

The diminution of the Soviet strategic threat in Europe has led to a significant evolution of NATO strategic focus from the defense of NATO member territories¹ to one that now includes out-of-NATO-area operations in missions such as peacekeeping, crisis response, and crisis management. Before the recent NATO reorganization, three regional commanders-in-chief (CINCs) commanded and controlled air operations in their sector of responsibility in support of Article 5 operations. This will not be the case in out-of-NATO-area operations, as both the areas of responsibility and the command structure will be different.

This shift in focus has had and will continue to have significant implications relating to how NATO nations' air forces are commanded and controlled. The United States—as a member of NATO and as an interested party in coalition operations with NATO members—must consider and effectively address the changes in C2 doctrine, organization, procedures, systems, and personnel that have arisen from this strategic shift.

At the NATO Summit held in Washington, D.C., on April 23–24, 1999, NATO released an updated Strategic Concept consistent with the

¹The authority for such actions was based on Article 5 of *The North Atlantic Treaty* (NATO, 1998), which states that “the Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all,” and on Article 51 of the *Charter of the United Nations* (United Nations, 1945), which recognizes the “inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations.”

new security environment.² This document describes the new security environment, specifies the Alliance's approach to security, and provides guidelines for adaptation of its military forces, particularly NATO's C2 structure:

NATO's command structure will be able to undertake command and control of the full range of the Alliance's military missions including the use of deployable combined and joint HQs [headquarters], in particular CJTF [Combined Joint Task Force] headquarters, to command and control multinational and multiservice forces. It will also be able to support operations under the political and strategic direction either of the WEU or as otherwise agreed, thereby contributing to the development of the ESDI within the Alliance, and to conduct NATO-led non-Article 5 crisis response operations in which Partners and other countries may participate.³

The case study discussed in this chapter examines elements of U.S. and NATO C2 strategic and operational structures, air campaign planning and execution practices and procedures, force-level planning systems, and information-sharing arrangements in the context of recent NATO reorganization and future out-of-area coalition operations.

We focus on interoperability between U.S. and NATO capabilities because only a few NATO countries have extensive national air C2 capabilities: most NATO allies rely on NATO-wide capabilities and rationalize their spending by investing in such capabilities. Therefore, if they participate in non-NATO alliance coalition operations with the United States, they will likely bring NATO C2 capabilities (practices, procedures, systems, and personnel). If these capabilities differ substantially from those of the United States, interoperability problems will arise that did not previously exist.

This case study highlights key differences and potential synergies between U.S. and NATO practices, procedures, and associated systems. It also emphasizes the importance of thinking about interop-

²See NATO (1999a).

³Ibid (para. 53c).

erability challenges from the strategic level to the technological level and the relationships between these levels.⁴

STRATEGIC LEVEL

The recently approved changes in command structure have important implications for the future of NATO. Although the Supreme Allied Commander Europe (SACEUR) remains a U.S. officer, other command structure changes reflect a somewhat more European emphasis. The number of Regional Commands (RCs) has been reduced from three (North, Central, and South) to two (North and South) (see Figure 5.1). One of these commanders (at RC NORTH) has become a European billet, rotating between a British and a German officer. The RC SOUTH commander remains a U.S. flag officer.

Accompanying these changes in the top-level command structure is the concept of Joint Sub-Regional Commands (JSRCs), whose commanders are subordinate to the regional commanders. The JSRCs are army officers of seven host nations (Germany, Italy, Spain, Norway, Denmark, Turkey, Greece) who maintain a regional presence for the purposes of air sovereignty, infrastructure maintenance, and the like. These commanders also have responsibilities for accommodating an influx of forces during wartime. Therefore, the regional infrastructure, systems, and practices and procedures in place at a JSRC are likely to have an impact (at least initially) if forces from elsewhere are introduced to augment the existing presence.

Accompanying the JSRCs is a set of Combined Air Operations Centers (CAOCs). Under the NATO reorganization, there are nine “static” CAOCs (in Germany, Italy, the United Kingdom, Norway, Denmark, Spain, Portugal, Turkey, and Greece), plus two deployable CAOCs (DCAOCs) garrisoned in Germany (the exact location is not

⁴Because of the hierarchical nature of C2, we found it useful to follow the multilevel construct (strategic, operational, tactical, technological) for presenting the results of our interoperability analysis. Although the importance of thinking about interoperability from the strategic to the technological is important for the other case studies as well, we found that construct to be awkward for presenting the analysis because it is difficult to separate the results into each of the levels. In several case studies, we found that a historical or programmatic approach was more useful.

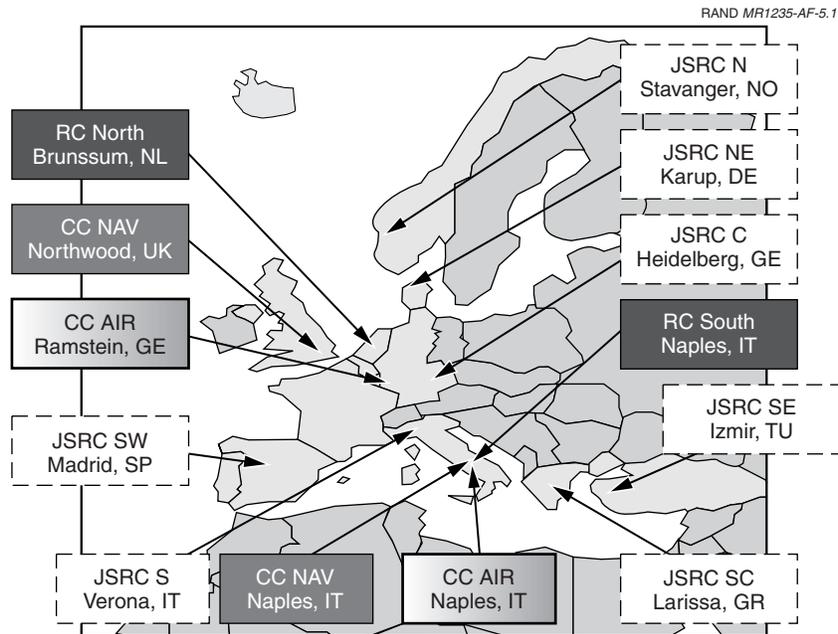


Figure 5.1—New NATO Regional and Subregional Command Structure

finalized) and Italy (see Figure 5.2). As with the JSRC command posts, host nation “ownership” is important for two reasons. First, these CAOCs serve as a starting point for augmentation from the NATO air component commanders (CC AIR) in Germany and Italy, as well as national forces. Second, during peacetime the CAOCs also fulfill certain national functions, such as air sovereignty, for host nations. The distribution of CAOCs and JSRC posts is a result of both external, threat-related factors and political considerations within NATO.

Current Command Constructs

Four basic types of command arrangements can be envisioned in coalition operations with NATO allies. The most common operations in recent history were not conducted within the NATO com-

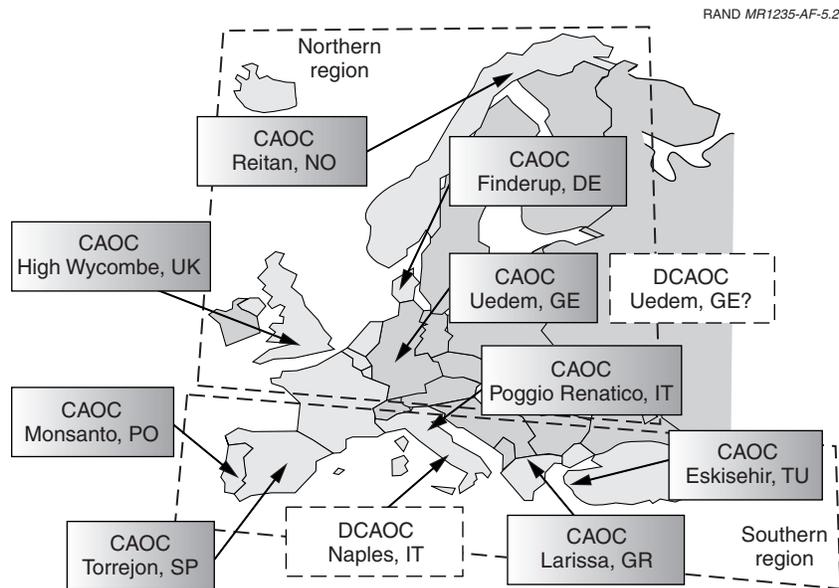


Figure 5.2—New NATO Combined Air Operations Centers

mand structure; many operations have been led by the United States with the participation of a limited subset of NATO allies and other coalition members.

In such cases, the United States will likely bring the greatest assets. Because the preponderance of political will, C2 assets, and combat forces will likely come from the United States, it is also likely that U.S. practices and procedures will be followed. However, this reasoning does not underestimate the key contributions of allies in terms of overflight rights, basing, and other support infrastructure, which may provide great leverage depending on the exact circumstances of the conflict.

The most basic type of command arrangement within NATO is the traditional Article 5 operation in defense of NATO. This type of operation has been practiced for years, and as pointed out earlier, the institutions and practices and procedures of NATO itself have been constructed for this type of contingency. For these reasons, and

given that the European allies will be the largest stakeholders in this case, NATO systems and doctrine are likely to dominate.

Both the U.S.-led coalition construct and the Article 5 construct represent relatively well-known situations. However, two other types of command arrangements currently evolving in NATO represent important changes at the strategic, operational, tactical, and technological levels. These two constructs will be examined in turn.

Evolving Command Constructs

An evolving CJTF doctrine has been drafted that has significant implications for the conduct of power projection and out-of-area operations. From the operational level downward, the CJTF doctrine appears on the surface to be very similar to U.S. CJTF doctrine. However, important differences exist at the highest level of command relationships. In the event of an out-of-area contingency, SACEUR is authorized to designate a CJTF commander (ComCJTF) from anywhere within the NATO command structure. Thus, a regional commander (North or South) may or may not be chosen to be the ComCJTF. For example, a different European flag officer may be chosen owing to regional familiarity or relevant service knowledge (air, maritime, land). Air, maritime, and land component commanders are selected to support the ComCJTF; they will provide the CJTF with forces from the standing NATO component commands (CC AIR, CC NAV, and JSRCs) and from supplemental national sources. One of the DCAOCs would likely be deployed to support the Combined Joint Force Air Component Commander (CJFACC) by augmenting the battle staff of the appropriate CAOC.

Although doctrinally similar in many ways to the U.S. CJTF concept, the new CJTF doctrine has two important distinguishing features. First, the appointment of a ComCJTF who is not a regional commander has the potential to represent a deviation from existing practices and procedures used within the standing peacetime command structure. Second, the authority and responsibility with respect to SACEUR, the North Atlantic Council (NAC), and national command authorities remains unclear. These points are discussed in the next section.

The second emerging command construct is known as the joint operational area (JOA) construct. In the case of an emerging regional conflict near a NATO border, a JSRC may request support in from the air, maritime, and land component commanders. As in the case of the CJTF construct, the question of practices and procedures at the level of the JSRC and supporting static CAOC becomes an issue.

Both the CJTF and JOA command arrangements represent potential sources of divergence from established U.S. practices and procedures, but they should also be viewed as targets of opportunity to exert influence to the degree to which they remain uncertain and are still evolving.⁵ The lack of constructive U.S. participation within organizations responsible for making changes at this level can have a substantial, cascading impact at the operational, tactical, and technological levels. The nature of these impacts will be described in the following sections.

OPERATIONAL AND TACTICAL LEVELS

At the operational and tactical levels, discrepancies in policies, practices, and procedures place constraints on the maximum level of interoperability that can be attained between forces. The lack of top-level consensus on strategic and operational objectives can also constrain the ability to work together effectively. As we have defined interoperability, effectiveness is the key metric of interoperability. If discrepancies in force mix, practices, and procedures between the United States and NATO are taken as a given, every effort should be made to provide workarounds so that negative impacts on effectiveness are minimized.

The enduring principle of C2 in the United States has been “centralized control with decentralized execution.” To the extent that this principle is threatened, the efficiency and perhaps effectiveness of coalition operations are also threatened. The lack of top-level consensus on objectives can have a cascading impact on

⁵We are suggesting the adoption of U.S. warfighting practices and procedures for two reasons: (1) in the near future, the preponderance of C2 assets and combat forces will likely come from the United States, and (2) the United States has developed and established CJTF and air operations center (AOC) practices and procedures that have proven effective over time for a variety of operations.

the effectiveness of a campaign. A campaign plan with clear, well-articulated objectives and strategy is essential to maximizing chances of a successful outcome. If these conditions are not met, a number of possible consequences may result.

First, because of political sensitivities, the delegation of decisionmaking authority to subordinate commanders may not occur. Information technology increasingly allows top-level decisionmakers to observe detailed aspects of combat in near-real-time. It also allows force-level decisionmakers to be easily distracted by tactical issues and to concentrate less on operational issues.

Second, the sharing of tactical information—such as targeting data, ATO information, and airspace control order (ACO) information—that normally happens as a matter of course may become a matter for negotiation at higher echelons of command. Alternatively, information sharing may have to occur at lower echelons on an ad hoc basis to prevent highly undesirable results, such as fratricide. Workarounds that result from these circumstances may not be entirely adequate or uniform across the force.

Most workarounds are, by definition, not matters of policy but instead result from interactions between individuals or small groups who are familiar with each other. The trust and respect essential to accommodating these workarounds may be gained only over time. For example, procedural workarounds between airborne controllers and fighter pilots can occur only if these groups interact with each other face to face, which implies that they are based from the same location and interact on a daily basis. If the United States intends to pursue network-centric warfare, U.S. principles will need to be shaped by these personal considerations, which are part of peacetime and coalition operations.

Operational issues include not only activities at the CAOC, but the activities of crucial air and ground control and surveillance assets as well. In the case of AWACS, U.S. doctrine has incorporated the notion of air control (in addition to surveillance) for some time. In NATO, however, NATO Airborne Early Warning Force Command personnel have only recently begun to perform this function, and new NATO aircraft retrofits will include more consoles that can potentially be used as weapon control stations.

The operational doctrine and training of U.S. and NATO AWACS (and U.K. and French AWACS) should be harmonized to decrease the burden on personnel, since shortfalls are difficult to accommodate with augmentees on a fixed-size aircraft. At a minimum, the capabilities of these aircraft should continue to be harmonized to ensure that the different platforms are fungible at the level of functionality. With respect to ground surveillance and control, the same principles apply. These areas will be discussed in subsequent case studies on airborne surveillance and control (see Chapters Seven and Eight).

At the tactical level, rules of engagement (ROEs) and weapon systems will likely differ substantially between the United States and NATO. While the United States is rapidly acquiring standoff and PGWs, many NATO allies are moving more slowly or are buying smaller quantities of munitions. These differences also affect ROEs, with many European nations requiring eyes-on-target. Different mixes of fighters also help determine under what circumstances different capabilities (fast and low versus high and slow) should be allocated at the force level. In many cases, even similar weapon systems with different munitions (say, F-16s with precision versus nonprecision weapons) are not fungible and may be employed only in a certain threat environment or under certain weather conditions. These factors complicate the force-level planning process. This subject will be discussed in the case study on fighters and weapons (see Chapter Ten).

TECHNOLOGICAL LEVEL

In this section, we concentrate on force-level planning and execution monitoring and on information exchange. As we have seen, information exchange is a broad topic that encompasses issues at different levels, from intelligence-sharing policies at the strategic level to procedures for sharing data at the operational and tactical levels and now, in this section, to hardware and software needs (for example, network security protocols) at the technological level.

Currently, the United States uses the Contingency Theater Air Planning System (CTAPS) as its force-level planning system. The United States is also developing the Theater Battle Management Core System (TBMCS) as its follow-on force-level planning system. The NATO Consultation, Command, and Control Agency (NC3A) has

developed the Interim CAOC Capability (ICC) software for force-level planning, and NATO has recently awarded a contract to a consortium led by Thomson-CSF for a follow-on system known as the Air Command and Control System (ACCS).

Although much interest has been expressed in defining interoperability requirements and standards between these systems, a number of factors complicate this process, including differing objectives, practices, and procedures; an increasing need for dynamic planning; the development of a COP; and the use of standards.

Differing Objectives, Practices, and Procedures

CTAPS. The concept and design of each of these systems have proceeded with different objectives, practices, and procedures in mind. CTAPS has been the U.S. operational system since shortly after Operation Desert Storm. It is meant to accommodate large air campaigns of up to 3000 sorties per day. The design of CTAPS (and its companion intelligence module, the Combat Information System [CIS]), is based on a large number of interconnected modules, each devoted to a particular function within the air campaign planning process (preparing target folders, planning tanker orbits, etc.). CTAPS is also designed for a relatively large (600 to 800) AOC staff, where each staff member might be responsible for operating a small number of functional modules. Each module has a private database, and limited data are passed from one module to the other as common data. As a result of these factors and the integration of intelligence data within the process, the functionality and computational power of each module can be made relatively complex. At the same time, however, training and ease of use are significant challenges to the implementation of CTAPS with inexperienced personnel during wartime.

TBMCS. TBMCS is aimed at expanding the functionality of CTAPS by adding more integrated intelligence data and computational models to the ATO planning process. TBMCS also has consolidated the number of databases to two: the Air Operations Database (AODB) and the Modernized Integrated Database (MIDB). This move toward more common databases should enable TBMCS (in principle) to allow near-real-time updates to common data by a number of modules so that different modules have access to data earlier than if the

process were serial, as in CTAPS. Accompanying this database consolidation is a replication engine designed to copy the AODB and MIDB regularly between different sites (e.g., AOC, air support operations center [ASOC], wing). Mission reports (MISREPs) are filed by the wings via a messaging system that updates the databases at the AOC. Much of the design of TBMCS is based on a relatively free exchange of information between different portions of the planning process, with the exception of intelligence production. Here, a suite of applications is responsible for the development of top-secret information (such as imagery) on a secure network ring, and secret-level data are passed down via National Security Agency–approved security guard software (e.g., Radiant Mercury for text and ISSE Guard for imagery).

ICC. The current NATO system, ICC, is substantially different from U.S. systems in its doctrine, practices, and procedures. In NATO, the CAOC is not quite analogous to the AOC in that the CAOC is primarily a battle management organization (as opposed to a C2 organization). As a result, the responsibilities for many force-level planning functions that rest with the U.S. concept of an AOC actually rest with higher-level headquarters in NATO. These differences are borne out in the design and implementation of ICC.

First of all, ICC is much more lightweight than CTAPS or TBMCS. It is designed for between 200 and 1000 sorties per day and includes little support for the integration of intelligence information. It is organizationally oriented and is designed principally for functions such as the allocation of sorties and the deconfliction of airspace. ICC is designed for a relatively small CAOC staff, who may be generalists with responsibility for a large number of functions within the planning process; hence, the software is aimed at “ease of use” as opposed to “depth of function.” ICC includes little capability for the preparation of target folders, the integration of threat data, or weaponing. In part, this reflects NATO practices and procedures, where most intelligence sharing is negotiated at higher echelons of command or where weaponing calculations are made within national wings.

ACCS. Basic specifications for the forthcoming NATO ACCS have been available for some time and include the integration of ground radars and sensor fusion posts, which makes ACCS similar to the U.S. Theater Air Control System (TACS) in scope. However, the ACCS

force-level module specification calls for a primarily air defense-oriented functionality with limited offensive planning capability. ACCS is planned to be linked with the NATO Battlefield Information Collection and Exploitation Systems (BICES), an evolving intelligence-sharing system for NATO designed to bring together information from a number of existing systems. The extent to which ACCS specifications may change, given the desire that NATO participate in more out-of-area operations, remains unclear.

Interoperability Issues. Recognizing that two force-level systems exist for the United States and for NATO, each of which accommodates different practices and procedures, is a crucial step in selecting an appropriate way to harmonize the programs to achieve interoperability. Currently, interoperability issues between CTAPS and ICC are being addressed by a wide variety of players, including the NATO Air Command and Control Management Agency (NACMA), NC3A, the USAF Electronic Systems Center (ESC), the U.S. J6, and the United States Air Forces in Europe (USAFE). To date, the solution has been to define messaging standards for communicating between systems at a basic level. Most significantly, standard ATO and ACO formats have been advanced (ATO-98 format) to allow for the exchange of ATOs (and some other messages, such as MISREPs) between the two systems. Although the necessary changes have yet to be fully implemented and fielded in both systems, negotiations will need to continue to ensure that subsequent changes to data formats by the United States or NATO are carried through to the messaging standard. Given the capabilities of both systems at present, messaging interoperability and the exchange of ATOs are likely to constitute an appropriate level of interoperability.

For ACCS and TBMCS to be used in support of contingencies ranging from small peacekeeping operations to MTWs, they must be scaleable. A systems architecture for software that enables the use of different modules by different users in different contingencies might allow significant flexibility in the functionality or capacity of a force-level planning system. Successful development of such an architecture requires major investments in modular software engineering and configuration management techniques. In some cases, simple workarounds (such as loading ATO parsing information on a laptop computer and linking to basic office automation tools) can be somewhat effective. Only modest progress in these areas of computer sci-

ence have been made. Robust and flexible software systems of the future should incorporate these advances in order to minimize DoD's sunk software development costs and maximize the use of these systems by the warfighter in a range of contingencies.

Cost Implications. The cost of these force-level planning systems is relatively low. The Air Force has spent approximately \$350 million on the TBMCS program to date, with another \$100 million budgeted over the next six years. At the same time, the United States is funding approximately \$170 million of the \$700 million cost of the ACCS program. This commitment has been made over several years, so the annual costs are in the few tens of millions of dollars.

U.S. participation in the ACCS program provides for U.S. insight and influence on the direction of the program. This U.S. contribution can be viewed as an expenditure to ensure interoperability of U.S. forces with those of NATO in future operations. In the absence of compatible systems, laborious and often inefficient workarounds have to be devised, often at some cost in force effectiveness.

Given the importance of force-level planning and monitoring systems, the United States should leverage its investments in ACCS and TBMCS to ensure that they are interoperable. An agreement on a common ATO format is an important step in this direction.

Dynamic Planning

In the future, however, as the capabilities of both systems expand to include the possibility of dynamic ATO planning beyond deliberate planning, the level of interoperability required may increase substantially. In this case, increased requirements for timely data will most likely require a number of capabilities. First, communication channels between force-level planners working from different locations or at different levels of classification will be required. Multilevel security network devices will likely be needed to facilitate these communications. A number of candidate architectures (such as double-encryption or virtual private networks) and data filters (Radiant Mercury, etc.) exist for these requirements, but both the United States and NATO must be convinced that the benefits of automated data sharing outweigh the operational risks of potential security compromises.

Clearly, these policy decisions must take into account more important strategic considerations in addition to the technological ones described here. Linking the U.S. MIDB with intelligence-sharing data systems such as NATO BICES—which comprises data from Linked Operational Intelligence Centers Europe (LOCE), the Maritime Command and Control Information System (MCCIS), and the Crisis Response Operation in NATO Open System (CRONOS)—is another optional part of this process. Again, secure technical architectures exist for this purpose, but limitations developed at the policy level on comingling of U.S. and NATO data tend to dominate these considerations.

Common Operational Picture

Integrating situational awareness data via the COP is another essential aspect of information sharing for dynamic air control. Currently this information is shared at the CAOC level through use of a single U.S. system (the Global Command and Control System [GCCS] COP) with large projection displays. But other users at lower echelons of command (e.g., wings) often receive these data too late to be useful for ongoing operations. In recognition of the fact that a variety of users may require near-real-time information on at least a subset of this information, an effort should be made to facilitate the exchange of situational awareness data (air, maritime, and ground) on a near-real-time basis.

Finally, the exchange of tactical data between the CAOC, airborne control and surveillance assets, and fighters is necessary and will become more so in coming years. Interoperable data and voice links such as Link 16 and Have Quick (or SATURN) are essential to completing the loop between these parties (see Chapter Nine).

Standards

No discussion of system interoperability and information exchange is complete without a discussion of standards. Although standards discussions do, in fact, permeate many working groups on interoperability in the military and commercial sectors, it is important to recognize their value. Standards can add value where they simply codify an existing (or a negotiated) consensus on an operational

issue that involves technology. Predicting the success or failure of standards is similar to predicting the relative success of military operations in that strategic and operational consensus among major stakeholders is required. However, standard setting is often difficult to achieve when it also involves economic interests.

Widespread, cost-effective standards rarely take the form of bureaucratically produced documents that later become products made by several parties. Instead, the most popular standards are tantamount to specific technologies with well-identified “owners” who have an economic interest in being responsive to their user base and in changing the standard or technology accordingly. This “economic interest” or profit motive is important when a large user base is to be addressed.

In some cases, such as HTML and LINUX, professional recognition and fame (not necessarily economic gain) can be important motivators for technology creators, but usually only in the early stages of development. This “pride of ownership” is vital in the early stages of technology, where fluidity in the overall direction of the technology may be required. In fact, the temptation for overregulation of technology development at an early stage tends to stunt the success of the product in many cases. Once a technology does gain clear support (through a de facto or informal standardization process), significant resources are usually required to bring it into the mainstream.

Simply stated, standards are most effective when they codify existing consensus, or represent de facto public consensus, such as in the case of a popular product. By contrast they tend to fall flat when they serve as a surrogate for the consensus-making process or when the interests of key stakeholders are ignored.

OBSERVATIONS AND SUGGESTED ACTIONS

Although NATO has modified its strategic focus to include non-Article 5 operations, CJTF doctrine and concepts of operations are still evolving. Current constructs represent potential sources of divergence from established U.S. practices and procedures. For example, they may not adhere to the C2 principle of centralized control and decentralized execution that governs U.S. air operations.

The Air Force should thus help NATO develop the CJTF concept of operations (CONOPS), associated processes, expert personnel, systems, and information-sharing protocols for out-of-area operations. In particular, the Air Force should ensure that the key doctrinal concept of centralized control and decentralized execution, which is inherent in U.S. joint-service air CONOPS, is institutionalized in the NATO CJTF concept.

Further, leveraging its expertise and capabilities in planning and executing air and space operations in power projection missions, the Air Force should man key positions in the emerging deployable and key static CAOCs to maintain the influence of U.S. practices and procedures in NATO. It should also develop and maintain a cadre of experts who can provide support to higher NATO headquarters (if needed) to help develop air campaign plans and assist in execution monitoring.

Information sharing is also a major interoperability challenge. This includes establishing intelligence-sharing policies at the strategic level, defining procedures for sharing operational and tactical data, and developing hardware and software capabilities at the technological level to facilitate information sharing among systems. In many cases, strategic policy considerations negate lower-level solutions and workarounds. For example, the sharing of tactical data (e.g., targeting data, ATO information, and ACO information) that should normally occur at the tactical level may become a matter for negotiation at higher echelons.

The Air Force should help NATO define the desired level of information sharing between planned U.S. and NATO force-level planning and execution-monitoring capabilities (organizations, procedures, personnel, and systems). This can be accomplished during the development of the CJTF CONOPS, which should clearly define the information exchange requirements for scenarios involving the NATO CJTF and U.S. coalitions.

Because of the importance of force-level planning systems, particularly to air operations, interoperability between U.S. and NATO systems is crucial. Given the current capabilities of TBMCS and ACCS, messaging interoperability and the exchange of ATOs are likely to constitute an appropriate level of interoperability. As these

systems evolve to support advanced warfighting concepts such as dynamic planning and execution, the level of interoperability will likely increase substantially.

Therefore the Air Force should first define the desired level of interoperability between TBMCS and ACCS and between TBMCS and ICC, and it should then ensure that this level has been achieved. At a minimum, a set of common messaging standards for information exchange should be defined for TBMCS and ACCS. The Air Force should also develop incentives that facilitate dialogue between the TBMCS system program office (SPO) and the ACCS program director (NACMA) or directly between contractors (Lockheed Martin and Thomson-CSF/Raytheon).