolds does suggest there are different kinds of trust. He notes that when there is a single, clear, shared goal and shared penalties for failure, then it is possible to develop trust very quickly. However, he cautions that this trust is “brittle” and tends to last only until the goal is achieved or abandoned.[15]

To build trust that is more robust – the kind of trust that is necessary when facing long, difficult challenges – requires more than an immediate threat and the instincts of survival. Shockley-Zalabak et al. argue there are four main principles that underpin and build a relationship of trust: competence; openness; reliability; and concern.[16] While the principles of competence, reliability, and concern are interesting in their own rights, it is the principle of openness that relates most to the coalition challenges of technological compatibility and information disclosure raised in this paper.

How does openness influence trust? In the business world there is little argument, “High trust organizations ensure that their people know the truth.”[17] Further, Larry Reynolds explains that there are two reasons why openness is critical. First, secrecy is the enemy of trust. Second, “You can’t expect people to contribute in any meaningful way unless they know what they are contributing to.”[18] Additional research supports this, and identifies that trust requires accurate information, explanations for decisions, and openness.[19]

[14] Shaw, 209.
[15] Reynolds, 21.
[16] Shockley-Zalabak et al., 38.
[17] Reynolds, 27.
[18] Ibid., 65.
[19] Shockley-Zalabak et al., 37..

*"Trustworthiness is the backbone of any credible organization," and it needs both open communication and truthfulness to be established.*"[20]

"Trust, however, comes with a price. The more we trust, the more we risk disappointment, if not harm."[21] Although Robert Shaw was writing in a business context the translation to military trust is straightforward. Effective coalitions are risky – they are based on vulnerability to a common threat, and they expose members' dependencies. To be effective other members in the coalition have to be trusted. To build and maintain that trust requires openness and information sharing.

### ***Network-Centric Warfare***

Network-centric warfare will have a profound impact on trust within future coalitions. To understand why, it is important to put network-centric warfare in context and identify what makes this new warfare so different.

In the information age there has been considerable debate on whether information technology is pushing changes in warfare, or whether the concepts and doctrine of warfare are pulling information technology along. In their analysis, Alvin and Heidi Toffler declare discovery of a "step-by-step progression from initially narrow technical concerns toward a sweeping conception of what will someday be called "knowledge strategy".[22] The Tofflers may be right. In just a few years the tone and content of U.S. thinking on information age warfare has changed significantly. In Joint Vision 2010, the

[20] Brownell, Eileen O. "How to create organizational trust." *Manage*, Nov/Dec 2000: 11.
[21] Shaw, 28.
[22] Toffler, 139.

focus is on information superiority.[23] In contrast, current discussion addresses information dominance and network-centric warfare.

Network-centric warfare “connects sensor platforms with weapons (or shooters) platforms in a robust network, giving a commander the ability to match weapons to targets irrespective of platform.”[24] What is envisioned is a seamless system of systems approach with fully integrated intelligence, surveillance, reconnaissance and command and control. Weapons systems on remote platforms would engage targets detected, tracked and identified by other remote nodes in the architecture. Network-centric warfare is expected to increase combat power, accelerate the speed of command and enable synchronization.[25] L.R. DIRusso, of the U.S. Naval War College, identifies the basic tenets of network-centric warfare to be shared awareness, speed of command, self-synchronization, greater lethality and increased survivability.[26]

Network-centric warfare is fundamentally different than any warfare that has preceded it because it intends to operate in real-time using all sources of information to establish unprecedented battlespace awareness. “All sources” will include those that the United States highly protects because compromise of these sources would have an impact on long-term national security.

How fanciful is this kind of warfare? Carr, writing in 1999, suggests that, “Network-centric warfare is not a remote concept on a horizon, it is nascent in today’s maritime operations and inevitably will be the way in which the U.S. Navy will fight

[23] United States. Joint Vision 2010. Washington, D.C.: Government Printing Office: 16.
[24] Geraghty, B.A. “Will Network-Centric Warfare be the Death Knell for Allied/Coalition Operations?” Final Report, Naval War College, Newport, RI, May 1999: 2.
[25] Ibid., 3.
[26] DIRusso, L.R. “Casting Our Net: Can Network Centric Warfare and Multinational Operations Coexist?” Final Report, Naval War College, Newport, RI, February 2001: 14.

wars in the future."[27] Moreover, the concept of network-centric warfare has spread beyond the U.S. Navy. Joint Vision 2020 states, "The development of a concept labeled the global information grid will provide the network-centric environment required to achieve [U.S.] goals."[28]

### *Network-Centric Warfare Challenges to Future Coalitions*

When implemented, network-centric warfare will move real-time all-source information at the speed of light throughout a fighting force. This will complicate two existing challenges to coalitions: technological compatibility and information disclosure.

#### The First Challenge: Technological Compatibility

The challenge of information sharing in future coalitions and alliances is a concern in the United States. Some argue that allies "have not yet come to appreciate the value gained from a paradigm shift in the Information Age."[29] And looking at the future of naval warfare, " [network-centric warfare] is widening an interoperability chasm between American and allied forces who may fight alongside each other in the future." [30] "It raises concerns among our allies and potential coalition partners as to their ability to stay even with the United States and contribute to future operations."[31]

The U.S. debate on technological compatibility with allies and coalition partners suggests two alternatives: establishing and promulgating universal standards that partners could build to, or selling U.S. technology to coalition partners. The problem is that both

[27] Carr, 1.
[28] United States. Joint Vision 2020. Washington, D.C.: Government Printing Office, 2000: 9.
[29] Carr, 18.
[30] Ibid., 19.

approaches raise security concerns. M.B. Black notes that the potential security risk involved in the transfer of militarily-significant technology to coalition partners has been noted by senior defense officials.[32] Moreover, he writes that a "reliance on common systems and the adoption of common technical standards could cause the U.S. to surrender its technological edge."[33]

The alternative to building to common standards or using U.S. equipment would be to incorporate coalition members' technologies into the overall network. However, this would introduce vulnerabilities into the network. In general, information infrastructure is most vulnerable to intrusion, disruption and destruction at the least protected and sophisticated nodes. In the case of coalitions, the least protected and sophisticated of the nodes would be those of the least technologically developed coalition members. Clearly, "A key risk inherent in fostering greater connectivity is that the United States may expose itself to attacks on its own information infrastructure…".[34]

Exposing the United States to attacks on information infrastructure could be especially troubling. In leading in the implementation of knowledge-based warfare, the United States is becoming more dependent on that technology to fight wars. Degradation or disruption on information architectures would affect American war-fighting capability more so than the abilities of less sophisticated militaries. The caution: "In our quest for

[31] Geraghty, 5.

[32] Black, M.B. "Coalition Command, Control, Communications, Computer, and Intelligence Systems Interoperability: A Necessity or Wishful Thinking." Paper, Army Command and General Staff College, Fort Leavenworth, KS, June 2000: 55.

[33] Ibid., 54.

[34] Arquilla, John, and David F. Ronfeldt. In Athena's Camp: Preparing for Conflict in the Information Age. RAND, 1997: 432.

information dominance we must be careful to ensure we do not put the nation at risk through a growing dependence on information."[35]

In short, the challenge of coalition technological compatibility raises significant risks for the United States. First is the risk that technologies would be compromised and the U.S. edge lost. This clearly would be in direct opposition to the concept of information dominance. Second is the risk that less technologically developed coalition members will introduce vulnerabilities into the information infrastructure and systems. Third is the risk that degrading the information architecture would have the largest impacts on the U.S. itself once many of their weapons systems are dependent upon that information architecture. The response is not to slow down on knowledge-based warfare. Instead, the call is to protect the infrastructure.[36]

### The Second Challenge: Information Disclosure

Whether or not the technological compatibility risks can be managed to an acceptable degree, there is a second, perhaps more challenging, dimension involved in coalition members "staying even" with the United States in future. B.A. Geraghty, writing for the Naval War College, states, "Interoperability is not about technology compatibility alone, but also includes issues such as intelligence sharing…".[37] He continues, "The dilemma is twofold – technology and policy."[38] The policy he refers to is the policy on information disclosure.

[35] Orr, J.E. "Information Dominance: A Policy of Selective Engagement." Paper, Army War College, Carlisle Barracks, PA, April 1997: 17.
[36] Ibid., 18.
[37] Geraghty, 6.
[38] Ibid., 7.

The issues surrounding disclosure of information in coalitions are not trivial, nor have they been resolved. In a review of intelligence sharing in Bosnia between 1995 and 1997, B.K. Peavie states that "Progress is still needed in the classification and releasability of combined-joint intelligence information."[39] But such progress must be balanced with concerns for national security. From the United States perspective, "the need and desire for coalition interoperability must not outweigh the need and desire to protect national security."[40]

There are three general criteria for disclosure of American information to foreign nationals. First, the release of the information must be consistent with U.S. national security objectives. Second, the release must be seen to benefit the United States. Third, the disclosure must be unlikely to be harmful to the United States.[41]

There are many occasions in history when the United States has determined the three disclosure criteria apply and the information has been released to allies, coalition partners and others. For example, evidence of Osama Bin Laden's involvement in the attacks of 11 September, 2001, has been shared with members of the coalition against terrorism. Undoubtedly, the kind of information shared, and the timing of the sharing of the information were both carefully controlled so that the three U.S. disclosure criteria were followed. The question for the future is how will the three disclosure criteria be applied in an age of information dominance and network-centric warfare?

Arguably the information implicating Bin Laden in terrorism is strategic in nature. As such there has been time to sanitize the information through removal of "source"

[39] Peavie, B.K. "Intelligence Sharing in Bosnia." Paper, Army Command and General Staff College, Fort Leavenworth, KS, January 2001: 44.
[40] Black, 68.
[41] Gramer, 4.

identifiers prior to it being shared. This works during coalition building because potential partners are interested in what is known, not how the information was collected. In contrast, network-centric warfare is focused at the tactical level at which information must be validated and correlated in real-time. In network-centric warfare there is not time to sanitize the information to protect information collection capabilities. As a result, although release of the information could possibly meet the first two disclosure criteria, it is extremely difficult to meet the third criterion: to ensure the release cannot be harmful to the United States, in real-time.

Information disclosure is still more complex because while U.S. commanders must decide what is releasable, "U.S. joint doctrine … provides little substantive assistance or guidance to the commander to accomplish that mission."[42] U.S. commanders have faced this dilemma already. Kevin A. O'Brien writes that the U.S. did not meet European information and intelligence needs during the Kosovo conflict because it failed, "…to establish a clear policy and implementation plan to explain when and how coalition partners could be connected to U.S. systems for intelligence and data-sharing means."[43] Not only were clear policies not provided, U.S. commanders chose to restrict release of information during Operation ALLIED FORCE because of concern over potential harm to U.S. forces: a separate "U.S. ONLY" Air Tasking Order for U.S. forces was built daily and not released to the rest of the alliance. Moreover, the future of information disclosure is not bright. O'Brien notes that U.S. military chiefs have

[42] Ibid., 1.

[43] O'Brien, Dr. Kevin A. "Europe Weighs up Intelligence Options." *Jane's Intelligence Review*, March 01, 2001: 4.

expressed they would be unwilling to share intelligence data in the future due to concerns that sensitive data might be leaked.[44]

There is a final consideration in coalition disclosure that in effect assures that coalition partners will be working with different information during operations. Coalitions are cobbled together to achieve a specific mission or objective. As such, "Military coalitions may include partners whose reliability is stipulated on the threat at hand and will not last beyond the resolution of the contingency…".[45] A coalition partner against terrorism today may be an adversary tomorrow. As a result the amount of information shared, and when it is shared, must continue to be carefully controlled. While this is true today, the volume and immediacy of information that will be available in network-centric warfare will be significantly greater. The need to carefully control such information will preclude some coalition members from being authorized to join the network.

Overall it is likely that some information will be shared in future coalitions, particularly at the strategic level, but this information will be carefully controlled and time will be required to sanitize it. In contrast network-centric warfare is tactical and demands information in real-time. There will be inherent risks to the United States of harmful release of collection, processing and dissemination capabilities because there will not be time to sanitize the information resident on the network. Given the potential for significant, long-term harm to the United States of capability disclosure, it is unlikely that U.S. commanders will take the risk and authorize coalition partner access to the networks. Moreover, coalitions may be broad-based and objective-specific: today's

[44] Ibid., 6.

[45] Riscassi, 70.

coalition partner may not be one tomorrow. In the age of information warfare, the protection of capabilities will preclude full disclosure that access to networks would provide to coalition partners: the risks will be too high.

### *Knowledge-based Models of Future Warfare*

In the information age engaging partners at the tactical level will be risky for the United States. These risks will be significant: the risk of compromise of technological edge; the risk of introducing vulnerabilities to the networks themselves; the risk of undermining weapons systems; and the risk of compromising U.S. capabilities to collect and use information. To retire these risks the United States has two broad choices: unilateral action; or building coalitions with partners that will have very different accesses to information in real-time – clueless coalitions.

#### A Unilateral United States Model of Knowledge-Based Warfare

The first option is for the United States to act alone. American national security policy is very clear, "America must be willing to act alone when our interests demand it."[46] This is echoed by the Department of Defence, "… the United States will retain the capability to act unilaterally when necessary…".[47]

Unilateral action by the United States may become a more necessary approach if allied and coalition militaries lag far enough behind American capabilities. In a RAND corporation report, prepared for the United States Air Force in 2000, the authors note

[46] United States. A National Security Strategy for a New Century. Washington, D.C.: The White House, December 1999: iv.
[47] United States. Report of the Secretary of Defense to the President and the Congress. Washington, D.C.: Government Printing Office, 2000: 3.

that, “The gap between the capabilities of the U.S. and its key allies may also be widening to the extent that the NATO allies may not be able to perform military missions at U.S. performance levels.”[48] More to the point the U.S. after action report on Kosovo concludes, “unless addressed [allied] disparities will limit NATO’s ability to operate as an effective alliance over the long term.”[49]

Unilateral action greatly simplifies information protection, and there is discussion in the United States that it is time to consider new approaches to sharing information with allies. The thought is that the Cold War was a time of relatively free sharing of information with allies because this met national security needs. However, since the end of the Cold War, there have been calls for a more guarded approach to information sharing. In a 1997 RAND document the authors argue that “…there are good reasons to question military openness [with allies] as a predominant grand strategy.”[50] The good reasons are to preserve U.S. advantages in information collection, processing and dissemination.

Unilateral action is not being publicly championed in the United States. Nonetheless, the consequences of such an approach are being considered. Principle among the consequences is that if, in preparing to act alone, the U.S. adopts a more closed approach to information sharing, it “retains [its] predominance, but this might motivate allies, as well as adversaries, to enter into a new, information arms race with the United States.”[51] To a degree this is already underway: European intelligence needs were

[48] Hura, Myron, et al. Interoperability, A continuing Challenge in Coalition Air Operations. Project Air Force Document, RAND, 2000 : 30.
[49] United States. Kosovo/Operation Allied Force After Action Report. Washington, D.C.: Government Printing Office, January 2000: xix.
[50] Arquilla, 429.
[51] Ibid., 430.

not met by the U.S. during the Kosovo War.[52] As a result the Europeans are considering plans for a satellite-based reconnaissance system of their own.

Fundamentally the issue for allies is one of trust. Dependency contributes to trust when it is mutual. Dependency undermines trust when it is one-way. Moreover, trust is built on openness. The downside of a reduction in military openness would be to leave allies no alternative but to build competitive information collection, processing and dissemination capabilities.

### *A Coalition Model of Knowledge-Based Warfare*

The second option is to find an approach to coalition warfare in future that is compatible with information age capabilities. DIRusso believes that coalition warfare and network centric warfare can co-exist if the tasks are well understood and assigned. He argues the Joint Task Force Commander will have the task to integrate a network-centric-capable force and a less sophisticated one.[53] These forces would then operate under different sets of rules and could be effective as not all tasks would require the same level of situation awareness.[54] In effect, the apportionment of both responsibilities and access to information would be made based on the capabilities the coalition members bring. Geraghty is somewhat more pointed in his approach. He proposes that the more informed and capable US forces would slog away at the tough work and less important and less

[52] O'Brien,  6.
[53] DIRusso, 14.
[54] Ibid., 15.

risky ventures would be allocated to the less-well informed and less-capable coalition members.[55]

If such a coalition was cobbled together there would still be information needs. Writing just after the Persian Gulf conflict, but well before network-centric warfare and information dominance concepts were under consideration, Riscassi identified that, "Unless the architect incorporates the ability to share with, and in turn receive from, other national forces, the battlefield will not be seamless and significant risks will be present."[56] His concerns remain valid today: partners must share information or little coordination of effort is likely. Several options for information sharing are proposed in the current literature.

First, a shared information centre could be established. In the Gulf War, the Coalition Coordination, Communication, and Integration Center was "… a place to integrate the staffs of the coalition forces…[that] serves as a model for the commander in future operations."[57] The problem in the information age is that it will take time to sanitize information – and network-centric warfare does not have that time. This suggests access to information would be necessary – which again raises the issue of disclosure. "Without satisfactory levels of intelligence disclosure, the communications used for intelligence fusion or even the coalition headquarters could become off-limits to many coalition members."[58] It is difficult to imagine coordinated effort if some or most of the coalition partners are not authorized to participate in the coalition headquarters.

[55] Geraghty, 14.
[56] Riscassi, 69.
[57] Geraghty, 7.
[58] Gramer, 3.

Second, training with coalition partners has been helpful in the past. M.S. Wooley, writing in the early 1990s, argued that objectives, command and control, and interoperability are all inter-dependent and could be sorted out through training together. In short, "…the inter-dynamics of the elements of coalition warfare can only be attained through practice."[59] While this has been effective in the past, no amount of training can overcome the disparities in access to information that will result when one member is networked in and the other is not.

Third, information sharing could be handled by liaison teams. "The antidote to the fog and friction of coalition warfare is not technology, it lies in trusted subordinates who can deal effectively with coalition counterparts."[60] Robert H. Scales, Jr., argues this point and champions the development of a cadre of U.S. officers specially trained and employed in such duties. It is "trust, not technology" that binds coalitions together.[61] Clearly, liaison teams could be effective in sharing sanitized information, but real-time information, used by U.S. networked forces, could not be made available. Even with liaison teams the information gaps would remain.

Coalitions work based on burden sharing, shared risk and trust. Trust is based on openness. The clueless coalition concept outlined above would fail all of these criteria. Moreover, traditional approaches of special coordination centres, training and liaison officers will not bridge the real-time information gaps that will be a reality in network-centric warfare.

[59] Wooley, M.S. "Coalition Warfare: Implications for the Naval Operational Commander in the Way Ahead." Final Report, Naval War College, Newport, RI, June 1992: 23.
[60] Scales Jr., Robert H. "Trust, Not Technology, Sustains Coalitions." *Parameters,*_Winter 98/99, Vol. 28 Issue 4: 9.
[61] Ibid., 4.

In reality, coordination centres, training, and liaison officers are workarounds at the tactical level. However, the problem is strategic: a strategy of information dominance and network-centric warfare. For strategic issues “no amount of operational, tactical or technological workarounds can repair an interoperability problem whose origins are fundamentally at the strategic level.”[62]

***Conclusions***

Coalitions work because of burden sharing, shared risks and trust – trust that is built upon a foundation of shared information and openness.

Knowledge-based war-fighting in the information age has given rise to the concept of network-centric warfare. For network-centric warfare to work, information must be protected and access to the networks controlled. It would be risky for the U.S. to include allies and coalition partners in war-fighting networks. Moreover, the risks would be considerable: the risk of having technology compromised and losing the technological edge; the risk of increased vulnerabilities and having the networks degrade or fail; and the risk of losing direct war-fighting capability that is dependent upon the information architecture if it does fail. Given these risks the United States will be unlikely to include coalition partners inside the network.

As significant as these risks are, the greater challenge will be the disclosure of information to allies and coalition partners. U.S. disclosure policy would support the sanitizing of information for release to allies when there is time. But, in network-centric warfare there is no time – all feeds must be provided to the network in real-time. Sensors must feed shooters. Moreover, it is U.S. policy that the commander is to determine such

[62] Hura et al., 18.

information sharing in a coalition. Given the U.S. disclosure guidelines and the transient nature of coalitions, commanders will be unlikely to include partners inside the network.

To paraphrase Yogi Berra, the future of coalition warfare "ain't what it used to be". It seems that in order to effectively employ network-centric warfare the U.S. must engage in unilateral operations. This approach would eliminate the coalition-induced risks to U.S. capabilities and would be consistent with the U.S. disclosure policy. A second option would be for the U.S. to establish several levels of warfare within a coalition – with coalition members being granted different access to information. However, because of the technological risks and information disclosure rules it is unlikely that any coalition members would be inside the network. It seems clueless coalitions are inevitable if network-centric warfare is implemented by the United States.

Could clueless coalitions work? Is "Network-centric warfare … simply another factor to challenge the operational commander when planning coalition operations, requiring significant operational leadership."?[63] Clearly, traditional approaches of establishing coalition information centres, conducting coalition training, and establishing liaison officers that some call for would have little effect. Such approaches have been useful in the past because the pace of the battle allowed for review and sanitization of information prior to its release. That time will not be available within network-centric warfare forces.

The fundamental issue is that coalitions work because of trust. Trust based on shared burdens and risks. Trust based on shared understandings. Trust based on openness. Network-centric warfare would not share burdens and risks. Network-centric would not

[63] Geraghty, 15.

support shared understandings. Network-centric warfare would not support openness with allies or coalition members: the risks would be too high.

The elimination of trust in coalitions is a fundamental, strategic issue, as it would be a natural consequence of a decision to implement network-centric warfare. As a strategic issue, the resolution would have to come at the strategic level.

The U.S. has faced strategic compromises before and found the resolve to bend to preserve coalitions. Dwight D. Eisenhower begins his book, Crusade in Europe, noting that history is replete with examples of the ineptitude of coalitions at war, but ends by concluding that the single most enduring lesson of the war was that coalitions can be made to work. “The key to the matter is a readiness, on highest levels, to adjust all nationalistic differences that affect the strategic employment of combined resources.”[64]

In the information age the U.S. faces a strategic choice. The implementation of network-centric warfare would create clueless coalitions and prevent meaningful coalition trust and warfare. Clueless coalitions will not work.

[64] Eisenhower, Dwight D. Crusade in Europe. New York: DoubleDay, 1948: 451.

## Works Cited

Arquilla, John, and David F. Ronfeldt. In Athena's Camp: Preparing for Conflict in the Information Age. RAND, 1997.

Black, M.B. "Coalition Command, Control, Communications, Computer, and Intelligence Systems Interoperability: A Necessity or Wishful Thinking." Paper, Army Command and General Staff College, Fort Leavenworth, KS, June 2000.

Brownell, Eileen O. "How to create organizational trust." *Manage*, Nov/Dec 2000: 10-11.

Carr, J. "Network Centric Coalitions: Pull, Pass, or Plug-In." Final Report, Naval War College, Newport, RI, May 1999.

DIRusso, L.R. "Casting Our Net: Can Network Centric Warfare and Multinational Operations Coexist?" Final Report, Naval War College, Newport, RI, February 2001.

Eisenhower, Dwight D. Crusade in Europe. New York: DoubleDay, 1948.

Geraghty, B.A. "Will Network-Centric Warfare be the Death Knell for Allied/Coalition Operations?" Final Report, Naval War College, Newport, RI, May 1999.

Gompert, David C., Richard L. Kugler and Martin C. Libicki. Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs. Washington, D.C., National Defense University Press, 1999.

Gramer, G.K. "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders Have an Intelligence Dissemination Challenge." Final Report, Naval War College, Newport, RI, May 1999.

Hura, Myron, et al. Interoperability, A continuing Challenge in Coalition Air Operations. Project Air Force Document, RAND, 2000.

Morrocco, J.D. "Kosovo Conflict Highlights Limits of Airpower and Capability Gaps." *Aviation Week & Space Technology*, May 17, 1999:

O'Brien, Dr. Kevin A. "Europe Weighs up Intelligence Options." *Jane's Intelligence Review*, March 01, 2001:

Orr, J.E. "Information Dominance: A Policy of Selective Engagement." Paper, Army War College, Carlisle Barracks, PA, April 1997.

Peavie, B.K. "Intelligence Sharing in Bosnia." Paper, Army Command and General Staff College, Fort Leavenworth, KS, January 2001.

Riscassi, Robert W. “Principles for Coalition Warfare.” *Joint Forces Quarterly*, Summer, 1993: 58-71.

Reynolds, Larry. The Trust Effect. London: Nicholas Brealey, 1997.

Scales Jr., Robert H. “In War, The U.S. Can’t Go It Alone.” Future Warfare. Pennsylvannia, U.S. Army War College, May 1999.

---. “Trust, Not Technology, Sustains Coalitions.” *Parameters*, Winter 98/99, Vol. 28 Issue 4: 4-11.

Shaw, Robert B. Trust in the Balance. San Francisco: Jossey-Bass, 1997.

Shockley-Zalabak, Pamela, Katheleen Ellis, and Gaynelle Winograd. “Organizational Trust: What it Means, Why it Matters.” *Organizational Development Journal*, Winter 2000: 35-48.

Toffler, A., and H. Toffler. War and Anti-War. Boston: Little, Brown, 1993.

United States. A National Security Strategy for a New Century. Washington, D.C.: The White House, December 1999.

United States. Joint Vision 2010. Washington, D.C.: Government Printing Office, 1995.

United States. Joint Vision 2020. Washington, D.C.: Government Printing Office, 2000.

United States. Kosovo/Operation Allied Force After Action Report. Washington, D.C.: Government Printing Office, January 2000.

United States. Report of the Secretary of Defense to the President and the Congress. Washington, D.C.: Government Printing Office, 2000.

Wooley, M.S. “Coalition Warfare: Implications for the Naval Operational Commander in the Way Ahead.” Final Report, Naval War College, Newport, RI, June 1992.