3

Exploiting the Internet Revolution

VICTOR A. DEMARINES

WITH DAVID LEHMAN AND JOHN QUILTY

Effective command and control (C^2) capability — sometimes now referred to as C^4ISR — is crucial to the successful execution of military operations and, in fact, to sustaining the U.S. military advantage in the information age.[1] The innovative application of information technology, in concert with the re-engineering of warfighting processes to exploit these technology enablers, is often called the Revolution in Military Affairs (RMA).

Over the last decade, a revolution in information technology (IT) has transformed business processes as well as many aspects of individuals' daily lives. The combination of cheap and powerful computers with effective networking has enabled commercial companies to increase greatly both the efficiency of their operations and the speed with which they can respond to new opportunities and challenges.

History shows that the same technologies and techniques that create economic growth can be turned to military purposes, that the military organizations that are quickest to exploit them can derive

1. The current term in vogue for command and control is "C^4ISR." We believe the definition should revert to "command and control" (C^2), because intelligence, surveillance, and reconnaissance are really support functions, while computers and communications are technology enablers. Logically, their inclusion would mean that other support functions such as weather reports, battlefield IFF (identification friend or foe), navigation services, and logistics should also be considered in any design of a joint command and control system.

substantial advantages from doing so, and that military power is most affordable when it rests upon a solid civilian economic base. We need only think of the centuries during which the British navy and the British merchant marine supported each other's leading positions, the exploitation of railroads by the Union during the Civil War, or the conversion of the U.S. automobile industry in World War II to the mass production of armored divisions.

However, the potential of the RMA — the potential for this commercially available IT to further improve C2 — while reasonably well understood, has not been fully realized. The United States has an enormous opportunity today to exploit its leadership in commercial information technologies in order to sustain affordable U.S. military power well into the future. If we do not seize this opportunity, we must worry that other nations may do so, at least in some selected aspects, thereby bypassing the existing U.S. lead in the military technology of the twenty-first century. One purpose of this chapter is to address how C2 can be enhanced and made "joint" through improving the DOD management of technological opportunities.

The rest of this introductory section outlines three salient characteristics of the Revolution in Military Affairs: it is incomplete, it has vast potential, and it has two sides — increased vulnerability comes with increased capability. Then, to promote a full understanding of the overall problem, the chapter provides a brief discussion of the evolutionary nature of joint C2 and the complexity of joint operations. It describes some lessons learned from past endeavors in joint acquisition and operations, and presents a set of recommendations on C2. A discussion of "cyber information operations" follows, with specific recommendations that focus on the different demands of computer network attack and computer network defense. The chapter concludes with recommendations to address the inescapable need for expert talent: the human factor that is crucial to the success of C2 and information operations.

THE REVOLUTION IS INCOMPLETE

A key example of a C2 technology that has created the RMA is the Global Positioning System (GPS). GPS virtually eliminates the age-old inability of troops in motion to know exactly where they are; it enables precision strike by autonomous weapons; and it allows a greatly expanded range of operational concepts and tactics in all ter-

rain types. Precision strike, the first offshoot of the RMA to be applied in actual battle, is based upon information technology: databases, data fusion, networks and communication, navigation by means of GPS, visualization, and collaboration technologies. Precision strike was used to devastating advantage in DESERT STORM, with an impact analogous to the invention of the longbow, gunpowder, or the machine gun. Each brought about a change in range and lethality of weapons that enabled a dramatic change in combat tactics.

The overwhelming U.S. victory in DESERT STORM attests to the advantage of leading in the development and adoption of IT. The United States used GPS to guide cruise missiles precisely against air defense targets in the initial stages, thereby giving the allied forces immediate control of the enemy air space. A network of intelligence sensors located the enemy positions and movements, detected SCUD launches, identified moving targets, and found downed pilots. An enormous communications infrastructure sent this information ricocheting between support organizations in the continental United States (CONUS) and C2 in the field. Satellite imagery created thousands of highly accurate maps of Iraq. In essence, Iraq was blind and ineffective without IT-enabled C2, while the United States was nearly omniscient and therefore triumphant.

However, the penetration of IT into U.S. forces is incomplete and inconsistent, which leads to many time-consuming *ad hoc* arrangements in the field. True joint C2 requires not only that the force components from the various services be able to communicate with the Joint Task Force (JTF) headquarters, but that they also have effective tactical communications among each other. Mission planning systems and logistics tracking systems must be able to exchange information across service lines; for example, access to the Air Tasking Order should not require resorting to paper, as in DESERT STORM and Kosovo. Air defense capabilities from multiple services must cooperate closely in real time if friendly airspace is to be protected and fratricide avoided.

While the commercial world thrives on the basis of IT that enables the exchange of information among systems owned by separate companies — business-to-business commerce — jointness in military C2 has not yet been fully realized at the tactical level. As shown in Kosovo, many of the problems that plagued DESERT STORM still exist. Fundamental changes in command and control and fundamental

changes to the joint acquisition of C2 systems are required to take full advantage of IT.

At the most basic level, commercial IT enables a new approach to what the defense community has termed "systems of systems," also called the enterprise. The system-of-systems approach knits together systems that were developed separately. With modern IT, the collection of systems can approach a single enterprise view with interoperable databases, functions, and user interfaces.

THE POTENTIAL OF RMA

The most exciting possibility is that IT could enable the U.S. C2 system to evolve from its traditional hierarchical decision-making structure to a more flexible and more distributed form. We find this potential transformation easier to understand through an analogy to team sports. Traditional military operations can be compared to football, in which teams attempt to carry out fixed plays, carefully designed and rehearsed in advance. A single decision-maker determines which play is best in a given situation, and each player carries out its assigned role in accordance with previously received instructions.

Compare soccer or hockey, in which each player has a position assigned on the basis of the player's distinctive capabilities. Within the general guidelines of the position, each player decides for himself or herself what to do from moment to moment. Players maintain continuous "situation awareness," so that their decisions about what to do next are based on an understanding of where the other players are and what they are doing from moment to moment. Good players learn through practice how to anticipate each other's moves, so that a pass is successful not because the receiver is where a playbook says he or she should be, but because the receiver is where the passer has figured out he or she is most likely to go, given his or her skills and the tactical situation.

We believe that modern IT enables the construction of a C2 system that would allow the U.S. military to play "soccer" rather than "football," maximizing the flexibility of individual elements responding to a situation. Actions would be based upon IT-enabled situation awareness and well-understood doctrine, rather than on detailed plans or explicit orders. This vision of the future has been called "network-centric warfare" because decisions about how to act are based on shared information and collaborative decision-making supported by a

network of communications, rather than on communications up and down a hierarchical structure.

The great advantage of network-centric C2 is that it increases agility. As the experience of successful electronic commerce shows, there are two varieties of agility, both important. The first enables the organization to gather and process information rapidly in order to make quick decisions. The commercial system in which computerized cash registers send data to a system that can order accelerated production of the goods in greatest demand has its analogy in the military "sensor-to-shooter" systems. In each case, the use of IT enables faster response because information moves laterally rather than up and down a hierarchy. The second type of agility allows the entity to respond effectively to unexpected events. In a commercial situation, this might mean using the network to reconfigure supply chains rapidly in response to unexpected price competition. Analogously, the military could plan operations in response to a scenario never previously considered, on the basis of the full range of capabilities of the available forces, rather than the limited number of options in the "playbook." If it turns out that the enemy did not do what we had anticipated, or the weather did not follow our prediction, or our intelligence was not 100 percent correct, a network-centric C2 system could enable us to react much more rapidly to the unexpected opportunity or unexpected threat.

TWO SIDES TO RMA

IT also has its vulnerabilities, as evident in recent well-publicized hacker events. The pervasive use of IT and the ubiquity of computers and networks expose the C2 system to a new form of attack. Computer network attack (CNA) can take the form of denial of service, exploitation of the data within individual computers and throughout the network, or deception — actual alteration of the data within the computers and the networks, unbeknownst to the U.S. forces relying on the data.

Thus, the IT revolution can have two major impacts on warfare. First, it can transform the battlefield by solving the age-old problem of integrated, joint C2. This implies putting IT to work to allow rapid, distributed, accurate, and effective decision-making. Second, it can create a new battlefield: the cyber battlefield. To the extent that both sides utilize IT, each is exposed to computer network attack. To the

extent that they are exposed, both must protect themselves from attack through computer network defense (CND). The United States must learn how to conduct both offensive and defensive information operations. This chapter addresses both of these impacts in turn.

Joint Command and Control: From Interoperability to Integration to Interdependence

The first step toward a genuinely joint C2 system that fully leverages the potential of IT is *interoperability.* Movement in this direction is well under way. The services have come to recognize that each C2 system must share information with the C2 systems of other services. This recognition has led to some standardization of protocols and data formats that allow the systems to exchange data, or at least enable users to view the data.

As they share more data more frequently, the services will recognize the advantages of further integration. An *integrated* system stores data only once, and does not duplicate functions. The individual service systems will access the same databases, and each service will be responsible for maintaining only the data that its own systems generate, avoiding the problems of data synchronization and integrity that plague systems today.

As the systems become integrated and the services learn to trust and depend on each other's systems, *interdependence* will evolve. Concepts of operations will change, eliminating systems from one service's inventory as it begins to deploy only with support from another service that supplies the eliminated function.

For example, tactical signals intelligence (SIGINT) is inherently a joint function. The sharing of intelligence data among the services creates a more complete picture of the threat and disposition of enemy forces. Today, tactical intelligence is provided by service-unique assets, such as surveillance aircraft from the services including the Air Force's RIVET JOINT, the Army's Guardrail, and the Navy EP-3 systems. While each of these systems individually satisfies some service-unique requirements, the bulk of the data collected is common to all services.

Years ago, at the prodding of the Office of the Secretary of Defense (OSD) and the Commanders-in-Chief (CINCs), the service-unique systems were made interoperable through the establishment of sev-

eral processing centers and distribution networks. Now, anyone with a properly keyed satellite communications receiver has access to the combined data streams from the service-unique collection assets. The good news at this stage is that all users have a more complete set of SIGINT intercept data. The bad news is that this simple rebroadcast distribution creates redundancies, ambiguities, and correlation problems for every end user.

The Integrated Broadcast Service (IBS) program just entering development (again at the prodding of OSD and the CINCs) embodies the move toward the second step: integration of tactical SIGINT information. The primary goal of the IBS program is to create an integrated tactical SIGINT information management and dissemination service and an information repository based on processing inputs from service-unique as well as national intelligence assets. IBS would then distribute information from this repository to end users based on predefined profiles and knowledge of the bandwidth available to each user. The information distributed would thus be tailored automatically to end-user needs, free of the former duplications and discrepancies.

Possible evolution beyond IBS is, of course, conjectural, but might proceed as follows, with an emphasis on efficient data collection, rather than on efficient distribution. IBS central processing of SIGINT data would give rise to insights as to which sources provide the most accurate, timely, or detailed data under which circumstances. These insights would then begin to shape the tasking of these collection assets. The individual services would become more willing to concentrate on collecting more of "what they are good at," confident that the data they do not collect themselves would be available from the integrated information repository. As their confidence grew, the services would allocate their development and operations and maintenance resources to areas where their needs were not being met, so that overlap of SIGINT system assets would dwindle, along with the associated budgetary demands. Funds released would be used to increase capability and strengthen the defense-in-depth capability.

If we generalize from this example, we see that *interoperability* stems from the recognition that data sharing has advantages; *integration* comes from recognition of the need for further efficiency, speed, and collective application of resources; and *interdependence* evolves

from trust and establishes optimal relationships for mission execution. The example also illustrates that each of these stages of evolution — interoperability, integration, and interdependence — involves two distinct processes: first, discovery of requirements and incremental improvement of the systems supporting the current concepts of operation, and second, radical change, with the creation of new concepts of operation enabled by the use of new technologies. It is important to recognize both of these processes and to manage them and their interrelations in developing joint C2. In fact, proper management to spur more rapid progress in the command and control of inherently joint activities may well require a separate organization dedicated to joint mission analysis, one that can experiment with roles and functions for each of the services within the context of an overall joint mission.

A PERSPECTIVE ON THE DIFFICULTIES

The fact that there are four separate services can create great difficulties for joint C2. The joint C2 system can only be configured from C4ISR system "building blocks" acquired and fielded by the individual services and Defense agencies. Interoperability becomes a constant challenge and, as noted above, evolving doctrine — and RMA expectations — go beyond interoperability, demanding integration and even interdependence.

The need exists, then, to ensure that the service- or agency-provided "building blocks" can not only support the parent service or agency needs, but also be an effective part of a coherent capability that transcends service or agency boundaries. Put differently, the building of the needed C2 capability is an inherently horizontal challenge in a world of inherently vertical service authorities and prerogatives which, while fully legitimate from service standpoints, create a tension between serving local interests and the broader common good as described here.

CASE STUDIES: SUCCESSES, FAILURES, LESSONS LEARNED

To illustrate the need for interdependence, we now turn to some real-world cases in which the United States has addressed the challenge of building and fielding inherently "horizontal" C2 capability, crossing organizational (and cultural) boundaries, and confronting inevitable existing controls and prerogatives in an inherently vertical world.

These cases are significant because they demonstrate that properly motivated activities, with adequate funding and personnel resources, can accomplish a great deal without major and painful structural changes to the organization of the DOD. We conclude this analysis of past activities with the lessons that lead to our recommendations.

Of course, no historical case has the full scope and complexity of the challenge addressed here; notions such as "transformation," "RMA," and "network-centric" joint warfare, taken seriously and broadly, go beyond our experience to date. However, these identifiable cases present, in microcosm, many of the difficulties of a "horizontal challenge in a vertical world."

The cases address both *infrastructure* and *application* (or operational mission/function) capabilities within the domain of C2: the DOD Intelligence Information System (DODIIS), an infrastructure success; the Single Integrated Air Picture (SIAP), an applications failure (to date); and the Special Operations Command (SOCOM), an important model of a functional command, with both an instructive history and unique features.

DOD Intelligence Information System (DODIIS)

The DOD Intelligence Information System, known as DODIIS, comprises a collection of people and information systems whose mission is to provide intelligence to the military command structure. It is a twenty-five-year-old worldwide network, originally based on Arpanet technology, which has developed into a modern intranet that allows the intelligence community to share information and collaborate on information production. Thus, DODIIS is not merely a system; it is also a process that has functioned and evolved for over two decades to improve information systems in response to the growing information needs of military commanders and the increased opportunities provided by the explosive advances in IT.

While DODIIS is far from perfect, it is fair to say that the process has worked. DODIIS has moved ahead as rapidly as the information technology that supports it; indeed, DODIIS was a leader in the deployment of a wide-area intranet. At the same time, DODIIS has remained largely interoperable across all of the defense intelligence community. If the overall military C2 system were as technologically agile, as well integrated, and as cost-effective as the DODIIS portion of it, we could be confident that it was capable of supporting the RMA.

A particularly striking success was the development and deployment in 1994 of a system known as "Intelink," which enabled unprecedented collaboration and sharing of information between U.S. intelligence organizations using the just-emerging World Wide Web technology. DODIIS had already created and maintained a worldwide secure network that was fully modern by commercial standards, and had built a community of technical experts who worked in close coordination with the producers and consumers of intelligence information. Funding procedures were in place that allowed a response to an opportunity without years of effort to define a "requirement." For these reasons, the community was able to deploy an intelligence equivalent of the World Wide Web within six months of the time that browser technology advanced to the point where this was possible.

The success of DODIIS has resulted from several factors. First, DODIIS has always supported the Defense Intelligence Agency (DIA) system of "delegated production," in which intelligence analysts located at the various major commands around the world are responsible for generating intelligence products relevant to the commands they serve. Thus, for example, analysts at U.S. European Command produced estimates of the Soviet order of battle in Europe, while analysts at the Strategic Air Command (later Strategic Command) produced estimates of the strategic nuclear threat. These analysts used data from national intelligence systems as well as theater systems, and had to supply their products to DIA. This created a continuing need for interoperability between DODIIS systems at the commands and DODIIS systems at DIA headquarters — not simply connectivity, but interoperability at the data element level. Two points deserve emphasis here. Interoperability was not just desirable, but essential, if the DODIIS users were to do their jobs. Also, interoperability was used and thus tested on a daily basis, not only during occasional conflicts or exercises.

Second, most DODIIS systems have been funded through the General Defense Intelligence Program (GDIP) rather than through the ordinary service budgets. This funding mechanism had three desirable impacts. First, while the GDIP as a whole must compete annually with weapons systems, operations costs, etc., for funding, individual items of value to DODIIS had to compete for funding only with other intelligence capabilities, and decisions were made by a

staff that understood the value of DODIIS. Second, when funding shortfalls or technical difficulties required that some DODIIS requirements go unmet, the decisions on what to buy (or what not to buy) were made by a joint function rather than by a service, so that interoperability was less likely to be sacrificed. Third, when several systems with similar functions were available or under development by several different organizations, it was politically possible to choose a "best of breed" and insist that other systems migrate toward it.

Third, DODIIS systems were usually built, maintained, and used by a relatively small community of government and Federally Funded Research and Development Center (FFRDC) personnel who came to know each other and understand one another's perspectives. Regular meetings to address DODIIS issues enhanced this shared understanding.

Fourth, the leadership of DODIIS (including, significantly, the GDIP managers who controlled the money) believed in change, taking the attitude that "new technology represents opportunity" rather than "if it ain't broke, don't fix it" or "set requirements carefully and then leave people alone to allow them to meet the requirements." This leadership helped counter the risk that the small community of DODIIS experts would become responsive to each other's preferences rather than to the needs of the warfighters.

As a result, the system for managing DODIIS relied upon frequent incremental changes and the sharing across organizations of solutions to problems. This helped to keep DODIIS responsive to changing technological opportunities as well as changing user needs. It also provided a correction to the tendency of technical improvements to disrupt the interoperability of systems that change at different rates. It is symptomatic of this management approach that a revolutionary change — Intelink — was introduced as a rapidly and cheaply developed prototype, which then became operational in response to user demand. It is equally symptomatic that DODIIS standards were called a "reference model" rather than treated as something graven in stone that could dictate every decision.

Single Integrated Air Picture (SIAP)

For more than four decades, the U.S. military has been struggling to create a "single integrated air picture" — that is, a situation in which all U.S. forces concerned with a given region of airspace can know (and agree on) the track of each object flying there. The objective of

the SIAP is, informally, "a single track on each piece of metal in the sky." Despite years of effort, this objective has never been achieved.

Obtaining adequate data on everything flying in the airspace requires multiple sensors. Translating the raw data from these sensors into accurate tracks for airborne objects requires multiple communications links, multiple computer systems, and multiple command posts. But in practice, these multiple sensors and multiple data processing arrangements produce conflicting, competing, confusing, and redundant information. The fact that these sensors and processing systems are developed and owned by separate services compounds the formidable technical problems.

The crux of the matter is that no single sensor is perfect. Sensors and the associated communications and computers are designed with specific purposes in mind, and hence all of them see some things better than other things. Consider an enemy aircraft that is sensed by three different systems. One system may provide the most accurate information about its location, another about the type of aircraft, and a third about its velocity. If the data from all three systems are combined correctly, then we know what we need to know. If they are combined incorrectly, we may believe there are two or even three enemy aircraft — or worse still, two enemy aircraft and one "unknown" aircraft that might be friendly. The failure to obtain a reliable SIAP has three serious consequences: first, the failure to detect enemy activity early enough (for example, in using a ship-borne radar meant to cue a land-based interceptor missile); second, the risk of fratricide through misidentification of aircraft, or the risk of failing to attack an enemy aircraft due to fear of fratricide; and third, the inability to prosecute a battle on the basis of the clearest possible knowledge of what is going on in the battlespace.[2]

The failures that undermine interoperability have been called the "five deadly sins." They are:

- the lack of a common geospatial reference frame;

2. This ability is central to achieving "information superiority," a concept originally developed in a Joint Staff publication entitled *Joint Vision 2010* (Washington, D.C.: U.S. Joint Chiefs of Staff, 1996), and since used throughout the DOD to guide the evolution of C2 capabilities. The concept has been reaffirmed in the recent publication of *Joint Vision 2020* (Washington, D.C.: U.S. Joint Chiefs of Staff, July 2000).

- the lack of a uniform method for aligning platforms with true north;
- the lack of a common time reference among the platforms;
- the inability to correlate tracks from a local sensor with those from remote sensors; and
- the limited ability to use existing intelligence data to assist in the interpretation of observed data.

Each of the services has largely solved the first three problems — geospatial frame, compass alignment, and common time reference — for its own systems, but each has a different solution. The fourth and fifth issues — correlating data from local and remote sensors, and use of existing intelligence for interpretation — pose technical difficulties, but to achieve a SIAP, the tactical data links that carry and process the sensor information would have to be fully interoperable. Thus the services must arrive at common solutions to these technical problems as well.

In 1994, the Assistant Secretary of Defense for Command, Control, and Communications (ASD C3I) promulgated a standard called "Link 16" and directed the services to move toward implementing it. However, the interoperability problem has proven too complex to be dealt with by means of a single standard. At present, the Link 16 standard consists of several hundred pages of detailed technical information, but it still requires interpretation and technical judgments. Because no organization or mechanism exists to coordinate the judgments made by the many different programs implementing Link 16, different systems comply with the standard in different ways and cannot exchange data well enough to achieve a SIAP.

Recognizing that the individual requirements for individual platforms and systems do not include adequate demands for interoperability across systems and across services, the Joint Chiefs have created a Capstone Requirements Document (CRD) to address the need for interoperability. The initial CRD was relatively general in nature, and in 1999 DOD made an effort to centralize the funding needed to implement it under the sponsorship of the Ballistic Missile Defense Organization and the Joint Theatre Air and Missile Defense Organization. The services objected that this would impinge on their

responsibility to procure systems under Title X of the U.S. Code.[3] In response, the Joint Chiefs are drafting a more detailed Capstone Requirements Document.

However, the experience of several decades suggests that the critical decisions will be the engineering trade-offs necessarily made in the course of developing or modernizing any state-of-the-art system. At any given moment in time, the constraints of technology, budget, and schedule always require that some performance objectives be compromised in order to achieve others. A more detailed Capstone Requirements Document is unlikely to change the priorities of the individual system program offices, which tend to assign the highest priority to functionality, the second to interoperability with other systems of the same service, and only the third to joint interoperability.

Thus, efforts to attain a SIAP have two shortcomings. First, they lack a system that would drive those who make these trade-offs to place a sufficiently high priority on the requirement for interoperability with systems developed by other services, even at the expense of functionality desired by the service developing the platform or sensor. Second, there is no mechanism by which departures from interoperability are observed and recognized very quickly, so that they can be remedied without extensive redesign.

Special Operations Command (SOCOM)

The U.S. Special Operations Command (SOCOM) was created in 1987 by congressional action, which also gave this command its own acquisition authority, independent of the services. Congress did this, over the objections of the services, because of two perceptions: first, that the services never had given and never would give adequate priority to procuring equipment designed for the particular needs of the special forces rather than the needs of the "mainstream" forces; and second, that the debacle of the Iranian hostage rescue mission had resulted from the inability of the special operations forces of the various services to make joint plans and conduct joint training. Taking advantage of this unusual degree of autonomy, SOCOM has succeeded in forging a generally effective C2 system. The operations conducted by SOCOM units have demonstrated that joint C2 has become a reality in SOCOM.

3. Title X of the U.S. Code is the federal law that gives the services the responsibility to organize, train, and equip their forces.

SOCOM has from its inception placed a very high priority on understanding the needs of the regional CINCs who actually employ the special forces that SOCOM trains and equips. This has led to a heavy emphasis on making its C2 systems fully interoperable with those of the CINCs, even at the expense of standardization. For example, a special operations unit that moves from the Pacific Command to the European Command may require two full days to modify its organic C2 systems (applications on ruggedized laptop computers, etc.). If the bad news is that this is necessary, the good news is that it is possible and commonly done.

Consequently, SOCOM's organic C2 is effective, but expensive. Today, a decade and a half after its inception, SOCOM is engaged in a major effort to rationalize its C2 systems, retaining their effectiveness and their interoperability with each other and with the systems of the "mainstream" forces, while reducing their cost.

The main lesson we draw from the SOCOM experience comes as no surprise: a high degree of C2 interoperability and effectiveness is achievable if an organization is guided by joint priorities. Whereas the services procuring C2 systems for mainstream forces usually have other, higher priorities than interoperability with the other services or interoperability with all of the regional commands, SOCOM's priorities have been driven by its structure as a joint organization, and its recognition that it must retain the political support of the regional CINCs to survive. Congress has been supportive of these priorities, and indeed has frequently added funds to the SOCOM budget requested by the President. Like DODIIS, SOCOM has also benefited from being a relatively small community, within which it is possible to attain and sustain mutual understanding.

Finally, another contributing factor is that SOCOM's forces have frequently been involved in real operations against real enemies. SOCOM likes to think of itself as the "911" of the U.S. military, and considers a high state of readiness and a high operational tempo to be normal. One consequence is that SOCOM's C2 systems are frequently tested in operational conditions, thereby ensuring that any failures of C2 interoperability will be noticed and also that such failures will be remedied on an urgent basis. This is another parallel with DODIIS.

LESSONS LEARNED

The first lesson we draw from these cases is that joint C2 is never easy but is clearly worth the effort. An effective horizontal function in a vertical world requires continuing effort, and success will never be complete or final, but much can be achieved. In addition, we can identify from these case studies a set of more specific factors that seem to have facilitated success.

"Continuous" Use Through Day-to-Day Operations and Frequent Exercises and Tests

C2 capability — as built from C4ISR building blocks — has at least two important attributes. First, it has no utility until combined with people and procedures in an operational context to perform a mission. Second, its set-up and operation are complex, and often "the devil is in the details." The first point drives a need for continuous use as part of continuous learning, leading to co-evolution of the systems, the people, and the doctrine. The second point also suggests the need for "mission thread testing," that is, testing the complex chain of systems that must operate together effectively to accomplish a mission.

A Substantive "Blueprint" for Centralized Guidance and Decentralized Execution

The notion of a "blueprint," substantive but not prescriptive in detail, is crucial. Decentralized execution within a common framework established by such a blueprint has established itself as a formula for success in at least some cases. It allows local flexibility to accommodate local needs, and enables innovation. As a corollary, the advocate of the blueprint must engage in follow-up activities with the developers responsible for the building blocks.

Dedicated Funds for at Least Core Activities and Implementations

Dedicated funds under the control of the organization responsible for the mission are a prerequisite to success in order to orchestrate and integrate CINC, service, and agency efforts successfully. This need not involve control of all funds in the domain (e.g., C4ISR), but should include control of funds to support core activities, such as exercise, experimentation, and interoperability or integration "augmentations" to CINC, service, or agency activities.

Technical Capability Committed to the Horizontal Challenge

There is a compelling need for substantial, broad-based technical capability within or attached to the organization responsible for the mission and for integrating the CINC, service, and agency efforts. This technical resource must be structured and provided with appropriate incentives to assure that it has no other interest than that of the government as a whole. This capability is needed for formulating a technically based blueprint, informing budgetary and programmatic decisions, and brokering user needs to developers.

Adding Value and Building Trust

It is crucial that the central authority take a strong user-support orientation, add value for the users, and develop trust over time. When pushing for the "common good" across organizational boundaries, two key ingredients for adding value are, first, appreciating and struggling to accommodate legitimate local interests, and second, providing funding for "common good" investments that would otherwise be viewed as unfunded mandates. If this is done well, another essential ingredient for success is created: a sense of shared mission and community.

Interoperability is a Process, Rather than a Decision

There is no such thing as a complete "specification"; in fact, total reliance on completely specified requirements will result in failure. Interpretation and interaction are needed for the ideas embodied in the requirements to evolve. Moreover, enforcement by dictum will not work; the community is too large, the topics too complicated, and the failure paths too many to issue "orders" as mandates and simply expect them to be executed.

RECOMMENDATIONS

We have outlined the problems plaguing joint C2: problems of inadequate readiness, the difficulty of achieving horizontal integration in a vertically funded world, and delays in implementing technological and doctrinal innovation due to a turgid requirements-based acquisition process. These issues could be alleviated if:

- a worldwide Joint Task Force (JTF) C2 baseline system configuration existed;

- the baseline C2 system evolved through continuous daily use and interaction between the developers and the users in a requirements discovery process;
- the commands and services practiced assembling, adapting, and operating these joint C2 systems for JTF deployment scenarios;
- the component systems of the C2 system shared an integrated technical infrastructure;
- the service systems that comprise the JTF C2 system were designed from the outset to be more adaptable and interoperable;
- detailed joint mission analysis developed a blueprint for integrated and interdependent service systems, leading to true specialization for service development activities, rather than today's redundancy; and
- acquisition agencies had a defined wartime support role and trained for deployment with C2 systems.

To achieve these ends we recommend four major organizational and management changes. U.S. Joint Forces Command (USJFCOM) looms large in these recommendations. The recommendation call for taking further steps along a path that began with giving the U.S. Atlantic Command (ACOM) significant functional responsibility in 1993 for training and providing CONUS-based forces to support the needs and operations of other CINCs. Effective in October 1998, ACOM was assigned responsibility for the DOD's Joint Experimentation Program.[4] This program calls for a broad range of experimentation activities to explore new ways of fighting using IT as a key enabler. That same year, a number of important joint activities were attached to them.[5] In October 1999, USACOM was rechartered as the U.S. Joint

4. Joint Experimentation provides for exploring and validating future joint operations and concepts that will drive changes to doctrine, organization, training and education, material, leadership, and people (known collectively as DOTMLP).

5. These joint activities included the Joint Warfighting Center (joint training and doctrine), the Joint Battle Center (joint C2 capability and interoperability), and the Joint Communications Support Element (rapid-response deployable communications in support of crisis and contingency operations).

Forces Command, with a broad set of responsibilities for supporting joint operations, including that of Joint Force Integrator.[6] However, these programs are add-ons to existing service and CINC C2 systems, not integral parts of them. The recommendations that follow call for a major increase in both the role and the responsibility of USJFCOM. They would give USJFCOM the responsibility, authority, and money to create a joint C2 capability and to test and train with it prior to deployment. The result would be a USJFCOM with a dominantly functional role, a strong focus on joint C2, and the teeth to carry out its joint force integration role.

Put a Single Organization — USJFCOM — in Charge of Joint C2 and Make It Accountable

DOD should make USJFCOM the supporting CINC for C2, and strengthen its role as Joint Force Integrator. When a regional CINC requires a joint operation, USJFCOM would be responsible for rapidly augmenting, assembling, delivering, and operating a properly tailored joint C2 capability at the operational level of command (CINCs and Joint Task Forces). Today a joint C2 capability does not come into existence until troops have deployed and solved all the interoperability problems, weeks or months later. Under this recommendation, one organization would have the responsibility for creating and enhancing the joint C2 capability during peacetime so that the capability is ready when needed.

Stated differently, the ability to exercise joint C2 effectively can be thought of as an issue of readiness. Like other dimensions of readiness, it requires constant effort, and it costs money. But it is essential if the United States is to have an actual rather than merely a potential military capability. Thus it is necessary to give a single organization the authority and accountability for developing horizontal joint C2 across the existing vertical realms.

As a result of the recommendations that follow, USJFCOM would be able to provide core suites of deployable C2 capability for rapid-response, early-entry operations, which would complement the communications capabilities of the Joint Communications Support Element; deploy rapid-response, expert C4ISR "tiger teams," com-

6. The 1999 Unified Command Plan (UCP-99) assigned the rechartered USACOM as USJFCOM.

prising USJFCOM personnel, service experts, or contractor personnel, to support the inevitable adaptations required during real-world situations; and provide tools and trained personnel to support a CINC or JTF commander with the crucial task of configuring and managing joint networks.

Create an Office in USJFCOM to Exercise and Experiment Continuously, to Ensure that Joint C2 Systems Work and are Ready when Needed

To make more rapid progress in joint warfighting, and to stay ahead of others who have the same access to emerging IT, the U.S. military must increase the rate of evolution by creating many more opportunities for the services to experiment and train in joint situations. Identification of requirements and changes in joint concepts of operations can occur more rapidly if organizational and management structures exist that enable the services to experiment, exercise, train, and equip for C2 functions frequently and together. With the right management structures and leadership the services, their systems, and their concepts of operations can evolve together from traditionally vertical service C2 systems into an interdependent horizontal dimension that supports inherently joint functions. After all, that is how they will fight.

Today, in a crisis, the service-unique components of the C2 system are deployed to the field and connected in *ad hoc* arrangements that attempt to fit the situation. The adaptation is often limited by the incomplete knowledge that the deployed forces have of these systems. In many cases contractors must accompany the systems to the field to make them work or to adapt them to the specific situation. New systems, not yet fielded but near enough to production to be useful, are also rushed to the battlefield with contractor support in the expectation that they will provide some additional advantage (as, for example, with JSTARS, a ground surveillance system, in the Gulf War). To complicate the situation further, coalition partners throw their own systems into the mix.

This chaos in times of crisis will never be eliminated, but it can be managed more effectively and can produce a more effective C2 system faster. To this end, we propose an activity that is a cross between an exercise and an experiment, for which we have coined the name "expercise." It would be both an experiment, in which many changes to C2 are tried and failure is allowed, and an exercise, in which war-

fighters are trained in assembling, adapting, and operating C2 systems. The expercise would consist of operating a joint C2 system in a scenario-driven environment on a daily basis. Warfighters would operate this system in realistic scenarios, and they would be accompanied by and interact with the IT specialists who developed the C2 systems. The warfighters and developers would incrementally improve the C2 systems by working out the technical interoperability problems in the "expercise" environment rather than in an actual crisis. They would also discover requirements through constant use of the system, learning how to make C2 processes more efficient and how to fix persistent interoperability issues. Constant use would be critically important. Like F-15 fighters who train daily to be the best pilots they can be, C2 operators must use their systems daily to become proficient at C2 and understand how the supporting systems can be improved.

A continuous expercise would mean the dedication of expensive resources — people and equipment — that must be funded and staffed properly. We therefore recommend establishment of an Expercise Office, located within USJFCOM, that would be responsible for:

- working with the regional CINCs to devise a range of CINC operational plans, and with the services to define a C2 system structure to implement the operation;
- creating a JTF C2 system that supports these operational plans;
- providing the means by which the JTF C2 system can measure performance of C2 functions and monitor their continuous improvement;
- managing the execution of these regional CINC-based scenarios, using the JTF C2 systems staffed with warfighters and developers described above;
- conveying the requirements learned from these expercises to the service acquisition agencies for implementation;
- appointing a service as the executive agent for the acquisition, on behalf of all the services, of a joint system for any entirely new capability that might be discovered;
- developing modeling, simulation, and instrumentation as needed;

- maintaining updated descriptions of the configurations; and
- establishing active liaison with all other joint exercise activities to garner the lessons learned and apply them to joint C2 acquisition.

If successful, the expercise process will create joint C2 systems for each CINC that offer good starting points for adaptation to a specific deployment. Furthermore, and perhaps more important, the staff running the expercise process will form a cadre of personnel trained to adapt the C2 system quickly to new situations.

The normal expercise would look like a command post exercise but should be augmented periodically with live exercises, in which the equipment and troops are actually deployed. The military organization supporting a given expercise must be complemented by a dedicated, strong technical work force on the order of a hundred people, with attributes that we discuss below. The expercise emulates for C2 the Intelink/DODIIS model of development, in which intelligence systems were used every day and thus evolved rapidly. The expercise must use scenarios and simulations, unlike Intelink, to create an environment for daily use, but only with such constant use can interoperability issues be resolved and requirements discovered and implemented. Infrequent exercises would allow the use of "workarounds" that are effective only for the short duration of the exercise. In the expercise, by contrast, requirements would be derived from discussion between the users who are the real warfighters (rather than their representatives) and the developers. The expercise organization would then work closely with the service that would acquire and maintain the system to implement the requirement.

Use of the expercise would institutionalize, in the joint environment, the successes of the individual services. Examples of such successes include the following:

- The introduction of collaboration technology into the Air Force's Expeditionary Force Experiment dramatically decreased timelines for creating the Air Tasking Order by turning serial processes into parallel processes.[7] The reduction was accomplished by installing software on existing workstations that allowed geographically

7. The Air Force Expeditionary Force Exercise is an annual live-fly event in which the Air Force field deploys its C2 systems and experiments with new technologies and new concepts of operations.

separated individuals to work cooperatively and synchronously across a network.

- The Navy's command ship, the *Coronado*, was designed from the start to be reconfigured. Experimental systems are installed and exercised at sea, and then removed, refined, or made part of the operational system after the exercise.
- The Army's Task Force XXI experiment used "quick and dirty" installation of situation awareness displays on individual combat vehicles, along with digital tactical networks and collaborative technology for intelligence analysis, to prove the effectiveness of total situation awareness on the digitized battlefield.

In all of these service activities, innovation has been encouraged, technology inserted, and "failure" allowed. In none of them was the test community hovering around to pronounce the activity dead because some predetermined quantitative measure was not achieved. Instead, the services discovered requirements and took advantage of technological opportunities, emulating the commercial practice of shipping a product, learning from its users and the competition, and continually improving the product. The users who were trained on the systems and the developers who could adapt them teamed to make the systems work and to improve their functionality continuously.

Expercises would lead to constant interaction between the developers and the warfighters, who could thus continuously refine the interoperability, adaptability, and integration of the system and the concepts of operations prior to deployment. This model, in which discovering what the warfighter needs will lead to incremental improvement, more closely resembles the commercial relationship between marketing and product development, where new versions of products are churned out at a pace measured in months rather than years. In some cases, an expercise will identify an entirely new capability, and the expercise organization would appoint an executive agent to acquire it.

Establish a Joint C2 Blueprint Office Within JFCOM

The bottom-up, incremental improvement process recommended above, as well as the ongoing joint experimentation activity which seeks operational innovation enabled by technology, must be com-

plemented by an activity which defines a C2 target architecture toward which to strive. We recommend that this be implemented in the form of a Joint C2 Blueprint Office that would be charged with defining and developing a common, adaptive, and agile C2 infrastructure, and with driving the evolution of service-provided mission systems toward the effective and efficient support of joint operations. The activity would focus on providing a robust and rich set of information services that respond to and support operational innovation, maximize the exploitation of rapidly advancing commercial IT, and provide the foundation for extensive data networking down to the tactical level. The mission capability effort would be focused on assuring that service C2 system developments support and respond joint operations needs, as defined by the top-down joint experimentation activity and the bottom-up expercise process, as well as by the results of service multilateral efforts.

The Office of the Assistant Secretary of Defense for Command, Control, and Communications and the Joint Staff (J-6) have adopted the concept of a Global Information Grid (GIG), and are implementing it as a framework for guiding service and agency developments. Operational and system architecture efforts have begun. The current focus is on information system infrastructure. These efforts are applauded. However, responsiveness to the needs of the joint warfighter would be substantially strengthened if responsibility for C2 capability evolution were put more in the hands of an operational command. Additional funding leverage is also needed if substantial progress is to be made in orchestrating the programs of the services and agencies.

The Blueprint Office recommendation targets these shortfalls. The office would be responsible for experimenting with commercial technologies and guiding how systems should be implemented with standards that enable interoperability and integrated systems. The underlying architecture would rely on the capabilities provided by standards-based commercial technologies that allow and promote data sharing (e.g., web-based technologies such as extensible markup language [XML] and application service provider models). The Blueprint Office would be responsible for understanding the technical trajectory of the commercial world and its implications for new systems and legacy systems. It would test new technologies and develop guidelines for program managers of new systems and legacy

systems, to enable as much inherent interoperability among systems as possible. The architectures and guidance defined by this group would give the developers freedom to experiment in those areas of the technical architecture for which no single standard or solution is generally agreed upon among the commercial and military technical communities. From this diversity of approaches, clear winners would emerge and be included in new versions of the guidance.

In parallel with this focus on developing the blueprint for a common technical infrastructure, the Blueprint Office would build upon its JFCOM foundation (doctrine, training, experimentation/exercise, deployable capabilities) and work across the broader community to conceive, test, verify, and assure the acquisition of capabilities that support joint operations. The focus would be on a robust, modern infrastructure and mission systems that enable and support innovative doctrinal changes. Specifically, the Blueprint Office would, first, define concepts and drive the acquisition of C4ISR infrastructure and mission systems that would not otherwise evolve in response to the formal requirements process or the continuous joint expercise activity, but would be driven by potentially radical changes in joint warfighting concepts of operation emerging from joint experimentation or by new commercially based technology applied in innovative ways. Second, within this process, the Blueprint Office would identify common capabilities needed by CINCs or services whose acquisition could best be, but are not yet, managed centrally. The Blueprint Office would identify management options in such a case, such as a single service serving as the DOD's executive agent for acquiring particular capabilities. Finally, the Blueprint Office would place emphasis on maximizing adaptability and assuring interoperability in the technical infrastructure, by providing guidance regarding the design choices that the service acquisition agencies may make as they build and improve upon their systems.

This does not mean that the Blueprint Office would or should design a joint C2 system in detail as if it were simply a matter of specifying and executing. The lessons from past successes demonstrate that concepts of operations, system design, and implementations cannot be mandated or created top-down in organizations as large as the DOD or when problems as complex as C2 are involved. (See, on this point, Chapter 7.) The output of joint blueprint development should be minimally prescriptive but with appropriate incentives and enforce-

ment provided for the fundamentals (e.g., adopting the Internet paradigm).

The Joint Blueprint Office thus would develop the concepts for a highly agile C2 system able to adapt to a given situation and theater across a wide range of scenarios and circumstances. The resulting infrastructure would enable radical changes: changes that would not occur automatically through the expercise process because of the attendant political problems associated with the adjustment of service responsibility. The Blueprint Office would work with JFCOM experimentation and recommended expercise activities, with the Joint Staff, and with the CINCs to identify the critical mission activities and functions that are inherently joint. Initially, a few inherently joint missions or capabilities, such as theater missile defense or the Single Integrated Air Picture (SIAP), would be identified as a basis for "mission thread" experimentation and analysis. The Blueprint Office would look for efficiencies enabled by technological innovation in C2, intelligence, or weapons systems, or by eliminating redundancies. This would be akin to the concept of disintermediation in Internet business models that eliminate "middlemen," whose functions are replaced by a more direct flow of information (as, for example, bookstores are disintermediated by Amazon.com); such concepts would be investigated in parallel within the Joint Experimentation program.

Returning to fundamentals, this recommendation is part of a larger mosaic whose objective is to place the responsibility, authority, and capability for joint C2 capability evolution — with exploitation of advanced IT as a central theme — into the hands of JFCOM, the warfighting command that has been given the Joint Force Integrator job, along with an important but incomplete set of tools for its accomplishment. The Blueprint Office, in concert with other elements of JFCOM and the broader community, would orchestrate an end-to-end process for C2 capability evolution, ranging from exploring new doctrine and concepts within the framework of the Joint Experimentation program, through analyzing C2 contributions to mission effectiveness, to driving service and agency acquisitions toward realizing the RMA. The notion of a Blueprint Office has been developed here to make the objectives, responsibilities, and activities tangible. Addressing the topic of whether such an "office," as such, would even appear on a JFCOM organization chart, and how it would relate to other DOD activities, would be an important next step if agree-

ment could be reached on the basics. In any event, the recommended JFCOM blueprint activities would receive direction and ultimately derive delegated authority from both OSD — the Under Secretary for Acquisition, Technology and Logistics, and the Assistant Secretary for C3I in his or her capacity as Chief Information Officer — and the Joint Staff.[8]

Funding mechanisms as related to both enforcing and motivating all of this are addressed in the recommendation that follows. A later section deals with the other resource crucial to success: a skilled and dedicated workforce.

Centrally Fund Joint C2 Activities Through a New Joint C2 Integration Program Administered by CINC USJFCOM

Unfunded mandates for joint command and control would accomplish nothing. The money for the Expercise Office and the Joint Blueprint Office must come from a combination of a Joint C2 Integration Program, and the budgets for the services and the individual systems managed by the services. We propose the creation of such a new Integration Program, modeled after the General Defense Intelligence Program that provided the centralized funding that allowed DODIIS to succeed. The Commander-in-Chief of USJFCOM, as manager of the Integration Program, would balance the trade-offs internal to joint C2, free of service priorities and other entities competing for funds. He or she would annually allocate funds to requirements and recommend acquisition agencies. This funding would provide resources for the recommended new activities within JFCOM (the expercise process, the Blueprint Office) as well as for involvement in these activities by CINC and service C2 personnel and assets.

Additionally, this funding would be targeted on providing new or modified capabilities within service or agency programs to achieve the blueprint, thereby addressing the unfunded mandate issue. Much as the GDIP did for intelligence, it would create a C2 community, all

8. The Chief Information Officer (CIO) function was mandated by the Information Technology Management Reform Act of 1996 (P.L. 104-106). (This act and the Federal Acquisition Reform Act [FARA] of the same year are commonly referred to as the Clinger-Cohen Act.) It calls for a CIO position within each federal department or agency, and for performance-based management of IT investments and further streamlining of acquisition. The DOD ASD C3I is designated as the DOD CIO.

of whose members are dedicated to the same goal, with autonomy across the CINCs. This would allow each command to adapt the systems for its own situation and purpose. Ideas, architectures, and software developed centrally or by a CINC could be shared with and adapted by the other CINCs.

Thus, the Joint C2 Integration Program would fund the services' acquisition of joint requirements derived from expercises, as well as the expercise process itself, which needs funds for the expercise C2 systems, the USJFCOM personnel to operate them, and the regional CINC personnel to set CINC priorities, define scenarios, and judge usability. DOD has many activities underway to work on interoperable C2, some more effective than others. As this new process is implemented, DOD must examine the utility of these activities and either consolidate or eliminate them as appropriate.

Inherent in the expercise notion and funding model are two basic changes in the way systems are funded. The first change is that it allows managers to fund opportunity, not requirements. This notion is important; it is how commercial companies stay in business and prosper. When a new technology emerges, commercial companies invest in the opportunity to improve products, lower production costs, or extend themselves into a new business area. If the United States is to maintain a technological edge over adversaries, DOD must also be allowed to fund opportunity to speed the insertion of technology into defense systems. The Expercise Office and the Blueprint Office would have funding lines similar to the CINC Initiative funds to support experiments and the newly discovered requirements. Such unrestricted funding is not popular with Congress, but it is essential here in order to overcome one of the major obstacles to success: the funding handcuffs that hamper the acquisition community's agility to cope with rapidly changing technological opportunities.

The second change has to do with the funding cycle itself. No commercial company buys a network, maintains it until it cannot be maintained any longer, and then throws it away. Instead, companies have annual budgets to upgrade their networks and make trade-offs between maintenance activities and upgrades. As a GDIP-like funding source, the Integration Program would allow C2 systems to emulate this commercial practice. It would construct funding profiles that support incremental improvement of the software capabilities and recapitalization of the hardware on a reasonable schedule, and

adapt them annually. In this way, the systems would improve faster, last longer, be better managed, and cost less. Again, this runs counter to current practice, and members of Congress would lose some ability to claim credit for new programs and new contracts in their states and districts because there would be fewer new starts. However, they would maintain oversight over how the money is spent.

These four recommendations — accountability, expercise, blueprint, funding — address the fundamental difficulties with rapidly evolving a robust, modern IT–enabled, joint C2 capability ready for rapid deployment. We now address the other side of the IT revolution — the cyber battlefield.

Cyber Information Operations

"Information operations" are defined in various ways throughout DOD, with different definitions offered by the services, CINCs, and agencies. The lack of an accepted lexicon has led to much confusion, and the diffusion of responsibility has led to duplication, inefficiency, and increased cost as well as missed opportunity. In this section, we address "cyber information operations" as a subset of information operations, defining the term to encompass the systems composed of computer networks used in critical warfighting operations, and not the general use of IT or the more traditional electronic countermeasures and counter-countermeasures. The discussion of the topic is divided into two portions, one concerned with so-called computer network defense (CND), and the other concerned with electronic attack through the use of techniques to disable, interrupt, or otherwise inhibit the enemy's use of its system, called computer network attack (CNA).

The previous section discussed the concept of network-centric warfare. This concept links weapons, sensors, and command centers as needed. The architecture permits components to be added or subtracted as circumstance change, and reach-back allows support centers and weapons that may be thousands of miles apart to operate in a single network. Therefore, CNA is directed not at a pre-specified set of facilities, hardware, or software, but at whatever is critical to the performance of a key warfighting function. CND must address the defense not just of the network as it functions today, but of all the configurations of the network that a commander might find useful.

COMPUTER NETWORK DEFENSE

Network-centric warfare offers dramatic advantages, but they carry with them the risk of a major loss of capability if the network is disrupted. The more the United States relies upon computer networks to get information to its warfighters, and the more our military concepts of operations exploit the advantages of having very good information, the more important it becomes to defend these computer networks.

In dealing with CND, we must distinguish between the "outsider" threat and the "insider" threat. Most of the effort in defensive technology has been devoted to dealing with the outsider — the hacker who seeks to penetrate the network or overwhelm it. The insider threat is potentially much more serious, because an individual with legitimate access to a critical node can easily disrupt the network, copy sensitive information, or (with greater difficulty) substitute false data for accurate data. The outsider threat requires technical solutions that involve the use of cryptography and related techniques whereas coping with the insider, while having technical aspects, puts demands on such practices as personnel assessments and periodic evaluations. (See the discussion of this issue in Chapter 6 by Ashton Carter.) In the commercial world, only the financial services industry has paid serious attention to the insider threat, driven by the principle that it should never be easy for its employees to steal money.

Constraints of budget and schedule mean that there are always trade-offs in building or upgrading an information system. Frequently a program manager must decide whether to spend time and money on improving system protection or instead on system functionality. In DOD, as in the commercial world, functionality is what sells a system, and therefore programs experience constant pressure to shortchange security and protection.

Within DOD, the current mechanism for ensuring that a cyber threat is given due consideration is the System Threat Assessment Report (STAR), a validated formal document that is intended to be reviewed within the acquisition process. However, because of the difficulty of validating cyber threat, the process is ineffective in stimulating program managers to spend money on countermeasures.

Knowledgeable observers know that electronic commerce is far too vulnerable to electronic attack. Such attacks will eventually take place in ways that could cause major companies to lose large sums of

money, which will prompt industry to develop and deploy much stronger security measures than those in common use today. Through this process, the cost of effective security will decline as its availability increases. If this happens, DOD will of course purchase and make use of these new security technologies and products.

However, DOD cannot simply sit back and wait for industry to make network security affordable. First of all, with national security and the lives of our troops at stake, DOD cannot responsibly take the attitude that it must wait for a major disaster to create the demand for better security. Beyond that, DOD must assume that it confronts a far more sophisticated threat than that facing e-commerce. A foreign government bent on disrupting the critical warfighting networks of the United States can eventually obtain access to all the tools and techniques used by the hacker community, and it can develop additional CNA techniques that go beyond the hacker repertory.

A difficulty inherent in CND is that the attacker has the initiative, and the defender cannot know the time and place of the next attack. The standard military responses apply: vigilance and defense in depth. In the context of C2, defense in depth should include adopting the approach used by air traffic control. The designers of air traffic control systems know that bad weather will disrupt their systems, and that individual radars and computers will fail from time to time. They therefore design the overall system so that when failure or disruption occurs, there are procedures and systems already in place and fully tested that will permit continued operation even in a degraded mode. Air traffic control is designed so that even though bad weather or system failures may lead to delays, they do not compromise safety. C2 must be designed so that successful enemy attacks on our computer networks cause at most incremental losses of capability, but never a catastrophic failure.

COMPUTER NETWORK ATTACK

The ability to attack an enemy's critical computer networks will increase in importance as other countries modernize their warfighting information systems and move toward network-centric warfare. A critical characteristic of CNA, which creates numerous problems in planning its use, is its fragility. Many forms of CNA are most effective when the enemy does not realize that it is under attack, because they can readily be countered once the enemy learns exactly how the

attack is being carried out. For this reason, research and experimentation into the techniques of CNA are very highly classified and tightly compartmentalized. We believe this has led to considerable duplication of effort within the DOD.

The fragility of most CNA techniques means that there is no way of knowing how effective they will be until they are tried. Consequently, DOD has an urgent requirement for techniques to assess the effectiveness of our attacks in near–real time. Furthermore, DOD must develop channels that will let our own commanders know the extent to which the enemy has been crippled by CNA, with minimal risk of leaking information that would cause the enemy to repair its systems.

A related problem is that the choice of CNA techniques will not always be easy. Suppose, as an illustration, that we have identified a communications channel through which enemy headquarters sends orders to its field commands. One method of CNA is to destroy or jam this communications channel at a critical moment in the conflict, decapitating the enemy just when it most needs effective C2. A second method is to listen in on the communications, feeding information to our own commanders about the enemy's intent. This would be less certain to work, but more effective if it did. A third method would be to introduce spurious communications into the C2 channel, leading the enemy to do what we want it to do. This would be the least certain, but the most effective if it succeeded. However, the successful use of any of these techniques may limit our options to attack the enemy's C2 communications channel, or others like it, in the future. Such choices should be made by the responsible parties in the DOD, but they may have difficulty in learning enough to make a timely and informed decision.

BALANCING CND AND CNA

There is an inherent conflict between the requirements for effective CND and the requirements for effective CNA. This conflict arises whenever we discover a potential vulnerability in a computer network. If we keep this vulnerability secret, and if a future enemy does not independently discover the vulnerability and protect against it, then we can exploit it for CNA. But if we develop a defense against the vulnerability and deploy it widely in our own networks, we make it highly likely that the future enemy will learn about the vul-

nerability and the defense, and we will be unable to use it for CNA. However, if a future enemy discovers this vulnerability independently, and we have done nothing to protect our own networks against it, the enemy can use it to attack us.

In principle, we should evaluate the likelihood that a future enemy will discover the vulnerability independently, and act accordingly. In practice, we tend to be overly proud of our own discoveries, and slow to predict that others may be just as clever. This leads to a bias toward CNA over CND. This bias is reinforced by the fact that CNA is much cheaper than CND; they require broadly similar research efforts, but deploying an attack capability is far cheaper than modifying extensive networks to eliminate a vulnerability. Moreover, there are many possible enemies if one looks far enough into the future, and they are at different levels of technical sophistication. Preserving the ability to attack a less sophisticated enemy (by not deploying our defenses against a promising attack mode) may leave us vulnerable to a more sophisticated enemy that is able to duplicate our research.

Realign Responsibility for CNA and CND

The role given to the Commander-in-Chief for Space (CINCSPACE) under the 1999 Unified Command Plan encompasses both CNA and CND.[9] The activities are clearly interrelated through the need to understand vulnerabilities and to deal with decisions that balance the needs of defense against the needs of intelligence. However, other serious considerations must also be taken into account in choosing how to allocate these responsibilities.

We recommend that CNA, a warfighter function, remain with a CINC — CINCSPACE — but that CND, which is an infrastructure development topic, be treated as a criterion to be considered by developers in the acquisition community. Policy for setting criteria for

9. The U.S. Space Command (USSPACECOM) was created in 1985 to advance and orchestrate the role of space assets and capabilities in support of national security interests. USSPACECOM coordinates the use of service assets and capabilities to perform missions ranging from launching and operating satellites to providing space-derived information to military commanders. The 1999 Unified Command Plan (UCP-99) assigned responsibility for CND to USSPACECOM effective October 1, 1999, with assignment of CNA responsibility to follow.

CND systems should be established by the Chief Information Officer (CIO) within OSD. The policy will need to be adjusted for different situations, to deal with systems that range from protecting business and administrative systems to warfighting.

In recent years, leadership for policy issues has been provided through the Defense Department's Chief Information Officer (CIO). Substantial progress has been made toward providing leadership to the service and agency CIOs on a broad set of information management topics, including defensive aspects. Clearly, much more needs to be done, but it is recommended that the CND policy-development function become a primary responsibility of the CIOs and stay within the office of the ASD C3I, and that appropriate measures be taken to deal with the interaction between CNA and CND (discussed below).

The CIO function in support of CND should include the following related responsibilities:

- provide information-operations strategy and develop policy;
- provide military representation to U.S. national agencies, the law enforcement community, commercial industry, and our allies on CND issues;
- act as the user in setting requirements for the information assurance aspects of systems, working through the Blueprint Office proposed above, and expanding upon current activity, which is unduly focused on the short term and is underfunded;
- create a DOD common threat analysis center, consolidating the various current CND activities; and
- identify, develop, and oversee employment of best practices within DOD organizations for managing IT assets.

Above all, the CIO must act as an advocate for adequate computer network defense measures, even though such measures do not add functionality and are difficult, time-consuming, and expensive to implement. CINCSPACE, which currently has responsibility for CND as well as CNA, is poorly placed, as a field command, to participate fully in the process by which budgets for thousands of information systems are drawn up. Further, given that CNA is cheaper than CND and that the choice between them depends in part on an estimate of

our own efficacy relative to that of an enemy, the trade-offs between the two must be made at a very senior level.

Consolidate CNA Under a Single Organization

The development of USCINCSPACE as the DOD leader in cyber attack properly places responsibility at a CINC; it requires sustainable support. The organizational structure will take time to develop and will require not only funds, but also the attention of the key officials in DOD. Many related responsibilities of the services and agencies will require adjustment. USCINCSPACE may have to undergo the most profound change as it shifts its focus from conventional space activities to information operations. In our view, this new responsibility requires that CINCSPACE must:

- lead the effort within the DOD to reduce duplication of effort and consolidate resources, including clarifying the security and special access needs of information operations;
- establish minimum training, certification, and accountability standards for commanders with regard to CNA; and
- create a new functional component within CINCSPACE, which we would call the Joint Force Information Operations Component Commander (JFIOCC), to support Joint Task Force and CINC operations with respect to CNA.

The JFIOCC would represent a single point of contact to articulate CND and CNA activity to commanders in military terms (an improvement over the current situation in which commanders must deal with various intelligence agencies and service components, each with its own terminology). The resulting military-to-military interaction should provide significant improvement in effectiveness. In this role, USCINCSPACE would act as a supporting command, similar to the way in which it supports other functions, analogous to the way the Special Operations Command provides unique warfighting support. In its role of advising on military operations, the JFIOCC, in coordination with others as needed, would make the decisions to use CNA, balancing the various priorities against each other.

This consolidation also implies a critical set of actions regarding personnel: the creation of a highly trained group of officers specializing in CNA. These officers would have to bridge the gap between researchers on CNA techniques and field commanders whose own

expertise is in more conventional forms of warfare. They should also be able to bridge the gaps across the various compartmentalized research efforts conducted by a variety of separate organizations, although this would involve subjecting them to extremely intensive security investigation and accepting the risk of trusting them with a very large quantity of critically sensitive information.

Focus CNA Development

We have proposed giving USCINCSPACE the task of managing the CNA function for budgeting, and for managing deployment and operations. Responding to CINCSPACE direction, the National Security Agency (NSA) would be the interface with the intelligence community and will coordinate the technical development, either directly or through its service cryptologic elements. NSA would thus become an acquisition arm for this function, acting much like the service acquisition organizations for CINCSPACE. NSA would provide leadership in the intelligence community similar to the way cryptologic activity is managed today. Other organizations would be tasked by USCINSPACE to provide support in their areas of competency.

Create a Laboratory for CNA and CND

One of the main arguments for keeping the CNA activity apart from CND is that many vulnerabilities are fragile, meaning that if they are revealed by the CND elements, the CNA efforts that take advantage of these vulnerabilities would be reduced in value. We recommend that a laboratory be established under USCINCSPACE to model realistic networks and explore techniques and countermeasures. This laboratory could develop countermeasures in parallel with the evaluation of a potential CNA. If a CNA technique were judged viable, then a decision could be made at that point whether or not to develop and deploy the countermeasure. The countermeasure would be deployed if doing so would not reveal the vulnerability. Even if it were not deployed immediately, it could be deployed later if needed. If a CNA technique were judged not to be viable, the United States could still deploy the countermeasure in case our enemies make a different viability judgment. The key to making this work effectively is to ensure that experts be made available for the evaluation, at least for a limited period of time.

Stimulate Development of Protection by Creating an Information Assurance Institute

The topics of cyber attack on the U.S. infrastructure and the role of the DOD have been discussed since the 1997 Report of the President's Commission on Critical Infrastructure Protection.[10] In response to the report, Presidential Decision Directive (PDD) 63 and PDD 64 mandated a number of actions, most notably the creation of the National Infrastructure Protection Center at the FBI. Other actions mandated by these two PDDs, such as encouraging private/public information sharing on such matters as cyber attack descriptions, have had only limited success. While commercial industry will eventually make the kind of investment necessary to protect information networks, government leadership is necessary because solutions cost money with little perceived immediate benefit. The denial-of-service attacks against eBay and others in early 2000 should have been a wake-up call, but industry will only make the investments in response to a known threat as it affects financial bottom lines.

The DOD must take the initiative on this issue, for several reasons. The ability to execute war plans successfully depends critically on the infrastructure industries, particularly transportation (air, rail, shipping), communication, and electric power. While the responsibility for dealing with these industries has been assigned to other agencies in government, DOD's dependency requires more action. It can also be argued that the DOD is the only agency in government that has the technical and management capability to form the kind of relationships necessary to stimulate action, and even that DOD shares responsibility for protecting the nation in the event cyber attack takes on the scale of warfare or catastrophic terrorism.

For these reasons we recommend that DOD help establish a nonprofit National Information Assurance Institute to build a bridge between the public and private sectors, including industry, universities, and not-for-profit companies that are involved in IT. The Institute should be placed in the private sector and not be a part of government or any infrastructure industry. Its activity would provide industry with a mechanism for sharing information assurance tech-

10. The President's Commission on Critical Infrastructure Protection was established in 1996 by Executive Order 13010; the Commission's report, "Critical Foundations," was completed in October 1997.

nology that poses no competitive threat, and it could serve as a single point of contact between industry and the national security and law enforcement communities. It would research and disseminate best practices, and improve the nation's ability to recognize and recover from cyber attack. It could be the mechanism for government to share sensitive intelligence about threats to the information infrastructure, and could be a conduit for sharing the results of research funded both by government and by others. The Institute would create a government-industry forum for coordinating federal policy, regulation, and other actions affecting infrastructure providers.

We are just beginning to understand cyber operations. The subject will grow in complexity and scope as IT is universally adopted. Many other issues will arise. The recommendations presented above are seen as first steps. We now turn our attention to the most critical element to power any change: well trained and dedicated people.

The Three Essentials for Success: People, People, People

Just as in real estate, where the value of a house depends on "location, location, location," the value of all of these recommendations depends on "people, people, people" to implement them. We have two further recommendations, therefore, to address the training of the military staff for command and control and information operations in the field, and to ensure that the technical work force is available to plan and design the enterprise. (This subject is addressed in greater detail in Chapter 8 by David Chu and John White.)

Create Recognized Military Career Paths in C2 and Information Operations

Creation of recognized military career paths in command and control and in information operations would not only build the expertise that the military desperately needs to conduct operations in the field, but would also create a sense of community that would help make integration work despite the various organizational constraints. The career path would include training, specialization, and certification in the chosen field of command and control or information operations.

An illustration of an earlier attempt from which we can generalize a solution is the Army's Task Force XXI experience with the "digital battlefield," when the Army recognized the need for a new role within its operations. The new role was designated "Military Occupa-

tional Specialty (MOS) 74B," and was effectively a specialist-class position trained in the network and system administration skills necessary for operations in the field. This new designation was established to correct the situation that developed when the Army began using signal officers and staff to manage systems and networks within the Tactical Operations Center (TOC). They got fairly proficient at network and system administration, but because the Army did not formally recognize the uniqueness of these soldiers, and treated them like any other signal soldier, it had difficulty retaining these specially trained individuals. The Army's decision to create the new position was accompanied by specialized training and, more importantly, specific slots within the digital TOC staff, to ensure that these responsibilities were not treated merely as "other duties as assigned."

It is imperative to recognize the importance and specialization of IT specialists in C2 and information operations, as the Army did in creating the role of the MOS 74B. The services should create specialist class roles for C2 and IO. Specific manpower allocations should be assigned at the proper command levels to ensure dedicated and proficient operations, and should be supported through specialized education and training. This role would be viewed as a specialized career path and offer the service member enough opportunities to retain the talent over time.

Support Both USJFCOM and USSPACECOM with Highly Trained Civilian Technical System Engineering Resources

The availability of a high quality, technically proficient civilian workforce is an absolute necessity for the activities outlined and it is enormously difficult to attract and maintain such expertise in today's environment. A recent Defense Science Board report lists many of the impediments to hiring and retaining civilians in the government.[11] This is also a problem for private companies, given the competitive market for IT talent. In fact, the companies that focus on DOD activity have a particularly difficult situation since they are not viewed by potential employees as providing growth opportunity comparable to IT companies.

11. The Defense Science Board Task Force, *Human Resources Strategy* (Washington, D.C.: U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2000).

However, the DOD must turn increasingly to the private sector for many services that involve the design, testing, integration, and support of hardware and software components. Of these, integration is the most challenging since the workforce must gain familiarity with a large number of independently designed systems and construct effective linkages to ensure interoperability. Success in this endeavor requires a relatively stable workforce that can only be achieved with business practices that provide incentives for companies to attract and retain skilled people.

The need for increased capability to support government decisions is an absolute necessity as well. A technically proficient workforce on the government side is needed for sound budgetary and programmatic decision-making and the design of overarching technical architectures. The attributes of this essential workforce include intimate knowledge of systems in use by the DOD, a long-term commitment to the process, the ability to be objective in driving technical solutions without conflict of interest and, most importantly, proficiency in understanding state-of-the-art information technology. One solution could involve the use of FFRDCs, which have worked very well in similar capacities for the last forty years.[12] Another would involve empowering a private company to provide this service, as has also been done in the past.

In addition, alternative innovative concepts can be tried for specific purposes. For example, the CIA has formed a private venture called In-Q-Tel to influence and funnel new, commercial technology

12. The DOD uses Federally Funded Research and Development Centers that account for 6,000 highly trained professionals. FFRDCs are managed by independent companies or are affiliated with universities. They have the ability to adjust the skills of the workforce as needed, offering incentives similar to those offered by industry. Sponsoring agreements between the DOD and the FFRDC provide for long-term support (typically five years), and restrict activity that would undermine objectivity, in return for government support to maintain a stable environment, provide access to critical data, and provide funds for independent research and development. FFRDC research and development is used to hone skills needed by the government and to stimulate research that would not otherwise be undertaken by industry.

developments to the intelligence community.[13] This model should be evaluated for possible applicability to DOD.

Four Trends for the Future

Today we are only beginning to see the future of information technology. Wonderful new commercial applications have appeared and will eventually be integrated, driven by four trends in the commercial world: ubiquity, simplicity, what we refer to as "zero and infinity," and interactivity.

First, computing platforms will be *ubiquitous* and take on many different forms. It is anticipated that by 2003 several billion computing platforms will be operational worldwide. The largest proliferation of computer technology will be embedded in other systems and invisible to the user. These computers will become extensions of the human being, able not only to respond to requests but to predict action.

The second factor is *simplification*. The human capacity to handle information has not changed since we started to measure it, and it is not expected to change in the near future, short of biomedical invention. It is this very important fact that motivates simplification to mask the inherent complexity of a growing, interconnected computing environment. Computers will become intuitive; they will be able to sense the environment through many more modes than just keyboard inputs, including voice, gestures, expressions, and pressure, and to respond with a variety of actions. Computers will continue to converge with the network but they will also, to an accelerating degree, converge with the user. This user convergence will offer deep personalization and customization.

The third factor we call *zero and infinity*. Equipment costs are being driven down toward a hypothetical "zero" cost, while capacity is increasing in the direction of being infinitely large. For example, fiber optic cabling now spans the globe and continues to be laid at remarkable rates. This fiber currently supports 8 to 16 wavelengths or independent signaling paths; it is predicted that within a year, the same volume of cable will be capable of supporting in excess of 800

13. In-Q-Tel, funded annually by Congress, has the goal of stimulating investments from innovative IT companies for products that the CIA can use and that are also applicable to commercial industry. It can enter into creative partnership and financing arrangements the DOD cannot.

wavelengths. One of these cable bundles can be expected to carry as much in an hour as three months of today's worldwide Internet traffic. These effects are tearing down barriers to entry and creating an asymmetrical effect in government, military, and industry, where otherwise small players can become dominant forces.

The fourth factor is *interactivity*. The next wave of services to be introduced on a large scale will be interactive services that will enable communities to band together in a virtual environment. The most rudimentary of these services, often referred to as "chat," is already in widespread use. With broadband technology, chat expands into a full collaboration suite to include shared applications, video, audio, and document sharing. It is projected that the number of software clients with on-line and interactive access will grow from 20 percent of all user applications today to greater than 70 percent of all user applications within the next few years. As technology matures and bandwidths increase, the desire for interactivity will lead to telepresence, or the ability to project virtually anything, anywhere, at any time.

These attributes will become available to the U.S. military, and, if embraced, will keep us ahead. To ride this inexorable commercial information technology wave, the DOD must reorganize and invest in order not to fall permanently behind.