The NATO Response Force

Facilitating Coalition Warfare through Technology Transfer and Information Sharing

Jeffrey P. Bialos and Stuart L. Koehl

Report of a study conducted by the
Center for Transatlantic Relations and
Funded by the Center for Technology and
National Security Policy

Center for Technology and National Security Policy

National Defense University

September 2005

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **SEP 2005**	2. REPORT TYPE	3. DATES COVERED **00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE **The NATO Response Force. Facilitating Coalition Warfare through Technology Transfer and Information Sharing**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,300 5th Avenue,Washington,DC,20319-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES **114**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

Jeffrey P. Bialos is the Executive Director of the Transatlantic Security and Industry Program at the Johns Hopkins University Paul H. Nitze School of Advanced International Studies Center for Transatlantic Relations, and a partner in the law firm of Sutherland Asbill and Brennan. Mr. Bialos previously served in a number of senior positions in the Clinton Administration, including most recently as Deputy Under Secretary of Defense for Industrial Affairs. He received the Defense Department's Distinguished Service Medal for his service. He has published numerous articles and reports on defense and security issues, and conducted studies of a variety of issues concerning the transatlantic armaments market, NATO and related subjects. He was also appointed by Governor Mark Warner of Virginia to serve on Secure Virginia, a panel overseeing Virginia's homeland security efforts. Mr. Bialos is a graduate of Cornell University (A.B. with honors), the University of Chicago Law School (J.D.) and the Kennedy School of Government, Harvard University (M.P.P.)

Stuart L. Koehl is a Fellow at the Center for Transatlantic Relations, where he focuses his research activities on transatlantic security and industrial issues. A graduate of Georgetown University, Mr. Koehl has been a defense analyst for twenty-five years and has conducted a wide range of analyses for both government and industry on defense technology, strategy, and transformation issues.

Acknowledgements. This study is based on a review of unclassified, open literature and interviews with selected U.S. government, NATO, and industry personnel. We acknowledge the support and assistance of these individuals, who took time out from busy schedules to talk to us. We acknowledge Johns Hopkins University's Center on Transatlantic Relations (CTR) and National Defense University (NDU) for their support of this project. In particular, we appreciate the helpful advice and comments of Hans Binnendijk and Richard Kugler at NDU and Dan Hamilton at the CTR. As always, however, the responsibility for content is that of the authors, not the institutions with which they are affiliated, nor the sources on which they drew.

Jeffrey P. Bialos and Stuart L. Koehl
Washington, D.C.

Defense & Technology Papers ***are published by the National Defense University Center for Technology and National Security Policy, Fort Lesley J. McNair, Washington, DC. CTNSP publications are available online at http://www.ndu.edu/ctnsp/publications.html.***

Contents

Tables

Figures

Executive Summary

At the Prague Summit in 2002, NATO Heads of State announced the creation of the NATO Response Force (NRF), a relatively small expeditionary force for spearhead operations in out-of-area conflicts. The central concept was to create, over time, an advanced, primarily European force for high-intensity conflicts that would catalyze force transformation and capability acquisition in Europe, promote Transatlantic force interoperability, and provide Europe with out-of-area capabilities to match its new strategic direction and reorient NATO toward out-of-area expeditionary operations. The hope was and is that this type of operational force would, along with other steps, help to revitalize the NATO alliance and improve Transatlantic security relations in these times of tensions and drift.

The NRF is intended to be a transformational force that will not only be able to meet the security needs of NATO in the 21st century but also serve as an agent of change whereby all the member nations of NATO will be able to bring new technology, capabilities, and concepts of operations into their national forces. While the NRF is still a work in progress, the threats and missions that the Force is intended to address will undoubtedly require, and encourage the acquisition of, strategic mobility and deployability, battlefield agility, and high lethality. Unlike previous joint forces, which tended to fight in a segregated fashion (by virtue of either roles or geographical boundaries), the NRF is intended to be fully integrated, i.e., units will be able to fight within the same battle space without regard to national origins and unconstrained by geographical boundaries. Significantly, this coalition warfighting construct implies the need to fully share information within the Force at the tactical and operational level, something that can only be done if there is a significant level of technical, tactical, and operational inter-operability—to say nothing of a common doctrine and concept of operations.

Undoubtedly, the sharing of U.S. technology and technical information would facilitate, and in some cases be essential to, the development and fielding of a highly capable and interoperable NRF. Unfortunately, however, the history of recent Transatlantic armaments initiatives suggests that the complex problems associated with such technology and information sharing with the United States could be a significant limiting factor in standing up the NRF, and that new or special approaches should be considered to address these issues. If the NRF is to succeed, both in its primary mission as NATO's fast reaction, cutting-edge force, and as an instrument of military transformation within the Alliance, then information-sharing and technology transfer issues must be identified, addressed and resolved expeditiously. Hence, this study is primarily an examination of the issues associated with transferring U.S. technology and information needed for standing up such an advanced force for early entry into high-intensity conflicts.

In the course of evaluating these issues and making recommendations on ways forward, this essay also makes a number of additional, and broader observations about the nature of 21st century coalition warfighting, the centrality of network-centric warfare to coalition operations, and the importance and complexity of improving force interoperability in an increasingly network-centric environment. In this regard, the NRF is really a microcosm of broader crosscutting issues and challenges inherent in developing an effective coalition warfighting capability and cohesive alliance for the 21st century. Undoubtedly, the NRF will not provide a

basis for solving all of these complex challenges. But it does offer an opportunity for experimentation and testing—the essence of military transformation—and the forging of creative solutions.

Specifically, in organizing this analysis:

- Section I sets forth an understanding of the purposes, operational realities and developmental path of the NRF—which is critical to establishing a conceptual baseline for identifying and assessing the technology transfer needs associated with the Force.
- Section II seeks to identify and prioritize the technology transfer and information sharing needs associated with standing up the NRF, including those related to Force operational and doctrinal needs, ensuring force interoperability, and incentivizing the acquisition of enhanced capabilities. As the NRF is still a work in progress, we have, of necessity, made educated guesses about its likely trajectory in order to identify technology and informational needs.
- Section III assesses the specific technology transfer issues, concerns, and impediments likely to arise with respect to the releasability of needed technologies and information sharing under applicable U.S. laws, rules and policies, and makes recommendations on specific and realistic steps needed to address these concerns so that the NRF can achieve its stated purposes.

As discussed in more detail below, this study has found the following:

1. The NRF: The Tenuous Link Between Its Goals and Operations. Specifically, the purposes of the NRF are relatively clear:

- Provide NATO a *capability* to act rapidly and lethally in out-of-area conflicts and, in so doing, strengthen its *raison d'etre* as a military alliance that can handle 21st century security threats;
- Operate as a catalyst for focusing and promoting the *transformation* of the Alliance's military capabilities to meet these threats; and
- Enhance *interoperability* between the multinational elements of the NRF in order that it can effectively achieve its mission goals.

Since the Prague Summit, SHAPE has made significant progress in moving the NRF from concept to operations. A six-month rotational force, the NRF will have three phases of development, including: the stand up of an initial "spearhead" force in 2004-6; full operational capability in 2006 (using European ground elements together with U.S. "enablers" in areas such as intelligence, surveillance and reconnaissance (ISR), lift, and so forth); and, in 2013 and beyond, the integration of European or NATO enablers as Europe and/or NATO acquires advanced capabilities in key areas such as airlift, precision munitions, missile defense and Command, Control, Communications Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).

Despite these promising beginnings, there are several significant realities concerning the NRF that warrant serious consideration and make it more difficult to assess the Force's technology transfer needs:

- Given SHAPE's operational focus and the necessary priority on standing up the NRF soon, there has been little longer-term focus to date in NRF force planning on explictly linking the NRF's long-term development to its underlying capability acquisition goals (e.g., lift, precision munitions, and the like). While the NRF undoubtedly will integrate new European capabilities as they come on line, there is no specific plan or roadmap as to how the NRF will catalyze the acquisition of such capabilities.
- There also is no clear plan to facilitate NRF interoperability (i.e., to ensure that the forces of participants, with different levels of capability for years to come, will be able to operate together on the battlefield).
- Finally, there is no clarity concerning the extent to which the United States will contribute its advanced network-centric enablers during NRF Phase II when they are critical to the Force's operation as a cutting edge spearhead force (i.e., when advanced European enablers in areas from lift to network-centric warfare are still on the drawing board).

These uncertainties about the NRF—issues of concern in their own right—make it more difficult to assess the NRF's technology transfer and information needs.

2. Critical NRF Technology Transfer Needs Relate to Interoperability and Long Term Capability Acquisition. The reality is that, for the most part, the *capability* needs of the NRF in its early phases can largely be met by existing European capabilities and European industrial capabilities—and without significant U.S. technology transfer. The key NRF needs for technology and information sharing, and where the significant and complex policy issues undoubtedly will arise, are twofold:

- To ensure force *interoperability* in NRF Phase I (which will require at least secure communications and avoidance of friendly fire), Phase II (i.e., when European ground and naval forces link up to and take advantage of outputs from current U.S. enablers of network-centric warfare) and Phase III (i.e., when the NRF is linked to significant U.S. network-centric capabilities under development and new European capabilities as they emerge that will provide full situational awareness and ability for collective engagement). Significantly, interoperability is less about transferring enabling technologies than sharing classified and unclassified information necessary for full situational awareness and friendly fire avoidance, including access to ISR and command and control systems (linkages and software), real-time, actionable outputs from such ISR assets, and detailed technical information concerning network architectures, interfaces, protocols, and file structures needed to allow the seamless transfer of information between national systems.
- To meet the long term goal of European *capability* acquisition for NRF phase III. While some capability areas do not require significant U.S. technology (strategic lift, ground vehicles), other areas (sensors, ISR capabilities) would significantly benefit from U.S. technology.

The Need for Heightened Focus on Interoperability: The overwhelming focus by the United States and NATO on European *capability acquisition*, reflected in the Defense Capability Initiative and the Prague Capabilities Commitment, has effectively resulted in far less attention being paid to improving *interoperability* between U.S. and allied forces. While Europe may acquire some or all of the PCC capabilities, the reality is that numerous of these acquisitions and the fielding of these capabilities will occur years hence—if at all. Thus, the United States and its partners should, in the context of NRF and otherwise, undertake robust and focused efforts in the near- and mid-term on enhancing interoperability of coalition forces likely to operate at very different levels of capability for the next decade and beyond. This new shift in focus inevitably changes the priorities of potential Transatlantic collaboration. In this regard, wholly distinct from the list of capabilities developed at Prague, with its focus on lift, precision guided munitions and the like, the spectrum of interoperability runs from secure communications and friendly fire avoidance to establishing common levels of situational awareness, and, at the high end, having the ability for cooperative logistics, cooperative asset tasking and cooperative engagement. Plainly, in this new era, the focus on interoperability must be achieved through the development of coordinated and, to some extent, common network-centric capabilities, including the establishment of a common architecture into which nations can "plug and play" and thereby achieve secure communications, similar levels of situational awareness, and other potentially higher order forms of interoperability.

3. Current U.S. Policy and Processes Would Likely Result in A "Dumbed Down NRF." Regrettably, the application of current U.S. armaments cooperation, technology transfer, and information sharing processes and standards, including the U.S. National Disclosure Policy for release of classified information and the International Traffic in Arms rules governing the export of unclassified technical data, would likely result in: 1) lengthy, non-transparent, fragmented, and ultimately frustrating review processes; and 2) eventually, a "dumbed down" NRF with limited interoperability along the spectrum outlined above, limited connectivity to advanced U.S. network-centric warfare enablers, and, hence, less potency as an expeditionary force, greater risk of casualties (from friendly and unfriendly fire), and little real opportunity for leveraging U.S. technology for capability acquisition. A key question is whether any NATO country will be willing to put its forces at risk in 21st century high-intensity encounters with "second best" capabilities in these circumstances.

To highlight the critical problems:

- The cumulative thrust of current U.S. policies and programs undermines rather than facilitates allied force interoperability and the development of true coalition warfighting capability. The lack of foreign participation in any significant U.S. C4ISR or network-centric warfare development programs—even areas like tactical radios—and the U.S. refusal to release even to close allies a range of technical information—from daily GPS codes to current and future U.S. military communications codes—are contrary to our interoperability goals. In effect, there is a significant gap between our stated transformational goals, which include interoperability, and our willingness to take needed steps, including the sharing of technology, training and other measures, necessary to effectuate those goals. In an era when the United States is focusing on its own force jointness, true efforts at interoperability have been afforded a lower priority in practice.

- U.S. National Disclosure Policy decision-making, done on an ad hoc, fragmented, country-specific basis in response to a specific crisis or operation, is at odds with the notion of a rotational, multi-national force designed to handle a host of potential missions. Under current U.S. policy, it would be very difficult for the NRF to train together using U.S. enablers in advance of an exigency justifying the need for such information, and it would prove very difficult to ensure that NRF participants had the same level of situational awareness needed for true coalition warfare.
- Despite U.S. government policy level support for greater technology sharing in order to advanced coalition warfighting capabilities, the old paradigm—of maintaining U.S. security through our technology leadership, even vis-à-vis close allies—continues to be alive and well in some parts of the U.S. defense bureaucracy. Indeed, a variety of special committees and modalities outside the traditional technology transfer process, including the low observable-counter low observable review process and anti-tamper regimes, emerged to pose significant hurdles to technology transfer to close allies. Thus, the difficulties in technology sharing between the United States and its allies that have plagued virtually all of our few Transatlantic programs, from Joint Strike Fighter to MEADS, continue unabated and are likely to recur. And the "lessons learned" on major programs have not been institutionalized through needed reforms; there is little evidence of a changed approach.
- Indeed, there is a sense of "déjà vu all over again" when approaching the tired but real need for reform of U.S. technology transfer rules that has been evident across both the Clinton and Bush Administrations in order to reflect a changing security paradigm that places more emphasis on coalition warfighting. Regrettably, a minority in Congress has stymied major reform efforts and, at this writing, has agreed to an informal stand down with the Bush Administration—no major reforms or country-specific export control waivers in exchange for no new and more onerous legislation.

Of course, the United States should not shoulder all the responsibility for this situation. European under investment in defense, slow recognition of the revolution in military affairs and concepts such as network-centric warfare, and lack of focus on interoperability in their own programs and priorities also are partly responsibility for current circumstances.

Interoperability Initiatives Have Not Been Successful. Moreover, the modest steps taken by the United States and its allies to enhance force interoperability, within NATO and otherwise, have not borne fruit. As reflected in a range of recent conflicts, from the Balkans to Afghanistan to Iraq, the ability of the United States and its allies to meaningfully fight wars together is limited. The interoperability initiatives taken to date—including the development of common standards and increasing reliance on open systems and commercial interfaces and technology—simply have not and will not solve the range of fundamental problems that exist. While NATO has undertaken some limited efforts and developed some degree of common or joint architecture, the efforts have been piecemeal and not systemic. The inherent complexity and proprietary nature of network-centric warfare systems currently fielded and under development, especially in the United States, and the lack of compliance with NATO interoperability standards (which are voluntary), mean that more focused and substantial efforts will be needed, including, most notably, the establishment of a common plug-and-play backbone architecture that nations can utilize for coalition operations (presumably in NATO) and a fair degree of information sharing.

The “Interoperability Gap” Will Worsen, Not Improve, Due to Divergences in Transatlantic Spending Patterns. Unfortunately, with the very sizable and accelerated U.S. investment in transformational network-centric technologies, the interoperability gap between fielded U.S. systems and European systems is likely to increase in years to come. As U.S. forces become more joint and move to our future architecture for C4ISR and we continue to limit release of or access to these new modalities, ad hoc attempts at integration of the NRF will be much more difficult and the degree of “dumbness” is likely to increase. Experience in the commercial business environment has consistently shown that disparate networks cannot be integrated smoothly without extensive prior planning and agreement on the sharing of network and database architectural and structural information. Network-centric warfare, which is in essence an attempt to superimpose distributed commercial business processes on war, will take place in a much more demanding environment. It is therefore unreasonable to expect that multinational military forces will be able to do under the exigencies of combat what commercial enterprises cannot do in a relaxed, peacetime environment without a concentrated, disciplined effort beyond those now underway.

Moreover, while the “network-centric divide” between Europe and the United States may very well be a product of funding rather than technology, [1] the funding differences are meaningful and have implications. In other words, absent significant spending changes in Europe or refocused priorities, the fact that Europe has the technology will not allow it to magically catch up or hook into U.S. advanced capabilities without significant U.S. cooperation.

Thus, both the United States and Europe face a strategic choice about the nature and degree of interoperability of coalition partners in the NRF (and NATO more generally), and the potential overall effectiveness of the NRF and the overall alliance as military coalitions. In effect, on both sides of the Atlantic, we must decide whether and to what extent we really want to develop truly interoperable coalition warfighting. If we do, we need to give higher priority and more focus to the interoperability issues highlighted herein in addition to the known problems of capability acquisition.

While nations can perhaps form “coalitions of the willing” for political purposes on an ad hoc basis, they cannot do likewise in true military coalitions. In this regard, 21st century coalition warfare is not like a pick up game of basketball at the gym, where we choose sides on a given day and fight together—working out the roles and relationships as the “game” progresses. Particularly with the emergence of network-centric warfare, it will take years of planning, information sharing, cooperative development efforts, the creation of interoperability bridges, and shaping plug-and-play architecture to develop true coalition warfare capabilities.

As discussed below in depth, to facilitate NRF interoperability and capability acquisition, we need to:

[1] Gordon Adams, Guy Ben-Ari, John Logsdon and Ray Williamson, “Bridging the Gap: European C4ISR Capabilities and Transatlantic Interoperability,” (Washington, DC: George Washington University, October 2004).

1. Develop overall C4 architecture (whether in NATO or otherwise) for use with potential coalition partners (which will help frame the parameters of what we are willing to share with our allies);
2. Adopt a range of other necessary steps to improve interoperability, including training together in network-centric warfare techniques; and
3. Adopt new “top down” approaches to technology transfer and information sharing, with significant leadership attention, “one-stop” shopping modalities, and other more flexible mechanisms that recognize the necessities of sharing information on a sustained basis during the planning, training, and actual operations necessary for successful coalition operations.

Undoubtedly, there will be limits to U.S. information sharing occasioned by a range of security considerations. However, we can and should adopt a more flexible approach to information sharing that gives more priority to coalition warfare as an element of U.S. national security strategy.

Finally, once and for all, the Bush Administration should tackle the “enabling” issue of technology transfer reform early in its second term (and not in year three or four, as in the past), exert its leadership, and develop meaningful and comprehensive modalities for facilitating the information sharing and technology transfer necessary to advance coalition warfighting capabilities and force interoperability, both in the context of the NRF and more generally. Only with strong leadership by the Administration and a commitment to advance coalition warfighting as an element of national strategy can the NRF and the broader operation of NATO as a military alliance be sustained.

I. The NATO Response Force: From Conception to Operations

As a threshold matter, it is important to have a sound understanding of the concept, purposes and operational realities of the NATO Response Force (NRF) as a baseline for assessing the technology transfer needs associated with it.

A. The NRF Concept

As proposed by Secretary of Defense Donald Rumsfeld and adopted by NATO Heads of State at the 2002 Prague Summit, the NRF was conceived to be a multinational spearhead expeditionary force that would operate under NATO auspices in the initial phase of high-intensity conflicts. Specifically, as stated in the Prague Summit Declaration, NATO committed to "[c]reate a NATO Response Force (NRF) consisting of a technologically advanced, flexible, deployable, interoperable and sustainable force including land, sea, and air elements ready to move quickly to wherever needed, as decided by the Council."[1]

As announced at the Prague Summit and evolved at subsequent ministerial meetings, the NRF is a combined arms, multi-national, multi-service force consisting of land, air, and naval contingents. Ultimately, at full capability, the NRF will consist of a deployable headquarters staff, a reinforced brigade combat team (2,500-3,000 troops) with mission-tailored elements; a rapidly deployable composite air group (approximately 40 aircraft and helicopters) with C4ISR capabilities; and an amphibious support force (6-12 ships, including frigates, amphibious assault ships, logistic support ships, and possibly an aircraft or helicopter carrier).[2] The ground component of the NRF will eventually include up to three light infantry battalions (either motorized or air mobile), plus one or more light armored battalions, an artillery battalion, a special operations element, and supporting engineer, nuclear, chemical, biological (NBC) defense, and logistic units.

Intended to provide NATO with a fast reaction force capable of engaging in high-intensity combat on a modern battlefield, either independently for up to 30 days, or for longer periods as part of a NATO Combined Joint Task Force, the NRF also includes an "early entry contingent" consisting of light infantry, special operations forces, and a small air contingent; this will be capable of deploying out-of-area within 72 hours to secure a lodgement for follow-on forces. In early 2004, this early entry element was activated to provide a preliminary NRF capability and to exercise basic command and control

[1] See Prague Summit Declaration, Paragraph 4, Issued by the Heads of State and Government participating in the meeting of NATO's North Atlantic Council in Prague on 21 November 2002. Available online at: <http://www.nato.int/docu/pr/2002/p02-127e.htm>.

[2] Organizationally and conceptually, the NRF is quite similar to a U.S. Marine Corps "Marine Expeditionary Force", which consists of a reinforced regimental combat team, a Marine Air Wing, and a U.S. Navy amphibious task group.

functions. In addition to its high-end combat capability, the NRF will also be able to conduct low-intensity "Petersburg" missions such as peacekeeping and humanitarian assistance. According to former SACEUR General Joseph Ralston, "the NATO Response Force has got to be across the board from high-intensity conflict all the way down to lower levels, whatever the political authorities tell us to do." [3]

B. The Purposes and Roots of the NRF

As articulated at Prague and more recently, the purposes of the NRF were multiple:

- Strengthen the bonds between the United States and its NATO allies—nations that cannot and do not fight together are less likely to work cooperatively in other areas.
- Give NATO a capability to act rapidly and lethally in out-of-area conflicts and, in so doing, strengthen its *raison d'etre* as a military alliance that can handle 21st century security threats.
- Be a catalyst for focusing and promoting both the *transformation* of the Alliance's military capabilities" to meet these threats and improved *interoperability* between the multinational elements of the NRF.

While these NRF purposes seem simple and clear, they in fact reflect a complex underlying history and gradual evolution in thinking about Transatlantic geopolitical relationships, the future role of NATO and the need for the acquisition of European military capabilities as well as better force interoperability. In effect, the NRF is a microcosm of these broader considerations—the tensions in the alliance, the different security perspectives and different force doctrines and trajectories—and must be understood in this context.

Geopolitical Underpinnings

The geopolitical context for the NRF's creation was increasing and significant divergences in U.S relations with its European allies over a range of issues, from defense to trade to global warming, and the Bush Administration's desire to strengthen the Transatlantic relationship in the security context, especially in the aftermath of the September 11, 2001 attacks, and the desire in Europe to show solidarity with the United States on terrorism and other issues.

These divergences, which have deep roots, began after the end of the Cold War, long before the Bush Administration took office. While the United States and its European partners have a history of shared values, close security relations, and the largest two-way

[3] "Keeping NATO's Military Edge Intact", Luncheon Address by General Joseph Ralston, SACEUR, NATO/GMFUS Conference, Brussels, 3 October 2001. Available online at: <www.nato.int/docu/speech/2002/s021003d.htm>.

trade and investment relationship in the world,[4] recent years nevertheless have witnessed the rise of significant countervailing tendencies that have driven a wedge in the relationship. Fundamentally, different degrees of concern over security and different approaches to ensuring it began to take root on both sides of the Atlantic. With the end of the Cold War, Europeans became less concerned over security generally and less apt to favor military solutions.[5] Indeed, the relevance of NATO was questioned on both sides of the Atlantic and various efforts have been made for years to address this issue.

Moreover, serious efforts have gained steam in Europe to move toward a separate "European" security identify, defense capability, and supporting industrial structure. The centerpiece of these efforts is the European Common European Security and Defense Policy (CESDP), which includes, among other things, new European Union institutional structures for defense and security policy and the establishment, as part of the so-called "Headline Goals," of a European rapid reaction force capable of handling Petersburg missions. More recently, the European Union has decided to create an EU armaments agency.

These European security developments reflect a number of dynamics, including a Europe coming of age and integrating successfully in other areas as well as a European reaction to its inability to deal with the Balkan crisis in the 1990s and its forced reliance on NATO and the United States to address the most significant post-Cold War region crisis.[6] Also underlying these European developments are the economics of small defense budgets and the need for cooperative efforts to improve affordability, and the industrial policy desire to maintain significant defense industrial capabilities away from national autarky in defense. However, at the core of these developments, there is no mistaking the political impulse in Europe (stronger in some European countries than others) to create a counterweight to perceived U.S. hegemony and what some have called its "overdependence" on the United States, and assert a more independent European role and leadership on foreign policy and defense—in effect, to achieve a "rebalancing" of the relationship.[7] In turn, the United States has gradually begun to look at Europe as less of an equal partner in security matters. The United States reaction to CESDP has varied from outright opposition and concern it will undermine the NATO alliance to constructive efforts to link it inextricably to NATO.

Despite periodic efforts to revitalize NATO and tie it to CESDP and Europe's invocation of Article 5 of the NATO Charter after September 11, the reality is that Europe and the

[4] Hamilton, Daniel and Quinlan, Joseph, *Partners in Prosperity: The Changing Geography of the Transatlantic Economy*, Johns Hopkins University-SAIS Center for Transatlantic Relations (Washington, DC) 2004. Executive summary available online at: <http://www.transatlantic.sais-jhu.edu/Publications/books_monographs.htm>.

[5] Robert Kagan, "Power and Weakness", *Policy Review*, June 2002.

[6] "The Future of the European Security and Defence Policy (ESDP) and the role of the European Commission," Speech by The Rt. Hon. Chris Patten, CH, Conference on the Development of a Common European Security and Defence Policy, pgs. 2-3, (Berlin, 16 December 1999). Available online at: <http://europa.eu.int/comm/external_relations/news/patten/speech_99_215_en.htm>.

[7] NATO Handbook, Chapter 4, pg. 2, "The European Security and Defence Identity", "Evolution of the ESDI." Available online at: <http://www.nato.int./docu/handbook/2001/hb0401.htm>.

United States have continued to drift apart on security matters. The perceived unilateralism of the Bush Administration has accelerated these tendencies and fueled geopolitical tensions. Indeed, both at the time of the Prague Summit and today, U.S.-European relations on security matters stand at historic lows, with major divergences over Iraq, Iran, China, and many other major security matters.

Moreover, other centrifugal forces have been at work. In armaments, there has been little meaningful Transatlantic cooperation in recent years outside the Joint Strike Fighter (JSF) program (and even that effort has been plagued by continuing tensions over technology transfer and work share). Technology transfer remains a sensitive issue: European allies continue to raise serious concerns about U.S. unwillingness to share technology, even in support of coalition warfare efforts.[8]

Indeed, while the United States continues to exhort European nations to spend more on defense capabilities, the United States also appears, from a European perspective, unwilling to share the technology needed to facilitate this capability acquisition.

Similar tendencies are also present in the economic arena, where there have been contentious and intractable trade and economic disputes between the United States and the European Union. The Transatlantic dialogue today, like the U.S.-Japan dialogue of years past, increasingly focuses on areas of dispute rather than areas of common cause. These issues run the gamut from global warming to the WTO-illegal U.S. foreign sales corporation tax exemption to EU treatment of imported bananas, beef hormones, and foodstuffs containing genetically modified organisms to U.S. legislation imposing extraterritorial sanctions against Cuba, Iran, and Libya and U.S. import restrictions on European steel products. While there have been efforts to resolve some of these issues and broaden U.S.-EU economic cooperation (for example, in the new WTO round), these issues nevertheless reflect serious underlying differences in cultures, institutions, economic and industrial policies, and cannot be submerged for long—as witnessed by the current escalating dispute over alleged Airbus subsidies.

Thus, it is in this context of drift in Transatlantic relations that the Administration sought to shape a NATO initiative for Prague that would be its own positive contribution to reinvigorating the Transatlantic relationship and changing the dynamics away from drift toward tangible and useful security cooperation.

Revitalizing NATO for the 21st Century: The Thrust Toward Out-of-area Operations

Another fundamental underpinning of the NRF is to shift European mindsets from fixed, stationary defense—the traditional strategic approach utilized against the threat of a Soviet invasion through Central Europe—toward a 21st century approach to security that assumes that many of the threats will be out-of-area. The structure, operational doctrine,

[8] Dov Zakheim, "Military Planning and Export Controls", CSIS Working Paper No.7, 29 September 2000. Available online at: <www.csis.org/export/articles/zakheim.pdf>.

equipment and training of most European force structures, with an emphasis on heavy ground forces, have until recently been based on this traditional, Cold War era paradigm. In contrast, for reasons of geography and history, the United States has long had a more established approach to the deployment of its forces beyond American territory.

The out-of-area issue takes on particular significance in the NATO context, where the entire thrust of the alliance has historically been focused on defending members' territories against the Soviet Union. In the post–Cold War era, the out-of-area debate was central to NATO's future—whether and how should NATO be re-invented to address new and emerging 21st century threats, from terrorism to conflicts in Third World countries that damage NATO's interests. The idea of expanding NATO's out-of-area operations capabilities gradually emerged in the mid-1990s[9] and was adopted as part of NATO's new Strategic Concept at the 1999 NATO Summit in Washington, DC. Specifically, NATO recognized that "alliance security interests can be affected" by "risks of a wider nature, including acts of terrorism, sabotage and organized crime, and by the disruption of the flow of vital resources," and specifically noted the prospect that NATO may carry out out-of-area crisis management operations to address such threats.[10] This new approach, which went beyond NATO's longstanding defensive doctrine, was also reflected in its new force posture approach, which included guidelines that reflected the need for operational capabilities such as deployabililty and mobility as well as greater force interoperability and the use of mobile headquarters.[11]

While the Washington Summit resulted in the adoption of a new approach on paper, the real challenge was to facilitate the actual transformation of NATO member forces to align with the new strategic shift toward possible NATO expeditionary actions. A RAND report released in 2000 found that:

> The military forces of NATO's member states should be structured and postured for expeditionary operations. Achieving a more expeditionary posture entails expanding and modernizing transportation fleets (principally military airlift, but also sealift), acquiring more mobile logistics assets, upgrading infrastructure in selected countries, and modernizing the forces themselves so that light, more mobile units can be more effective in a wide range of missions. This will entail, among other things, exploiting recent advances in surveillance, information processing, communications, and

[9] Kugler, Richard L., *The Future of NATO and U.S. Policy in Europe, RAND Report P-7800* (Santa Monica, CA: RAND, 1992); Kugler, Richard L., *NATO's Future Conventional Strategy in Central Europe: Theater Employment Doctrine for the Post-Cold War Era*, RAND Report R-4084-A (Santa Monica, CA: RAND, 1992); Harris, Scott Allen, and James Steinberg, *European Defense and the Future of Transatlantic Cooperation*, RAND Report MR-276-USDP (Santa Monica, CA: RAND, 1993); Naslund, Willard E., *NATO Airpower: Organizing for Uncertainty*, RAND Report MR-215-AF (Santa Monica, CA: RAND, 1993); Asmus, Ronald D., Richard L. Kugler and F. Stephen Larrabee, "Security for All of Europe, in Seven Tricky Steps," *St. Petersburg Times*, 29 August 1993, p. 8D; Kugler, Richard L., "Building a New NATO," *Foreign Affairs*, Sept/Oct 1993, pp. 40-41;Kugler, Richard L., *U.S.-West European Cooperation in Out-of-Area Military Operations: Problems and Prospects*, RAND Report MR-349-USDP (Santa Monica, CA: RAND, 1994); and Gompert, David, and Richard Kugler, "Free-rider Redux: NATO Needs to Project Power (and Europe Can Help)," *Foreign Affairs*, January 1995, pp. 7-13.

[10] "The Alliance's Strategic Concept," NATO Press Release NAC-S(99)65m, paragraphs 10, 24, and 31 (April 23 1999). Available online at: <http://www.nato.int/docu/pr/1999/p99-065e.htm>.

[11] Id., at paragraph 52.

> precision weapons so that the military assets of adversaries can be rapidly located, identified, and destroyed with minimal collateral damage.[12]

As the Prague Summit of 2002 approached, the idea began to take shape of a highly capable European expeditionary or spearhead force that would be able to conduct, on short notice, out-of-area, high-intensity missions together with more advanced U.S. forces. Conceptually, the idea for the force, outlined in a series of articles by Hans Binnendijk and Richard Kugler of the National Defense University,[13] was that Europe need not transform all of its forces at once to match U.S. capabilities, but should "configure a portion of their forces for swift power projection and high-tech strike operations with U.S. forces."[14] The creation of such a force was viewed as a catalyst to move European members of NATO toward transforming their overall forces in order to provide expeditionary capabilities; the changes required are significant in nature and necessitate changes in European force structures, doctrines, equipment, and the like. The notion of a NATO spearhead force for high-intensity conflicts also is complementary to the European plans for a rapid reaction force for low-intensity Petersburg missions.

The need for such a force was embraced in the White House's "U.S. National Security Strategy," issued in September 2002:

> NATO's core mission—collective defense of the transatlantic alliance of democracies—remains, but NATO must develop new structures and capabilities to carry out that mission under new circumstances. *NATO must build a capability to field, at short notice, highly mobile, specially trained forces whenever they are needed to respond to a threat against any member of the alliance*….To achieve this, we must:….ensure that the military forces of NATO nations have appropriate combat contributions to make in coalition warfare;…take advantage of the technological opportunities and economies of scale in our defense spending to transform NATO military forces so that they dominate potential aggressors and diminish

[12] David Ochmanek, "NATO's Future: Implications for U.S. Military Capabilities and Posture, RAND Report MR-1162-AF (Santa Monica, CA: RAND, 2000), p. viii.

[13] The National Defense University's Center for Technology and National Security Policy originated the idea for the NRF in November of 2001. It was designed as a result of NATO's inability to support U.S. operations in Afghanistan after NATO declared that an Article V commitment was in effect. Hans Binnendijk first presented the idea formally to the annual meeting of the NATO Parliamentary Assembly in December 200l. It first appeared in print in the *International Herald Tribune* on February 16-17 in an op-ed article by Hans Binnendijk entitled "A European spearhead force would bridge the gap." Binnendijk and Richard Kugler presented the concept to the National Security Council Staff and to Pentagon officials at several meetings in February and March 2002. Kugler provided programmatic details for the NRF in a paper called "Toward a NATO Defense Transformation Initiative" in March 2002. Binnendijk and Kugler presented the idea publicly to several Washington audiences in the Spring of 2002, including the Atlantic Council, the Center for Strategic and International Studies, Johns Hopkins SAIS, and the Heritage Foundation. Binnendijk and Kugler presented the idea in detail in the Autumn 2002 issue of *Survival* pp. 117-132. Once formally proposed by the United States, they wrote an oped in support of the concept in the October 24 addition of the *International Herald Tribune* entitled "Europeans should say yes to Rumsfeld". In early 2003, together with Stuart Johnson, Binnendijk and Kugler prepared briefings on "Implementing the NATO Response Force" which were presented in Washington and in Europe.

[14] Richard L. Kugler, "Preparing NATO to Meet New Threats," *U.S. Foreign Policy Agenda* [online], Vol. 7, No. 1, 27 March 2002. As Rand analysts and later at the National Defense University, Binnendijk and Kugler were instrumental in formulating the NRF concept and pushing it before senior U.S. policy-makers.

> our vulnerabilities; streamline and increase the flexibility of command structures to meet new operational demands and the associated requirements of training, integrating, and experimenting with new force configurations; and maintain the ability to work and fight together as allies even as we take the necessary steps to transform and modernize our forces.[15](Emphasis added.)

Thus, the creation of the NRF, together with major reforms announced at Prague (i.e., improvements in NATO command and control mechanisms needed to facilitate deployability), were designed to ensure that NATO actually has the capabilities necessary to implement, and put flesh on the bones of, its new out-of-area strategy.[16]

Capabilities and Interoperability

The NRF goal of incentivizing European capability acquisition is the latest in a series of initiatives, to date largely unsuccessful, to address the continuing and increasing capabilities gap between the United States and its European allies that developed after the Cold War and to improve interoperability.

The capabilities gap that emerged during the 1990s was a function of a number of factors, including: overall declines in defense budgets in Europe after the Cold War; the very wide resulting gap in spending between U.S. and European armaments development (at barely one-fourth of U.S. levels); the fragmented and inefficient nature of European defense procurement; continued European reliance on an overly large, aging and largely immobile force structure inherited from the Cold War era; and the resulting need to spend more and more of European defense budgets on operations and maintenance rather than future investment. To address the problem, NATO decided at the Washington Summit in 1999 to adopt the Defense Capabilities Initiative (DCI), which ultimately became a list of some fifty-six specific capabilities that European NATO forces needed.

What Has DCI Achieved? DCI has led to a heightened European focus on the need to transform forces for the future and to organized European efforts (under EU auspices) to identify and address the gap areas. On balance, however, DCI led to very few results. Why? For one thing, the DCI list that emerged was so broad that no priorities were set. Also, European nations, facing severe budget constraints, pre-existing commitments to

[15] The White House, *The National Security Strategy of the United States of America* (Washington, DC: The White House, September 2002), pp. 25-26.

[16] A final agreement on "NATO's new streamlined command arrangements" was reached at the 'Meeting of the North Atlantic Council of Defence Ministers' in June of 2003. These will consist of two strategic commands: one to control three 'operational' commands (two Joint Force Commands and one Joint Headquarters) as well as a number of "tactical" commands (Joint Force Component Commands and Combined Air Operations Centres); the other strategic command to "guide and encourage the transformation of forces and other capabilities…" through a Joint Warfare Centre ("with a subordinate Joint Force Training Centre and a Joint Analysis and Lessons Learned Centre"), and a number of nationally- or multi-nationally sponsored Centres of Excellence….". See "Final communiqué: Meeting of the North Atlantic Council in Defence Ministers session held in Brussels on Thursday, 12 June 2003," *Press Release (2003)065*, 12 June 2003, and "Ministerial Meeting of the Defense Planning Committee and the Nuclear Planning Group held in Brussels on Thursday, 12 June 2003: Final Communiqué," *Press Release (2003)64*, 12 June 2003.

defense programs (such as Eurofighter), and increasing operations and maintenance expenses, have made few real commitments to take specific actions on new capability acquisition, and no real timetables were adopted. Moreover, the United States, over several Administrations, has done little more than exhort European nations to acquire more capabilities or encourage European firms to buy U.S. developed capabilities, from missiles to fighter jets. Yet Europe has increasingly shied away from this approach and has sought to develop its own capabilities. Moreover, in this arena, the United States has not engaged in significant armaments cooperation designed to incentivize capability acquisition and has continued to limit technology transfer in ways that have slowed and undermined European efforts to develop enhanced capabilities.

Recognizing the shortcomings of DCI, a major focus of the Prague Summit, in addition to creating the NRF, was to identify a shorter set of priority military capabilities and establish specific commitments for European nations to meet these goals. Specifically, at Prague, NATO Heads of State also committed to the Prague Capabilities Commitment (PCC), under which individual allies made "firm and specific political commitments to improve their capabilities in the areas of chemical, biological, radiological, and nuclear defense; intelligence, surveillance, and target acquisition; air-to-ground surveillance; command, control and communications; combat effectiveness, including precision guided munitions and suppression of enemy air defenses; strategic air and sea lift; air-to-air refueling; and deployable combat support and combat service support units."

The NRF is in turn designed to incentivize the fulfillment of the Prague Capabilities Commitments by establishing a force intended to ultimately have such transformational European capabilities in key areas such as lift, C4ISR and the like. The concept is that the actual need to field high-level European forces in the NRF will create more focus on, and serve as a basis to prioritize and catalyze, capability acquisition.

The NRF goal of having the force be interoperable also is the latest NATO commitment designed to redress growing issues of force compatibility between the United States and its allies. While most analysis tends to blur the capability and interoperability concepts, the reality is that they are quite distinct. In *Joint Vision 2010,* the U.S. Joint Chiefs of Staff recognized that "[s]ince our potential international partners will have varying levels of technology, a tailored approach to interoperability that accommodates a wide range of capabilities is necessary." *Joint Vision 2020* in turn states that "[i]nteroperability is the foundation of effective joint, multinational and interagency operations." Thus, U.S. military doctrine recognizes explicitly that there is a distinction between military capabilities and military interoperability, and that symmetry of capabilities is not a prerequisite for interoperability in a coalition environment—quite the opposite, in fact; asymmetrical capabilities among coalition partners are assumed to be the norm, not the exception.

In fact, the preponderant U.S. and NATO focus on European capability acquisition over the last decade has tended to blur the concepts and submerge the desire for improved interoperability to a second-level priority. Yet, the reality is that interoperability remains as significant a concern as the capability gap and a somewhat distinct problem. The

United States and its allies have undertaken a number of steps to address interoperability, including the development of NATO common standards (STANAGs) to facilitate interoperability, the development of some NATO rudiments of a C4 architecture, and a thrust toward open architecture and commercial standards. Moreover, numerous fora have been established to address interoperability concerns, including the Multinational Interoperability Council, composed of six leading nations (Australia, Canada, France, Germany, the United Kingdom and the United States) likely to lead future coalitions. Yet, the reality is that these efforts have been largely ineffective to date. NATO standards are voluntary in nature and not adhered to in practice in many instances. Many network-centric systems have significant proprietary elements (despite a theoretical emphasis on open architecture), and military needs have precluded full adoption of commercial standards and architectures.

Despite these various efforts, the cold reality is that across a series of recent conflicts, from the Balkans to Afghanistan to Iraq, the United States and its allies remain unable to meaningfully fight wars together.

- In Bosnia and Kosovo, the United States was unable to share air tasking and targeting data with its NATO partners, severely restricting the ability of NATO aircraft to fly the same missions or even in the same airspace with U.S. aircraft. Airspace management and deconfliction remained a problem throughout the conflicts in Bosnia and Kosovo.
- The U.S. was unable to share remote sensor information in a timely manner with its NATO partners because of security restrictions and incompatible communications and battlefield information systems. This problem remained unresolved in Afghanistan, and even in Iraq, where British forces found their flexibility and operational tempo constrained by the inability to access U.S. targeting systems such as JSTARS and Global Hawk.
- Shortages of precision munitions and aircraft cleared to deliver them limited the numbers and types of targets that could be engaged by NATO aircraft; suppression of Enemy Air Defenses (SEAD) remained a major weakness through both operations.
- Combat Identification has remained problematic, despite significant effort devoted to operational solutions. The loss of Canadian troops in Afghanistan and British aircraft in Iraq to U.S. “friendly fire” points out the difficulty of operating multinational forces in a common battlespace.

Network-centric Warfare: The Focus of 21st Century Interoperability

Finally, interoperability takes on important new meanings and dimensions in this era of military transformation and the shift toward “network-centric warfare.” While a somewhat amorphous term, network-centric warfare is generally defined as the linking of distributed sensors, weapons systems, command nodes and maneuver units over several interconnected digital networks, so that capabilities are seen as residing “on the network” rather than with specific units or platforms. Sharing of sensor information allows (in theory) greatly enhanced situational awareness (of both friendly and enemy forces), minimizing uncertainty and accelerating the tempo of operations. Commanders sharing a common relevant operational picture can also access a wide range of weapons and maneuver units to execute their concept of operations, now defined as generating a particular desired "effect" on the enemy—hence the advent of what are sometimes called "effects-based" operations. In effects-based operations, a commander decides what he wants to do to the enemy, then examines the full spectrum of systems and capabilities available to him, choosing the ones that best meet his needs. In a network-centric, effects-based system, distinctions between platforms, military services, and (in theory) national components become transparent. These categories are replaced by functionalities: surveillance, target acquisition, precision strike, close combat, etc.

This new approach to warfare inevitably changes the focus of interoperability of multinational forces like the NRF. As advocates of the NRF recognized, there must be an emphasis on:

> [t]he need for allied information systems and networks that can interoperate with U.S. networks … In the coming era, interoperability will come mostly from establishing connectivity between U.S. and allied information nets rather than from equipping troops with identical weapons and munitions.[17]

In a certain sense, interoperability is no longer about having the same missiles or tanks, but about having the ability to securely communicate, to have access to the same level of situational awareness, and to have the types of command and control capability to allow execution based on the real-time sensor inputs. Thus, interoperability is more a matter of compatible software and codes and information sharing than technology transfer.

The prospect that the NRF can become interoperable with U.S. forces is threatened by the unrivalled and very expensive U.S. transformational efforts to develop and field a broad panoply of network-centric warfare capabilities. All of the U.S. services are focusing on the development of the necessary enabling systems and system architectures. Early elements of network-centric warfare were demonstrated both in Afghanistan and Iraq, where the U.S. military has given it the lion's share of the credit for the rapid end of the conventional phases of combat.

While these concepts are beginning to catch on in Europe, the degree and breadth of commitment, level of spending, and number of programs lag far behind the United States. The United Kingdom is developing a "Network-Enabled Capability" in which specific systems will be designed to plug-and-play on other countries' networks. Sweden is moving toward a full, end-to-end network-centric capability. Most other European countries at best intend only to develop specific elements of a network-centric system, relying to some degree on other countries (i.e., the United States) to provide other critical capabilities. NATO similarly intends to develop a NATO Network-Enabled Architecture into which various member nations can plug their own network-centric systems.

[17] Hans Binnendijk and Richard L. Kugler, "Adapting Forces to a New Era: Ten Transforming Concepts," *Defense Horizons* No. 5 (Washington, DC: NDU Press, November 2001), p. 5.

The widening network-centric warfare gap is not necessarily a matter of different spending and technology levels across the Atlantic. For a number of reasons, other European nations have been slow to embrace network-centric warfare and a few have been somewhat hostile to it (while, paradoxically, embracing selected elements of it). Concerns raised in Europe include cost (an "end-to-end" network-centric capability would be prohibitively expensive), potentially increased dependence on the United States (as cost limitations will drive most to plug-and-play with U.S. architecture rather than develop their own) and differing national approaches to warfare deeply rooted in historical experience. Both the Germans and the French, for instance, have less faith in technological solutions to the problem of uncertainty on the battlefield, and prefer instead to rely on training to teach officers and men to make effective decisions in the presence of uncertainty.[18]

Interestingly, the U.S. transformation strategy embraces interoperability as a priority. However, the United States has to date taken few steps to translate this goal into reality. The reality is that the OSD Office of Interoperability, as well as the Joint Forces Command, are both primarily focused on the increasing jointness of the U.S. services, and have taken few meaningful steps to ensure allied interoperability in the context of network-centric warfare.

In any event, the widening chasm between U.S. and European network-centric capabilities make it that much harder to create even rudimentary levels of interoperability (compatible secure tactical communications, combat identification, etc.). Thus, the NRF commitment to an interoperable force offers the opportunity for focus on these increasingly difficult issues in an operational context and to translate U.S. rhetoric of interoperability into coalition warfighting reality.

In sum, the NRF highlights both the challenges and opportunities facing the United States and its allies as they seek common ground in forging a 21st century security strategy. Certainly, the NRF is not a panacea and should not be expected to provide answers to all of the longstanding and complex issues of capability, interoperability, and the like. In a certain sense, however, the NRF is an incubator or test bed that, if successful, can allow us to identify the overall architecture needed for effective coalition warfare and a stronger overall Transatlantic security relationship.

[18] There also is concern that massively integrated networked systems can be prone to single point failures, information saturation, and enemy counter-information operations. In addition, some European military officers note that network-centric warfare is inherently designed to deal with conventional modes of war against an enemy with large combined armed forces, and that most network-centric capabilities are of little value against an asymmetrical adversary employing guerrilla warfare or terrorism—as witnessed in Iraq and Afghanistan today. Given that this is perceived to be the dominant form of warfare in the future, European critics wonder at the relevance of network-centric warfare, given the cost and complexity of its implementation. These critics also point to the risks of creating an operational and tactical monoculture in which the unique capabilities of each European military force are subsumed into a single, overarching operational method—one that allows potential enemies to exploit the inherent weaknesses of the system and play upon the margins of its capabilities.

C. The NRF in Operation

Since the Prague Summit, planning for the NRF has gone forward expeditiously and the force has moved from paper to an operational force very quickly. The rapid stand up of the NRF was facilitated by NATO's decision to allow the Supreme Headquarters, Allied Powers Europe (SHAPE) to develop the force rather than NATO Force Development, which would have been more inclined to view the NRF notionally and rely on concept planning and establishing national commitments. In contrast, SHAPE approached the stand up of the force from an operational perspective, focusing on the steps necessary to stand up an actual force, command, control, communications, and intelligence (C3I) and on the development of an "expeditionary mindset" within NATO. As one SHAPE official put it, "Transformation is a process that takes place between the ears." Thus, SHAPE sees the NRF as an integral part of the larger NATO command transformation process, and tends to view the development of the NRF through the prism of operational doctrine.

Because of resource constraints and developmental lead time, whether technology or operations driven, the NRF will follow an evolutionary course of development, moving from basic to more advanced capabilities, and from heavy reliance on U.S. systems to increasing independence through the development of indigenous capabilities.

NRF's Phased Development

As now planned, the NRF will have three phases of development:

1. Phase I Prototype Effort (04-06). The idea is to field a very small spearhead of a spearhead force with minimal changes to existing composition and equipment of national contingents. This would initially be a reinforced light infantry battalion supplemented by 6-8 special operations teams, an artillery company, engineer, communications, and NBC and other combat service support elements. Intended as an early entry force, its main purpose in the near term will be to exercise the command and control functions of the Deployable Joint Task Force headquarters unit and to iron out problems before fielding a full-scale NRF contingent; enhancements to C4I systems would be made as needed to facilitate integration within NRF and between the NRF and the NATO Combined Joint Task Force Headquarters. Communications systems and battlefield information systems will either be standardized or brought up to a common standard of interoperability, and first-iteration command and control procedures established. While the naval contingent of this early-entry force is sufficient to meet envisaged operational requirements, the air component appears to be deficient in the number of AWACS, surveillance, transport, and fighter/attack aircraft committed; there are not enough of these assets to sustain a 24–hour operational cycle.

2. Phase II U.S.-Enabled NRF (2006-2012). In phase two, a full NRF would be fielded in 2006, with both European ground elements and U.S. enablers, including airlift, strategic and tactical C43ISR (such as JSTARS, Global Hawk, satellite

surveillance and broad band satellite communications) and theatre missile defense. Advanced network-centric and other new capabilities of individual NATO members, such as the Medium Extended Air Defense System (MEADS**),** will be integrated into NRF as they become available. Given the short time frames involved, however, it is unlikely that Europe will have most of its planned advanced capabilities ready for integration into NRF in this period. While less certain, NATO may gradually develop and integrate some elements of its own C4ISR architecture as it becomes available based on building blocks now underway, such as the Coalition Aerial Surveillance and Reconnaissance (CAESAR) Advanced Capability and Technology Demonstration (ACTD) and such cooperative efforts as the Multifunctional Information Distribution System (MIDS).

3. Phase III Integration of European or NATO enablers (2013-Onward). As Europe and/or NATO acquire advanced capabilities in key areas such as airlift, precision munitions, missile defense (possibly a NATO owned and operated Pac III), and C4ISR (e.g., the AGS system, EuroHawk, NATO IV Satcomm) by decade's end, these would be integrated into the fielded force as it gradually shifts toward a more transformational objective force.

Rotational Structure and Certification Process

Significantly, the NRF is not a fixed force; its composition and organization will change in accordance with a six-month rotation schedule. Also, SHAPE will utilize a certification process already employed with the NATO Graduated Readiness Headquarters—that is, a set of objective standards and normative capabilities to which each rotational national contributor must commit, and on which the readiness and deployability of each NRF rotation will be based.

According to current plans, individual NATO states will bid to contribute force elements to an upcoming NRF rotation roughly 18 months before that rotation is scheduled to deploy as a combat-ready unit. Twelve months prior to deployment, the various NRF components will begin joint training exercises. Six months later (and six months prior to deployment), SHAPE will conduct an operational readiness evaluation of the NRF rotational force and will decide whether to certify it as combat ready to undertake the needed missions (which may change from one rotation to another) and be listed among NATO's deployable assets. After six months of operations, the rotational force will stand down and be replaced by the next NRF rotation. Thus, at any given time, there is one NRF rotation in the process of formation, one in training, and one ready to deploy. Ultimately, a total of six NRFs are planned—one active and five in ready reserve, theoretically capable of mobilization at short notice.

Significantly, SHAPE plans to create *escalating* certification requirements with each rotation. Thus, those countries committing to the first rotation will have to meet a baseline standard, while those contributing to each subsequent rotation will have to meet ever-higher certification requirements.

Plainly, the object of the rotational structure and certification process is to maximize the effect of the NRF as a "catalyst of transformation." By passing as many units through the NRF as possible, it is hoped that each national military force will develop a nucleus of modern, high-technology forces suitable for out-of-area operations. This presumes, of course, that each participating country will choose to make a new investment in equipment for each rotation in which it participates rather than just rotating a single set of equipment through each unit it contributes to the NRF.[19] Further, by continually upgrading the certification requirements, SHAPE intends to promote or incentivize capability enhancement.

Of course, the price the NRF pays for using a rotational and certification structure is a high degree of turbulence, with all the associated problems that come with it. More than anything else, the rotational structure ensures that each force entering the rotation will have a steep learning curve to climb before being certified as deployable. Moreover, the NRF will barely have developed cohesion and a sense of unit identity before it must disband and the process must begin anew.

Multinational Composition

Finally, SHAPE has had to wrestle with precisely how multinational the NRF should be and whether the NRF's reinforced land brigade should be drawn from multiple countries, which directly raises issues of interoperability. Brigades normally fight as task-oriented combat teams, with integration of subunits down to the company and even platoon level. This would suggest, for example, that an Italian tank platoon could be attached to a French infantry company supported by an Italian mortar platoon. Yet, the reality is that issues of language, diverse and often incompatible equipment, and differences in operational doctrine and training severely limit the ability to have a truly multinational force, with brigade elements from multiple nations fused together. In short, there are trade-offs between the degree of force integration—designed to promote political goals underlying the NRF—and efficiency considerations. Indeed, existing NATO multinational forces are generally limited to the divisional or corps echelons to avoid these problems. The NRF, with its rotational system and limited opportunity for six months of common training, would make this approach even more difficult.

SHAPE resolved this issue by requiring that the primary maneuver component (i.e., the armored and infantry battalions) in initial rotations come from a single national contingent or from a multinational force with a longstanding "habitual association." Other discrete combat support and specialist units, such as NBC units, could come from other countries. In the long term, SHAPE is open to the idea of composite brigades that

[19] This approach has been used repeatedly over the years to enable budget-constrained countries to meet specific materiel commitments. For instance, a NATO initiative to enhance broadband satellite communications among naval forces required the acquisition of X-band antennae terminals, but few navies purchased a sufficient number to equip all of their combatant ships. Instead, they acquired a number sufficient to equip those ships on station at any given moment, moving the terminals from one ship to another as they rotated through the dockyards. While this created the illusion of capability, in fact it left the navies in question incapable of meeting surge requirements or of coping with an unexpected casualty to the deployed ships.

integrate maneuver battalions from several countries and operate together— but the responsibility for working out the operational issues would rest with the component armies, not SHAPE.

As shown in Table 1 on page 23, the contribution of assets by NATO member states to the first NRF rotation reflects this principle of unified maneuver forces. While no fewer than fourteen individual countries contributed assets, plus NATO-controlled assets, the paratroop battalion contributed by France is the principal maneuver element. Apparently, most other countries found it much simpler to earmark ships or aircraft for the force, as bringing ground units up to a uniform standard and making them interoperable with other ground forces in the rotation is far more difficult than making an individual ship or handful of aircraft interoperable (indeed, many already met the existing standards for capabilities and interoperability).

D. Relevant Issues and Uncertainties on the NRF's Development

To date, SHAPE has made significant strides in making the NRF operational on schedule. Moreover, the commitments made by NATO members and the willingness of countries like France—which previously had a very circumscribed role in NATO's military activities—to participate is welcome and suggests that NRF will be a real rather than only a paper force. Indeed, somewhat paradoxically perhaps, the U.S. Operation *Iraqi Freedom* appears to have enhanced interest in NRF among the European allies, including France. Several senior Europeans we met with at NATO noted that the performance of U.S. forces in Iraq was eye-opening to European military leaderships and has created a new impetus on developing European transformational capabilities in "high-end" missions. In the past, as reflected in the European Headline Goals, Europe has primarily coalesced its collective force development around Petersburg (or, low-intensity) missions such as peacekeeping. Hence, France's interest and its reported intent to field forces in an early rotation suggests its calculation that the NRF will get off the ground, and that it wants to take a leadership role among European countries in developing this type of capability.

Table 1.1 Force Contributions, NRF Rotation No.1

Country	Troops	Assets/Capabilities
Spain	2,200	Ships, aircraft, helicopters
France	1,700	Paratrooper battalion, ships, aircraft, helicopter, vehicles
United Kingdom	1,200	Ships, aircraft
Germany	1,100	Ships, aircraft
Turkey	600	Ships, aircraft, helicopter
Italy	600	NBC protection troops, military police, ships, aircraft
Greece	300	Airmobile company, two frigates, one C-130H
United States	300	Ship, aircraft
Belgium	250	Paracommando company, ship, six F-16s, two C-130s, A109 helicopters
Netherlands	200	Ship
Norway	150	Ships, aircraft, JWC (Stavanger)
Denmark	100	Ships, helicopter
Czech Republic	80	NBC equipment and vehicles
Poland	20	EOD unit
NATO	700	AWACS (SHAPE, AFNORTH, AIRNORTH HQ/E-3A Component)

Source: Nicholas Fiorenza, "First NATO Response Force Is Larger Than Expected," *DefenseNews*, 20.

At the same time, the current NRF force structure and developmental process raise a host of issues and uncertainties, any number of which can be the subject of serious analysis. For example:

- Can the rotation system produce viable combat units, and how will "lessons learned" in one rotation be passed on to the next?
- How will common operational doctrine for performing missions be developed and imparted to participating elements? Will there be training and warfighting exercises?
- Will European nations make the investments needed in the short and long term to meet NRF certification requirements, or will the NRF be another in a growing line of efforts to enhance capability acquisition?
- Will NATO ever develop a consensus to actually deploy and then employ the NRF? French President Chirac's recent rebuff of proposals to use the NRF to enhance security in Afghanistan during local elections does not bode well in that direction.

Of direct relevance here are several key issues and uncertainties concerning the NRF's structure and development that bear directly on the question of what types of technology transfer and information sharing will be needed to facilitate the force's fulfillment of its objectives.

The NRF's Limited Nexus to Capability Enhancement

A critical question is whether and to what degree the NRF, as currently being structured, will achieve its goal of catalyzing the European acquisition of transformational capabilities and at what rate capabilities will be integrated into the force? In fact, the linkage between the NRF and the enhancement of specific capabilities is limited, with no future roadmap or plan—leaving it to national participants to shape their own approaches.

While SHAPE's leadership on NRF has been beneficial and has led to significant attention on making the force operational in the short-term, it has had unintended consequences. As discussed above, by virtue of SHAPE's warfighting focus, it necessarily views the NRF as a catalyst for transformation in a very operational sense—focusing on needed changes in doctrine (encouraging European focus on an expeditionary force), organization, training and warfighting methods, and emphasizing the importance of jointness by facilitating interoperability in C4I systems.

At the same time, however, there has been little focus to date in NRF force development/planning on explicating linking the NRF's long-term development and evolution to its underlying armaments capability acquisition goals (lift, precision munitions, and the like). As noted above, SHAPE plans to rely heavily on its certification process to require participating national forces to acquire a gradually escalating level of capability and interoperability, and hopes to disseminate these capabilities throughout the national forces of the Alliance through the rotation process. SHAPE believes, based on its experience with the Graduated Readiness Headquarters (GRHQ) program, that the commitment of national prestige to the NRF will be sufficient to ensure compliance with certification requirements. Yet, this approach has serious limitations. The process has no clear benchmarks and, based on interviews, it appears that SHAPE's planning, by necessity, reflects the notion that the NRF will be comprised of what forces actually exist rather than those SHAPE would like to see for the future. Thus, under SHAPE's approach, as more advanced capabilities come on line, they will incorporated into NRF certification requirements and integrated into the NRF. In effect, this resembles a type of spiral development that is increasingly popular in the U.S. armaments community—where new capabilities and technologies are phased in as they become available in a kind of evolutionary acquisition strategy. Yet, the difference is that there is no long-term "spiral road map" to follow. In other words, the NRF certification process is likely to follow armaments capability development and innovation rather than catalyze it.

Other NATO elements also have not developed any more explicit linkages between NRF and NATO's capability enhancement goals. Within NATO's Resource Management, the NRF is perceived as a new avenue for the promotion of existing procurement priorities, such as AGS and MEADS, which are already planned (whether or not these actually support or facilitate transformation), rather than as a tool to catalyze or prioritize additional capability enhancements.[20] Officials in NATO Force Planning also viewed the NRF as just a fire brigade analogous to ACE Mobile Force-Land (AMF-L), ignoring the differences in role and mission between the two forces;[21] they do not have ambitions to utilize the force as a catalyst for capability acquisition and view this as a separate process driven by national budgetary and other considerations.

In short, there is at present no apparent NATO planning or other process designed to make a more direct or explicit linkage between the future development of the NRF and the acquisition of enhanced capabilities. There is little focus on what capabilities are needed to forge the NRF into a truly transformational force that can meet projected mission needs.

The NATO planning gap is readily explicable. In most national forces, system development and procurement is "requirements driven;" i.e., commanders work from assigned roles and missions down through doctrine, operational methods, and tactics, to a set of operational requirements that in turn fuel the development of new systems. Forces of technology push also operate to encourage the use of new developmental efforts. Yet, these normal processes of demand pull and technology push are largely lacking in the NATO context. There is no rigorous planning to develop a future NRF roadmap that focuses on what objective transformational set of capabilities the NRF needs to carry out its projected missions and catalyze the acquisition of such capabilities. At present, current and future NRF requirements are being developed from a set of abstract propositions derived from analysis and simulation; in the absence of real field experience, NATO requirements developers must rely on projections of future combat operations or battlefield simulations whose outputs are only as sound as the fundamental assumptions that drive them. Such a process of force development has never been tried in the past and, given the weaknesses of combat simulations as a predictive tool, is a path fraught with multiple unknown dangers.[22]

In reality, therefore, the NRF objective of catalyzing the acquisition of new capabilities has been subordinated to the realities of NRF operational necessities. As a result, there is a growing disjunction between the operational and technological aspects of the NRF, without any firm roadmap for technological insertion or any mechanism to incentivize technology investment and military transformation. Thus, these circumstances—the lack

[20] Interview with Robert Bell, NATO Assistant Secretary General for Defense Investment, October 2003.

[21] AMF-L, the land component of the ACE Mobile Force, was a brigade-size force composed of UK, U.S. and Norwegian troops for the defense of the Norland against a Soviet invasion via North Cape. As such, it was purely territorial, with a single mission and a single are of operations. Its capacity for out-of-area operations was limited at best, and with the evaporation of the Soviet threat, its rationale also disappeared. On the other hand, as a standing force, AMF-L did manage to develop a coherent doctrine and operational method, with considerable interoperability among the national components, something that the rotational nature of the NRF makes much more difficult to accomplish.

[22] See S. Koehl, T.N. Dupuy and D.A. Cohen, "Modeling Suppressive Effects in Battlefield Simulations: SBIR Phase I Technical Report," JHF & Associates, Inc. (Vienna, VA) 1994; and Blumenthal, D. and Davis, P.K., "The Base of Sand Problem: A White Paper on the State of Military Combat Modeling (RAND Note), 1989."

of a capability driven technology roadmap—make it very difficult to assess what the technology transfer needs of the NRF should be.

Uncertainties Over Plans for NRF Interoperability

As noted above, one of the NRF's purposes is to facilitate the development of a high-intensity European combat force capable of interoperating with U.S. forces on a modern battlefield. However, at this juncture, there seems to be no coherent interoperability plan in place to facilitate this requirement; there is little detailed focus on what types of interoperability make sense, let alone on what types of enabling technology transfer or sharing of technical information is necessary to achieve it. This is not surprising in light of the continued focus on capability acquisition by the U.S. and its European allies. While the rhetoric often mentions interoperability, there is little focus on these issues.

A starting point for considering the degree of interoperability required for the NRF is two baseline conditions. First, as noted above, there are trade-offs between interoperability and efficiency, and, as SHAPE has apparently decided, it makes little sense to bring interoperability down to the brigade level. Second, in the near to mid term, at least, the NRF must depend on U.S. enabling systems for intelligence, reconnaissance and surveillance, and other critical functions. Thus, assuming this baseline, three different types of interoperability must be achieved:

- Architectural compatibility between the NRF and existing or developmental U.S. C4ISR systems to ensure that NRF elements have access to the best available situational awareness produced by U.S. ISR assets.
- Interoperability with the C4 architecture deployed by other NATO member states and the NATO Multinational Regional Headquarters.
- Interoperability among the NRF elements within a given rotation.

Uncertainties Over U.S. Commitment to NRF

Even with this set of baseline interoperability requirements, there remain considerable uncertainties in this area. First and foremost is the question of what enablers will the U.S. provide the NRF; will it offer its latest capabilities and best situational awareness and actionable, real-time firepower control, or will it insist on dumbing down its offerings? To date, there is no clarity on what enablers the United States will commit to NRF. Will it provide JSTARS and Global Hawk, for example, and if so, will it allow actionable information from these key capabilities to be provided to NRF war fighters? Also, assuming U.S. commitment of advanced capabilities, how will interoperability be ensured between these U.S. enablers and the NRF so as to make it an advanced, transformational force?

NATO's C4 Architecture

The successful integration of U.S. C4ISR enablers with the NRF probably requires the development of an overall NATO or NRF architecture or backbone structure into which new capabilities can be plugged. That, in turn, requires the development of a set of explicit standards and specifications for interfaces, none of which are yet in place for the NRF, let alone for NATO as a whole. The NATO C4ISR Agency has been tasked to try to develop an overall C4ISR architecture for the NRF. However, at this writing, this effort has not made significant progress. Thus, at present, there is no vision of whether the NRF will have its own (or be part of a broader NATO) C4ISR architecture with national plug-and-play capabilities or will simply use existing NATO building blocks and national assets as they find them. Key issues of data fusion and ensuring that the NRF components see the same integrated battle space picture are recognized at NATO, but have not yet been meaningfully addressed.

Finally, the need for the NRF to be interoperable with U.S. ISR capabilities has significant implications for the force's evolving technology transfer requirements. It means that the central issues in the area of interoperability are not so much about what enabling technologies will be shared so as to facilitate capability acquisition as about what developed software and what outputs from U.S. ISR assets will be shared to ensure full situational awareness and prevent fratricide, among other things.

In sum, the NRF being developed and deployed in the near term is really a microcosm of broader cross-cutting issues and challenges inherent in developing an effective coalition warfighting capability and cohesive alliance. Undoubtedly, the NRF will not provide a basis for solving all of these complex challenges. But it does offer an opportunity for experimentation and testing—the essence of military transformation—and the forging of creative solutions.

II. Identifying Critical Enabling Technologies and Information for the NRF

The next question that arises is what specific enabling technologies and technical information (software, data output from sensors, and the like) are critical to the success of the NRF in light of its goals, structure, and probable evolution, as described above. The task of identifying these technical drivers is made more difficult because the NRF's capability trajectory roadmap and planned degree of interoperability are unknown at this juncture. It is tempting to assume that the NRF will utilize new capabilities as they emerge and will draw on U.S. enabling capabilities as they become available. In this scenario, the technology and informational needs of the NRF would be relatively modest. For purposes of this analysis, however, we have rejected this minimalist approach and instead have assumed, for the purposes of analysis, that NATO will try to develop the NRF in a manner consistent with its stated goals.

This means that the NRF will require access to the technology and information needed to:

- Develop the doctrine, operational methods, tactics, and training necessary for out-of-area expeditionary warfare (operational needs),
- Catalyze the acquisition of capabilities needed for such high-intensity missions (capability needs), and
- Ensure robust interoperability between the NRF and U.S. forces to allow the NRF to exploit the capabilities of leading-edge U.S. ISR assets and other enablers (interoperability needs).

As a threshold matter, it is important to understand that this analysis represents a snapshot of presently identifiable technology and technical informational needs, which undoubtedly will change over time. As the NRF's development proceeds in an iterative and interactive process, a combination operational (demand) pull and technology push, will cause the migration of capability requirements, doctrines, operational methods, and tactics. Initial high-intensity mission requirements will drive development of a preliminary doctrine and operational method, mainly using existing technologies and capabilities. As it gains operational experience, the NRF will identify capability and interoperability shortfalls that in turn will drive new capability and interoperability requirements. Thus, this initial analysis of technologies and technical information needs is subject to change over time.

With these baselines in mind, this essay attempts to identify the specific categories of technology and informational requirements of the NRF during the three phases of its development: initial capability (Phase I, 2004-06), reliance on U.S. enablers (Phase II, 2007-12), and phase in of advanced European capabilities (Phase II and Phase III (2013 and beyond). In the absence of existing roadmaps, we have developed prioritized taxonomies of operational, interoperability, and capability needs to use as guideposts. We then take a series of deeper dives into the key areas of technology and technical data access we have identified.

A. A Taxonomy of Technology Transfer Needs Related to NRF Operational, Capability, and Interoperability Goals

NRF technology transfer requirements are related to the NRF's three goals: shifting to expeditionary warfare, catalyzing capability acquisition, and facilitating coalition warfighting interoperability.

Limited Operational Needs

In developing the doctrine, tactics, and operational methods for an NRF-type expeditionary force, SHAPE probably does not need significant technology transfer or sharing of technical data. In attempting to organize and field a high-intensity, multinational expeditionary force, SHAPE is operating on something of a level playing field and has its own internal capability drawn from different NATO members, including the United States. Something of this type has not been tried before.[23] Indeed, there is today little by way of doctrine, tactics, and operational methodologies for a national network-centric force, let alone a multinational force. In the United States, the development of doctrine for joint service operations has been ongoing for some time but has not yet reached maturity. Thus, the NRF goal of creating operational modalities probably can proceed without significant access to sensitive technical information or technology. Of course, one aspect of the NRF doctrine will have to relate to the sharing of technical information needed for interoperability among NRF participants; this is addressed below in the interoperability discussion.

A Taxonomy of Capability and Interoperability Needs

The NRF need for access to U.S. technology and technical information flows largely from the need to: 1) catalyze capability accession and 2) establish effective interoperability for coalition warfighting.

Capability Needs. As a starting point, it must be recognized that the NRF accession of new and advanced capabilities will, by its nature, be long term. The transformational programs just started or underway from which NRF can benefit, such as Airborne Ground Sensor (AGS) and the Medium Extended Air Defense System (MEADS), are unlikely to reach initial operating capability (IOC) for 6–10 years. Paradoxically, however, the technology transfer needs related to these programs are immediate and pressing; given the developmental lead times, it is important that relevant technology be provided as early as possible to facilitate lateral technology insertion and spiral development in order to accelerate the acquisition of advanced capabilities.

The Prague Capabilities Commitment (PCC) is the starting point for understanding capability needs; it set forth certain high-priority capabilities needed to provide NATO with the wherewithal for implementing an expeditionary strategy. Thus, the PCC called for NATO to acquire a fleet of long-range transport aircraft, aerial refueling tankers,

[23] At least not recently. The only successful example, already noted, was the U.S.-Canadian 1st Special Services Force in World War II, which bore little resemblance to the NRF.

NBC defensive systems, ballistic missile defenses, an airborne ground sensor system, unmanned air vehicles, and so forth. The PCC, however, did not directly relate these capability requirements to the mission-oriented operational requirements of the NRF. The link between capabilities accession and force development remained implicit rather than explicit. Moreover, with SHAPE's emphasis on the operational aspects of raising, training, and deploying the NRF, the link has become more tenuous still.

Nonetheless, it is possible to develop a taxonomy of capabilities that relates specific PCC capabilities to specific phases in NRF evolution. This taxonomy, set forth in Table 2.1 below, essentially matches the NRF's development concept for each phase with specific enabling PCC capabilities. Thus, in Phase I, where the NRF will put a small spearhead force in place that will largely fight "as is," capability needs relate to rudimentary capabilities needed for these missions (force protection, precision strike, and close combat). In Phase II, while the NRF will rely primarily on U.S. enablers, the notion of having a full operational force suggests that European strategic mobility or lift, missile defense and additional precision strike capabilities should be phased in; there are programs in place to develop these capabilities, and the timetables involved make their fielding realistic if appropriate European investments are made. Finally, in Phase III where the goal is to phase out U.S. enablers and create an autonomous, high-capability, primarily European force, the more advanced capabilities (in C4ISR and other areas) would be introduced.

Table 2.1 Taxonomy of NRF Capabilities by Implementation Phase

NRF Implementation Phase	**Capability**	**Enabling Systems**
Phase 1	Tactical Mobility and Logistic Sustainability	* High-Mobility Tactical Trucks * Utility Helicopters
	Force Protection	* NBC Detection and Decontamination Equipment * Mine Detection and Clearing Equipment * Body Armor * Armored Personnel Carriers * Short-Range Air Defense (SHORAD)
	Precision Strike	* JDAM * Laser-Guided Bombs * Tactical Standoff Missiles * Guided Artillery Rounds
	Close Combat	* Light Tanks * Anti-Tank Guided Missiles * Mortars * Night Vision Devices (GEN III/III+)
Phase II	Strategic Mobility	* Long-Range Transport Aircraft (A400M) * Aerial Refueling Tankers * Amphibious Assault Ships
	Force Protection	* Tactical Missile Defense (MEADS) * Improved NBC Defense
	Precision Strike	* Tactical Cruise Missiles
Phase III	C4ISR	* Airborne Ground Sensor (AGS) * HALE Unmanned Air Vehicle (EuroHawk) * Airborne ESM Platform * High-Resolution Surveillance Satellite * Broadband Military Communications Satellite
	Precision Strike	* Joint Strike Fighter * Unmanned Combat Aircraft
	Force Protection	* Theater-Wide Ballistic Missile Defense * Robotic Ground Vehicle
	Close Combat	* Advanced Combat Vehicles

The Spectrum of Interoperability. Figure 2.1 depicts the spectrum of NRF interoperability needs in terms of the degree of interoperability (the horizontal axis) and relative complexity (the vertical axis). Admittedly, there is no theoretical optimal level of interoperability. How the NRF will be organized and operate, and the intensity and nature of the operations it will undertake, will determine the appropriate scope and level of interoperability required. However, it is possible, as set forth in Figure 2.1, to identify and prioritize interoperability levels in the context of a network-centric environment.

At the lower left corner of the spectrum are certain basic interoperability requirements, without which any form of coalition (or even joint) warfighting is either impossible or at least very difficult. These include: combat identification (necessary for the prevention of fratricide) and secure tactical communications (for basic command and control functions). Achieving these aspects of interoperability is not particularly complex from a technology standpoint.[24] Indeed, much of the required capability can be achieved through doctrine, training, and standard operating procedures, although some technical information sharing will be needed**.**

As Figure 2.1 highlights, the present state of interoperability between U.S. and allied forces, as demonstrated in Operation *Iraqi Freedom*, is relatively low on the spectrum. Both combat identification and secure tactical communications were achieved, albeit imperfectly, between U.S. and British forces operating in Iraq.[25] The initial rotations of the NRF will be at an equal or even slightly lower state, but will advance as it moves up the spectrum of interoperability.

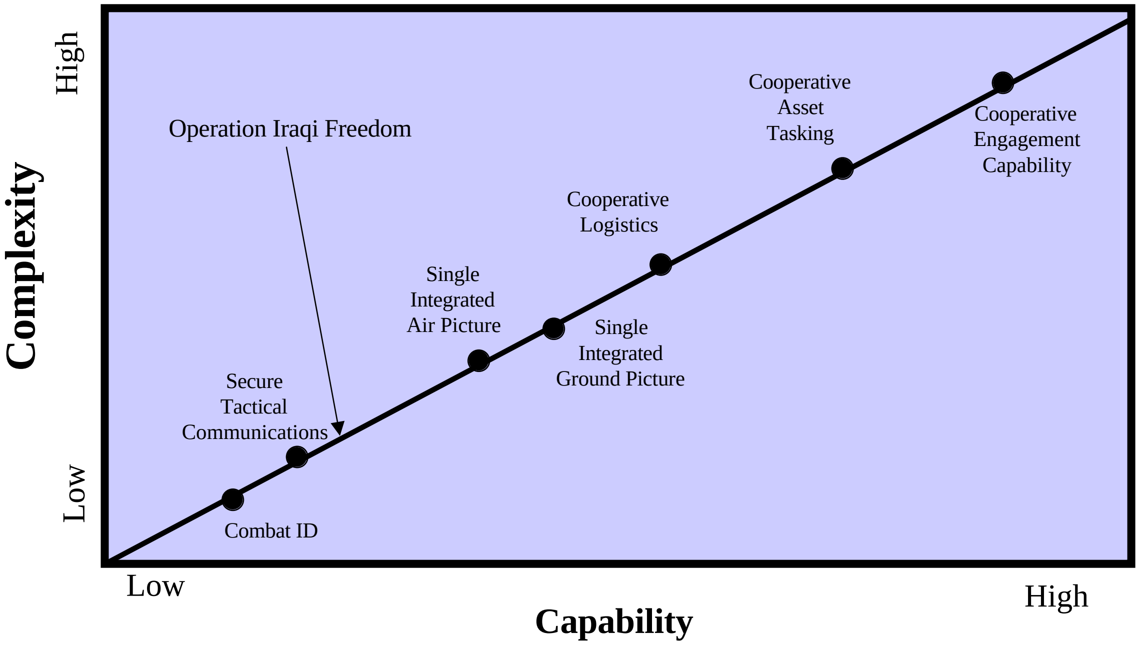
Inevitably, the need to provide the NRF with access to U.S. network-centric enabling systems and the services they provide will drive the NRF to a higher degree of interoperability. Specifically, further along the interoperability spectrum in Figure 2.1 is the development of a single integrated air picture (SIAP) and a single integrated ground picture (SIGP). The United States is seeking to develop a holistic common relevant operational picture (CROP), which would include both SIAP and SIGP. Under CROP, information from many different sources, including airborne, ground and space-based sensors, electronic intelligence, human intelligence, and situation reports, will be fused and displayed as a map showing the location and status of all friendly and enemy forces. Every unit in the area of operations will be able to access the CROP, or at least that

[24] Even with regard to combat ID, the most technically challenging of the Phase I requirements, needs can be met with off-the-shelf solutions assuming that a degree of commonality and/or interoperability can be attained; the emergence of a NATO STANAG for Combat ID systems represents an important step in that direction. As shown below, most of the systems under development or in service today support NATO standards.

[25] As far as can be determined, there were no instances of friendly fire losses involving U.S. or British ground forces. However, at least two aircraft, one U.S., the other British, were lost by accident to Patriot air defense missiles. The war in Afghanistan saw a considerable number of friendly fire casualties, most attributable to human error. In one notable instance, a U.S. forward observer forgot to reinitialize his Global Positioning System receiver after replacing the battery, and inadvertently gave his own position as a target location to a U.S. attack aircraft, which then dropped a GPS-guided bomb on the coordinates. After the war, four Canadian soldiers engaged in a training operation were accidentally bombed by U.S. aircraft that had not been informed of their presence in the vicinity. Both examples demonstrate the role non-technical factors play in achieving reliable interoperability.

portion of it that pertains to its own area of interest. If successfully implemented, CROP would automatically solve the combat ID problem (since commanders will know where all friendly forces are located), as well as facilitate a more rapid operational tempo and reduce the chance of enemy surprise.

Figure 2.1 Spectrum of Interoperability


High
Complexity
Low
Operation Iraqi Freedom
Cooperative Asset Tasking
Cooperative Engagement Capability
Cooperative Logistics
Single Integrated Air Picture
Single Integrated Ground Picture
Secure Tactical Communications
Combat ID
Low
Capability
High

Finally, moving further along Figure 2.1's spectrum of interoperability for NRF are the following types of more complex forms of coalition warfighting cooperation:

- Cooperative logistic systems, in which supplies will be delivered to units only as required by them (a variation on the just-in-time inventory system used by commercial industries).
- Cooperative asset tasking, in which commanders can allocate resources such as sensors, fire units, and ground and air forces as needed to achieve a desired effect, without regard to "ownership" of particular systems.
- Ultimately, a cooperative engagement capability—the ability of a command center to engage a target with a fire unit belonging to another service or country, based on fire control information provided by yet another service or country.

Significantly, the development of CROP is a prerequisite for these more advanced capabilities; having full situational awareness is critical to managing logistics, allocating resources, and having a cooperative engagement capability. At present, CROP itself is under development. These other core elements of advanced interoperability are in early phases of development, and all of these network-centric capabilities present some daunting technical challenges.

These interoperability elements, including the needed enabling technologies to achieve these elements, are shown in Table 2 below.

B. The Phased Timeline for Technology Transfer

The NRF need for access to technology and technical information for its operational, capability, and interoperability development will vary over its phases of operation. The technology transfer and information sharing needs each phase of the NRF are separately assessed below.

Near Term: Limited Technical Needs for the "Pickup Team"

In the near term, the focus is on bringing the NRF together as a force, producing a baseline doctrine, and achieving operational readiness. In this phase, with the emphasis on operational needs, the NRF has no choice but to employ systems already in service with the national contingents, with minimal augmentation to facilitate command, control, and communications, and to rely on the United States for enabling capabilities (strategic lift, air support, logistics support, and ISR). Thus, for the first several rotations, the NRF will effectively resemble a pickup basketball team selected ad hoc at the gym one day: each participating nation will contribute one or more units "as is", with integration of disparate capabilities left to the training phase of the rotation.

With little prior experience on which to draw, the NRF commander and his staff will have to improvise an operational method and tactics that reflect the capabilities and tactics of the individual components of the force. In effect, this means that early rotations of the NRF will employ variants on conventional combined arms operational methods and tactics. Presuming that the NRF will be built around motorized infantry and light armored battalions supplemented by special operations teams and combat service support units, it will employ some combination of fire-and-movement tactics on the attack, with a mobile, elastic defense. Indirect fire and air support will be essential for success on both attack and defense, with close air support and battlefield interdiction, either by fixed-wing aircraft or attack helicopters providing the bulk of the firepower, especially in the early phases of an operation.

As currently envisaged, the NRF may fight on its own for a period of several days to several weeks, but ultimately it must be reinforced and sustained by follow-on forces. Thus, at some point, the NRF must be fully integrated into a larger NATO multinational expeditionary force. This is accommodated through the NATO Graduated Readiness Corps headquarters structure, which consists of several Combined Joint Task Force (CJTF) headquarters, each with a multinational land, air, and naval contingent. Within the CJTF, the NRF is controlled by a Deployable CJTF (D-CJTF) capable of providing command and control for an expeditionary force centered on a brigade-size ground component, an amphibious assault task group, and a small composite air group.

Since the NRF Phase I rotations will largely fight as is, the insertion of new European capabilities is, by definition, not on the near-term agenda, given the time horizons for weapons development. However, consistent with the goal of establishing a small but advanced operational force, there are several capability areas where European capabilities should and can be modestly augmented to provide the minimum credible level of logistical support and tactical mobility so as to sustain itself in the field and move throughout the battle area, and a minimum credible level of force protection, precision strike, and close combat capability. In this regard, it is noteworthy that the relatively small NATO contingent in Afghanistan is absolutely unable to support itself and is entirely reliant on the U.S. supply system for fuel, rations, ammunition, and spare parts; this experience helps suggest the baseline needs of the NRF. Significantly, Europe today has the ability to provide these modest capability augmentations, and with little or no technology transfer or information sharing; the only requirement is for European funding, which also would be relatively modest.

The most important of the capability upgrades in Phase I is the acquisition of high-mobility trucks and utility helicopters to provide the force with tactical mobility and logistic sustainability.[26] The European automotive and aerospace industries have several eminently satisfactory systems in production[27]; they simply need to buy them in sufficient numbers to support the NRF. The same can be said of force protection assets; Europe makes excellent NBC defensive systems, body armor, light wheeled armored personnel carriers, and short-range air defense systems[28], but needs to field them in numbers sufficient to meet the NRF requirement. This is also true for precision strike and close combat capabilities. Several European air forces are now pursuing JDAM compatibility for their existing fighter-bombers; this initiative should be extended to the entire NATO fighter force (except for those aircraft which are physically incapable of carrying the weapon, or which will be phased out of service in five years or less). JDAM compatibility should be incorporated into the new Eurofighter *Tyfun* at the earliest opportunity.[29] In the interim, several European countries either co-produce the U.S. Paveway family of laser-guided bombs, or, like France, have developed fully-

[26] In contrast to the United States military, which assumes the requirement to operate in “undeveloped” theaters, most European armies have not procured significant numbers of high-mobility trucks (e.g., the 2.5- and 5-ton LMTV 6x6 trucks, the HMETT 8x8 10-ton truck, and the HET 60-ton tractor), relying instead on militarized commercial trucks. Given that the primary mission of NATO was the defense of Western Europe, where paved roads were plentiful and lines of communication relatively short, this made sense in the Cold War era. However, commercial trucks have proven less than satisfactory when deployed to places like Afghanistan and Iraq, because they lack the ruggedness and off-road mobility needed in those theaters. In both Afghanistan and Iraq, helicopters have proven invaluable, not only for tactical transport of troops, but also for aerial resupply of widely-scattered forces in rough terrain. However, few European nations have invested in sufficient numbers of utility helicopters to support this task, and many helicopters in the inventory are aging and difficult to maintain.

[27] France, Germany, Britain, Sweden, and Switzerland all produce excellent tactical trucks for their own forces and for export (the U.S. 6x6 FMTV is based on a Swiss design), while Westland Augusta and Eurocopter have both the EH-101 and NH-90 helicopters in production.

[28] As an example, the USMC’s LAV-25 and the Army’s Styker Interim Armored Vehicle are both derived from the Swiss MOWAG Pirhana APC.

[29] The ability to exploit the full capabilities of JDAM, particularly against relocatable targets, requires Europe and the United States to address various issues of C4ISR interoperability, such as access to daily GPS encryption codes; see Section III, below.

interoperable equivalent systems. One of the few success stories of the Defense Capabilities Initiative has been the buildup of NATO stockpiles of precision-guided munitions. This success should be leveraged into new areas of precision munitions, such as guided artillery and mortar shells (France, Sweden, Germany, and the UK all have different systems in production or development) and tactical air-launched standoff missiles (TASMs). In close combat systems, Europe merely needs to leverage its global leadership in light tanks, anti-tank guided missiles, and mortars.

Finally, night vision devices, particularly Gen III and III+ image intensification and thermal imaging systems, have provided U.S. forces with a substantial technical edge and force protection capability. Europe has proven quite adept at development of its own indigenous night vision systems, often refining older technology to perform at the same level as current generation systems when precluded from acquiring the latest versions by U.S. export control laws. Under the current Figure of Merit (FOM) method for determining releasability, European NATO countries can acquire systems approximately 1-2 technology generations behind the current U.S. systems. Because the newer technology works better under marginal operating conditions (fog, precipitation, smoke, and dust), European forces will require an equivalent capability to fight alongside U.S. forces in those environments.

In Phase I, the NRF will also require minimal-level interoperability, which will in turn require some sharing of technical information. Thus, as shown on Figure 2.1 above, even at this early phase, the minimum interoperability requirements include secure, tactical communications and some form of fratricide avoidance or "blue force tracking" (BFT*)*. The need for interoperable secure communications is obvious: as each national contingent comes to the NRF with its own specific tactical communications equipment, this equipment must either, 1) be made compatible and interoperable (through hardware or software "patches"), or 2) replaced by a common set of communications equipment. Theoretically, having the same equipment is the best insurance of 100 percent interoperability; although this solution may initially be more expensive it has greater long-term payoff. Some of the participants may balk at this approach, particularly if the system adopted by the NRF is not backward compatible with the existing communications gear in the rest of their armed forces.[30] Yet, the alternative solution, the use of patches, tends to be less reliable in the long term and more difficult to maintain over time, resulting in higher life-cycle costs. It also should be recognized that the NRF must have communications connectivity not just within the force, but between the Force and the D-CJTF and with any NATO or other follow-on forces that may be deployed in the same battle space. Patches also do not lend themselves to the integration of disparate battle command and combat information systems due to the complexity of the interfaces and variances in the formatting and definition of data**.** This problem tends to push not only toward the use of a single, integrated tactical communications system, but also to a single battle command/combat information system.

Moreover, since the NRF will be relying very heavily on air support in the initial phases of its deployment, reliable communications also must be maintained with any supporting

[30] See Sandra L. Irwin, "Sticker Shock Felt as New Radios are Acquired", *National Defense,* July 2004.

air contingents—the most likely provider of which would be the United States. Thus, from its inception, the NRF must plan to be interoperable with American forces, even though these are not integrally part of the NRF itself. This requirement extends not only to tactical communications, but to command and control systems, particularly those used for deconfliction of airspace and the prevention of fratricide by air attack. From an American perspective, the ideal solution would be adoption of U.S. communications and battle command systems. However, this is not likely to win favor with the various European national contingents. The practical solution therefore would lie in developing bridges to facilitate interoperability between U.S. and NRF systems (and, again, the difficulty of developing and supporting multiple bridges tends to push for homogeneity of both communications and battle command systems within the NRF).

To sum, during NRF Phase I, Europe is capable of filling most capability needs in the NRF from its own resources—with only limited technology transfer sharing needs. In a certain sense, whether Europe is willing to fund these types of relatively modest needs will reflect its level of commitment to the NRF concept and its political will to transform NATO. Interoperability needs (secure communication and blue force tracking) will require some technical information sharing and transfer of technology (either software/hardware patches or new systems).

Mid-Term: Technical Needs Primarily Driven By Increased Interoperability, Not Capability

In the mid-term (2006–12), the development of the NRF, as currently contemplated, will have several distinct elements:

- the evolution to a network-centric operational methodology;
- primarily reliance on U.S. enabling systems, particularly for critical ISR capabilities; and
- addressing interoperability problems arising from operational experience.

SHAPE plans the evolutionary development of the NRF through what might be termed “spiral development” or “lateral technology insertion;” based on the experience of the previous rotations, SHAPE will formulate new operational, technical or material requirements to be met by future rotations. Consistent with the military transformation underway, a key SHAPE goal will be to develop the NRF’s capabilities for network-centric warfare, which is becoming the central paradigm of modern warfighting. Indeed, it is generally assumed in SHAPE and throughout NATO that the NRF will eventually evolve into a high-technology, network-centric force capable of emulating the emerging U.S. style of warfare and interoperating with U.S. forces within a common battle space. The NRF, in fact, is directed toward this long-term goal, with the recognition that the transition itself will take many years.

A key point in understanding NRF development is that, as noted above, the European acquisition of most enablers—from network-centric capabilities to ISR to precision strike—is considerably in the future. For a number of reasons, Europe will not field an indigenous air-ground sensor (AGS), or strategic unmanned air vehicles, or sophisticated surveillance satellite systems, or wide-area tactical ballistic missile defense systems for years to come.[31] Thus, in the medium term, these systems or enablers will have to be provided by the United States.

Hence, during NRF Phase II, a critical priority will be on the need to become interoperable with existing U.S. enabling systems in order to access the data and services they can provide. These include: JSTARS, Global Hawk and Predator UAVs, Rivet Joint ELINT aircraft, satellite reconnaissance and broadband satellite communications. Accessing the capabilities of these systems embedded in a network-centric architecture requires access to the network itself through a variety of digital communications and battle command systems. Thus, for the NRF to actually deploy and operate alongside and within the same battle space as U.S. forces and have the benefit of the increased situational awareness provided by these U.S. systems, the degree of interoperability required between the NRF and supporting U.S. forces inevitably must increase—especially as compared to the rather basic interoperability needed in Phase I. Specifically, in Phase II, the implementation of network-centric warfare concepts while relying on U.S. enabling systems for ISR services, would require development of a single integrated air picture (SIAP) and a single integrated ground picture (SIGP), eventually merged into a single Common Relevant Operational Picture (CROP) providing full situational awareness.

Accordingly, one significant point from a technology transfer standpoint is that the NRF Phase II technology transfer needs are, for the most part, driven by interoperability, and not capability, goals.

Of course, the NRF phases are somewhat artificial and will blur together. Thus, in the latter part of Phase II, it certainly is appropriate and realistic to establish some capability acquisition goals as part of a robust, forward leaning NRF roadmap. In this regard, Europe should be called on to redress shortfalls in strategic mobility, force protection and precision strike—for the most part by bringing ongoing programs to production:

- Europe should make a firm commitment to the production of the A400M to provide the NRF with an indigenous strategic airlift capability. Modified A400Ms or some other platform also should be acquired to provide sufficient aerial refueling capability to offload support of European fighters and transports from the hard-pressed U.S. tanker fleet (tanker availability often being one of the principal constraints on the tempo and scale of aerial operations).
- Several amphibious assault ships similar to U.S. Navy LHAs or LHDs should be built to provide the means for moving heavy equipment and supplies and offloading them over a beach or undeveloped port.
- In the area of force protection, the prospective fielding of MEADS will provide the NRF with an effective area defense system to supplement its existing SHORAD capability, together with a point-defense system against short-range

[31] MEADS, which is now scheduled for deployment ca. 2006-08, can provide only a point defense capability against ballistic missiles.

ballistic missiles. Without MEADS, the NRF will remain vulnerable to missile attack (both ballistic and cruise missiles), and would have to rely on less transportable U.S. systems such as Patriot PAC-3. This capability is important, as NATO commanders have repeatedly stressed that they would not deploy forces to a theater in which ballistic missiles were a threat unless they could provide an effective missile defense. Completion of the MEADS development program and rapid transition to production are thus critical to standing up a full NRF capability in Phase II, pending acquisition of an area defense system such as the U.S. THAADS or a European equivalent.

- In tactical strike, NATO could enhance its capabilities by fielding the several tactical cruise missile systems presently in development, of which the most noteworthy is the MBDA Storm Shadow/SCALP; it has a range of some 250 km and can attack both point and area targets. Acquisition of such weapons would enable the NRF air contingent to attack high-value targets without penetrating high-risk areas.

Significantly, these capability acquisition goals do not for the most part (with the exception of MEADS) require the transfer of U.S. technology. Ironically, while most of the debate over U.S. technology transfer to our NATO partners focuses on capability programs (radar technology for the AGS, stealth for UAVs, engine technology for the A400M, guidance, propulsion and fusing technology for precision weapons), the reality is that interoperability considerations in NRF Phase II will generate a considerable and difficult range of release issues with respect to the accessibility of U.S. technical information (from software to sensor outputs) needed for better NRF interoperability.

Long-Term: Indigenous European Capabilities

In the long term, the goal is for the NRF's so-called objective force to include significant European enablers of modern warfare and more robust network-centric warfare supported by the development of indigenous European C4ISR systems.

Thus, over time, Europe would presumably begin to field advanced enabling systems of its own design that would be integrated into the NRF, thus allowing the NRF to function independently without significant U.S. involvement. From a capability standpoint, AGS would replace J-STARS; EuroHawk or some comparable UAV will replace Predator and Global Hawk; new satellite surveillance systems will supplement and supersede U.S. reconnaissance satellites; new precision strike weapons will supplant JDAM and other U.S. weapons.[32] Specifically:

- The most noteworthy of the European ISR programs is the NATO AGS, which will provide NATO commanders with the ability to track and classify enemy

[32] At this point, in theory, the NRF could potentially become a completely self-sufficient, network-centric force. However, it does not seem likely that Europe will be able to deploy these enabling systems in numbers sufficient to support sustained operations. Consistent with the "early entry" notion of the NRF, in any large-scale NATO expeditionary operation, the United States will inevitably continue to provide a significant proportion of the forces.

ground forces at night and in poor visibility. A number of issues pertaining to AGS have yet to be resolved, including the mix of platforms on which the system will be mounted (will they be unmanned or manned) and various technology transfer issues.

- There is also growing interest in Europe in High Altitude, Long Endurance (HALE) unmanned air vehicles (UAVs), such as the U.S. Global Hawk. Negotiations are being conducted at this time for license production or co-development of a European derivative to be called EuroHawk; France is also developing its own HALE systems.[33]
- A manned or UAV-based ELINT platform is needed to supplement the U.S. Rivet Joint (and its replacement, the E-10A MC2A).
- Europe, and particularly France, Italy, and Germany are working to develop high-resolution remote imaging and radar satellites to provide military as well as commercial reconnaissance and surveillance.
- To exploit the information collected by these new ISR systems, Europe will also need to replace its aging military communications satellites and their terminal infrastructure. The UK is already developing Skynet V broadband satellites as a privately financed initiative, while France is deploying the Syracuse III military communications satellite with Ka-band terminals. Spain and Italy likewise are investing in military Ka-band satellite communications. NATO as a whole is also subscribing to the U.S. Advanced EHF (AEHF) secure, protected broadband satellite program—not by participating in the space segment, but by co-producing AEHF-compatible terminals.
- In precision strike, NATO's capabilities will be enhanced by the introduction of the FA-35 Joint Strike Fighter, which will be able to carry both existing JDAMS and the new Small Diameter Bomb (SDB) as well as advanced tactical missiles. Precision strike capabilities will be further enhanced if NATO acquires or develops an equivalent to the U.S. Unmanned Air Combat Vehicle (UCAV). This will serve as a "can-opener" system to attack very heavily defended high value targets and provide real-time bomb damage assessment.
- Force protection capabilities would be enhanced by: deployment of a NATO Theater-Wide ballistic missile defense system, providing area defense against medium- and intermediate-range missiles; and adoption of robotic Unmanned Ground Vehicles (UGVs) for scouting and reconnaissance, NBC reconnaissance, and mine detection.

The acquisition of some of these capabilities raises significant technology transfer issues. In some cases, like AGS, these issues have already been raised and to some extent addressed. In UAVs, the United States is only beginning to grapple with thorny issues. Significantly, while the timelines for introducing these types of capabilities are long, the technology transfer and information sharing issues must be addressed soon in order to avoid schedule delays.

[33] Global Hawk has been demonstrated for the German MoD. However, budget shortfalls may derail plans for system acquisition. One mission for which Germany, at least, would like to use EuroHawk is electronic intelligence (ELINT) gathering.

This Phase II plan also implies an even greater degree of NRF interoperability. In Phase II, the NRF accesses a CROP generated mainly from U.S. sources and the NRF commander accesses U.S. precision strike systems. In contrast, in Phase III, European systems as well as U.S. systems would feed data to the sensor network to generate the CROP, and the U.S. commander and the NRF commander must be able to access both U.S. and European strike systems. Also in Phase III, full interoperability would mean a shift toward the acquisition of collaborative logistics, cooperative asset tasking, and cooperative engagement capabilities. At this level of integration, there must be a much greater sharing of information, not only at the tactical and operational levels, but at the technical level as well. All subscribers to the sensor and strike networks must know the technical parameters of all the different sensors and weapons.

Designing seamless interoperability in this manner will require intimate knowledge of each other's network architectures. Proprietary standards probably would need to be replaced by open standards, with all the implications that has for maintaining controls over access, releasability, and technology transfer. But this is the inevitable and unavoidable logic of pursuing a network-centric approach to defense transformation in a coalition warfare environment.

Thus, in sum, NRF Phase III raises serious questions of information sharing and technology transfer relevant to meeting interoperability goals and some difficult technology transfer issues pertinent to the acquisition of advanced capabilities (although some of these issues have already been addressed).

III. A Taxonomy of Technology Transfer and Information Sharing Issues

In light of the NRF's purposes, projected roadmap and technology and information needs, this section evaluates the specific technology transfer and information sharing issues inherent in standing up the force. Within the framework of the current U.S. regulatory process (Point I), we separately evaluate the technology transfer and information sharing issues that arise in: 1) meeting the NRF's interoperability and network-centric warfare goals (Point II); and 2) acquiring other enhanced European capabilities (Section III).

A. The U.S. Regulatory, Policy, and Institutional Framework for Technology Transfer: The Reality of Continued Impediments to Coalition Warfare

1. The Legal and Regulatory Basics

The transfer of U.S. technology and sharing of technical information relevant to the NRF must be evaluated in the context of the applicable U.S. legal and regulatory framework and the current and projected operating policies for technical transfer and information sharing under these rules.

Arms Export Control Act and International Traffic in Arms Regulations. The Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) promulgated thereunder[34] establish the process for U.S. government case-by-case decision-making on the transfer abroad of U.S. arms and technology (i.e., U.S. technical data and services relating to the design, development, and manufacture of weapons). The ITAR licensing and review process is inherently complex, involving several different government departments (Defense, State, and others, depending on the nature the product or technology), and various DOD components (including the Defense Technology Security Agency and, in complex cases, the armed services and other DOD components). Depending upon the results of the review, the decision may be passed on to an interagency committee or special executive committees for additional review. The U.S. Conventional Arms Transfer Policy[35], last updated in 1995, articulates the criteria for U.S. decision-making under the auspices of the AECA and the ITAR.

[34] 22 USC Sec.2751 *et seq.;22 c.f.r. Part 120 International Trade in Arms Regulations.*

[35] A broad outline on "International Trade in Arms Regulations" was revealed in a White House Fact Sheet dated February 1995. It states that all arms and technology transfer decisions must be made on a case-by-case basis, in accordance with four broad policy objectives [emphasis added]:

- Assisting allies and friendly nations deter or defend against aggression, *while promoting interoperability with U.S. forces when combined operations are required*;
- Promoting stability in regions critical to U.S. national interests while preventing the proliferation of weapons of mass destruction;

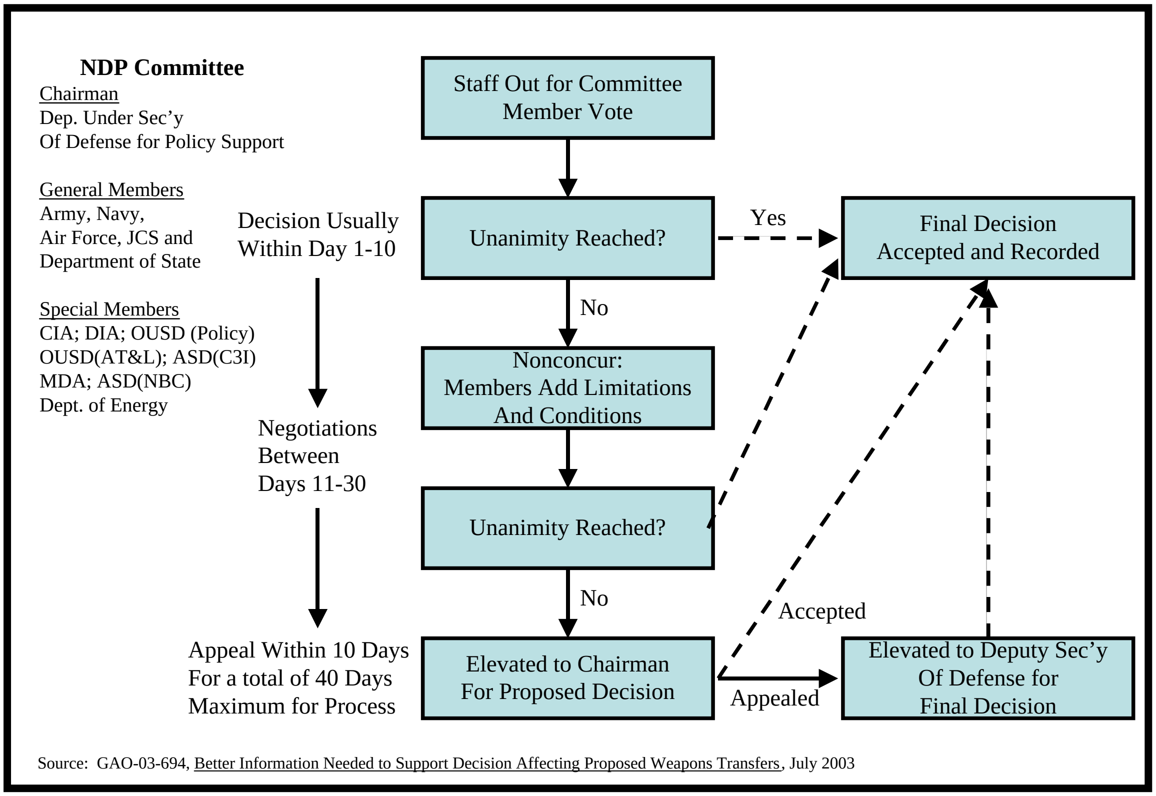
National Disclosure Policy. National Disclosure Policy (NDP), which is not well understood, establishes the framework for transfer of classified information to foreign governments (including information incident to sales of arms and arms development, intelligence, data related to ongoing operations or otherwise). [36] While the release of classified information on advanced weapons is closely related to the ITAR review process, it is nevertheless distinct and includes its own review mechanisms by separate DOD and service offices and components and its own criteria. Under NDP, an initial request for advanced systems or technology is initially referred to the military service or agency responsible for its development, which then coordinates with different bureaucratic entities to process the request and arrive at a release decision. Depending upon the results of the initial review, the decision may be passed on to an interagency committee or special executive committees for additional review. If the requested item is not covered by the NDP, or exceeds the NDP classification level authorized for the requesting country, then the request is referred to a National Disclosure Policy Committee (NDPC) for inter-agency review;[37] the NDPC review process for exceptions to the NDP is shown in Figure 3.1 below.

- Promoting peaceful conflict resolution, arms control, democratization, human rights and other U.S. foreign policy objectives; and
- Enhancing the ability of the U.S. defense industry to meet U.S. defense requirements, *maintain long-term technological superiority*, and reduce costs.

[36] Established by National Security Decision Memorandum 119, “Disclosure of Classified Military Information to Foreign Governments and International Organizations” (Approved 20 July 1971, amended 6 June 1978)**,** and implemented through DOD Directive 5230.11, “Disclosure of Classified Military Information to Foreign Governments and International Organizations” (16 June 1992, supersedes previous version dated 31 December 1984), the NDP encompasses eight broad categories of classified information, including information relevant to arms and arms technology. These include: 1) organization, training and employment of military forces, including tactics, techniques, doctrine, intelligence and counterintelligence techniques; 2) military materiel and munitions, including specific items already in production or in service, and the information needed for operations, maintenance and training; this category includes items on the U.S. Munitions List, but not items in research and development; 3) applied research and development information and materiel, which includes fundamental theories and designs, experimental investigation into possible military uses, engineering data, operational requirements and concepts, and military characteristics needed to adopt an item for production; 4) production information, including designs, specifications, manufacturing techniques and related information; 5) combined military operations, planning and readiness, including information necessary to plan, ensure readiness for and provide support to the achievement of mutual force development goals or participation in combined tactical operations and training exercises, but excluding strategic plans and information related to homeland security; 6) U.S. order of battle, including information pertaining to U.S. forces in a specific area; 7) North American Defense, including plans, operations programs and projects (but excluding data and equipment) related to North American defense, including U.S. homeland defense; and 8) military intelligence, which includes all military information pertaining to foreign nations, but excluding national intelligence and secret compartmented information controlled by the Director of Central Intelligence. See DOD Directive 5230.11, op.cit., Section E.2, Para E.2.1.2—Definitions.

[37] DOD Directive 5230.30, op.cit.

Figure 3.1 National Disclosure Policy Review Process



Source: GAO-03-694, Better Information Needed to Support Decision Affecting Proposed Weapons Transfers, July 2003

The NDP establishes four criteria for the transfer of classified information or materiel which are applied on a country-specific and situation-specific basis. These include whether:

- Disclosure is consistent with U.S. foreign and national security objectives concerning the proposed recipient foreign government;
- The recipient government cooperates with the U.S. in pursuance of military and policy objectives compatible with those of the United States;
- A specific U.S. national purpose, diplomatic or military, will be served; and
- The information will be used in support of mutual defense and security objectives.[38]

In practice, the consideration of whether a transfer is consistent with national security objectives has effectively resulted in a focus on the effect of the transfer on U.S. technological advantage and the maintenance of U.S. military superiority. These criteria are sufficiently broad to allow various DOD and other U.S. government participating agencies to interpret them in different ways and emphasize different considerations; the result is an ad hoc decentralized process with little uniformity.

[38] Ibid. Sec. E.3—NDP-1 Disclosure Criteria, Conditions and Limitations.

Multi-Lateral Disciplines. Finally, there are a series of multilateral arrangements, including Missile Technology Control Regime (MCTR), to which the United States is a party, that are applicable to the transfer of certain types of technology abroad. In practice, MCTR issues are examined as part of the review under the ITAR of proposed transfers. Generally, the Assistant Secretary of State for Non-Proliferation takes the lead in addressing MTCR and other proliferation issues for the U.S. government, and sensitive issues are addressed by an inter-agency committee under the auspices of the National Security Council.

2. Entrenched Problems in the Technology Transfer Process

Unfortunately, since the late 1990s, it has become clear that the labyrinth of applicable U.S. rules and technology transfer processes that have developed thereunder is outdated and based on antiquated Cold War paradigms and has effectively become a major stumbling block to sharing of technology with our closest allies. Given the U.S. lead in many areas in spending and development, the reality is that U.S. technology sharing is vital to ensure Europe acquires enhanced capabilities and also can improve interoperability. This is particularly the case in C4ISR and other transformational areas (precision munitions) where the U.S. lead is probably growing.

The myriad problems in the ITAR export licensing process uncovered by the DOD in the late 1990s were deep-rooted and reflect the fact that the Cold War system had not kept pace with changes in the business world, including industrial integration across borders and the multi-country development and production—even in the defense world. The antiquated system was not designed to deal efficiently with multi-country international cooperative armament programs or distributed manufacturing projects involving commercial and defense products, components, and technologies and the participation of foreign engineers from numerous countries.

As a consequence of these problems, the perception that the system was broken grew on both sides of the Atlantic. From a European perspective, the main shortcomings of the U.S. technology transfer process are the complexity of the process, its apparent arbitrariness, its lack of transparency and, in the end, the difficulty in securing release of enabling technologies. These considerations have caused Europeans to consider designing around U.S. components and technologies where possible. This perspective is also shared by many in the U.S. defense industry who seek expanded participation in the European defense market.

Of relevance here, some of the central problems inherent in U.S. arms transfer policy directly affect efforts to enhance European capabilities, improve interoperability and fight coalition operations, for example, they relate directly to situations like the NRF.

a. U.S. armaments cooperation policy continues to be divorced from technology transfer policy. Technology transfer issues have continued to plague a series of major international cooperative armaments programs in which the United States and various

European countries participates, including the Joint Strike Fighter Program (JSF), MEADS, the U.S. Missile Defense Program, and the NATO Advanced Ground Surveillance (AGS) System. While the specific technology transfer issues vary across the programs (as discussed below), the results have been similar.

In each case:

- The United States has made a policy commitment at senior levels of government to enter into a cooperative armaments program and share the necessary technology to sustain and foster it.
- Enormous resistance to technology sharing surfaced in the U.S. bureaucracy (either the services or other DOD components that deal with export controls and acquisition programs) that undermined the overall goals of the program.
- Significant tensions were created in the bilateral relationships.
- Enormous time and attention of senior policy makers was required to address the issue.
- In most, but not all cases, some compromise (usually uneasy and not satisfactory to foreign participants) have been worked out, at least for a period of time, but numerous restrictions on technology sharing were also imposed.

In the case of JSF, for example, the U.S. government actively promoted and solicited international participation in the program. Yet, nevertheless, the United States subsequently has made a series of restrictive decisions that effectively bar technology release and cooperation on key subsystems of the platform, including avionics and radar, even with close allies like the United Kingdom. These decisions were made under a variety of U.S. government review processes, including NDP and otherwise. Thus, not surprisingly, U.S. credibility today in the area of cooperative armaments is extremely low and our most significant efforts in this arena are struggling and at risk.

b. Adverse Impact on Coalition Operations and Undermining of Interoperability Goals. Export controls interfered with coalition operations during the Kosovo campaign and other recent campaigns. Examples include:

- A U.S. company license request to sell Air-Sea Rescue Flares to the Italian Coast Guard to use to rescue NATO airmen during the Kosovo crisis was initially turned down even though it was eventually approved and is a product that had already been approved for sale to 30 countries.
- The Netherlands waited months for a U.S. export license to import digitized maps for the Chinook helicopters. The license was not granted in time, even after requests for an emergency exemption, and the pilots had to operate without the digitized maps.[39]

[39] Colin Clark, "U.S. Export License System Broken, Say Allies," *Defense News* (Internet version), April 24, 2000. Available online at: <http//:www.defensenews.com>.

- Another U.S. company waited seven months for a license to supply technical data to a Netherlands contractor that was building components for a U.S. fighter engine.

At their heart, the technology transfer problems can be broken down into:

- Process issues—problems resulting from the cumbersome licensing processes and related requirements; and
- Release issues—the unwillingness to release technology even to close U.S. allies.

3. Limited Effectiveness of Attempted Solutions

Across the Clinton and Bush Administrations, there have been well intended reform efforts made to address these issues, especially concerning process. The reality today is that these efforts have had limited effect, been incomplete, and in some ways have proven counterproductive. While it may be difficult to imagine the complex process becoming more dysfunctional, this is in fact what appears to be happening. One has a sense of "déjà vu all over again" when approaching these issues.

Clinton Administration Reform Efforts

In 2000, the last year of its tenure, the Clinton Administration announced the Defense Trade Security Initiative (DTSI), a package of predominantly licensing reforms that included:

- ITAR country waivers or exemptions, along the lines of the Canada exemption, for close allies and trusted firms within those countries. The idea was to share more technology with countries that agreed to improve their own export control systems in various respects. Such governments and firms would be afforded access to certain unclassified technology related to armaments without obtaining specific licenses in advance of export.
- Various types of global licensing agreements designed to facilitate significant transatlantic projects, programs and joint industrial activities, joint ventures and the like.
- Process reforms to speed up procedures and create some process transparency.
- Reform of the U.S. Munitions List, so as to eliminate articles and technologies that no longer warrant inclusion.

Unfortunately, these reforms, which deal more with process issues than releasability, have to date not been implemented fully and have in some ways been counterproductive.

- The idea of country-specific exemptions for close allies, while promising, has been stymied by congressional opposition. While the United States has signed such exemptions with the UK and Australia, a minority in Congress—especially Congressman Henry Hyde, Chairman of the House International Relations

Committee, and his staff—have effectively stopped the waivers from becoming effective by refusing to grant relief from legislation that creates very high, some might say unrealistic, standards for such exemptions**.**

- Similarly, while the idea of large, blanket licenses for major programs has promise, it too has been ineffective. The only such major license issued to date, on the JSF program, was riddled with provisos that undermined the very purpose of this type of license and imposed significant and new compliance burdens. There are real questions about this model for the future. Indeed, some companies have opted out of the Global Project Authorization (GPA) issued for the JSF program and instead chose to rely on traditional technical assistance agreements in order to avoid the compliance burdens and costs.
- Moreover, even some U.S. "win efforts," like reducing approval times, may have actually been counterproductive. First, the reduction in processing time appears to have resulted in a greater number of restrictive provisos (apparently because time pressured reviewers now make more conservative, risk-averse decisions); while this issue is being addressed, it continues to be a problem. Second, companies are now taking much longer to prepare licenses in anticipation of trying to get them through and offering the needed detail required.
- Finally, the effort at Munitions List Reform, begun under the Clinton Administration and continued under the Bush Administration, failed to achieve any meaningful reductions in coverage.

Bush Administration Reform Efforts

While the Bush Administration has had some change initiatives underway and is introducing some needed structural and management reforms into the traditional defense trade control bureaucracies (State Department Directorate of Trade Controls (DTC) and the DOD's Defense Technology Security Administration (DTSA)), the reality is that these efforts have also been incomplete, limited in scope and subject to new developments in the security environment that have created yet additional constraints on technology transfer.

The Unfulfilled Promise of Export Review

On July 21, 2002, President Bush announced a review of Defense Trade Export Policy and National Security, which called for a comprehensive assessment of the effectiveness of U.S. defense trade policies, to identify changes necessary to ensure that those policies continue to support U.S. national security and foreign policy goals. The review, which was to be completed in six months, included promising elements designed to promote coalition warfighting, including facilitating friends' and allies' efforts to increase capability and interoperability. Thus, among other things, the review directed the identification of the top U.S. weapons acquisition programs for which increased industrial participation or greater access to U.S. technology by allies, and vice versa, would improve military effectiveness of U.S. coalitions.

One idea the Bush Administration explored was to address the problem, inherent in cooperative programs, where European firms had engineers of numerous nationalities resident in facilities in a particular European country. Thus, the idea of an enterprise license was explored to address this issue (i.e., and license many of such nationals). This approach to the so-called "deemed export" rule (i.e., the licensing of data disclosures to foreign nationals from one country working in another)) had merit and could have been potentially useful for the NRF.

Unfortunately, however, despite the fanfare surrounding the reviews announcement and the promise it held out, at this writing, it is two and a half years and counting (and nearly two years behind schedule). There are indications, however, that the review rejected major changes in the U.S. approach to technology transfer, including approaches to address application of the deemed export rule to multinational companies and efforts to change release policies on certain technologies. Moreover, there are indications that congressional concern over review proposals to raise the threshold for congressional notifications became a stumbling block.

Indeed, prior to the 2004 Presidential election, an informal temporary stand down was put in place. Congress (notably Congressman Hyde) apparently agreed not to pursue pending legislation to amend the AECA that would tighten restrictions in exchange for an Administration decision not to proceed with changes or the ITAR waivers with the UK and Australia noted above.

Additionally, since September 11, one has the sense that technology release has actually walked back, especially in areas like electro optics, and that more scrutiny is being applied to release. While the release policies (for the most part, not written) vary from one technology area to another, the overwhelming reality is one of continued limited releasability and greater scrutiny in the context of the war against terrorism.

New or Expanded Bureaucratic Hurdles (Special Committees): Stealth and Anti-Tamper

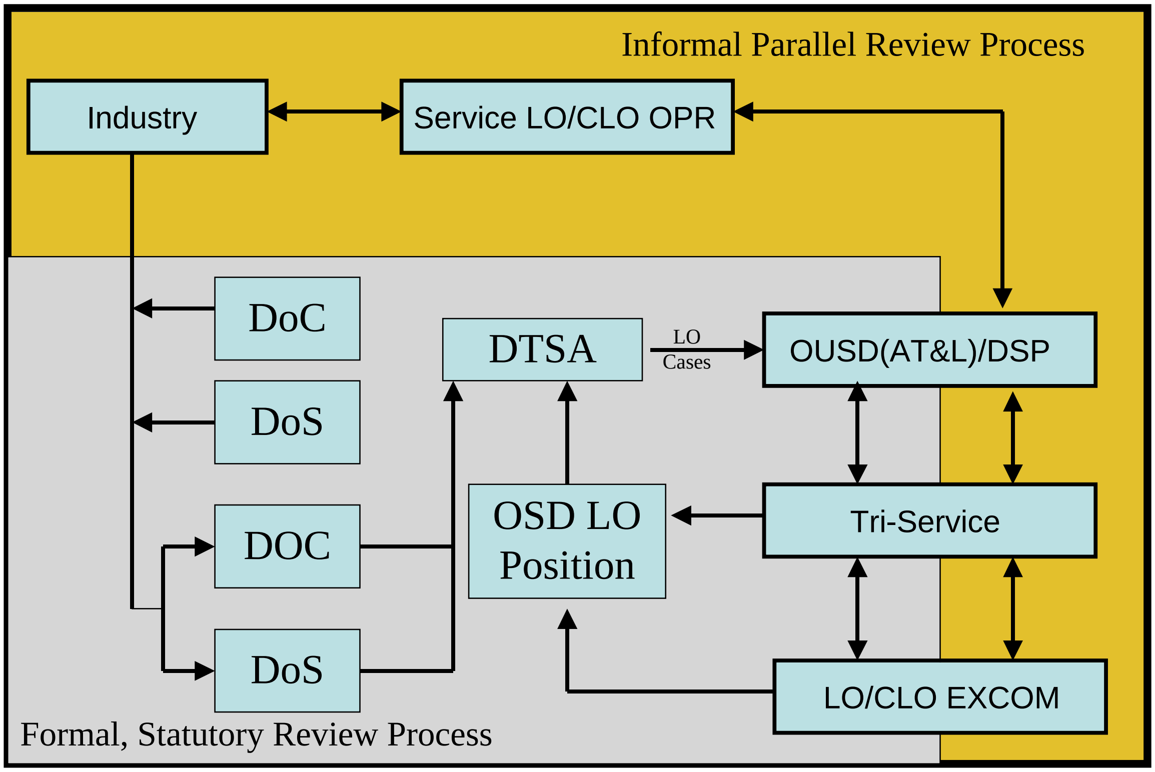
Different Special Committees and other bureaucratic mechanisms have gradually emerged to pose significant hurdles to technology transfer to close allies. Significantly, these decisions are made by different bureaucracies outside of the ODTC/DTSA orbit and through different types of standards.

The releasability of classified and unclassified Low Observable/Counter Low Observable (LO/CLO) technology, stealth and counter-stealth, is managed at DOD through an elaborate process supervised by the Director of Special Programs (DSP) now situated in the Office of International Technology Security (which reports to Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)).[40] Under the

[40] The mandate for the LO/CLO process is found in DOD Directive 5220.22M, "National Industrial Security Program Operations Manual"; and "Security Classification Guide for Department of Defense (DOD) Low/Counter Low Observable (LO/CLO) Programs (U), 2 October 2000. For a review of the

LO/CLO process, low observable cases are initially reviewed by the Air Force and counter low observable cases are referred to the Navy along with ship low observable cases and ground vehicle cases to the Army. Decisions are generally made on a precedent basis. Sensitive cases are referred to a Tri-Service Committee chaired by the DSP, and some complex or extraordinary cases that require exceptions to existing LO/CLO policy precedents are elevated to the LO/CLO Executive Committee, which includes the USD(AT&L) and the Vice Chairman of the Joint Chiefs) for final decision.[41] DOD, which deals with, has become a significant roadblock to technology sharing in a broad range of technology areas relating to stealth and counter-stealth technologies. The LO-CLO review process is shown in Figure 3.2.

Figure 3.2 Process for Review of Signature Control Technologies



Source: GAO-03-694

There are a number of issues inherent in the current LO/CLO process:

LO/CLO process, see "Better Information Needed to Support Decisions Affecting Proposed Weapons Transfers," GAO Report GAO-03-694, July 2003.

[41] The LO/CLO committee also includes the Deputy Under Secretary of Defense for Policy Support, the military services and representatives of the Joint Chiefs of Staff, the intelligence agencies, the Missile Defense Agency, the Assistant Secretary of Defense for Nuclear, Chemical and Biological Defense, and the Department of Energy.

- Its ambit is very broad in scope; it seems to have expanded to cover anything related to LO/CLO in recent years.
- There are no firm deadlines. ITAR license applications that have not been subject to LO/CLO review are typically returned without action and are resubmitted after LO/CLO review, which can take lengthy periods of time.
- The standards, which apparently are entirely informal (or at least not available in open sources), appear based on industrial rather than national security considerations.
- Its decision-making is not transparent (which is not surprising given the highly classified nature of some of the technologies involved).

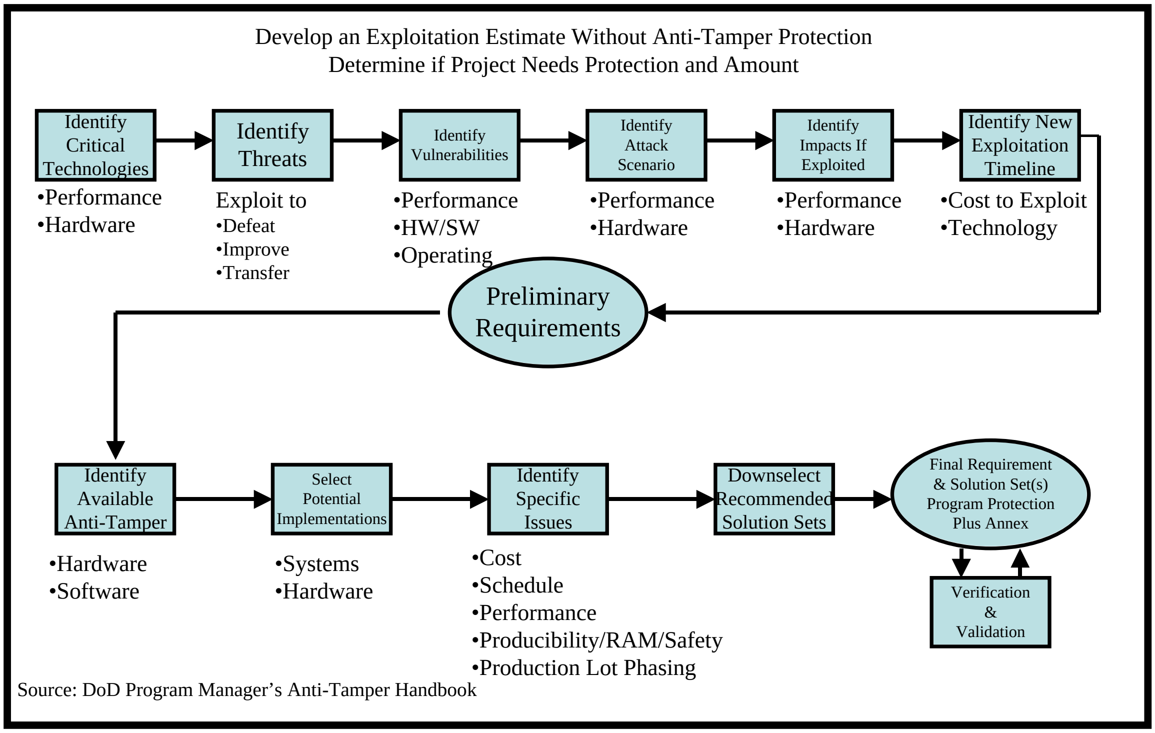
A fundamental dilemma is that the technology experts staffing the LO/CLO process in OSD (particularly in DOD/AT&L) have strong views on technology protection, distrust the export licensing process and safeguards it establishes (i.e., do not believe in their effectiveness to stop improper technology transfers), and believe technology will likely be transferred through informal osmosis—talk among engineers notwithstanding rules and safeguards. Moreover, it is often difficult for more senior officials, especially political appointees without technical backgrounds, to feel comfortable overruling the technical judgments of these experts.

Thus, the LO/CLO process tends to be a black box, and the Executive Committee can exercise a veto over release applications without providing a rationale for the decision. The LO/CLO process also has had a distinctly different operating approach and apparent philosophy in different Administrations. In the Clinton Administration, the LO/CLO EXCOM was a forum where senior leadership sought to change the technology transfer paradigm and provide more support for coalition warfare. Indeed, senior DOD acquisition officials were committed to facilitating greater defense supplier linkages among allies in order to promote greater interoperability, and AT&L became a voice of reason in LO/CLO decision-making (which a shift in emphasis toward coalition warfare as a security mantra and a corresponding shift away from sole reliance on technology dominance even vis-à-vis allies). Moreover, AT&L was closely integrated into DOD's overall technology release policy, as DTRA, which then housed the overall DOD export licensing function now contained in DTSA, reported to both AT&L and Policy.

In contrast, in the Bush Administration, coalition warfare goals have become less pronounced and there has been far less enthusiastic support for these goals throughout DOD, including senior DOD acquisition officials. Thus, in this different context and without more affirmative guidance in support of coalition warfare, the DOD LO/CLO bureaucracy has been left more to its own, more protectionist instincts (i.e., which tend to focus more on technology protection and less on technology sharing as a means of ensuring U.S. security). Moreover, the role of the DOD acquisition community in export licensing has shifted markedly. Early in the Administration, AT&L lost its leadership role over DTSA and eventually created its own office to focus on technology security issues, now called the International Security Office. This office, which lacks line authority over export licensing, is functionally more disconnected from overall Pentagon export licensing, including DTSA, then in the past and has developed its own independent approach with less emphasis on coalition warfare and more on technology protection and dominance. Indeed, its website notes that its mission is to "identify, assess and protect U.S. 'technological dominance' for the U.S. war fighter, while influencing and supporting globalization."

Anti-Tamper. Similarly, the new focus in DOD decision-making on creating anti-tamper mechanisms threatens to undermine cooperation. Over recent years, DOD initiated an anti-tamper policy for acquisition programs that is becoming a significant factor in technology transfer decisions. Initially established by DOD directive in 1999, the idea was to require programs to include anti-tamper measures in requirements development for new and upgraded programs and to be considered for systems developed with allied partners or exported. Yet, this initial guidance has now matured into a firmer policy that now requires anti-tamper mechanisms as a condition of export. Specifically, DOD has now established the Air Force as the DOD Executive Agent for Anti-Tamper; it is charged with overseeing an annual budget of some $8 million to develop anti-tamper technology intended to protect sensitive hardware and software from theft or corruption by hostile powers. In practice, individual program managers are responsible for considering potential anti-tamper measures for any weapons systems with critical technologies. Anti-tamper techniques vary depending upon the type of technology to be protected and the level of protection required. It could include such measures as software encryption, opaque coating of micro electronics, self-destruct devices, auto-erase provisions for mass storage devices, etc. Figure 3.3, below, sets forth the current anti-tamper decision process at DOD.

Figure 3.3 Anti-Tamper Executive Authority Decision Process


Develop an Exploitation Estimate Without Anti-Tamper Protection
Determine if Project Needs Protection and Amount
Identify Critical Technologies
•Performance
•Hardware
Identify Threats
Exploit to
•Defeat
•Improve
•Transfer
Identify Vulnerabilities
•Performance
•HW/SW
•Operating
Identify Attack Scenario
•Performance
•Hardware
Identify Impacts If Exploited
•Performance
•Hardware
Identify New Exploitation Timeline
•Cost to Exploit
•Technology
Preliminary Requirements
Identify Available Anti-Tamper
•Hardware
•Software
Select Potential Implementations
•Systems
•Hardware
Identify Specific Issues
•Cost
•Schedule
•Performance
•Producibility/RAM/Safety
•Production Lot Phasing
Downselect Recommended Solution Sets
Final Requirement & Solution Set(s) Program Protection Plus Annex
Verification & Validation

Source: DoD Program Manager's Anti-Tamper Handbook

At first blush, the anti-tamper regime sounds sensible and designed to achieve legitimate policy ends. However, this constructive idea in fact has some troubling aspects in practice. First, it has evolved from an elective approach used to help provide a basis for facilitating exports to a requirement on programs. Second, like LO/CLO, the anti-tamper decision-making process is outside the scope of the traditional DTSA and service review of ITAR licenses as well as the NDP process. Hence, it has, as some officials has suggested, become another basis on which U.S. reviewers could effectively say no to exports. Moreover, there is no clarity on what technologies are critical—the DOD critical technologies list used in anti-tamper reviews is very outdated—and in practice program managers have broad discretion—with no clear guidelines—for determining whether anti-tamper techniques are needed and for which countries.

Indeed, not surprisingly, a recent GAO report highlights that the anti-tamper policy is being inconsistently applied, with different concepts of critical technology applied and different standards about what level of protection is needed.[42] Unfortunately, DOD rejected the GAO's suggestion that a centralized mechanism be established to ensure consistent treatment of technologies on programs. Also, there is no clarity, in an export context, when such anti-tamper techniques are needed vis-à-vis close allies with strong export control track records.

Thus, as a practical matter, anti-tamper policy is becoming a new effective barrier to the release of advanced technology to allies—and affords DOD acquisition and technology communities another and separate methodology by which to oppose or slow technology transfer even to close allies. Depending upon how anti-tamper is applied, it could have a very significant effect upon the cost of developing new systems. Undoubtedly, anti-tamper will be a significant issue for many of the types of information sharing and technology transfer needs related to the NRF.

By way of example, it was announced recently that anti-tamper requirements have added close to $1 billion to the program costs of the Joint Strike Fighter (JSF); these are designed to protect the stealth features of the air craft and develop a sanitized and less stealthy configuration of the aircraft.[43] One can seriously question the need for this protection and, hence, whether this enormous expense is justified. Given the millions of lines of code involved in various JSF subsystems, it remains to be seen whether foreign engineers working on the development phase of the program or foreign governments that acquire production models could ever backward-engineer these systems or subsystems. This precedent thus is a potentially troubling one for other Transatlantic programs.

[42] "DOD Needs to Better Support Program Managers' Implementation of Anti-Tamper Protection," General Accounting Office Report to the Committee on Armed Services, U.S. Senate (GAO-04-302, March 2004).

[43] See Bill Sweetman, "JSF Security Costing Up to US$1 Bn", *Jane's International Defense Review*. Available online at: <www.janes.com/aerospace/military/news/idr/idr040416_1_n.shtml>.

4. Study Assumptions: Continued Release and Process Issues and Lack of USG Consensus for Overall System Reform

Today, in light of the foregoing, the fundamental realities of technology transfer to U.S. allies are as follows:

a. The Licensing Process. There is some overall sense that the overall licensing process is better; licenses are processed more quickly and the system is more disciplined. In some program and product areas that are less controversial, there is an overall impression that the system functions in a reasonable and predictable manner. Yet, significant problems remain.

Continued Failure of Industry to Use Global Licenses. The new broader licenses have essentially remain unused—probably out of industry's concern that JSF type licenses have high costs of compliance and limited benefits in terms of coverage as well as liability risks for the prime on the program.

The Funnel Effect in Export Licensing. There is an increased demand for precision in the description of what technical data or services is covered—leading to the preparation of more, rather than less, limited technical assistance agreements and other licenses. Moreover, despite efforts to create uniform provisos, there continue to be many extra very limiting provisos on licenses. Thus, the combination of more precise and, therefore, narrow license coverage and more provisos has created a funnel effect in export licensing—resulting in a patchwork of very carefully conscribed licensing vehicles that undoubtedly will raise significant compliance problems in the future for licensees. The limited nature of these licenses—with many exceptions—create situations where full and sustained compliance is highly unlikely even with the best of intentions; can engineers on programs really be fairly expected to abide by these complex, narrowly tailored licenses in discussions with foreign engineers—is this workable? Thus, the funnel effect is likely to increase compliance costs and risks for U.S. firms.

Overall Licensing Times May Have Increased. While the USG licensing process times have declined, there is a sense that corporate licensing process times have increased; firms spend much more time and effort than before meeting the increased need for precision in drafting of such licenses. Moreover, licenses are rejected (usually "returned without action) because there has been no LO/CLO release decision prior to submission. Hence, parties have now recognized the need to seek this review first before submitting a license– and no time limits exist. These reviews do not show up in the DTC data on licensing times that continue to show very low totals.

Lack of Progress in Major Acquisition Program Technology Transfer Decision-Making. Finally, there is no sense of any effort to develop modalities to quickly and effectively establish technology transfer rules for major U.S. programs; problems inherent in JSF, MEADS, and other programs have continued. Foreign participants, especially close allies, are vocal in their continued complaints and highlight that unless the U.S. government is made to really care about these issues, the technology transfer issues linger for lengthy periods of time. Thus, the continued reality is that for transformational U.S. programs that are important to European capability acquisition or interoperability, technology transfer issues will continue to be intractable and require a slog through the complex bureaucratic process. Simply put, there is no clear process designed to achieve an agreed upon solution in a transparent and reasonable manner.

b. Technology Release Policy: Focus On Industrial Policy Rather than Coalition Warfare Goals. Ironically, while most of the export control reform initiatives, like DTSI, dealt with licensing process issues, the reality is that when all of the licensing process underbrush is cleared away the harder issues appear to lie in the area of technology release. Fundamentally, the underlying sense is that protectionism and the maintenance of technological and industrial leadership continue to be the fundamental drivers of U.S. government technology release decisions. In effect, the old paradigm is still in effect—that is, that the fundamental source of U.S. national security, at least in the export control community, is perceived to be U.S. technology and industrial leadership—even vis-à-vis close allies. Working with allies is viewed as a second best way to achieve true security. This is especially true in circumstances, where, as in the Bush Administration, there is less senior level policy-making focus on encouraging technology sharing with allies—which is critical to tackling the problems inherent in an entrenched bureaucracy. This problem was hard enough in the Clinton Administration, where senior officials labored to fix the process; it is yet harder in the absence of senior leadership focus.

Moreover, what makes changing the paradigm more difficult is that the U.S. decision-making process that makes technology transfer and NDP judgments is highly decentralized —dispersed among acquisition program executives, representatives from the operational side of services, the intelligence community and the defense research and development community. Thus, the inherent problem is that: 1) release policies in most areas are not written in some type of objective guidance statement but are inherently subjective and not clearly established; and 2) in the absence of clear written standards, these are judgments and decisions being made on a decentralized, program-specific or activity-specific basis throughout the Pentagon bureaucracy.

Part of the problem is the absence of any clear priority consideration for coalition warfare in the U.S. technology transfer decision-making process. The AECA does not establish interoperability or European capability acquisition as significant factors in export control decision-making; they are nowhere mentioned**.** Indeed, the AECA focuses only on whether "the export of an article would contribute to an arms race, aid in the development of weapons of mass destruction, support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control or nonproliferation agreements or other arrangements."[44] Moreover, the 1995 U.S. Conventional Arms Transfer Policy[45] provides a basis for relying on technological leadership in decision-making. It states that all arms and

[44] AECA, Section 2778(a)(2).

[45] Its broad outline was revealed in a White House Fact Sheet dated February 1995**.**

technology transfer decisions must be made on a case-by-case basis, in accordance with four broad policy objectives:

- Assisting allies and friendly nations deter or defend against aggression, while promoting interoperability with U.S. forces when combined operations are required.
- Promoting stability in regions critical to U.S. national interests while preventing the proliferation of weapons of mass destruction.
- Promoting peaceful conflict resolution, arms control, democratization, human rights and other U.S. foreign policy objectives.
- Enhancing the ability of the U.S. defense industry to meet U.S. defense requirements, maintain long-term technological superiority, and reduce costs.

While the Conventional Arms Transfer Policy clearly establishes that promoting interoperability with U.S. allies (which requires greater releasability) should be a policy objective in release decisions, it also establishes that maintaining long-term U.S. technological superiority (which implies withholding technology from foreign competitors) and the ability of the defense industry to meet U.S. requirements are similarly important factors. Plainly, there is a tension between these considerations. And, in practice, interoperability and capability acquisition have definitely taken a back seat to the protection of perceived U.S. technology and industrial leadership in critical transformation areas, resulting in a widening, rather than a closing of the interoperability gap with the NATO allies. Moreover, the CATP provides no basis for affording a priority to coalition warfighting and capability acquisition goals over technology leadership. Thus, perhaps one reasonable approach is to reformulate the AECA and CATP to afford a priority to coalition warfighting where the United States is satisfied that sensitive technology would not fall into third party hands and will be sufficiently protected (i.e., potential adversaries or their allies).

However, while changes in laws, regulations and new policy guidance will help, the reality is that paper alone has not and will not effectuate change; there have been efforts to afford priority to coalition warfare before that have not done the job. The more significant challenge is changing the culture within the export licensing community of reflexive rejection of applications for technologies in which the U.S. is perceived to have a substantial industrial lead—at the expense of interoperability in coalition warfare. While achieving cultural change within the license review community has been a priority of the leadership of Defense Technology Security Agency (DTSA), which oversees licensing and release at the DOD level, this is a slow process when dealing with career civil servants of entrenched habits. Moreover, reform in DTSA does not address the issue of review within the services (where foreign governments often are viewed with great suspicion). The fact that the CATP explicitly states that interoperability is one of the primary objectives of armaments and technology transfer has not resulted in the elevation of interoperability to a high priority among the technology transfer review community.

c. Lack of Reform Consensus. Finally, there is no consensus for significant reform of the existing U.S. technology transfer system and no apparent willingness of senior Administration officials to afford a high priority to such reforms. Plainly, such reform is not plausible in the absence of sustained senior leadership focus on the issue. Moreover, even if such a consensus was possible, the issues are difficult ones. There are no quick or easy fixes here. The problems inherent in releasability cannot be solved through a rule change or review of the Munitions List.

Thus, for the purposes of this essay, we: 1) assume that the overall U.S. technology transfer system is unlikely to undergo significant change and continue to have dysfunctional elements; 2) explore the specific information sharing and technology transfer issues relevant to NRF below within this framework; and 3) propose specific recommendations for new modalities, short of total system reform, that could potentially be developed for the NRF (some of which have potentially broader application). The challenge is to develop realistic modalities that constrain or limit the inherent discretion of myriad bureaucrats in the export control system in order to facilitate development of the NRF.

B. Information Sharing and Network-Centric Warfare

The technology transfer and information sharing issues related to ensuring interoperability—which largely focuses on linking the NRF to U.S. and European network-centric enablers—breaks down into the three sets of discrete issues discussed below:

1. Connecting the NRF, especially during NRF Phase II, to existing U.S. ISR enabling systems;
2. Linking the NRF to U.S. network-centric capabilities now in development and likely to be fielded in the next 5-10 years; and
3. Linking the new European network-centric enablers with U.S. enablers as they become fielded and available.

Connecting the NRF to Current U.S. ISR Enablers

One core set of technology transfer issues arise from the need for the NRF, during Phase II, to access the capabilities of U.S. intelligence, surveillance and reconnaissance (ISR) enabling systems prior to the development and fielding of European enablers in order to ensure interoperability and provide a high level of support for high-intensity operations. The key U.S. enabling systems, and the requirements for interoperability requirements, are shown in Table 3.1.

Table 3.1 Key ISR Enabling Systems

System	Capability	Interoperability Requirements
J-STARS	Airborne Ground Surveillance Moving Target Indicator Targeting Sensor Cuing	J-STARS Ground Terminal Access to Tactical Internet Interoperable Combat Information System
Global Hawk	Airborne Ground Surveillance Overhead Imagery Target Acquisition & Designation ELINT Communications Relay	Global Hawk Ground Terminal Access to Tactical Internet Interoperable Combat Information System
Predator	Overhead Imagery Target Acquisition & Designation Target Engagement	Predator Ground Terminal Interoperable Combat Information System
Rivet Joint	ELINT SIGINT	Secure Data Link Interoperable Intelligence System Access to Tactical Internet
Surveillance & Recon Satellites	Visual and IR Imagery Synthetic Aperture Radar ELINT SIGINT Missile Early Warning	TENCAP Terminals Access to SIPRNet
Global Positioning Satellite	Precision Navigation Precision Targeting and Strike	Access to Encrypted L1 and L2 Bands
JDAM	Precision Strike	GPS Daily Code Access for Attacks on Relocatable/Mobile Targets

Significantly, the key issues concerning each of these U.S. enablers, such as J-STARS, Global Hawk, Rivet Joint, Predator and various national intelligence assets, is whether the United States is willing to provide the data outputs of these enablers to NRF participant nations on a real-time, actionable basis. To do this, the United States must agree to: share the data outputs of these U.S. enabling systems, which often are classified, with the particular NRF country involved, on a real-time, actionable basis; and export the software or terminals that allows a participating NRF country to access the data and some type of interoperable command and control system that allows the real-time exploitation of the ISR data from the particular enabling system.

In practice, each of these issues can be complex. Since the data outputs of these U.S. systems are in most cases classified, the U.S. sharing of such data outputs requires a determination of releasability under NDP for each system. The exportability of the software or equipment to access the data as well as information about the system and command and control architecture necessary for the data to be utilized in real time also raises issues with respect to unclassified data under the ITAR.

These issues, vary to some extent from one capability area to another, and are analyzed below on a capability-specific basis:

Joint Surveillance and Targeting System (J-STARS). The E-8C Joint Surveillance and Targeting System (J-STARS), a premier U.S. electronic ISR system, consists of a sophisticated ground mapping synthetic aperture radar (SAR) with ground moving target indicator (GMTI) capability. Able to look hundreds of kilometers into enemy territory to detect tanks, trucks and other moving vehicles, J-STARS can provide commanders with early warning of enemy movements and intentions as well as a means of cueing other sensors and precision strike weapon systems. Since its introduction in Desert Storm, the U.S. military has assiduously integrated J-STARS capability into C4ISR architecture, with options for relaying J-STARS data via satellite or to a specified ground terminal; the data is then disseminated to subordinate units via broadband networks like SIPRNet or the tactical internet. J-STARS data can be stored and displayed on a range of U.S. combat information and battle command systems, and overlaid with topographical, tactical, logistical and imagery data.

In Operations Enduring Freedom (Afghanistan) and Iraqi Freedom (Iraq), data from J-STARS were made available to coalition partners—but only indirectly and not in real-time, executable form. Data were first downloaded from the sensor platforms to terminals located at the Coalition Air Operations Center (CAOC), thence to the theater commander's HQ, where the data was processed (and in some cases, filtered or degraded), then forwarded via a dedicated bridging link to the headquarters of coalition partners. This process was time consuming and prevented the exploitation of ISR data in near-real time. Also, by filtering or degrading the quality of the data provided to the allies, the U.S. reduced its value to coalition partners and their ability to employ the data for planning and targeting purposes.

To fully exploit J-STARS data in real time in operations, the NRF would need to: 1) have some means of access (via its own J-STARS terminals, or access to the U.S. tactical internet[46]); and 2) combat information and battle command systems compatible with J-STARS tracking and targeting data so as to allow the information from the sensor to be displayed in a way meaningful to NRF commanders and utilized. This in turn will require the United States to release significant technical information regarding the internal functioning of J-STARS, its system specifications and limitations, communications protocols related to J-STARS track file messages, and the means by which J-STARS data is displayed on U.S. battle command systems. The U.S. may or may not choose to "hide" certain J-STARS capabilities (and limitations) from the NATO Allies, but in so doing it would undermine the ability of the NRF to exploit the system's full capabilities.

Other U.S. Enabling Systems (Global Hawk, Predator, and Rivet Joint). The technical information sharing issues with respect to the U.S. Global Hawk and Predator unmanned air vehicle (UAV) systems and the RC-135 Rivet Joint electronic intelligence (ELINT)

[46] The *Tactical Internet* is the term used to describe this integrated battlespace communications network. The term is appropriate due to functional similarities to the commercial Internet and because the *Tactical Internet* communications infrastructure is based on Internet technology. A key feature is the ability to exchange VMF messages using the commercially based Internet Protocol (IP), which is mandated in the ATA and is common across all segments of the *Tactical Internet*. At brigade and below, the Tactical Internet will extend the Army Battle Command systems to the soldier and weapons platform. The Tactical Internet passes battle command and situation awareness data. The Tactical Internet must provide tactical, mobile, simultaneous multi-band, multi-mode, voice and data (and possibly video) communications while providing routing and network services.

are similar to JSTARS. NRF users must have a means of access (via a compatible terminal for each, or a link to a U.S. command and control network) plus a means of disseminating the information and displaying it in a useful format through a battle command system. While the terminals could be acquired directly from the U.S. with little in the way of technology transfer, using the information would require the release of substantial technical data on each system as well as the network architectures used to support the intelligence they provide. Thus, both the imagery and information on network architectures probably require exceptions from current NDP policy or establishing new NDP policy for systems not yet released. To date, information on these systems has been shared only with a select group of partners, most notably the United Kingdom. As noted, above, however, this has so far been done by first routing the data through U.S. communications nodes and processing centers so that the data going out to foreign users has been reviewed and, if necessary, scrubbed. This has effectively eliminated the ability to utilize this data in real time in operations for targeting and other purposes. As this scrubbing is now done manually, and would be very difficult to automate, the process imposes further time delays, or latency on targeting data, which often renders it less valuable for addressing time-sensitive mobile or relocatable targets.

<u>Intelligence Data</u>. Accessing the data outputs of various U.S. national intelligence assets, including NRO imaging and ELINT satellites, Defense Support Program (DSP) missile warning satellites, present similar issues but also may involve sensitive intelligence sources and methods. Since the end of the Cold War, there have been a variety of programs intended to integrate the capabilities of these systems with the theater and operational levels of conflict; most notable is the TENCAP (Tactical Exploitation of National Capabilities) program, under which highly secure, protected data links (terrestrial and satellite) transmit national intelligence asset data directly to commanders in the field, bypassing much if not all intermediate processing. Again, NDP issues are raised. It is highly unlikely that the United States will allow the NRF real-time, direct access to this information, with the possible exception of DSP (which already is shared over a theater-wide warning network, but which does not really provide detailed tracking and targeting data).[47] Establishment of protocols for the exchange of this information will be one of the more intractable operational issues to be addressed in NRF Phase II.

<u>Daily Global Positioning System (GPS) Encryption Keys</u>. Another somewhat different information sharing issue concerns the releasability of the daily keys for the encrypted military GPS signal (P-Code) that provides greater accuracy and faster initialization. This information is compartmentalized communications security (COMSEC) data, the access to which is controlled tightly by the National Security Agency (NSA). To date, the United States has not shared the daily codes with U.S. allies or NATO, presumably out of concern over the proliferation of its daily encryption keys and the information this might provide about its encryption methodology. Yet, access to the encrypted signal is

[47] Sharing of DSP information, not merely with NATO but also with the former Soviet Union, was instituted after Desert Storm as a confidence-building measure in light of the risk of accidental ballistic missile launch or attacks from rogue states. DSP data is now routinely directed to the NATO Air Operations Center, and both DSP and its future replacement, the Space-Based Infrared System (SBIRS) are already incorporated into the notional NATO ballistic missile defense architecture.

essential for striking mobile or relocatable targets (i.e., Scud launchers). With access to the encrypted P(Y)- Code[48], it takes one-tenth the time to initialize a GPS-guided weapon such as the Joint Direct Attack Munition (JDAM). While several European air forces are integrating JDAM capability into their F-16 fighter aircraft, without access to the daily GPS decryption keys the weapons are useful only to attack fixed targets.[49] Ultimately, should the U.S. fail to release these codes, it seems likely that Europe will develop its own satellite-guided weapons so as to rely on the European Union's Galileo satellite navigation system now in development rather than the U.S.-controlled GPS.

In a certain sense, the United States now has it both ways on global navigation. On the one hand, the United States has fought hard to maintain the integrity of, and freedom from interference with, its current and future military signals in negotiations over the shape of Galileo, a European navigation system under development. Yet, while the United States achieved this goal and continually reinforces the reliance on GPS as a critical element of NATO strategy, it at the same time denies allies the ability to make best use of the precision GPS data needed for precision targeting in coalition operations. This choice effectively highlights that the United States has not afforded a high priority to coalition warfare in its decisional process concerning the release of such data.

When viewed in totality, the United States has, would and should share some of the data outputs from these enabling systems with our allies during exigencies in order to achieve force interoperability and establish the NRF as an effective coalition force for high-intensity missions. Indeed, in light of lessons learned from recent conflicts, the United States has put bilateral memorandums of understanding in place with certain coalition partners that would provide a basis for release of some of this data and ensures that coalition partners will maintain security of such data. Moreover, within Afghanistan and Iraq, field commanders have been delegated the authority to release certain types of actionable data.

[48] GPS uses two different signal frequencies, L1 and L2. The L1 signal carries a publicly-useable and less precise acquisition (C/A) code as well as an encrypted P(Y) Code. The L2 signal normally only carries the P(Y) Code. Only the U.S. military and approved civil users can access the encrypted P(Y) Code, using a very long sequence of pseudo-random binary bi-phase modulations on the GPS carrier at a chip rate of 10.23 MHz. The keys required to directly use the P(Y) code are tightly controlled by the U.S. government and are generally provided only for military use. Using the P(Y) Code on both the L1 and L2 signal bands effectively doubles the number of positioning sources open to each user, allowing for more rapid and accurate acquisition. In spite of not having the P(Y) code encryption key, several high-end GPS receiver manufacturers have developed techniques for utilizing this signal to increase accuracy and remove error caused by the ionosphere. The U.S. appears willing to supply selected European allies with access to the keys for P(Y) on the L1 band, but not for L2. This would allow those users to achieve a higher degree of accuracy, but not with the accuracy or speed available through use of L1 and L2 together.

[49] Lack of P-Code access also limits the capabilities of other GPS-guided weapons, including BGM-109 Tactical Tomahawk cruise missile, the AGM-154 Joint Standoff Weapon (JSOW), and the AGM-158 Joint Air-to-Surface Strike Missile (JASSM). Of these, both Tactical Tomahawk and JSOW have been offered for release to the UK and Australia, among others, while JASSM, a much more capable missile with low observable technology, has not been released to date.

Nevertheless, in the context of creating a standing, rotational force, the release of such information relating to current U.S. network-centric enablers to NRF participating nations raise significant NDP (and, to a lesser degree, ITAR) issues.

The Tension Between Ad Hoc NDP Decision-Making and A Standing, Multi-National, Rotational Force. The ad hoc nature of NDP decision-making—the application of the general NDP criteria on a case-by-case basis to requests from individual countries—raises serious tensions with respect to standing up a multi-national, rotational standing force.

First, the current NDP policy has resulted in separate disclosure policy parameters for each NATO country, both general and specific in nature to programs. Thus, as a general matter, which level of classified information (Confidential, Secret, Top Secret and compartmentalized data) can be released varies for each country. Also, within these general levels, whether data specifically related to or produced by certain specific systems are releasable to that country can vary materially; decisions are program specific and require the involvement of the program "owners" in the judgment. Thus, while some data outputs from these systems is releasable to some NATO countries (especially the United Kingdom), there is no uniform policy and some data outputs may not be releasable today to all NATO countries, especially on a real-time, actionable basis. Clearly, this current U.S. NDP approach, with different levels of disclosure for different NATO allies on different systems, does not mesh well with the rotational structure of the NRF and the fact that different NATO countries will be participating at the same time. Can we provide some data to one NRF participating country's NRF contingent but not another when they are in the same rotation or the next one? Should we have a separate NDP process for these systems for each separate country in each rotation? Needless to say, this would not only exhaust the NDP process, but the ultimate prospect of different disclosure levels would thoroughly undermine coalition warfare and render some of the force "dumber" than other force elements—to the detriment of the NRF's operational capabilities and overall force protection.

Second, the ad hoc, case-by-case nature of NDP decision making does not mesh with the idea of a standing, rotational force that would, on a sustained basis, be ready on rapid notice to take on a range of spearhead missions. Rather, NDP decision making tends to be tailored to specific situations, allowing for what GAO has called "judgment and interpretation of the unique circumstances surrounding each transfer."[50] In other words, the broad NDP standards noted above are subject to interpretation and the interpretations can vary from one case and one official involved to another; State Department officials may focus on impacts on regional stability and DOD officials on technology security or operational impacts. Thus, traditionally, data might be releasable to a *particular* participating coalition partner during a *specific* exigency such as Operation *Iraqi Freedom* or the Balkan wars. Indeed, DOD has delegated disclosure decisions to U.S.

[50] "Better Information Needed to Support Decisions Affecting Proposed Weapons Transfers," General Accounting Office report to Ranking Minority Member, Subcommittee on National Security, Emerging Threats and International Relations, Committee on Government Reform, House of Representatives (GAO-03-694, July 11, 2003), p. 13.

commanders in a theatre of operation. However, there is no overall approach by which such data could be releasable in advance of such contingencies—on a global basis in anticipation of a future need in light of NRF missions.

The reactive and case-specific nature of NDP decision-making thus poses significant problems vis-à-vis the NRF, where, in each rotation, there would be six months of training prior to certification and deployment. Thus, under the current approach, such U.S. data outputs generally would not be available during the training phase and would only be afforded during a specific operation on an as needed basis. Critically, this ad hoc quality to national disclosure decision-making preludes NRF participants from using this data while training together in advance of operations—a necessity for coalition warfare participants that need experience in using such data output and makes sharing with some countries difficult. It is unrealistic to expect nations that do not train together, and do not train in advance in the actionable use of such sophisticated data outputs, to be able to rely on these enablers in the context of actual operations.

<u>The Fractured Nature of NDP Decision-Making</u>. The fact that the NDP decision making is shared among a number of DOD and other USG entities, while ultimately subject to review by the NDPC, also makes holistic decision-making difficult. The disclosure of some data (human intelligence, satellite imagery) generally is decided, in the first instance, by the U.S. intelligence community and the disclosure of communications security data (GPS daily codes, intercept messages, encryption capabilities) would generally be decided by the National Security Agency. Thus, it is difficult to obtain an overall perspective based on specific policy parameters set for NRF.

<u>Difficult Disclosure Issues; Exceptions Required</u>. Finally, even assuming a fair and reasonable process, there are sensitive issues concerning the release of some of the data involved and the United States will probably, and understandably, restrict some types of data. For example, the United States does not, to date, allow foreign access to the SIPRNet, the Tactical Internet, ground stations for key enabling systems or the U.S. command and control systems used to execute this data. Thus, the questions of whether and how to allow access to this data will be significant ones. The SIPRNet is employed by a range of U.S. Government agencies, including the intelligence community, and foreign access to it would pose serious, if not insurmountable, challenges. The U.S. willingness to allow access or details about our leading battle command and control systems that utilize this data would pose difficult issues; we might perhaps be willing to provide sufficient information to allow NRF participants to ensure that their own systems could utilize the data.

Indeed, a number of the needed data transfers would involve classified information on programs on which the DOD has not yet set a disclosure policy or which exceeds existing U.S. disclosure guidelines—necessitating high-level reviews by the NDPC and other special committees (i.e., the LO/CLO Executive Committee). Fortunately, in contrast to the ITAR system, there is a central database, although far from perfect, that can be used to identify the NDP precedents in a particular area.[51] In all events, seeking favorable

[51] See GAO-03-694, op. cit.

outcomes on these issues would require a significant change in policy that provided a significant priority to creating coalition warfighting capabilities such as the NRF (i.e., and offset considerations such as maintaining technological advantages over our allies and otherwise). It would also undoubtedly require agreements with NATO and its members to ensure security of this information.

In sum, the fragmented NDP process, with ad hoc decisions, different U.S. decision makers and different disclosure policies for each NATO member, and the need for senior level reviews, would pose significant challenges for the NRF. Significantly, there is today no unified integrated effort by DOD to review the disclosure issues relevant to the NRF (or NATO interoperability more generally) on any type of global or wholesale basis.

Thus, DOD needs to consider standing up a group that would make a comprehensive disclosure policy for the NRF (and not on an ad hoc or rotation-specific basis). The United States should share some of the data outputs from these key enablers and develop modalities to provide access, as well as sufficient knowledge for allies (or NATO) to develop compatible command and control mechanisms that can utilize these data outputs in real time. In the absence of such an effort, we undoubtedly are headed toward a dumbed down NRF that only obtains last minute, ad hoc access to data from these enablers and is probably therefore unable to execute actions based on this information in real time.

Accessing Developmental U.S. Network-centric Programs

As discussed above, the interoperability of the NRF with U.S. enablers becomes that much more complex given the wide range of cutting-edge U.S. network-centric systems now under development to provide enhanced situational awareness and information dominance.

As the U.S. transitions from its present pastiche of disparate, stand-alone combat information and battle command systems to a more integrated C4ISR architecture, interoperability between U.S. and Allied command, control and communications systems will become both more critical and more difficult to accomplish. With the completion of the digitization process and the transition from voice to data (machine-to-machine) as the principal mode of communications, frequency and even waveform compatibility is no longer sufficient. Interoperability demands that forces exchange detailed technical information concerning network architectures, interfaces, protocols, file structures and so forth, merely to allow the seamless transfer of information between national systems. Internal details of combat information and battle command systems will also be needed if forces are to share the same operational pictures and emulate each other’s tactical displays.

Table 3.2 Interoperability Enhancements and Technology Transfer

Phase	Capability	Definition	Enabling Technologies	Minimum Required Capabilities	Technology Transfer Requirements
I	Secure Tactical Communications	The ability of different national forces to communicate seamlessly over common communications networks with minimal risk of enemy interception and jamming.	Spread-Spectrum Communications TDMA/FDMA Techniques Data Encryption Low Probability of Intercept (LPI) Open Data Architecture	Seamless voice and data communications across national networks	SDR Technology (JTRS) Waveforms & frequency-hopping algorithms Encryption methods Data formats and protocols
I	Combat Identification	The ability to distinguish between frienly and enemy forces on the battlefield so as to avoid fratricide (Friendly Fire).	Non-Cooperative Target Recognition GPS-Based Vehicle Tracking Radio Ferequency Transponders Cellular Communications	Ability to distinguish between allied and enemy forces in all weather down to the vehicle level.	Transponder codes Blue Force Tracking System
II	Single Integrated Air Picture	The ability of different national forces to access and display the locations of all friendly and enemy air assets through the merging of track files from multiple sensor systems reporting over a single sensor network.	Track Correlation Algorithms Sensor Fusion Algorithms Bandwidth Compression Techniques Network Video Techniques	Digital Command & Control Network Upgraded Air Defense Systems Upgraded Airspace Management	SIAP Algorithm & Software Develop Sensor Technical Specifications Network architectures Data Architectures Bandwith compression techniques Broadband data links
II	Single Integrated Ground Picture	The ability of different national forces to access and display the location of all friendly and enemy ground units through the merging of track and intelligence files from multiple reporting systems over a single reporting network.	Sensor Fusion Track Correlation Bandwith Compression Network Video Techniques Measurement & Signature Intelligence	Digital command & control network Digitized Combat Vehicles Digitized Soldier Systems	SIGP Algorithm & Software Develop FBCB2 Architecture and File System Warfighter Information Network-Tactical (WIN-T) Architecture Warfighter 2000 Blue Force Tracking System Data Architectures Bandwith compression techniques Broadband data links
III	Cooperative Logistics	The ability of different national forces to monitor friendly unit status, draw supplies, and provide maintenance support through a common logistics management system employing "just-in-time" logistic techniques	Logistic Management Software Secure Networks Common Network Architecture Common Data Element Dictionary Sensor Fusion GPS-Based Asset Tracking Smart Cards Common Relevant Operational Picture	Digitized logisitic system Digitized Command & Control Net Smart Card-Based Inventory Management	Mostly COTS-based logistic management and inventory control systems Interfaces between battle command and integrated logistic systems Information exchange on unit status Exchange of logistic data
III	Cooperative Asset Tasking	The ability of different national forces to control sensors and other assets belonging to a different national force.	Battle Management Software Secure Digital Networks Common Network Architecture Common Data Element Dicturenary Sensor Fusion GPS-based Asset Tracking Common Relevant Operational Picture	Digitized command & control network Digitized Sensor Network Advanced Sensor Capabilities (e.g. Counter-Low Observables, Low Porbability of Intercept Transmission)	Common Operating Standards System Operating Specifications Sensor System Specifications Command System Specifications Intelligence-Sharing Protocols Asset Prioritization Protocols
III	Cooperative Engagement	The ability of different national forces to direct weapon systems belonging to another national force using a wide range of sensors and fire control assets belonging to its own and/or other national forces.	Battle Management Software Secure Digital Networks Common Network Architecture Common Data Element Dicturenary Sensor Fusion GPS-based Asset Tracking Common Relevant Operational Picture	Digitized command & control network Digitized Sensor Network Advanced Sensor Capabilities (e.g. Counter-Low Observables, Low Porbability of Intercept Transmission) Precision Strike Systems	Common Operating Standards System Operating Specifications Sensor System Specifications Command System Specifications Intelligence-Sharing Protocols Asset Prioritization Protocols Rules of Engagement

Thus, NRF interoperability with the spectrum of emerging U.S. network-centric capabilities, from secure communications to CROP to cooperative engagement, would require the transfer of technology and information for the resolution of outstanding technical issues, including algorithm development, enhanced broadband communications, high speed data processing and fusion, and visualization and decision aids. Table 3.2 summarizes these technology transfer and information sharing needs. A number of operational issues must also be addressed, including the sharing of intelligence from these new assets, the exchange of salient sensor characteristics, sensor network access, and the sharing of information about the underlying architecture and methodologies inherent in these systems. While some of these issues can be resolved through doctrine and training, others will require difficult technology transfer decisions due to the sensitive nature of the information exchanged.

When reviewing the technologies on Table 3.2 and emerging U.S. capabilities, there are several important realities that make these technology transfers difficult.

1. Little Cooperative Engagement

Significantly, there are few cooperative programs or other substantial joint efforts by the U.S. and its coalition partners to develop common network-centric capabilities. Moreover, and perhaps more significantly, there is virtually no foreign participation in any of the leading U.S. network-centric warfare programs. Table 3.3 sets forth the major U.S. network-centric warfare programs. Significantly, there has not been significant foreign engagement or participation in any of them**.**

Thus, even in program areas where near- term interoperability is important and should be a major focus, such as secure communications and blue force tracking, cooperation is limited and no easy answers exist.

- On tactical radios, the United States and its European allies have largely independent next generation secure communications programs underway, with little focus on interoperability. The United States is moving toward Software Defined Radios (SDRs) such as the Joint Tactical Radio System (JTRS), while most European countries are still deploying single-band radios similar to the U.S. SINCGARS developed in the 1970s. Attempts to create a multinational Future Multiband, Multiwaveform Modular Tactical Radio program foundered over issues of cost and the releasability of SDR and encryption technology. Since then, most European countries have initiated their own national tactical radio programs. Sweden, Finland and France are all developing SDR concepts, but the most important system (from a coalition warfare perspective), the British Bowman tactical radio family, uses conventional single-channel technology. There has been no coordinated effort to ensure interoperability among these next-generation communications systems. The most prominent, the U.S./UK JTRS/Bowman Interoperability Initiative, requires the British to release to the United States the Bowman waveforms and encryption engine, allowing the U.S. to develop software to emulate the Bowman system.[52] Given that Bowman is a hardware defined radio, there really was no other viable solution, but it did have the virtue (from an export control standpoint) of protecting U.S. SDR technology and the JTRS encryption engine. Refusal to release those technologies has prevented the development of interoperability standards for European software defined radios.[53]

[52] In the same manner that SoftPC© allows the Windows© operating system and applications to run on a Macintosh© computer.

[53] See Appendix A for additional details.

Table 3.3 U.S. Transformational Programs and Releasability Status

Program	Sponsor	Type	Releasibility	LO/CLO
Advanced Broadband Satellite	Joint	Communications	No	
Aegis BMD	Navy	Missile Defense	Some	Yes
Airborne Common Sensor (ACS)	Army	ISR (ELINT)	No	
Airborne Tactical Data Link	Joint	C3I	No	
All Source Analysis System (ASAS)	Army	Intelligence	No	
Army Airborne Command Post (AACP)	Army	C3I	No	
Army Field Artillery Tactical Data System (AFATDS)	Army	Artillery Fire Control	No	
Blue Force Tracking	Army	C3I	No	
Broad Area Maritime Surveillance System	Navy	C3I	No	
Combat ID	Joint	C3I	Some	
Cooperative Engagement System	Navy	C3I	No	
Digital Terrain Simulation System (DTSS)	Army	Intelligence	No	
E-10A MC2A	USAF	C4/ISR	No	Yes
FAADS C2	Army	C3I	Some	
Future Battle Command Brigade & Below (FBCB2)	Army	C3I	No	
Future Combat System (FCS)	Army	System Architecture	No	
Gapfiller Communications Satellite	Joint	Communications	No	
Global Hawk	USAF	ISR	Some	Yes
GPS Encryption	Joint	C3I	Some	
Inter/Intra Flight Data Link	USAF	C3I	No	
JLENS	Army	Sensor	No	Yes
Joint Tactical Radio System	Joint	Communications	Some	
Maneuver Control System (MCS)	Army	C3I	Some	
MEADS Engagement Radar	Army	ISR	Some	Yes
Missile Defense Battle Management	Joint	C3I	Some	
Mounted Battle Command on the Move	Army	C3I	No	
MP-RTIP	USAF	ISR	No	Yes
Rosetta Stone	Joint	C3I	No	
Single Integrated Air Picture	Joint	C3I	Some	
Single Integrated Ground Picture	Joint	C3I	No	
SPY-3 Radar	Navy	ISR	Some	Yes
UCAV	USAF	Precision Strike	Some	Yes
Warfighters Information Network-Tactical (WIN-T)	Army	C3I	No	

- On Blue Force Tracking, the United States has leased the initial version of the Blue Force Tracking System (BFTS) to UK forces in Iraq and Afghanistan, where it has worked well, though there were still a number of friendly fire incidents and the Coalition Command did not have sufficient faith in the system to deploy U.S. and UK forces in the same battlespace. While the UK seems content with BFTS, other European countries, notably France, are developing their own Blue Force Tracking capabilities. These are simple interrogate-and-respond systems like the U.S. Battlefield Combat ID System (BCIS)—for which NATO STANAG 4579 provides minimum interoperability standards[54]—but are not compatible with BFTS, which provides continuous, real-time reporting of blue force positions (and potentially unit status information as well). Thus, without some effort in the direction interoperability, European forces will not be able to provide input to BFTS (unless, of course, they are willing to accept BFTS on U.S. terms). Moreover, BFTS is a significant input to the Single Integrated Ground Picture (SIGP) or the Common Relevant Operational Ground Picture (CROP). Without BFTS interoperability, not only is the risk of fratricide increased, but the entire situational awareness capability on which network-centric warfare rests will be undermined.

[54] See Appendix A.

In more advanced areas (CROP, cooperative engagement) there is virtually no foreign participation in key U.S. programs and little cooperative activity. Indeed, the areas of collaboration have been few and far between:

- Single Integrated Air Picture. Cooperative development is limited to part of the NATO Airspace Management program, and the AEGIS air defense system. Within the NATO Airspace Management Program, the emphasis in on European homeland defense, through the integration of civil air traffic control radars and NATO and national military air surveillance systems, fused to provide a single integrated picture of European airspace at several regional airspace management centers. SIAP is being developed as part of AEGIS for the purpose of enhancing defense against anti-ship cruise missiles (by providing an over-the-horizon detection, tracking and classification capability), and to expand the capabilities of AEGIS ballistic missile defense (by allowing the fusion of missile track data from several off-board sources such as early warning satellites, ground-based radars, and other AEGIS-equipped ships). Due to the miniaturization of AEGIS and a concomitant reduction in costs, the system is being installed on new European frigates and destroyers, which can thus interoperate seamlessly as part of a U.S. naval battle group.

- An affordable Link 16 (JTIDS) terminal intended for NATO forces and other U.S. allies, the MIDS program was initiated in 1994 by the U.S. Navy Space and Warfare Center (SPAWAR) to enhance interoperability in coalition environments. Because the U.S. JTIDS Class 2 terminal was simply too large for many allied ships and aircraft, and too costly for most European countries, MIDS was conceived as a smaller, lighter version of a Class 2 terminal.[55] At present, five countries, the U.S., France, Britain, Italy, Spain and Germany, are full participants in the MIDS program, with most NATO countries committed to purchasing the terminal; future sales outside of NATO are anticipated. Under the MOU that established the MIDS program, system development responsibility is assigned to MIDSCO, a U.S.-chartered joint venture company under contract to SPAWAR. MIDSCO not only designed and developed the terminal, but also has responsibility for qualifying other companies from participating countries to produce and/or assemble components, subsystems and entire terminals.

- CAESAR**:** The Coalition Airborne Surveillance and Reconnaissance (CAESAR) program, initiated as a multinational Advanced Concept Test and Development (ACTD) experiment during the latter phases of the war in Kosovo, has developed a range of hardware, software and procedural solutions to integrate different data links and information management systems, thereby eliminating the so-called “sneaker links” that had to be used to transfer information from U.S. to allied command and control systems and vice versa. Though not yet fully operational, CAESAR is an excellent example of a relatively low-key international initiative that has yielded significant benefits for interoperability.

[55] With production plans for more than 4,000 terminals already in place, the anticipated cost of a MIDS terminal is on the order of $250-300 thousand, as compared to more than $1 million for a JTIDS Class 2 terminal.

Plainly, if Europe is to narrow the C4I gap sufficiently to make interoperability with developing U.S. systems a realistic hope, then there must be an increased degree of European involvement in U.S. transformation programs.

2. Limited or No Release

Significantly, for some of these leading C4 programs, the United States has a policy of limited or no release. For others, in early development stages, there is no overall release policy yet in place and we do not know whether and to what degree the software or architectures associated with them can be released to third countries under the U.S. national disclosure policy. Among these critical programs are:

- *Future Combat System* (FCS), the U.S. Army's network-centric system of systems for the next generation, including new vehicles, weapon systems, and C4ISR capabilities (no release);
- *Future Battle Command—Brigade and Below* (FBCB2), the U.S. Army's next-generation tactical command and control system, without access to which the NRF will be unable to operate effectively with U.S. forces (no release);
- *Blue Force Tracking* (BFT), an element of FBCB2 allowing commanders to keep track of all friendly forces down to the individual vehicle level, without which the NRF will not be able to avoid fratricide (limited release[56]);
- *Army Field Artillery Tactical Data System* (AFATDS), the Army's new field artillery and air support fire control system, without which the NRF will not be able to access U.S. fire support assets (limited release[57]);
- *E-10A Multi-Mission Command and Control Aircraft* (MC2A), the USAF's replacement for J-STARS, AWACS and Rivet Joint (no release policy);
- *Digital Rosetta Stone*, a system for bridging new and legacy C4I systems, an essential aid for creating bridges between the NRF and U.S. C4I systems (not releasable);[58] and

[56] The Blue Force Tracking System (BFTS) was leased to British forces in Iraq on a "black box" basis without any transfer of technical data; the principal purpose was to prevent U.S. forces from attacking British forces. See *Operations in Iraq: Lessons for Future Conflict*, UK Ministry of Defense (London) December 2003. However, the technology, and particularly the encryption engine for the system, are not releasable to foreign entities**.** This makes it difficult for the allies to develop their own compatible BFT systems, and encourages them to develop national systems using their own unique protocols and standards, whch may not be compatible with the BFTS.

[57] A less capable export version of AFATDS is being developed by Raytheon, but has not yet been approved for sale to foreign governments.

[58] Digital Rosetta Stone (DRS) Model is a framework for capturing and maintaining methods necessary for the retrieval and display of digital information stored on obsolete or incompatible media or using obsolete software. While originally developed to facilitate the archiving of government documents, its utility as a bridge between new and legacy hardware/software systems makes it an important tool in the development of a fully-integrated C4ISR network involving new and legacy systems, as well as systems owned by several different services or countries. See Alan R. Heminger, "A Delphi Assessment of the Rosetta Stone Model", *Proceedings of the 37th Hawaii International Conference on System Sciences-2004*. Available online at: <http://csdl.computer.org/comp/proceedings/hicss/2004/2056/04/205640104b.pdf>.

- *Warfighter's Information Network—Tactical* (WIN-T), the future information network over which the U.S. plans to transmit the bulk of its broadband C4ISR data[59] (not releasable).

3. Limited Foreign Participation in Joint Warfighting Experiments.

Further, the U.S. Joint Forces Command (JFCOM) is conducting a series of Advanced Warfighting Experiments (AWEs) that focus, among other things, on joint operations between U.S. forces and the utilization of network-centric capabilities. Conducted by the U.S. services individually, or more commonly, as joint exercises under the auspices of the U.S. Joint Forces Command, AWEs are intended to test new concepts, technology and tactics in a simulation environment. The results of AWEs are used to direct research and development and to refine acquisition priorities.[60]

Significantly, there is very limited foreign participation in these experiments. In the absence of such training and experimentation together, it will be very difficult to identify the detailed nature of interoperability requirements regarding these future systems. Connecting these future capabilities with those of NRF participants will take considerable time and effort, and cannot meaningfully be done on the fly in the context of a particular exigency when the force is called to action.

In short, without any affirmative U.S. actions to address this issue, the capability and interoperability gaps that exist today are likely to widen significantly in the future. In some of these program areas, the United States may be willing to ultimately sell some of the new network-centric capabilities to its European allies and share the software, but may only want to offer a more limited version for export or may not be willing to share source code. In the past, the black box approach was grudgingly accepted by most European countries *faut de mieux*, because their defense industries were not yet sufficiently developed to provide the requisite capabilities indigenously at a competitive price. Such is not the case today: anything the United States can develop, Europe can also develop, albeit somewhat later and probably at somewhat higher cost. Failure to allow full access to the technology in cooperative systems creates the impression that the U.S. considers its European allies second class partners; and that it wishes to deny them access to technology in order to protect the U.S. defense industry and suppress competition. It also creates the suspicion among some Europeans that the United States

[59] WIN-T is Army XXI's tactical telecommunications system consisting of communication infrastructure and network components from the maneuver battalion to the theater rear boundary. The WIN-T network provides C4ISR support capabilities that are mobile, secure, survivable, seamless, and capable of supporting multimedia tactical information systems within the warfighters' battlespace. WIN-T's infrastructure provides commanders and other users the ability to communicate via voice, data, and video *simultaneously* at all levels of security up to Top Secret. WIN-T supports the warfighter's requirement for Command and Control On-the-Move (C2OTM) by integrating the major WIN-T elements into warfighter mobile tactical operations center (TOC) platforms while leveraging the Joint Tactical Radio System (JTRS), wide-band digital radios, and wireless local area network (LAN) technologies.

[60] Best known among the AWEs are the Millennium Challenge series of exercises that have run periodically since the late 1990s. For a description of Millennium Challenge 2002, see: "Millennium Challenge 02", U.S. Joint Forces Command. Available online at: <www.jfcom.mil/about/experiments/mc02.htm>.

might use the black box to deprive them of certain critical capabilities omitted from export variants. Objections to the black box approach have been seen recently with regard to the MEADS engagement radar, with the MP-RTIP radar proposed for AGS, and with regard to some elements of the AEGIS air defense system.

On the other hand, with regard to certain systems, some European countries still appear willing to accept a black box approach. The United Kingdom, for instance, is buying the Cooperative Engagement Capability (CEC) data link for its new aircraft carrier as a black box via FMS. Also, in regard to the JTRS-Bowman Interoperability Initiative, Britain has voiced no opposition to an approach that amounts to a black box. In the case of CEC, it appears that the UK has determined that co-development would not be economically feasible at this time. With regards to JTRS-Bowman interoperability, the operating principles of Bowman are so different from those of JTRS as to make a more collaborative solution impossible, while the cost of Software-Defined Radios (SDRs) such as JTRS remains prohibitive for the fiscally-constrained British MoD. The acceptability of black box solutions thus depends entirely on how badly the Europeans want a particular capability, and whether they think it is economically feasible to bypass the United States to develop it themselves.

Given the general lack of U.S.-European cooperation on the development of network-centric solutions, the United States should consider holistic approaches for integrating the NRF and our NATO allies more generally into our advanced efforts if it truly seeks to promote coalition warfighting capabilities. Under the current NDP approach, this would require country-specific and program specific decisions, again rendering the matter very complex. The better approach would be to identify a set of core programs needed to ensure interoperability in the emerging era of network-centric warfare and facilitate foreign participation in them.

Linking New European Network-Centric Capabilities to U.S. Enabling Systems

Finally, in the long term, the introduction of indigenous European capability systems such as the Airborne Ground Sensor (AGS), advanced UAVs, high-resolution reconnaissance satellites and broadband communications satellites, does not diminish the need for interoperability with U.S. forces. Indeed, if fully network-centric concept of operations is adopted, interoperability will become a two-way street, with U.S. forces drawing information from European systems in addition to European forces tapping U.S. systems. With the advent of cooperative logistic support, cooperative asset tasking, and ultimately, cooperative engagement capabilities, total interoperability between communications networks, combat information systems, and battle command systems will be essential. Information will pass automatically from machine-to-machine, with commanders acting upon seamlessly fused information for situational awareness, maneuver control, and effects-based operations (see Appendix A for detailed interoperability requirements in Phase III).

To achieve this degree of interoperability, the United States and Europe must either develop common command and control systems, or must exchange detailed technical data on their respective systems in order to develop the proper interfaces and bridges between systems. Unfortunately, at this time, there appears to be little cooperation in the area of command and control, and little exchange of information on battle command systems being developed or implemented on either side of the Atlantic, and little U.S. release of technology or other technical information, classified or otherwise, in these areas. Thus, while there have been some bright spots such as the acquisition of CEC by the Royal Navy, and the U.S.-UK JTRS-Bowman Interoperability Initiative, for the most part the European allies have been closed out of critical C4I programs, including the Army's FBCB2 tactical battle command system, the Army Future Combat System (FCS), WIN-T, and the USAF's E-10A MC2A among others. And the military has been loathe to release certain critical communications technologies to anyone, such as the encryption engine and other SDR applications for JTRS.

By excluding the Europeans from meaningful participation in these and other transformational programs, the U.S. has made it difficult if not impossible for the NRF to achieve the required degree of interoperability with U.S. forces to exploit key U.S. ISR enablers in Phase II, and to execute effects-based network-centric operations with U.S. forces in Phase III.

In sum, the United States faces a strategic choice about the nature and degree of interoperability between the United States and its coalition partners on the NRF and the potential overall effectiveness of the NRF.

If the United States approaches this issue on a business-as-usual basis and applies its current complex and ad hoc processes and restrictive policies on sharing the technical information relevant with other countries (ITAR, NDP and others), we will end up adopting an unsatisfactory least-common-denominator approach to sharing these capabilities in a coalition environment (NRF or otherwise). This would surely result in a dumbed down NRF that lacks the top line enabling capabilities, has very limited interoperability with U.S. network-centric enablers and, hence, would not be as potent an expeditionary force offensively and will face greater combat risks of casualty.

The degraded NRF would not be able to receive and process all data passed to it by U.S. forces from various ISR and information systems.[61] On an absolute level, this will reduce the effectiveness of the NRF in high-intensity combat by limiting its access to all available ISR data and reducing its ability for real-time use of such data for more opportunistic and precise combat operations. In relation to U.S. forces, it will inhibit if not prevent the NRF from operating in the same battle space with U.S. forces, thus forcing coalition commanders to segregate it in a separate area of operations. Clearly, this defeats the one of the core purposes of the NRF—to establish an advanced and interoperable expeditionary fighting capability for high-intensity warfare.

Alternatively, the United States could and should make a strategic choice, consciously and holistically, and not on an ad hoc basis, to afford more priority to the NRF and

[61] See, for instance, the previously noted development by Raytheon of a less capable, export version of the Army Field Artillery Tactical Data System (AFATDS).

coalition warfighting and take actions to follow through on this policy choice. This would mean more advanced training with NRF partners in the use of these enabling assets and the creation of mechanisms (through software, hardware, interoperable architectures, etc.) to facilitate the real-time use of these capabilities.

C. Capability Requirements

Table 3.4 below sets forth the areas of potential technology transfer relevant to the enhancement of NRF capabilities (other than in C4 area discussed above).

Table 3.4 Capabilities and Technology Transfer Requirements (Non-C4I)

NRF Implementation Phase	Capability	Enabling Systems	Technology Transfer Req'ts.
Phase I	Tactical Mobility and Logistic Sustainability	High Mobility Tactical Trucks	None
		Utility Helicopters	None
	Force Protection	NBC Detection & Decontamination Equip.	None
		Mine Detection and Clearing Equipment	None
		Body Armor	None
		Armored Personnel Carriers	None
		Short-Range Air Defense (SHORAD)	C3I Integration
	Precision Strike	JDAM	GPS Daily Codes
		Laser-Guided Bombs	None
		Tactical Standoff Missiles	None (GPS Code), MCTR
		Guided Artillery Rounds	None
	Close Combat	Light Tanks	None
		Anti-Tank Guided Missiles	None
		Mortars	None
		Night Vision Devices (GEN III/III+)	Possible Licensing Req't.
Phase II	Strategic Mobility	Long-Range Transport Aircraft (A400M)	Minimal
		Aerial Refueling Tankers	None
		Amphibious Assault Ships	None
	Force Protection	Tactical Missile Defense (MEADS)	Engagement Radar, Missile Tech
		Improved NBC Defense	Minimal
	Precision Strike	Tactical Cruise Missiles	Possible GPS Code, Low Obser
Phase III	C4ISR	Airborne Ground Sensor (AGS)	Vestigial Radar Issues
		HALE Unmanned Air Vehicle (EuroHawk)	Airframe, Payload, ECM, MCTR
		Airborne ESM Platform	SIGINT/ELINT
		High-Resolution Surveillance Satellite	Special Access Programs
		Broadband Military Communications Satellite	Special Access Programs
	Precision Strike	Joint Strike Fighter	LO/CLO, Sensors, Avionics
		Unmanned Combat Aircraft	LO/CLO, Commo, Sensors
	Force Protection	Theater-Wide Ballistic Missile Defense	Sensor, CLO, Guidance, MCTR
		Robotic Ground Vehicle	Autonomous Operation
	Close Combat	Advanced Combat Vehicles	Propulsion, Vetronics, Armor

It should be recognized that in many of these areas Europe has technology, but simply has not invested to the degree and at the pace of the United States. Thus, while Europe could in theory develop these capabilities on its own, U.S. technology transfer and greater Transatlantic collaboration could potentially provide significant geopolitical, interoperability and security benefits:

- First, by allowing Europe access to the U.S. technology base, the European development time for new systems and costs would be reduced, which in turn would allow the procurement of a larger number of systems, thereby increasing Europe's capabilities.
- Second, employment of U.S. technology in these systems would allow the U.S. to retain some control over technology proliferation through end-user certification (which, even if imperfect, is better than having no control proliferation of over purely European systems).
- Third, transfer of U.S. technology implies participation by U.S. industry, which helps maintain the U.S. defense industrial base, reducing costs for the U.S. military.
- Fourth, collaborative programs can bind the U.S. and its allies closer together, and create a feeling of solidarity and commitment to European defense transformation as an Alliance issue.
- Fifth, it is easier to ensure interoperability (in both directions) when systems are developed collaboratively, due to better understanding of technology and operating principles, as well as the development of common protocols and interface standards.

For the purposes of analysis, this essay assumes that the U.S. government would value some of these benefits sufficiently to engage in greater technology sharing. If not, then the degree of interoperability in the NRF and NATO more generally will remain significantly limited, and European capabilities should not be expected to increase materially for a considerable period of years to come.

1. The Range of Capability-Related Technology Transfer Needs

The technology transfer needs for enhancing NRF capabilities tend to be grouped in certain areas:

Force Protection. Ensuring adequate force protection systems will require extensive technology transfer.

- NBC defense would be improved through exploiting U.S. advances in remote, hyper spectral sensing in order to scan large areas quickly and track weapons of mass destruction back to their source.
- Enhanced air and missile defense would be provided by the access to the far more extensive U.S. investments in missile defense technologies.
- Generation III and IV electro optic capability (night vision equipment, etc.).

ISR Sensors. Access to U.S. sensors would be beneficial in facilitating European acquisition of cutting edge ISR systems similar to JSTARS, Rivet Joint, and Global Hawk. European industry has proven quite capable of developing the requisite technologies on its own (i.e., Synthetic Aperture Radars, infrared sensors, data links, visualization applications, etc.). U.S. refusal to share technology merely delays the development of these systems and raises costs to the point where either systems cannot be procured in sufficient numbers or are cancelled altogether. Failure to develop sensor systems cooperatively with Europe prevents the U.S. from amortizing its development and production costs over larger production runs, and undermines the quest for systems interoperability. From a proliferation standpoint, the U.S. has no control at all over systems without any U.S. technology content.

UAVs/Cruise Missiles. In some UAV and cruise missiles areas, Europe is as advanced as the United States (see, for instance the Matra-BAE Apache/Black Shadow missile), and in some areas, such as propulsion, may be ahead. Collaboration with Europe would permit the insertion of advanced European capabilities in exchange for U.S. technology on guidance, autonomous target recognition, and low observables.

Advanced Combat Vehicles. The U.S. Army is now developing an entirely new family of very lightweight manned and unmanned combat vehicles under the Future Combat System program. These vehicles will feature advanced, lightweight armor, highly lethal weapon systems, and radical hybrid-electric propulsion systems that will reduce fuel consumption and thermal signature. However, the program is running behind schedule and is over budget, placing the most technologically advanced elements, including the ground vehicle segment, at risk. Europe, for its part, has always relied more on light armored vehicles and has more design and development experience than the United States (i.e., both the USMC's LAV-25 and the Army's Stryker Interim Armored Vehicle derive from a Swiss design). This is another example of an area in which greater cooperation would benefit the United States while allowing the Europeans to develop their own capabilities through cost and risk sharing.

2. Technology Transfer Policy Issues

In practice, the following policy issues arise with respect to the types of technology transfers set forth in Table 3.4 above.

a. Short-Term Needs: Mundane and Licensable. As noted above, there are limited needs for technology transfer relating to NRF capability acquisition for NRF Phase I as Europe has many of the technological and industrial capabilities needed. Thee short term technology transfer needs that may exist (primarily where European governments chose to acquire U.S. existing solutions rather than develop or modify their own) are largely mundane and can be readily handled through normal licenses and/or ITAR country exemptions if and when they are eventually ratified. The licensing of trucks, utility helicopters, body armor and related items should not pose difficult problems. The only area of apparent sensitivity is night vision equipment, discussed separately below).

b. Medium and Long-Term NRF Needs: More Sensitive, Complex and Related to Major U.S. Programs. Many of the medium and long term technology transfer needs for NRF II and III set forth on Table 3.4 are not mundane and concern technologies and information the United States has viewed as sensitive and raise complex export control and national disclosure policy questions. There are several important considerations relating to these technology transfer needs.

Many involve significant and transformational U.S. defense programs that today have little foreign participation and which are either subject to limited release or have not been reviewed for releasability. As shown on Table 3.2**,** the vast majority of transformational programs presently are not eligible for foreign release, making meaningful cooperation in them impossible. Among the few exceptions have been:

- The Joint Tactical Radio System (JTRS), in which the U.S. presently has a bi-lateral interoperability program with the British Bowman system.
- Aegis BMD, in which some aspects of the system have been released to Japan and Australia pending their procurement of Aegis BMD capability for homeland defense.
- The SPY-3 radar associated with the AEGIS BMD system (though the depth of technology sharing remains unknown).
- The Global Hawk long-endurance UAV, now being evaluated by the German Luftwaffe, mainly as an ELINT platform.
- The MEADS engagement radar system (but see above for the disputes over black boxing of key technologies.
- The Unmanned Air Combat Vehicle (UCAV), but limited to the United Kingdom.

More significant, however, are those programs on which there is no foreign release allowed or no foreign release policy established:

- Future Combat System (FCS), the U.S. Army's network-centric system of systems for the next generation, including new vehicles, weapon systems, and C4ISR capabilities.
- The E-10A Multi-Mission Command and Control Aircraft (MC2), the USAF's replacement for J-STARS, AWACS and Rivet Joint.

The lack of foreign participation in or U.S. willingness to disclose technology concerning these programs highlights the ongoing disconnects between our overall policies of promoting interoperability and capability and our unwillingness to share these technologies. We exhort European allies to obtain capabilities but are largely unwilling to share the relevant technologies that could facilitate such acquisitions. This is a continuing and sustained discontinuity in U.S. policy that bears on the NRF and more generally the difficulties inherent in U.S.–European technology sharing.

The Medium-Long Term Technology Transfer Issues cannot be addressed through solutions like the ITAR country exemption but require holistic, program specific solutions.

- The ITAR country waivers do not apply to a wide range of sensitive technologies and classified information. These types of data are exempt from the licensing waivers.
- JSF Type Solutions: Solutions will be more along the lines of JSF type program licenses which address, at one time and in advance, a complex range of technology transfer and NDP issues.

c. Specific Technologies Issues. More specifically, each of the various capabilities areas raises discrete, technology based NDP and technology transfer issues.

Night Vision Systems: Prior to 2001, the U.S. had cleared all NATO countries plus Japan, Australia, South Korea, Egypt and Israel for Generation (GEN) III night vision systems; all other requests for GEN III required automatic review.[62] However, beginning in 2001, the U.S. implemented a new figure of merit (FOM) system for determining the release of night vision technology. FOM is an abstract measure of image tube performance, derived from the number of line pairs per millimeter multiplied by the tube's signal-to-noise ratio. Under the FOM system, there are different levels of GEN III performance, with different countries are allowed to buy image intensifier systems up to a particular FOM threshold. To summarize:

- U.S. Forces are now receiving GEN III and GEN III+ systems with an FOM of about 1700-1800.
- NATO, Australia, Japan, South Korea, Israel and Egypt get GEN III with an FOM of 1600—roughly equal to what the U.S. procured circa 1996.
- Other countries can get GEN III tubes with an FOM of up to 1250, roughly equal to U.S. Army GEN II tubes.

Through reliance on the FOM parameter, the United States effectively ensures that its forces will always remain one or even two iterations ahead of even its closest allies in this critical tactical capability area, even while ostensibly loosening constraints on the export

[62] Though no longer used to determine releasability, it is still common to characterize night vision devices by their technology "generation" as either GEN I, II, or III (with GEN IV on the horizon). Generations of imaging tubes can be described as follows:

- GEN I: Vietnam-era technology, with short tube life and considerable distortion, most commonly found on commercial, imported tubes.
- GEN II: Late 1960s development with microchannel plate (MCP) amplifier for higher resolutin and reduced size.
- GEN II+: From the 1970s, with increased image tube bias for increased gain (brightness); a glass faceplate was added to improve resolution.
- GEN III: From the 1980s, with substantially improved gain and bandwidth reaching into the near-IR region, plus improvements to the MCP and gallium arsenide photocathode for increased tube life and performance.
- GEN III+/GEN IV: From the 1990s, includes improved MCP and photocathode for further increases in gain and resolution.

See Michael J. Brower, "Do You See What I See?" *Special Operations Technology Online*. Available at: <www.sotech-hmi.com/print_article.cfm?DocID=314>.

of GEN III technology. However, this approach is subject to debate since indigenous modifications to releasable technology has in the past allowed European, Israeli and Japanese companies to develop capabilities equivalent to non-releasable technology (i.e., to develop GEN II and GEN II+ systems equal or better to early GEN III systems). There is no reason to believe that the FOM approach will inhibit future activities of this nature, which tend to move night vision technology completely out of U.S. control.

Radar and IR Sensor Technologies. As shown in Table 3.4**,** most of the most sensitive technological issues arise with respect to sensor technology. Given the U.S. desire to maintain information dominance on the battlefield, the United States is highly sensitive over the transfer of advanced sensor capabilities in areas like radar, electronic warfare, advanced imaging, SIGINT and ELINT and sensors in missile defense programs on UAV and manned surveillance platforms. These issues span ITAR release and NDP disclosure policy, which are of course interrelated.

Two cases highlight the problems inherent in these areas:

1. U.S. Medium Extended Air Defense System (MEADS). The United States has been consistently resistant to releasing technical data, especially concerning the MEADS engagement radar, with respect to this joint U.S., German, and Italian program.[63] The United States instead has at various times offered to provide these as a black box. Europeans have consistently balked at this approach, viewing it purely as an attempt by the United States to protect the industrial lead of Lockheed Martin, the radar system prime contractor. Elements of the missile guidance system, derived from the U.S. Patriot PAC-3 missile, also have been restricted, creating tension within the international consortium (MEADS International) established to develop the system. Technology transfer issues have repeatedly threatened the survival of MEADS, without which the NATO Response Force will have no effective mobile ballistic missile defense. In the case of MEADS, tensions over the releasability of the engagement radar data package and other elements has, at various times, alienated European governments and industry, and placed the future development of the program in jeopardy. Ultimately, after long and difficult negotiations and periods when disclosure issues caused the program to creep to a near halt, the MEADS partners reached agreement on the technology transfer issues. Italy and the United States have already signed a Memorandum of Understanding for the Design and Development Phase; German approval is expected next year. The only black box item now in the MEADS radar is the U.S. supplied exciter.

2. AGS. In the case of AGS, there also have been a series of complex technology transfer issues. Initially, the USG was reluctant to release many of the technologies related to the system. This reluctance was only overcome through high level U.S. consideration of these issues linked to building support for an international program that

[63] Intended to defend deployed forces, MEADS is a strategically deployable, tactically mobile system that can be loaded onto a C-130, can transition between march and firing mode in under 15 minutes, and can provide 360° area defense against air-breathing threats and point defense against short-range ballistic missiles. In its initial operating capability, MEADS will employ the same missile as the much less mobile Patriot PAC-3 system, though later MEADS production blocks may use an enhanced missile.

has been virtually a decade in the making. As NATO members considered making real commitments to a funded AGS program in the 2001-2004 period, the U.S. came under enormous pressure from NATO officials and others to be more flexible on technology transfer issues; U.S. technology sharing was viewed as critical to the program's future as it would enable the European industrial participation that was helping to build support for the program among reluctant European governments. Eventually, through focused U.S. senior leadership attention, the categories of data for which U.S. release were authorized expanded sufficiently to allow the program to move forward. This included an agreement in principle to cooperative development of the ground tracking radar—essentially an effort to bring together the European SOSTAR and U.S. NP-RTIP program development efforts. Indeed, in the roll up to the Prague Capabilities Commitments, the United States developed a matrix that appeared to show an overall reasonable approach, with release of technology in many non-controversial areas. Yet, critics point out that this approach was somewhat misleading in that it showed releasability in many mundane areas but nonetheless showed continued U.S. resistance to release of key radar technology central to the program, including the release of the information package on MP-RTIP.

Subsequently, an issue arose with respect to the export of monolithic power amplifiers (MPAs)—a key subsystem of transmit-receive modules used in advanced radar applications such as AGS. In this regard, in 2002, TriQuint, a small U.S. firm that produced the modules, had sought and obtained State Department export licenses to ship nearly 1,400 of the modules to the European Aerospace and Defense Systems Corporation (EADS) for use in space satellite applications (i.e., the TerraSar remote sensing radar satellite system for commercial and scientific applications). Inadvertently, the Triquent license request did not mention that the plan was for EADS to utilize most of the modules on the SOSTAR radar system under development. EADS realized the error when the MPAs arrived in Germany, halted all work on SOSTAR, and in July 2003 TriQuint sought USG approval to utilize many of the MPAs for the AGS development effort. In fact, what seemed a simple and relatively mundane request, one consistent with the overall U.S. policy mandate for joint radar development on AGS, rapidly turned into a controversial and significant dispute involving the LO/CLO Executive Committee described above. Ultimately, this licensing request was denied.

In fact, the original export license for the modules had not been reviewed by the LO/CLO committee (apparently because the space application did not suggest that stealth and counter-stealth was involved). When the committee learned of this, its staff was very concerned and insisted on reviewing the request. Thereafter, the LO/CLO community raised serious concerns, apparently on the grounds that the T/R module would provide capability for very sensitive radar that potentially had counter-stealth qualities. In particular, the Office of International Technology Security in DOD/AT&L, with its focus on protecting the U.S. dominance in radar technology, apparently even vis-à-vis our close allies, became an ardent opponent of the licensing request. Other DOD components, including DTSA, and the State Department, took a more positive view of this request (consistent with overall DOD policy guidance on AGS) and a considerable dispute ensued. Indeed, at one point, AT&L sent a team to Europe to assess the level of radar technology and concluded that Europe has significant capabilities and that there was little point to withhold the MPA. Nevertheless, after consideration at senior levels, the licensing request was denied.

In the deliberative process leading up to this decision, a number of options were considered by NATO and the United States, including: 1) revoking the USG license altogether, thereby denying the use of the MPAs in both space applications and AGS, and requiring the return of the modules (already in Germany)—an approach favored by DOD AT&L; 2) allowing use of the MPAs for AGS; and 3) allowing use of the U.S. MPAs only for the TerraSAR satellites, but not for AGS. In this third option, AGS would be developed with European MPAs designed by European industry, with the option of providing U.S. MPAs later if the European development efforts are not completed on schedule. DOD AT&L also wanted U.S. inspectors to have significant access to European facilities utilizing the MPAs. When U.S. resistance to use of the MPAs for AGS became clear, the European industry determined that it could actually develop its own variant of the MPA based on work already underway by EADS, Thales and BAE Systems. However, this required additional non-recurring costs (raising the question of who would pay) as well as program risk (would the development work be complete on schedule and provide sufficient technical performance). At NATO, there was considerable concern that if the development of the T/R module held up the fielding of AGS, the NATO military committee would be reluctant to deploy forces—to put them in harm's way.

Ultimately, after considerable inter-agency and intra-DOD debate, the USG decision was made to allow use of the MPAs in the European TerraSAR satellites but not in AGS.

This decision has a number of noteworthy implications. First, it highlights some difficult issues, both process and policy, with respect to the LO/CLO review process. From a process standpoint, the LO/CLO review was outside the normal export licensing review process—a process unto itself, non-transparent in nature, and without clear procedures for appeals of such judgments. Moreover, from a substantive standpoint, the LO/CLO community apparently has a strong policy preference in favor of maintaining U.S. technological dominance in radar, taking the view that such capabilities should not be exported even where close allies are involved, the project is a high profile one that has tangible U.S. policy benefits (European capability acquisition, coalition warfighting and strengthening of NATO), and a denial could encourage the development of foreign capabilities that could, over time, pose more of a proliferation threat than licensed U.S. capabilities. The ultimate decision to favor U.S. technology dominance or protection rather than coalition warfare again reflects the familiar problem that our overall security policies (here, in favor of AGS and collaborative development of radar on the program) continue to be disconnected from our technology transfer policies. The prevailing LO/CLO view also reflects the somewhat questionable notion that European industry could reverse engineer the MPA and an unwillingness to accept any risk in this area or trust close allies. Even if European firms had the ability to engage in this conduct, this basis for decision-making would essentially require denial in most export cases vis-à-vis close allies.

The case also has difficult implications for Trans-Atlantic cooperation. The European experience on this issue—the time required, the attitudes in the U.S. bureaucracy, and the need for repeated high level U.S. policy-makers intervention to resolve it– only serves to weaken European resolve for Transatlantic cooperation and reinforce a preference for developing autonomous European capabilities and avoiding reliance on U.S. technology. Indeed, this is precisely the result of the USG exporting licensing denial decision on MPAs. Ultimately, the decision was made in Europe to build the TerraSAR satellite using indigenously developed MPAs and T/R modules rather than rely on U.S. products or technology. Further, on the military side, Germany has recently conducted sea trials for a new class of air defense and command frigates (the F-124 SACHSEN) that have advanced multi-function, active phased radar and multi-beam, long range radar (the APAR and SMART-L 3d) made of components "wholly developed and produced in Europe by European companies."[64] A recent article on the program notes that these radar systems "are based on precisely the same components elements that U.S. technology transfer regimes have prohibited from sharing with U.S. allies in and through cooperative programs such as [MEADS] and whose transfer caused numerous problems associated with the European TerraSAR-X radar satellite."[65]

The increased European reliance on indigenous capabilities that has apparently resulted from the U.S. denial decision on the MPAs highlights the dilemma in maintaining tight U.S. control in such circumstances. If, as appears to be the case, Europe could and did in fact replicate the U.S. capability (or a closely analogous approach), this capability would be, and in fact is, outside the scope of U.S. export controls. Hence, this uncontrolled European technology actually poses a greater and more sustained proliferation threat than if Europe simply acquired U.S. MPAs that were export controlled, dedicated to AGS and could not be used for any other purpose or re-exported or backward-engineered without prior authorization.

In sum, these cases illustrate that any European participation in U.S. programs involving advanced sensors relating to NRF undoubtedly will face the same types of difficulties, including generalized resistance to release and particular concerns arising in the LO/CLO context. Plainly, these situations need to be addressed as part of program-specific holistic solutions where the degree of sharing is established up front and reaffirmed, and overall U.S. policy on NRF-related development programs are consistent with our technology transfer policies on such programs.

MCTR Issues. A final set of issues relate to the application of the MCTR regime to missile defense capabilities, cruise missiles and unmanned aerial vehicles for various purposes. Under MCTR, which is designed especially to stem the proliferation of missiles and weapons of mass destruction they might carry, the export of Category I articles and any design and production technology directly associated with such articles is subject to a strong presumption of denial. Articles covered in Category I include:

[64] *Defence Systems Daily* (August 27, 2004).
[65] Id.

> complete rocket systems (including ballistic missile systems, space launch vehicles and sounding rockets) and unmanned air vehicle systems (including cruise missile systems, target drones and reconnaissance drones) capable of delivering at least a 500 kg payload to a range of at least 300 km as well as the specially designed "production facilities" for these systems.

Further, under MCTR, the transfers of such articles are only allowed to be authorized

> on rare occasions and where the Government (A) obtains binding government-to-government undertakings embodying the assurances from the recipient government … and (B) assumes responsibility for taking all steps necessary to ensure that the item is put only to its stated end-use.

Needless to say, this and other MCTR disciplines make the transfer of technology related to cruise missiles, UAVs, and missile defense systems very difficult and complex—and often subject to the Category I presumption of denial– even for close allies. This would make it very hard to provide technical information on cruise missiles or UAVs, which often have longer ranges, to European governments. The problem is equally troublesome for missile defense. As noted above, there needs to be some type of theatre missile defense system for the NRF and NATO forces more generally; follow-ons to current NATO missile studies undoubtedly will run up against this issue.

Specifically, the MCTR makes no distinction between offensive and defensive missiles (focusing only on the kinematic range), which creates problems for technology transfer related to the development of a European theater-area missile defense system. The velocity that allows a theater ballistic missile interceptor like the U.S. THAADS to protect a wide area from medium and intermediate-range ballistic missiles also potentially gives it a range of several hundreds of kilometers in a surface-to-surface role. Hence, such systems fall squarely into MTCR category I and subject to the strong presumption of denial, thereby making it very difficult for the United States to supply enabling technologies or components.

Recognizing the complexity of these issues, the Bush Administration announced in December 2002 that it would conduct a six-month study of impediments to international cooperation on missile defense and specific issues associated with squaring missile defense cooperation with the MCTR. To date, however, over two years later, there has been no action on this issue. Moreover, while the Administration has approved certain technical assistance agreements for industrial cooperation on missile defense on a case-by-case basis, these have come with killer provisos that effectively block in-depth cooperation.

In short, facilitating cooperation on missile defense, UAVs and cruise missiles, for NRF or to improve coalition warfare generally, will pose considerable challenges.[66] In all

[66] Issues also exist concerning UAVs under the Conventional Forces in Europe (CFE) Treaty, which similarly does not distinguish between manned aircraft and UAVS. When UAVs were generally smaller than manned aircraft, this was not particularly relevant. But with the advent of long-endurance UAVs, such as Global Hawk and Predator, the case is being made in arms control circles on both sides of the Atlantic

probability, the United States and other regime participants need to revise the MTCR guidelines or re-interpret them in order to create more flexibility; this can be done by: distinguishing offensive and defensive missiles; creating an exception for force protection or surveillance in connection with coalition warfighting; or utilizing existing exceptions (i.e., there is a presumption of denial not an absolute prohibition). In any of these scenarios, it also would be important to create additional safeguards against proliferation or conversion to offensive use. Notwithstanding such safeguards, however, the overall risk is that such exceptions undermine the effectiveness of MTCR as an instrument of proliferation control and open the door to national exclusions the United States does not agree with. Ultimately, this is a policy issue that must be resolved at the highest levels of government.

In sum, it is evident that the application of the current U.S. technology transfer and information sharing processes and standards would result in a dumbed down NRF with modest connectivity to current and future U.S. enablers and little real opportunity for leveraging U.S. technology for capability acquisition. Leaving the matter to normal bureaucratic modalities would be counterproductive to the NRF's key goals. Thus, as discussed below, some top down approaches, with significant leadership attention, one-stop" shopping modalities, and other more flexible approaches, are needed to facilitate NRF interoperability and capability acquisition.

that such UAVs should be treated as aircraft under the terms of the treaty. Thus, to remain within the treaty ceiling for aircraft, the deployment of one UAV would in theory have to be matched by the withdrawal of one combat aircraft. The weaponization of UAVs like Predator, and the development of specialized Unmanned Combat Aircraft (UCAVs) are likely to strengthen this argument.

IV. Conclusions and Recommendations

As discussed at the outset, the NRF really is a microcosm of the broad range of complex issues facing the United States and our alliance partners in shaping a mutual security policy and developing and enhancing 21st century coalition warfighting capabilities. While this essay primarily has focused on the technology transfer and information sharing issues relating to standing up the NRF, the analysis herein has led to a series of broader observations on coalition warfighting and specific recommendations concerning the development of the NRF set forth below.

A. General Observations

1. The Need for a Robust Interoperability Agenda. The overwhelming focus by the United States and NATO on European capability acquisition, reflected in the DCI and the PCC, has effectively resulted in far less attention being paid to improving interoperability between U.S. and allied forces likely to operate at different levels of capability for years to come. While Europe may acquire some or all of the PCC capabilities, the reality is that numerous of these acquisitions and the fielding of these capabilities will occur years hence, if at all. Thus, in the near-term and mid-term, the United States and its partners should shift focus and undertake robust and focused efforts on enhancing interoperability of coalition forces likely to operate at very different levels of capability for the next decade and beyond.

In this new era, the focus on interoperability be must be achieved through network-centric capabilities: establishing a common architecture into which nations can plug-and-play and thereby achieve similar levels of situational awareness and other higher order forms of interoperability set forth in Figure 2.1 above. The reality is that, in contrast to the large costs associated with acquiring advanced capabilities, facilitating interoperability may be more cost effective; relatively small investments have potentially high coalition warfighting payoffs. Indeed, such solutions as bridging software to link disparate command, control, communications and intelligence (C3I) systems and manage legacy systems while new C3I systems are developed and the adoption, as appropriate, of commercial standards for information technology would be relatively low key and low cost.

2. 21st Century Warfighting Coalitions Require Significant Advanced Planning to Address Interoperability Issues. While we can perhaps form “coalitions of the willing” for political purposes on an ad hoc basis, the reality of 21st century warfare is that we cannot do likewise in true military coalitions. If the analysis above shows anything, it is that 21st century coalition warfare is not like a pick up game of basketball at the gym, where we choose sides on a given day and fight together, working out the roles and relationships as the game progresses. Particularly with the emergence of network-centric warfare, it will take years of planning, information sharing, developing interoperability bridges and shaping plug-and-play architecture to develop true coalition war fare capabilities. Experience in the commercial business environment has consistently shown that disparate networks cannot be integrated smoothly without extensive prior planning and agreement on the sharing of network and database architectural and structural information. Network-centric warfare, which is in essence an attempt to superimpose distributed commercial business processes on war, will take place in a much more demanding environment.

Yet, today, there is a marked disconnect between U.S. and European rhetorical support for interoperability and our lack of actions, in NATO or otherwise, to support it. Indeed, the cumulative thrust of current U.S. policies and programs, including the lack of foreign participation in U.S. C4ISR development programs and the U.S. refusal to share a range of key enabling information with even our close allies, undermines, rather than facilitates, interoperability.[67] Thus, on these current trajectories, we truly are headed toward a dumbed down NRF with second best coalition warfighting capabilities where U.S. allies will have markedly less capable situational awareness and face greater risks in fielding forces. A key question is whether any country would be willing to put its forces at risk in these circumstances in 21st century high-intensity encounters.

Moreover, with U.S. C4ISR capabilities advancing rapidly through accelerated investment in transformational technologies, the interoperability gap between fielded U.S. systems and European systems is likely to increase, not improve, in the years to come. As U.S. forces become more joint and move to our future architecture for C4ISR and we continue to limit release of or access to these new modalities, ad hoc attempts at integration of the NRF will be much more difficult and the degree of "dumbness" is likely to increase. The United States cannot, however, shoulder all the responsibility for this situation. European under investment in defense, slow recognition of the revolution in military affairs, and lack of focus on interoperability in their own programs and priorities also are partly responsible for current circumstances.

Thus, both the United States and Europe must decide whether and to what extent we really want to develop truly interoperable coalition warfighting. If we do want true coalition warfighting capabilities, we need to give higher priority and more focus to the interoperability issues highlighted herein.

3. The Critical Technology Transfer Needs for NRF Relate to Interoperability and Long Term Capability Acquisition. The reality is that, for the most part, the early phases of the NRF (I and II) can be stood up without significant U.S. technology transfer (and minimal technology transfer issues) regarding capability acquisition. The capability needs can be met by existing European capabilities and from European industry without

[67] While there is in fact an Office of Interoperability within OSD, its principal mandate is to facilitate interoperability between and within the U.S. military services in order to implement the U.S. vision of network-centric warfare. Interoperability with allied forces in a coalition environment is a decidedly secondary consideration to which limited attention has been given to date. The general philosophy of the Office of Interoperability appears to be a reliance on commercially driven standards to force convergence among the various C4ISR systems under development in the U.S. and abroad, with the assumption that any U.S. network architecture that includes the majority of commercial standard interfaces will facilitate "automatic" interoperability—though of course, the experience of the commercial market demonstrates that such standards-based interoperability can be illusory.

significant U.S. technology transfer. The key needs for technology, and where the significant issues arise, are twofold:

- Information sharing (and release under U.S. NDP and the ITAR licensing process for unclassified items) is critical to ensure NRF interoperability in NRF phases II (using current U.S. enablers) and III (linking the NRF to U.S. network-centric capabilities under development).
- The long-term goal of European capability acquisition for NRF phase III (which would enable the NRF to utilize European enablers) would substantially benefit from U.S. technology transfer.

B. NRF Recommendations

1. **Develop A Long-Term Force NRF Force Planning Roadmap to Explicitly Link Force Development to Transformation, Capability Acquisition and Interoperability.** As a key goal of the NRF is to move toward a transformational force with European enablers and incentivize European capability acquisition, it is not enough that the NRF simply integrates new capability as it comes on line or iteratively change its certification requirements to reflect such new capabilities. Rather, NATO should develop an NRF force planning roadmap that makes this linkage between the NRF and transformation/capability acquisition explicit:

a. <u>Mission-Oriented Planning</u>. The roadmap should evaluate potential NRF missions and seek to ensure that the NRF evolves into a transformational objective force with cutting edge capabilities and inter-operability; it should be updated from time to time to reflect changing missions, operational lessons learned and the evolution of technology and capabilities.

b. <u>NATO plug-and-play Architecture for C4ISR</u>. The roadmap should include the development of a C3ISR architecture for NRF that builds on existing NATO building blocks like MIDS and CAESAR and develops a NATO infrastructure that can be complemented with plug-and-play national sensors and other assets, including a NATO-owned and operated AGS. The roadmap should consider but not be limited to the Prague capability commitments. A plug-and-play NATO architecture will facilitate interoperability and allow more controlled information sharing. The United States undoubtedly would be more comfortable sharing data outputs from its current and future enablers through a NATO architecture in which NATO participants in NRF can plug and play as they participate in rotations; this would allow some greater degree of protection of sensitive U.S. data and can also establish NATO as a fulcrum for true coalition force interoperability (not only the keeper of standards).

c. <u>NATO Acquisition of Certain Equipment</u>. NATO should consider the merits of acquiring the modest types of equipment or capabilities recommended for NRF Phase I above, including tactical radios, battle command information systems, data link terminals, and combat ID systems. This would facilitate cost sharing and the availability of this equipment for all NRF rotations. In some cases (e.g., advanced night vision equipment), NATO acquisition and retention, with "loan outs” as needed to national forces, may ease technology transfer issues associated with the export of this equipment.

2. **U.S. Steps to Facilitate NRF and Allied Interoperability.** If the United States decides it is serious about coalition warfare and following through on its rhetorical commitment to interoperability, we must consider taking a series of concrete steps regarding the NRF and beyond:

a. <u>Provide Robust Enablers to the NRF; Stand Up DOD-Wide NRF Interoperability Planning Effort</u>. The United States must decide on what enablers it will provide the NRF. Should the United States deny European partners access to our best enablers and not share the outputs of this advanced technology in real time? To do so would commit coalition partners to fighting with a second best capability—the antithesis of what the NRF is supposed to be. Thus, we should seriously consider making advanced U.S. assets and their outputs available during NRF Phase II. In all events, to address this issue, the United States should stand up a DOD-wide effort, possibly centered in the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics[68], the Joint Chiefs of Staff or U.S. Joint Forces Command, focused on what enablers can be made available and how to make such U.S. enablers, both those existing and on the drawing board, interoperable so as to ensure NRF force best available situational awareness etc. This effort would include a focus on operational interoperability today and future issues associated with new U.S. architectures and other C4ISR programs coming on line. These efforts coming on languages cover effort would form the baseline for the establishment of a holistic, overall NDP approach for NRF (see below) on what access to networks to provide, what sensor output to provide, and so on.

b. <u>European Participation in Advanced Warfighting Experiments</u>. The United States should establish advanced experiments with NRF rotations in the six months prior to their certification, focusing on identifying interoperability problems and needs. For example, these experiments should seek to utilize such U.S. assets as JSTARS and Global Hawk with European ground capabilities. Broader European participation in other existing U.S. warfighting experiments conducted by JTC also should be considered.

c. <u>Cooperative Programs Focused on Interoperability</u>. The United States should consider joint programs or foreign participation in key U.S. enabling programs on network-centric warfare in order to facilitate interoperability; all existing U.S. programs with respect to secure communications, CROP, etc. should be considered from this standpoint as well as any new ones that are stood up. This would require a sea change in mindset that places a higher priority on coalition warfighting in program development. Such program areas as blue force tracking, where no optimal solutions currently exist, and CROP are possible candidates for

[68] The Office of International Programs within USD (AT&L) technically has the mandate to oversee the Coalition Warfare Initiative, which is intended to promote joint development of systems to facilitate coalition warfare capabilities. However, the initiative lacks focus and has only been funded to the order of $6–7 million annually.

these types of efforts. Also the U.S. should expand its ACTD program to include more emphasis on interoperability solutions.

C. Steps to Improved Technology Transfer and Information Sharing

Finally, recognizing the centrality of U.S. export control reform to facilitating the development of the NRF as a transformational vanguard expeditionary force, the United States should consider a number of critical export control steps. As discussed above, the issues here run deep and there are no quick "silver bullet" solutions. But a number of steps can be taken to effectuate change with coalition warfighting in mind:

1. **One-Stop U.S. Disclosure Decision-Making for NRF Interoperability Needs**. Once DOD develops a full out interoperability plan (as recommended above), DOD should stand up an inter-agency group that would be tasked with establishing a single, wholesale disclosure policy for the NRF that allows accessibility to networks and release of technical data needed for the NRF to meet its interoperability goals. This would replace piecemeal decisions on data for each rotation and each country, and allow joint training. These decisions can be for NRF purposes only so that individual participating nations cannot utilize such access on a broader basis. As noted above, the development of a NATO architecture for NRF and NATO more broadly, into which nations can plug and play and gain needed access, would make U.S. decisions easier and facilitate limiting recipient nations from access outside of the NRF context. The U.S. can also build into appropriate software bridges and access rights inherent technical limitations that allow it to deny access in exigencies or limit access for non-NRF purposes. In standing up a NDP inter-agency group to focus on the NRF, the group should be given the following senior policy guidance:

    a. Coalition warfare and inter-operability are strong U.S. priorities, and the presumption should be in favor of disclosure to promote these goals even if release exceeds current standards or if no standards exist.
    b. Disclosure decisions for current and future U.S. release pertaining to current and future U.S. enablers of network-centric warfare would be made up front for NRF purposes and would not await the development of an exigency or need to commit the NRF to conflict.
    c. Disclosure would be made to nations within the NATO framework and for NRF purposes only. The United States would negotiate a multi-lateral agreement with NATO and its members to facilitate NDP release for NRF purposes which would embody appropriate safeguards and commitments to protect the security of released data.
    d. The distinctions, if any, between release policies for different NRF countries would be the minimal required, every effort should be used to release to all NRF participants subject to appropriate safeguards (on re-export or security), and specific justifications would be required to justify why release would not be permitted subject to safeguards; the approach should not result in least-common-denominator disclosure solutions.

e. NRF release decisions would be exempt from review through the LO/CLO and Anti-Tamper processes except that the findings of such bodies, as needed, would be taken into account in shaping appropriate safeguards.
f. Any decisions not to release would be subject to full review by the NDP Committee.

2. **Afford Higher Priority to Coalition Warfare Benefits in Technology Transfer Decision-Making.** While coalition warfighting benefits is a legally permissible factor today in arms export and technology transfer decision making under the Arms Export Control Act relating to unclassified technology, it is in practice afforded a lower priority than maintaining national capability leadership. Hence, where the release of technology or export of capability would have tangible coalition benefits for NRF, the presumption should be in favor of release unless the recipient's third country policies on re-export can be shown to provide undue risk of disclosure to third parties.

3. **Allow Release of Key Technologies and Information.** DOD should seriously consider the release of technology and the sharing of technical information (network access, software bridges, etc.) with respect to the following set of set of equipment and programs for NRF purposes (provided that recipients have sufficiently developed export control systems, and controls on third party transfers, to warrant such release):

   a. Capabilities Related
      i. Night vision up to current U.S. figure of merit
      ii. Programs for foreign participation
         1. MC2A
         2. MMA/BAMS
         3. Missile Defense
         4. Small Diameter Bomb
         5. FCS Manned and Unmanned Ground Vehicles
   b. Interoperability Related: Early emphasis has to be put upon combat identification, expanding into enhanced situational awareness systems such as SIAP, SGIP and CROP. That in turn will necessitate a higher degree of interoperability in tactical communications, combat information systems, network architectures, and battle command systems. In short, real interoperability requires the United States to accept an unprecedented degree of release of command and control technology and information sharing.

4. **One-Stop Technology Transfer Review; Exempt NRF Needs From LO/CLO and Anti-Tamper Review.** In the long term, the United States should develop a more systemic solution that eliminates the current problem of multiple, fragmented technology transfer reviews by different entities/agencies. As important as LO/CLO technologies are, it makes little sense today to have separate, stand alone technology transfer regimes for this and other sensitive areas. The same is true for anti-tamper review, which started as a vehicle to facilitate release and has morphed into a reason

to deny release. Thus, one-stop shopping should be established for all technology transfer (including disclosure, LO/CLO and the like) under the administration of DTSA and pursuant to the legal standards set forth in the AECA. Such processes as LO/CLO, national disclosure and anti-tamper should come under single leadership and one set of parameters (with inputs, of course, from relevant Pentagon communities). This ensures uniformity of policy and balanced, reasonable decision-making by the Pentagon bureaucracy established for this purpose.

In the short-term, however, it would be an appropriate solution to exempt NRF specific needs from these separate review mechanisms on the ground that coalition warfighting benefits should be afforded higher priority than these other considerations.

5**. Early Technology Transfer Plans for Armaments Programs that Contribute to NRF.** Recognizing the problems of past cooperative programs and the divorce between technology transfer and armaments cooperation policy, the Administration should require that an up-front technology transfer plan be approved before the start of any major cooperative armaments development program relating to NRF or NATO interoperability more generally and should require the approval of a more detailed plan (once requirements are more defined) early in its program life. All major DOD components with equities should be required to sign up to such a plan and be bound by it (even across Administrations). For any new programs linked to or with tangible benefits for NRF, the Bush Administration should commit to a time line for expedited development of such plans.

6. **Industry Should Come Forward With Proposals for Cooperation on NRF Using the Broad Licenses Established Under DTSI.** Where the program is consistent with NRF objectives, the U.S. Government should encourage such proposals and act to facilitate them. To facilitate this approach, DTC should offer a modified template for the GPA and similar licenses based on the JSF experience which:

- Addresses outstanding liability issues,
- Limits the compliance burdens of firms participating in return for an agreement to an *audit* rather than a *directive* approach to compliance, and
- Promises to avoid the multiple license exclusions and exceptions that limit the effectiveness of the JSF license.

In sum, the heart of the issue concerning the NRF and technology transfer is whether and to what extent the United States is committed to coalition warfighting (whether in the NRF or otherwise) as a real means of ensuring U.S. security in the 21st century. If coalition warfighting with close allies is a core element of our national security strategy, we should seriously consider the steps set forth herein.

Appendix
Critical Enabling Technologies and Key U.S. Programs

This appendix provides a detailed analysis of the specific types of technology or technical information sharing relevant to the NRF's development in each specific capability and interoperability area, organized by NRF implementation phase.

I. Phase I: Secure Tactical Communications and Blue Force Tracking

A. Secure Tactical Communications

The standard U.S. tactical radio, by which all others are presently measured, is the Single-Channel Ground-and-Airborne Radio System (SINCGARS), a spread-spectrum, frequency-hopping voice and data VHF radio which has replaced a wide range of older radios for short-range air-ground and ground-ground communications.[69] In contrast to older radios, which operated on fixed frequency, SINCGARS transmits over a broad frequency band, breaking up messages into small packets that are transmitted over different frequencies and reassembled at the receiving end. This reduces the ability of the enemy to locate the transmitter by triangulation and makes interception of messages almost impossible under tactical conditions.

While some other countries have either purchased SINCGARS for their own forces, or developed and deployed SINCGARS-compatible radios, many, even with Western Europe, continue to use fixed-frequency single-channel radios, making interoperability with U.S. forces a difficult and time-consuming process. As the Army's FM 100-32 states:

> (1) Planning for the SOI must include factors such as types of radios available in subordinate or allied units, cryptographic equipment, key lists, and frequency allocations available from the host nation(s) for the particular area of operation.
>
> (2) Equipment compatibility is a major issue in network planning for HF and VHF systems. The planning must cover FH and single-channel modes of operation. All U.S. forces use SINCGARS compatible radios, but allied nations

[69] SINCGARS is the primary means for short-range (less than 35 kilometers (22 miles)) secure voice C2 below division level. It is also the secondary means for combat support (CS) and combat service support (CSS) units throughout the corps. SINCGARS, like the current VHF-FM radios, is user-owned and –operated. SINCGARS can provide access to the area common-user (ACU) network through the Net Radio Interface (NRI) System, or its range can be increased by retransmission. Data and facsimile transmission capabilities are available to tactical commanders through simple connections with various data terminal equipment (DTE). Until the ADDS fielding is complete, SINCGARS will, on a limited basis, fulfill the data transmission requirements. However, avoid this when possible because voice has priority on the system. *FM 11-32*, *Combat Net Radio Operations*, U.S. Army Training and Doctrine Command, 15 October 1990.

> may not have compatible FH radios. Therefore, plans should address interface between single-channel and FH radios or lateral placement of compatible radios in allied command posts (CPs). SINCGARS requires special key list variables to operate in the FH mode. These variables are developed and distributed from the highest level possible (usually the J6), but they may be developed at a lower level for special operations within the theater.[70]

In practice, this has meant the distribution of SINCGARS transceivers to critical allied C3 nodes and the erection of bridges between the SINCGARS net and equivalent Allied fixed-frequency systems.[71] In the worst case, messages have had to be manually retransmitted, with inherent time delays and errors. Moreover, many Allied fixed-frequency systems are capable of either voice or data transmission, but not both, leading to additional duplication of equipment and networks.

Existing U.S. command and control systems are designed to accept input from SINCGARS or compatible systems; thus, interfacing directly with U.S. battle command networks requires SINCGARS compatibility. At present, few U.S. allies have this capability, which limits their interoperability with U.S. forces. This has become a major consideration in coalition operations in Iraq and Afghanistan, where coalition partners have had to resort to ad hoc measures to achieve even minimum interoperability. The British Army, for instance, has been ordering Harris PRC-117 Falcon tactical radios for its forces, bypassing its normal procurement system.[72] Harris has delivered Falcon II radios to Macedonia, Norway and several other European countries as a means of providing SINCGARS interoperability. On the other hand, Thales Group has successfully marketed its non-SINCGARS-compatible RITA 2000 spread-spectrum radio to the French and other European armies, creating a competing installed base[73]. Patches could be devised if necessary, but it would be a costly, time-consuming and suboptimal solution.

However, whatever progress has been made to provide interoperable tactical communications will soon be rendered moot when the U.S. begins deployment of the Joint Tactical Radio System (JTRS), a new multi-mode, multifrequency voice/data network radio that will replace SINCGARS and several other radio systems in U.S. forces.[74] The first software-defined radio (SDR), in which waveforms and frequencies are generated not by fixed firmware but by programmable software, JTRS is capable of

[70] FM 11-32, op. cit., Chapter 2, Sec. 2-1.

[71] And, conversely, that the U.S. has had to acquire foreign tactical radios to ensure interoperability with other forces. Thus, the USMC acquired 5000 Bowman tactical radio sets to ensure interoperability with British army forces operating in southern Iraq. See *Operations in Iraq: Lessons for the Future,* UK Ministry of Defense, December 2003.

[72] "Harris Corporation Rapidly Deploys Falcon II Digital Radios to UK Ministry of Defense", Harris Corporation Press Release, 22 October 2002.

[73] "Thales Communications at IDEX 2003", Thales Group, Paris, 2003.

[74] As an interim solution to the need for increased digital bandwith at the tactical level, the U.S. military is fielding the ITT Mercury Near-Term Digital Radio (NTDR) to support the development of the "tactical internet", thus creating a more complex interoperability problem within its own joint operating environment.

transmitting not just in VHF, but also UHF, HF and SHF. It can thus be used for short-range line-of-sight, for long-range non-line-of-sight, and for satellite communications simply by selecting different programs. Data security is enhanced through built-in cryptographic capabilities. New waveforms and data compression software also allow JTRS to exceed SINCGAR's 16 kilobit per second (kpbs) limit for data communications, a critical capability given the increasing demand for broadband data transmission in battle command applications. JTRS will be able to emulate SINCGARS waveforms, but in so doing it is bound by the limits of the SINCGARS system.[75]

Recognizing the need for greater throughput and networking flexibility, other countries are developing a new generation of tactical network radios, of which the most prominent is the British Bowman system. However, Bowman is not a software-defined radio, which means it lacks the inherent flexibility of JTRS, and efforts at developing an interoperability patch have focused on having JTRS emulate Bowman waveforms and data formats.[76]

Other European countries are working to develop their own software defined radio systems, but are beginning far behind the U.S. development curve, despite the fact that many of their programs date back to an abortive Future Multiband, Multiwaveform Modular Tactical Radio initiative in which France, Germany, the United Kingdom, and the United States would attempt to leverage the USAF's experimental Speakeasy SDR[77] into a common tactical radio for all four countries. After a promising start, the initiative broke down and each country began pursuing its own national programs.

Despite that failure, several countries now have SDR programs in place, including:

- Finland, where an SDR demonstrator is being developed for the Finnish MoD based on Spectrum Signal Processing's SDR-3000 system (also being examined by Sweden, Korea and Japan).
- Sweden, where the MoD has issued an RFP for a SDR Tactical Data Radio (TDR).
- France, where the Multi-Band, Multi-Mode Radio Demonstrator has proven the feasibility of software defined radio, and a *Poste Radio Programmable* (PR2) is

[75] To use a common computer analogy, a USB-2 connection is "backward compatible" with a USB-1 link, but when a USB-2 device is connected to a USB-1 link, data moves at the much lower USB-1 rate.

[76] The BOWMAN project is designed to provide a new tactical, secure voice and data communications system with greater functionality and wider interoperability capabilities for the British Army, Navy and Royal Air Force from 2005 through 2026. Its target in-service date, when a brigade headquarters and two mechanized battalions will be equipped, is March 2004. Earlier, the Personal Role Radio, a short-range non-secure section radio, was separated from BOWMAN and formally accepted into service in January 2002. Under BOWMAN, about 48,000 radios and 26,000 computer terminals will be supplied, in addition to approximately 45,000 Personal Role Radios. A U.S./UK team is pursuing an interoperability demonstration between JTRS and BOWMAN. See: "Will Software Radio Become Real—and When?" *COTS Journal*, January 2004.

[77] The linear predecessor of JTRS. See "Future Multiband, Multiwaveform Modular Tactical Radio (FM3TR)." Available online at: <http://mccoy/ucsf.edu/emondi/Public/FM3TR/FM3TR_Summary.html>.

being developed to replace legacy systems (Germany will probably become a co-developer of the latter).[78]

It should be noted that in the case of all three European programs that commercially developed dual-use technologies have been integrated into the respective systems, in some cases leapfrogging the U.S. technical advantage. However, merely the development of an SDR radio will not ensure interoperability with U.S. forces since each SDR would still use unique, proprietary waveforms and encryption methods. While the software basis of the new radios would make interoperability updates easier from a hardware perspective (there would be no need to replace internal processors, crystals or modulators), developing a common software set would take considerable time and a degree of cooperation not yet demonstrated by the United States.[79] Until standards and protocols are adopted for waveforms, frequency hopping, data formatting and encryption, even the deployment of SDRs by U.S. allies will not ensure real interoperability.

B. Fratricide Avoidance (Blue Force Tracking)

Throughout history, fratricide, or friendly fire, has typically accounted for 10 percent or more of all battle casualties.[80] With the decrease in overall casualties from enemy fire, the percentage of friendly fire casualties is certain to increase. In Operation *Desert Storm*, it accounted for some 24 percent of total coalition casualties. The number of friendly fire casualties has risen considerably as the power of modern weapons has increased.[81] In the past, friendly fire casualties were mainly the result of the inaccuracy of weapons such as bombs and artillery. Today, they are the result of their dramatically improved accuracy: what can be seen can be hit and destroyed; ergo, the absolute importance of knowing with great precision and confidence the location of all friendly forces. In multinational operations, fratricide avoidance has deeper geopolitical overtones: friendly fire inflicted on one's own troops can be politically embarrassing on a domestic level, but friendly fire affecting allied troops can undermine the foundations of a coalition and place strategic war objectives in jeopardy (e.g., the deaths of four Canadian troops from a U.S. bomb in Afghanistan).

Network-centric warfare inherently demands a high level of confidence in blue force locations, since the network-centric force is highly dispersed and seeks to control rather than occupy territory. Network-centric forces self-synchronize and move rapidly to exploit the fleeting opportunities created by the information dominance that the network provides to its subscribers. If reliable blue force tracking cannot be provided, then

[78] "Will Software Radio Become Real—and When?", *COTS Journal*, January 2004.

[79] The U.S. presently has an MOU in place with Japan for the development of SDR technology, and is in discussions with Australia, France, Germany, Italy, the Netherlands, South Korea, Singapore, Spain, and Turkey, but these discussions have not yet passed beyond the preliminary phases. See "Will Software Radio Become Real", op. cit.

[80] Recent estimates for the Battle of Cassino in Italy in 1944-45 put friendly fire casualties as high as 33% of the total, due mainly to misdirected artillery fire.

[81] In one noteworthy incident in Normandy in August 1944, some 600 American troops (including LTG Lesley J. McNair, Commander of U.S. Army Ground Forces) were killed when an aerial bombardment by the VIII Air Force fell short of the German lines.

commanders must fall back upon more traditional means of controlling and locating their forces, such as phase lines, fixed unit boundaries and areas of operations, bomb lines, forward observer lines, and rigid timetables. But these control measures by their very nature defeat the purpose of network-centric warfare. Blue force tracking is therefore a necessary precondition for the implementation of network-centric warfare, before any other criteria are met.

The United States and other countries have been trying to solve the fratricide problem since before the Operation *Desert Storm*, though the high proportion of friendly fire casualties gave added impetus to their efforts. Several different approaches have been tried to date, none of which has proven entirely successful to date. Among these are:

- Transponder-Based Systems
- RF Triangulation Systems
- Non-Cooperative Target Recognition

Transponder-based systems employ for ground forces the same principles used in airborne Identification, Friend or Foe (IFF) systems first developed in World War II: a coded radio signal interrogates unidentified vehicles or personnel, triggering a radio transponder that transmits a response positively identifying the vehicles or personnel as friendly. Alternatively, the transponder can be set to ping at predetermined intervals without interrogation, to provide constant updates of blue force locations. Additional information can also be included in the signal, such as unit designation, location, direction of travel, and even unit status; the proliferation of GPS devices makes accurate positioning very easy, in theory. Transponder systems have several disadvantages. RF signals cannot penetrate through certain types of terrain and have propagation problems in built-up areas. Signals can be intercepted by the enemy forces, and transponders can even be spoofed into broadcasting for enemy direction-finding equipment. All of these difficulties can be reduced by technology, but not eliminated entirely, to the point where one has a very high level of confidence. All of the problems inherent in IFF are also present in transponder-based blue-force tracking.

RF triangulation uses two or more receiving stations to determine the bearing of a blue force transmitter, using triangulation techniques to pinpoint the location. This system is used on instrumented ranges for both air and ground training (i.e., the Army’s National Training Center at Ft. Irwin, CA), in which it is possible to position direction finders with the best possible lines of sight. This is not possible for ground units moving into unsurveyed and hostile terrain. Triangulation therefore combines most of the disadvantages of transponder systems with the additional problem of getting a good fix on signals. With the advent of GPS, the locational value of triangulation is greatly diminished.

Finally, there is Non-Cooperative Target Recognition (NCTR), once seen as the “Great White Hope” of fratricide avoidance: vehicles, aircraft and other targets would be detected and classified by remote sensing systems (optical, passive RF, active RF, etc.) and classified by type based upon Measurement and Signature Intelligence (MASINT) techniques. This approach has even been applied with some success in fighter and AWACS aircraft, but it has never been used for tracking ground forces.[82] It had potential when the U.S. and its allies faced a discrete adversary whose forces were relatively homogeneous and used equipment radically different from that of the U.S. and its allies; i.e., the signature of a U.S. M1 Abrams tank is quite different from that of a Russian T-80 or T-90 tank. However, with the fall of the USSR, the U.S. finds itself involved in coalition warfare with allies whose equipment is similar, if not identical to that used by the enemy. Attempted implementation of NCTR also revealed other practical difficulties, such as the need to correlate tracks from multiple sensors, the fusion of diverse signature and measurement data from different types of sensors, and the development of reliable discrimination algorithms capable of working in near-real time. As a result, expectations for NCTR have been greatly reduced, though considerable amounts of research are still being performed with other applications in mind (i.e., Red Force Tracking, ISR, target acquisition).

In response to the friendly fire incidents of Operation *Desert Storm*, the U.S. Army acquired infrared beacons for its armored vehicles. Intended to provide a distinctive visual signature on the FLIR sensors of U.S. combat aircraft and helicopters, as well as the thermal sights of U.S. tanks and fighting vehicles, it was useful only at night and in good visibility. Sandstorms, fog, precipitation and smoke all greatly degraded its effectiveness. In its place, the U.S. sought a practical, all-weather, near-term solution.

The near-term solution was the Battlefield Combat ID System (BCIS), a millimeter-wave, interrogation (Q&A)-based millimeter wave (Ka-band) transponder system with a range of 150-1500 meters. Fully compliant with NATO STANAG 4579[83], BCIS is triggered when the targeting platform (whether airborne or ground) interrogates the potential target. An IFF display in the targeting platform then indicates whether the target is friendly or hostile. However, BCIS is useful only when forces are within direct line of sight of potential adversaries. It does not work for units beyond line of sight, nor does it report unit positions and status to the battle command network. Thus, BCIS is of limited utility for network-centric operations in which commanders need to know the actual positions of all units in near-real time.

Thus United States is now developing the Blue Force Tracking System (BFTS), which has been integrated into the Future Battle Command-Brigade and Below (FBCB2) command and control system. Essentially a transponder-based system, the BFTS is mounted on tanks, personnel carriers and other combat vehicles. Using GPS to derive accurate position data, the system reports either on an interrogation or timed response basis, using spread-spectrum, low-probability of intercept signals. During Operation *Iraqi Freedom*, some 1200 systems were installed on U.S. Army, Marine Corps and British army vehicles. Due to cost, however, the system could generally be installed only on one or two vehicles per company. Performance in combat was reasonably good, given

[82] However, this is of limited value when both friend and enemy fly the same types of aircraft.

[83] STANAG 4579 establishes standard frequency bands and waveforms for use in combat identification/IFF systems such as BCIS or the French BIFF. This creates the potential for interoperability, but does not ensure it, unless the same encryption, data formats and interrogation techniques are employed.

that terrain conditions in Iraq were ideal for the use of transponders. Despite this, there were still friendly fire incidents, and the Coalition command apparently did not have sufficient confidence in the system to mix U.S. and British forces in the same battlespace. A serious long-term objection to the direction of the BFTS is the size and weight of the system, which can only be installed on vehicles. Given that much of future U.S. and coalition operations are likely to feature dismounted combat in urban areas (i.e., Najaf and Faluja), the United States and its allies will need a smaller, lighter, less costly and man-wearable device to show the location of each individual soldier in a dismounted squad or platoon. Apparently such a system is under development by U.S. Army Soldier Systems Command as part of the Land Warrior XXI program.

European countries seem to be following suit. Britain, as noted, has leased the BFTS for its forces deployed in Iraq. France, for its part, is developing a system called Battlefield Identification, Friend or Foe (BIFF), which has been incorporated into France's LeClerc Battlefield Management System (LBMS). STANAG 4579-compliant, BIFF-equipped vehicles can interrogate potential targets, while individual vehicles can independently declare themselves friendly by transmitting the BIFF code. It is thus much closer in concept to BCIS than to BFTS, in that it does not have the capacity to capture automatically and display all blue force positions in a combat information system.

In March 2000, Thales Group received $36.9 million for the development and production of the first 1500 BIFF units, toward a total requirement for 5400 units. Assuming it is successful, BIFF will likely be adopted by the German *Bundeswehr*. However, BIFF has the same shortcomings as BCIS, and does not meet the requirement for true blue force tracking.

Ultimately, it would appear that the solution to the blue force tracking lies in the synergy of several different methods, including GPS-based vehicle tracking (possibly using satellite communications to transcend line-of-sight restrictions), interrogator-based systems, and non-cooperative identification methods, with data from all sources correlated and fused as part of the Common Relevant Operational Picture (CROP). Blue force tracking cannot therefore be solved until solutions have been reached for the Single Integrated Air Picture and the Single Integrated Ground Picture.

Phase II: Single Integrated Air Picture, Single Integrated Ground Picture, and CROP

A. Single Integrated Air Picture

Airspace management and integrated air defense are among the most complex tasks facing the modern theater commander. With thousands of friendly, hostile and neutral aircraft occupying the same airspace, at altitudes from nap-of-the-earth to 70,000 feet, and with targets moving as fast as twice the speed of sound, the seemingly simple task of keeping track of aircraft, deconflicting them to prevent collisions, directing friendly aircraft toward their targets and intercepting hostile aircraft is actually beyond the ability of a human being to accomplish manually. Indeed, just maintaining adequate situational awareness to make correct operational and tactical decisions is increasingly problematic.

In civil aviation, automated systems provide air traffic controllers with digitized displays. Yet even in this relatively benign environment, with aircraft flying at predictable speeds along well-defined corridors, and with transponders providing the air traffic control system with the identification, course and speed of all aircraft, air traffic controllers are hard-pressed to avoid data overload. The military airspace environment is much more complex and hostile. Enemy aircraft do not identify themselves, fly evasive routes, use jamming to degrade sensor performance. Low observable technology reduces the detection range of radar, and weapons are used to suppress the airspace management system by attacking its constituent radars stations. In addition to aircraft, the airspace management system must track incoming and outgoing missiles, and also correlate the airspace picture to the tactical situation on the ground.

At present, military airspace management in an expeditionary force such as the NRF tends to be centralized: a relative handful of ground-based radars cover specific, minimally-overlapping sectors, with air traffic control directed from a central Combined Air Operations Center (CAOC)[84] in which several controllers are linked directly to a specific radar. If an Airborne Warning and Control System (AWACS) is available, the CAOC can offload some of the airspace management tasks to the onboard controllers, while receiving a mirror air picture via data link (generally Link 16 JTIDS/MIDS). The CAOC and AWACS coordinate the movements of friendly aircraft, ensure that they stay within predesignated safe corridors, do not attack friendly ground forces, and vector them toward hostile air tracks.

In addition, the CAOC is responsible for coordinating ground-based air and missile defense. In practice, this means that the CAOC will cue individual air defense batteries to the approach of a threat (aircraft or missile), so that the battery can engage at the earliest opportunity. However, at present, each air defense battery is a stand-alone unit, with a single sensor feeding tracking and fire control data to a single battery command post (BCP), which in turn controls guns and/or missile launchers tied directly to that BCP. The CAOC and battalion tactical operations center (TOC) are not directly involved in the engagement of targets, except to provide authorization to fire under certain rules of engagement.

This approach worked reasonably well in the 1960s, but is woefully inadequate in the current threat environment. The four main issues facing conventional airspace management and air defense are:

1. Saturation
2. Terrain Intervisibility
3. Active and Passive Countermeasures

[84] A TAOC is used at the brigade and divisional echelons; corps and echelons above corps (EAC) employ a "Combined Air Operations Center" or CAOC, which performs many of the same function plus higher-level campaign planning and coordination.

4. Critical Node Failure

Saturation is accomplished when the enemy pushes an air attack on a narrow sector so as to exceed the capability of the radar, the airspace management system or the air defense system to cope with all the potential targets. The number of targets can be artificially enhanced with the use of decoy drones and electronic countermeasures, and more recently, through the use of tactical standoff missiles (TASMs).[85] Some of the incoming aircraft and missiles may be engaged and destroyed, but others will be missed in the clutter, and more will simply get a free ride because the system lacks the capacity to engage them all.

Terrain intervisibility refers to the blocking effect of hills, trees and other terrain that creates “dead ground” in which aircraft are invisible to line-of-sight sensors. Aircraft can use this ground to mask their approach to a target area.[86] AWACS can eliminate some, but not all dead ground; but its performance tends to be degraded when trying to track aircraft in clutter close to the ground. In the past, the difficulty of low-level, high-speed navigation made exploitation of terrain intervisibility a difficult and risky proposition (the proliferation of small-caliber air defense artillery in particular caused the loss of many more aircraft than the more glamorous surface-to-air missile). Thus, the United States and most of its allies have abandoned this method of attack in favor of using precision-guided munitions delivered from medium-to-high altitude, relying on a combination of stealth, electronic warfare, and defense suppression to neutralize enemy air defenses. Smaller, less well-endowed air forces cannot afford this costly, high-overhead tactic,[87] and so continue to practice low-altitude, terrain masking tactics. More threatening still is the proliferation of tactical cruise missiles that can fly preprogrammed, terrain-masking flight paths. Conventional air defense systems find these difficult to counter because (a) they have very small radar and infrared signatures; and (b) their use of terrain-masking flight precludes having an unobstructed line-of-sight for enough time to complete the engagement cycle.[88]

For these various reasons, the U.S. military has been pursuing the goal of creating a Single Integrated Air Picture (SIAP) that would display the total air situation within a

[85] A typical fighter aircraft can carry from 2–4 TASMs, which now have ranges in excess of 25–30 km. Thus, a single fighter can spawn as many as four daughter tracks, each a critical target moving at high speed. The effects on airspace management and air defense systems can be imagined.

[86] The famous karst outcropping known as “Thud Ridge” was habitually used by U.S. fighters approaching Hanoi from the west during the Vietnam war.

[87] In a typical U.S. air strike package, eight fighter-bombers might be supported by as many as two dozen other aircraft—AWACS, tankers, standoff jammers, escort jammers, fighter escorts, and “Wild Weasel” defense suppression aircraft. A high percentage of the strike package is thus devoted to “taking in the laundry” rather than to destroying the target.

[88] Most air defense systems require a direct line of sight from the weapon to the target throughout the engagement cycle. That cycle includes detection, classification, tracking, illumination or lock-on, launch, flyout, and post-engagement assessment. For most air defense systems, this cycle time is least 20–30 seconds; however, the typical unmask period for a low-altitude cruise missile is about 10–15 seconds. As a result, except in extraordinary circumstances, conventional air defense systems have a very low probability of intercepting a cruise missile.

theater of operations in near-real time, using all available sensors in a single fused track file. Achieving this goal requires the solution to four key problems:

1. Track Correlation
2. Sensor Fusion
3. Latency
4. Data Distribution

The track correlation problem is the most fundamental and, in some ways, the most intractable. In short, when two sensors observe an object, each reports the location of the object in a slightly different position, due to the inherent inaccuracy or “error budget” of the sensors. When three sensors look at the same object, they report three slightly different positions, leading to the generation of an “error elipse” within which the target is located. If multiple sensors look at the same set of multiple targets, it becomes difficult to determine which particular targets in the track file of one file match or correlate with the targets in the track files of the other sensors. If the tracks cannot be correlated successfully, then the merged track file will report false tracks (one object reported as two) or dropped tracks (two objects reported as one). The difficulty of solving the problem rises exponentially as a factor of the number of sensors and targets. Any terrain masking that may occur only adds additional layers of complexity, since correlated tracks going into dead ground can de-correlate while masked. A typical theater of operations, with several thousand air objects being tracked by a dozen or more sensors at any given moment, would require the solutions of hundreds of thousands of track correlation hypotheses at any moment. In the past, processor speed made a technical solution impossible under field conditions. Given the operation of Moore’s Law, processors are now fast enough to perform the correlation problem in reasonable time under ideal conditions, but the correlation problem is still far from being solved.

The sensor fusion problem is similar to, but distinct from track correlation. In this case, the issue is the merging of information from dissimilar sensor types (i.e., from a radar and an IR sensor) in such a manner that the sensors act synergistically to provide more information about the target than either sensor separately. This capability, critical for reliable NCTR, requires first the solution of the correlation problem (i.e., relating a specific radar track to a specific IR signal), co-registering them in the same coordinate frame, and then somehow merging the data from each and presenting it in a comprehensible manner to the human operator.

Doing track correlation and sensor fusion takes time, and time is the critical factor in airspace management, air defense and air combat: objects are moving at speeds from 250-700 meters per second, which means that a delay of only four seconds between the time a target is detected and the time the track is displayed on a screen represents a positional error of 1.0-2.8 kilometers (and in reality, the elapsed time may be several times greater). Positions on a situational awareness display, therefore, are really just approximations, representing elipses within which the target is located. Whether this degree of latency is operationally acceptable or not depends on the use to which the data is being put. It may be acceptable for overall planning and situational awareness, but it is not acceptable for targeting and fire control purposes. Thus, if we just want the SIAP in order to see where all the air objects are, latency of several seconds is fine, but if we want to use the SIAP to cue and guide missiles against incoming targets, the latency is too great.

Latency has several components. Sensor detection and reporting time is one component; correlation and fusion processing time is another. But the largest contributor to latency is the data transmission and distribution time. Sensor data files are extremely large, and moving them across a network, either by datalink or even by fiber-optic cable, takes time. Merged and fused multi-sensor track files are even larger. All of these have to be continuously transmitted across a sensor network to provide subscribers with the current SIAP, but there is a limit to how much bandwidth may be available for this purpose. If bandwidth is inadequate, then there will be increased latency between the time the SIAP update is published and the time it reaches subscribers.

From this discussion, it should be clear that there are several critical technologies required to provide a useful SIAP. To deal with track correlation and sensor fusion requires high-speed processors combined with efficient algorithms and software implementations. To some extent, that also deals with part of the latency problem. The rest of the latency problem requires solutions the bandwidth shortage, including more efficient and reliable data and bandwidth compression software, higher-capacity data links, and less processor intensive video processing firmware for moving sensor data over a network.

B. Single Integrated Ground Picture

The single integrated ground picture (SIGP) is analogous to the SIAP, but ground rather than air objects. The principal technical differences between the SIAP and the SIGP are the tempo of operations and the number and diversity of objects to be tracked. Whereas air targets are moving at very high speeds (250-700 mps), ground targets rarely move faster than 100 kph. As a result, latency is not as serious a consideration in the SIGP, not even in regard to fire control applications. On the other hand, the shear number and variety of objects to be tracked dwarfs that of the SIAP. There may be as many as a thousand targets in the air picture at one time, but there are more than 1500 discrete vehicular targets in a single armored/mechanized division. And whereas air targets can be divided into a relative handful of discrete categories, each with four or five specific types, there are literally dozens of different classes of ground target, with many more individual types in each class. Moreover, whereas airborne sensors are usually quite effective in detecting and tracking air targets at long range, ground sensors, both RF and optical, find it much more difficult to detect and track targets in the clutter of terrain and under camouflage. Only through the fusion of several different sensor types is it possible to reliably track and classify vehicular-sized targets, provided such targets are in fact in the open (and not hidden in barns or caves, or even under tarps and camouflage netting, as was the case in Serbia).

To detect concealed targets, as well as those enemy units too small or low-contrast to spot with remote sensors (i.e., a squad of guerrillas dressed in civilian clothing), SIGP must supplement remote sensor data with human intelligence (HUMINT), including situation reports from line units, long-range scouts, and covert intelligence operatives. Human intelligence, however, is not amenable to compression into fixed, quantitative data formats. Rather, HUMINT is highly variable and must be collated and assessed against other sources before being reduced to an input format compatible with SIGP. With combat increasingly devolving to squad-sized actions against dismounted irregular forces, HUMINT is gaining importance—as is the need to track both friendly and enemy forces down to the squad, fire team or even the individual level. Eventually, some form of GPS-based blue-force tracking system may suffice to locate friendly forces on the battlefield (but not if these troops are fighting inside buildings or even built-up areas where buildings create GPS dead zones and multipath transmission problems).

Thus, while the track correlation problem may be less critical for SIGP than for SIAP, the sensor fusion problem is much more difficult, while the two or three order of magnitude increase in the number of targets to be tracked (blue and red) creates an awesome data storage and transmission problem. Assuming these can be resolved, SIGP also creates daunting visualization problems. For example, the amount of information available to commanders at all levels is so vast that it creates data overload; the mind cannot assimilate everything being presented. Commanders must be able to parse the SIGP, focusing only on the level of information and the area of operations appropriate to their command responsibilities. This can be accomplished by intelligent, user-defined command information systems (such as the U.S. FBCB2) that not only filter out unwanted information, but also provide the commander with decision aids that suggest alternative courses of action.

Therefore, SIGP not only faces the same technical problems as SIAP, it adds several new ones of its own. Again, the potential solutions involve both hardware and software, including artificial intelligence systems, mass storage systems and visualization systems.

C. Common Relevant Operational Picture (CROP)

Recently, the U.S. has been moving toward the merging of SIAP and SIGP into a single product or service called the Common Relevant Operational Picture, or CROP. Given the increasing integration of air and ground operations, it is logical to combine the two in such a way that the commander can access both air and ground data to provide total situational awareness of his area of operations. This can be done either by physically merging the two track files into a single CROP file, or by maintaining them as separate files and combining them through battle command and visualization software. The former approach would result in a file too large to be manageable and which would not take into consideration the widely divergent reporting and latency requirements of SIAP and SIGP. It therefore seems likely that the latter approach will prevail eventually, however, this in turn puts even greater pressure on the development of high-speed processors, data fusion algorithms, visualization systems, and decision aids.

Phase III: Cooperative Logistics, Asset Tasking and Engagement

A. Cooperative Logistics

In conventional logistics, lines of supply are stovepiped by nationality, by service, and ultimately by unit. Thus, in a coalition theater of operations, one would normally find one separate line of supply for each country involved (unless a country's contingent was too small, in which case it would piggyback on the supply line of another), then one for each service within a national contingent, then one for each unit with each service, down to the brigade/wing/task group level. Through adoption of common standards for certain commodities such as fuel, lubricants and some classes of munitions, it may be possible to share supplies across national or service boundaries, but as a rule, sustained operations require distinct logistic trails for each service and component due to the diversity of systems, maintenance concepts, and even dietary requirements.

In the past, logistics normally have followed a supply-push model, in which supplies are transported into theater as rapidly as possible, then sent to forward depots as soon as they arrive, and then pushed onward to combat units without actually waiting for those units to call back for resupply. This is due to three factors:

1. Excessive Consumption. Though logistics planning usually includes consumption models, in practice these models have usually underestimated the rate at which supplies are expended. Rather than wait for this to become apparent at the combat unit, commanders push supplies forward in the expectation that the supplies will be needed by the time they arrive.
2. Operational Fluidity. Except in cases when operations are stalemated and become static for extended periods (i.e., Korea 1952-53), modern war is characterized by rapid and fluid movement of forces. Units that request supplies at one moment are likely to be in a different location by the time supplies arrive. The delay between the receipt of a request for resupply, the dispatch of a supply convoy, and the arrival of the convoy have traditionally made it difficult for logistic support to keep up with the forward echelons. Rather than trying to meet immediate demands in real time, logisticians have traditionally fed a continuous stream of supplies forward in the wake of advancing units.
3. Lack of Asset Visibility. In the past, it has been extremely difficult for supply officers to know the status of units and the location of all supplies in real time. Some materiel would be in rear depots, others would be in transit, some would be at forward depots, and others with units. But because most record keeping was performed manually and only at supply nodes, there was only a very approximate knowledge of where anything was at a given time. Similarly, the supply requirements of combat units would only be known as those units reported back, usually during intervals in operations, or when a critical supply shortage emerged. To minimize the effects of this lack of visibility in the supply chain, supplies were pushed forward as quickly as possible.

This supply philosophy had several effects:

- It required the acquisition and maintenance of excessively large stockpiles, with the associated costs of acquisition, maintenance and inventory control.
- It required excessive amounts of shipping and rolling stock to transport inter and intra-theater, which would otherwise be available for the transport of combat forces.
- It required an excessively large logistics footprint in-theater, with large supply depots and convoys, all of which are vulnerable to attack, and which therefore would require their own security detachments and base defense, imposing a form of "strategic consumption" on forces as they advance.
- The excess materiel shipped into theater would have to be shipped back to home base, or destroyed, at the end of each operation.

All of these shortcomings were observed during Operation *Desert Storm*. Not anticipating such a short ground phase to the war, the U.S. brought in far more fuel, ammunition and spare parts than was actually required. Most of this materiel never reached forward combat units, but rather was left sitting in large desert supply dumps or on the docks at Dahran. The inability of the supply services to clear the ports of incoming supplies resulted in the back up of supplies in and around the ports, where they were vulnerable to missile attack or sabotage.[89]

In response, the U.S. initiated a Revolution in Logistic Affairs (RLA) to parallel the ongoing Revolution in Military Affairs (RMA). In brief, the RLA called for the adaption of the commercial business practice of just-in-time inventory management to military logistics; instead of constantly pushing supplies forward according to a preplanned schedule, or simply as soon as they arrived, supplies would only be sent forward as needed, arriving "just in time"—i.e., when the unit needed to resupply without incurring critical shortages. If successfully implemented, the RLA would greatly reduce the size of supply stockpiles that the military would have to purchase and maintain in peacetime, with concomitant savings in the O&M account. It would reduce the demand for inter and intra-theater transport, and reduce the logistic footprint of combat units, thereby making them lighter and more agile. U.S. network-centric warfare concepts, with their emphasis on units widely dispersed throughout the battle area controlling but not occupying terrain, implicitly assume that RLA capabilities will be available to support combat forces.

Implementation of the RLA required the development of several enabling technologies:

- Automated Inventory Control
- Real-Time Asset Tracking
- Integrated and Automated Logistic Management Systems

[89] At one point, some 25,000 tons of munitions were sitting on the docks at Dahran, with more munitions waiting to be offloaded from ships at dockside and in the harbor. A single Scud missile landing there would have resulted in a catastrophic explosion which probably would have destroyed the port, sunk several ships, and killed thousands of U.S. troops and Saudi civilians.

Automated inventory control involves the use of bar codes, smart cards and associated electronic I/O devices to maintain inventory of stocks in an automated logistics database that keeps track of every supply item in inventory, from the main depot down to the forward unit. Wireless network devices allow stocks to be inventoried as they arrive, as they leave, and in transit.

Real-time asset tracking permits the continued tracking of supplies between nodes, whether by air, sea, truck or train. Various forms of vehicle tracking systems—some based GPS and satellite communications—indicate where a supply vehicle is at any moment, and can also keep track of changes in its load as cargo is on- or off-loaded.

All of this information is fed into an automated logistic management system, the supply equivalent of a command and control system, to present graphically to supply officers the status of all supplies moving at all points along the supply chain. To get a real-time picture of the demand side of the logistic situation, the blue force tracking element of the battle command system must feed combat unit logistic status into the logistic management system. Thus, each vehicle in each combat unit would be reporting on its fuel and ammunition status each time it reports its location. This information would be aggregated at the platoon or company level, and included in the platoon's position report. Platoon data would be aggregated at company, company at battalion, and so forth, until it reached the level at which supply decisions are made. The logistics officer would therefore have total asset visibility from end to end, and in theory, be able to forward precisely what supplies would be needed to the units that needed them, in real time.

Whether this is actually achievable in practice remains unproven. The United States partly implemented a number of RLA concepts on its dash up to Baghdad, but found that security along an extended line of communications remained a problem. Moreover, while there were never any serious shortages of fuel or ammunition, it must be recognized that some units came close to running out at several times, and that the U.S. faced no substantial organized resistance. In the south of Iraq, the British Army tried to apply its version of just-in-time logistics, and found its supply system in a state of collapse by the end of the war. The main problem seems to be a failure to recognize that in many cases, practices that work in the commercial business environment may not be applicable in the military environment. There is competition in the commercial environment, but it is inhibited by a web of legal and regulatory constraints which do not exist in war. Put another way, UPS and FedEx do not try to blow up each other's trucks; While in war, supply lines remain high-value centers of gravity to be destroyed or neutralized. Business is also much more predictable than war, which makes operations more predictable, whereas war remains characterized by great uncertainty.

The difficulties of implementing the RML are multiplied when extended to a multinational coalition. Not only are the number and variety of systems greater, but many of them operate to different standards and may even require different types of fuel and lubricant.[90] Standards regarding these basic issues can greatly reduce, but not eliminate the added complexity of cooperative logistics in a coalition environment.

[90] This is the case with the Polish contingent to the Coalition Forces in Iraq.

On the positive side, there is relatively little new technology needed to implement most of the RML. As noted, the idea was to import commercial logistic practices into the military environment, and most of the technology used in the RML is either commercial off-the-shelf or derived from commercial systems. This includes bar code and smart tag systems, vehicle tracking systems, automated inventory management and tracking, and even some forms of logistic management displays and visualization. The main technological developments related specifically to military requirements are a higher degree of information security, compatibility with military communications systems, and integrating the logistic management system with the battle command system in order to (a) receive information on unit supply status; and (b) provide the commander with a logistic situation overlay for the CROP. All of these appear to be relatively easy to accomplish at a purely technical level. The issue is whether this can be accomplished in a manner that allows interoperability with U.S. battle command and logistic systems now in development.

B. Cooperative Asset Tracking

In effects-based, network-centric warfare, commanders and warfighters can access the entire panoply of assets in a theater area of operations to implement the concept of operations and impose the desired effects on the enemy. Asset ownership and the traditional chain of command become less relevant as the military reorganizes around functions rather than services. In a radically flattened command system, units and assets may be tasked based upon their specific capabilities rather than on the basis of nationality or service. For example, a naval surveillance asset such as the P-3C Orion was widely used as a ground surveillance and reconnaissance platform, while USAF-controlled unmanned air vehicles provided coastal surveillance. In other examples, U.S. ballistic missile early warning satellites provided warning of missile attacks to British forces.

In a network-centric system, this approach is taken to its logical conclusion: any commander, anywhere, can in theory access and task the sensors and other assets of any other unit, whether it belongs to the same service, or even the same country. This poses profound challenges both to technology and to the predominant military culture developed over the course of the last 1000 years. If ownership and the chain of command become transparent, who decides who has ultimate control over an asset? How does the nominal owner schedule and deploy his assets? Since many important assets are high demand/low density (i.e., everybody wants them, but few are available), who gets priority for what missions? How can priorities be changed dynamically in response to a rapidly evolving ground situation? Who resolves conflicts? All of these are doctrinal issues that can only be resolved on the basis of operational experience, which will not be available until cooperative asset tasking becomes a reality.

Already some progress is being made in this area, particularly in regard to UAVs, NATO STANAG 4586, issued in 2002, sets forth standards for UAV interoperability. Focusing on the command data link interface between the UAV and its control terminal, the command and control interface between the UAV control system and the overall C4ISR system, and human interface controls, the STANAG ensures that all UAVs developed in accordance with this standard will have interoperable, plug-and-play architectures allowing differing degrees of cooperative asset control. This Joint Tactical Architecture identifies a common set of mandatory information technology (IT) standards and provides a common architecture for C4I, sensors, modeling and simulation. STANAG 4586 provides five different levels of interoperability to which UAV systems can be designed:

- Level 1—Direct Receipt of Secondary Data. This applies to UAV tracking and status information, allowing UAVs to be included in the SIAP and CROP through Blue Force Tracking.
- Level 2—Direct Receipt of Sensor Payload Data. Data from the sensor payload may be accessed by non-owning parties, either directly through a data link terminal, or over a sensor network.
- Level 3—Control of UAV Payload. Non-owning users can actually redirect the sensor package to look in particular directions or scan in particular modes of operation.
- Level 4—UAV Flight Control. Non-owners can take control of the UAV and fly it to areas of their choosing; alternatively, control of the UAV can be handed off from one ground station to the next without regard for ownership, allowing the UAV to operate beyond line of sight with its original ground station.
- Level 5—Launch and Recover UAV. Non-owners can either direct the launch of the UAV or control its recovery at a sight other than the original takeoff point.

All the capabilities of the lower levels are included at the higher levels. If fully implemented, Level 5 interoperability under STANAG 4586 would allow any unit in a coalition force to control the UAVs of other members of the coalition.

Similarly, the USAF is examining what it calls “dynamic sensor retasking” for its E-10A Multi-Mission Command and Control Aircraft (MC2A), in order to accommodate the conflicting requirements for sensor coverage from the various subscriber communities.[91] According to current plans, users in different services (and potentially from different countries) could direct the MC2A’s airborne ground sensor or ELINT system to look at specific areas of interest or switch from one operating mode to another. How well this works in practice depends on the standard operating procedures developed to prioritize requests and resolve conflicts.

From a technological standpoint, cooperative asset tasking requires the implementation of hardware and software standards for data communications, data processing and information display. Implementing the standards will require considerable exchange of technical data in order to design the proper interfaces and construct data element dictionaries, as well as to understand and interpret the information generated by sensors and other assets (i.e., range, resolution, operating limitations, etc.). If sensor data is accessed and assets controlled over the command and control network, then all battle command systems must be interoperable; i.e., able to access the same subsidiary systems,

[91] See Adam J. Hebert, “Building Battlefield Awareness”, *Air Force Magazine*, September 2004.

issue command, and receive and display data in a transparent and compatible manner. For example, the U.S. Army's Future Battle Command–Brigade and Below (FBCB2) will be the standard Army tactical command and control system in the near future. For other countries to access and control U.S. assets over the command and control network, their battle command systems must be compatible with FBCB2. Conversely, if the U.S. wishes to access foreign assets such as UAVs or the Airborne Ground Sensor, FBCB2 must be interoperable with foreign command systems.

C. Cooperative Engagement

Cooperative engagement is the fulfillment of the network-centric concept: a commander from one unit or service, using sensor data from a second unit or service, can task a unit of third unit or service to launch a weapon that destroys an enemy target. In essence it simply takes cooperative asset tasking to its logical—and lethal—conclusion. What distinguishes cooperative engagement from cooperative asset tasking is the need to provide timely and precise target acquisition and fire control information.

This problem was first confronted by the U.S. Navy in the development of the Aegis weapon system. Under the original Aegis concept, an Aegis ship would be able to access the sensor data of every other ship in the battle group, combine it with its own sensor data, and then pass weapon release commands to those ships within the battle group best positioned to destroy the incoming threat. However, until recently, the Navy was never able to implement this Cooperative Engagement Capability inherent in the Aegis system due to a lack of adequate communications bandwidth: neither NTDS Link 11 or Link 14, or even JTIDS/MIDS Link 16, could pass on the required targeting information fast enough to provide a reliable fire control solution. The Navy finally began to solve this problem with the development of a new data link system called (logically) the Cooperative Engagement Capability (CEC). Providing, in theory, an order of magnitude increase in throughput over Link 16, CEC has been used successfully in a variety of air and missile defense experiments, and is being deployed throughout the U.S. fleet on CG-47 and DDG-51 class Aegis ships. The United Kingdom became the first foreign customer for the CEC, buying several units under FMS for its Future Aircraft Carrier and Type 45 destroyers.

CEC, however, will not completely fulfill the requirements of network-centric cooperative engagement. In naval applications, the cooperative engagement architecture is relatively simple, since there are only a dozen or so ships in a battle group. Moreover, command in the battle group is centralized at a designated flag ship, which coordinates the actions of all the other ships, whereas in a truly network-centric architecture, command authority is dispersed, and the unit best positioned to exploit a fleeting opportunity would issue engagement commands. This requires a small, lightweight, and affordable communications link, which CEC in its present manifestation certainly is not. The USAF, for instance, has steadfastly refused to accept CEC as its standard broadband communications specifically because the CEC terminal is too large for airborne applications (which means it is certainly too large, heavy and expensive for ground systems). Instead, the USAF and U.S. Army have been investigating ways of stacking

Link 16 terminals and compressing data to achieve equivalent throughput at lower cost. So far results have been mixed.

Assuming that the bandwidth problem can be resolved, the remaining interoperability issues are both technical and operational. On the technical side, there must be full compatibility between the battle command systems used by all members of a joint or coalition force, in order to ensure that the proper intelligence and fire control information is transmitted and received in a timely and seamless manner. Operationally, it will certainly require a change in military protocols to give the authority to use lethal force to a commander from a foreign force. Formulating the new doctrine may be more difficult consuming than and time resolving the purely technical issues.