INFORMATION TECHNOLOGY in Desert Storm

Major Michael R. Macedonia, US Army

During operations* Desert Shield *and* Desert Storm, *communications were critical to controlling the scope of the operations. The author reviews how technology allowed the coalition forces to plan, coordinate and disseminate the required information for successful operations. He also looks at some of the areas that used computers and high technology to reduce tasks that had required days to accomplish to hours. Finally, he points out that* Desert Storm *showed the military that its current communications structure needs to be reviewed and upgraded to support the way commanders intend to fight in the future.

Uncertainty being the central fact that all command systems have to cope with, the role of uncertainty in determining the structure of command should be—and in most cases is—decisive.

—Martin van Creveld[1]

IN AUGUST 1990, the US Central Command (CENTCOM) current operations room at MacDill Air Force Base, Florida, seemed to be at the center of the world. The place was a frenetic hub at the start of Operation *Desert Shield*. The CENTCOM staff was trying to coordinate the largest deployment since the Korean War; maintain an eye on Iraqi forces; and control a dangerous blockade. Even the weather was closely monitored, with the appearance of a hurricane off the African coast.

The room exhibited powerful technology at work. Each member of the staff had a computer displaying the status of everything, everywhere; from the status of transport ships headed for the ports of Saudi Arabia to the current Iraqi order of battle. On the large, color monitors overhead was the constant vision of the Cable News Network and an electronic map on the center wall tracked the US carrier groups in the region and the transit of Iraqi merchant vessels. The CENTCOM staff could call instantly to the command ships and to the forward element in Riyadh over satellite phone circuits. Situation charts were constantly being updated on work stations and forwarded to the Joint Staff in Washington and other commands via fax machines. A curiosity 10 years earlier, the fax machines now helped relieve a saturated automatic digital network.

These powerful technologies were tied to the question of the moment—when would the command group and staff deploy to Riyadh? Deployment forward was an issue shaped by the command structure of CENTCOM and the information systems that supported it. In peacetime, the unified command had no forces but had to prepare to fight a wide spectrum of contingencies across vast distances, from Egypt to Pakistan. Though a modern facility existed in the Saudi Ministry of Defense (MOD) compound, the computer and communications resources were not there. The political pressure from Washington and Riyadh was to immediately establish the presence of the commander in chief of CENTCOM in the theater, with the purpose of assuring our allies, presenting a threat to the Iraqis and

avoiding the image of "chateau generalship." The irony of the modern age was that the CENTCOM commander, at the outset of the crisis, could gather more intelligence information and more effectively control his forces 7,000 miles away from the theater of operations than from the Saudi MOD. The command could deploy too early, only to have to call MacDill to find out what was going on in the theater. Not only did CENTCOM have to await the build-up of its forces but also the development of a communications infrastructure to fight the war.

The crisis surrounding the blockade demonstrated that the structure and location of the CENTCOM command systems were not theoretical issues, because they determined the scope and degree to which CENTCOM could manage wide-ranging events. The stakes were extremely high, requiring a fine grain of control of the US forces in the region and knowledge of the Iraqi situation and capabilities. The actions of the Iraqis were unpredictable and US enforcement of the blockade might have provoked them into attacking the Saudi oil fields, throwing the situation into chaos. The United States was also trying to gather support in the UN and did not want to appear too eager to provoke the Iraqis.

The level of control and the technology to support it were made evident one evening when General H. Norman Schwarzkopf, the CENTCOM commander, entered the middle of the current operations center. In a tense conversation, Schwarzkopf talked on a telephone with chairman of the Joint Chiefs of Staff, General Colin L. Powell in Washington. At the same time, he communicated by radio with the commander of a US ship in the Indian Ocean that was preparing to engage an Iraqi merchant vessel attempting to run the blockade.

These early command and control issues presaged how commanders would attempt to deal with uncertainty through technology during the war; in turn, shaping the structure and function of command. Operation *Desert Storm* provided clues toward understanding the future of warfare and how the battlefield has changed dramatically from the influence of late-20th-century information technology. The pervasive use of the computer and data networks by all participants—from the tactical to strategic level of war—surprised the world and military commanders. The command systems employed by

The irony of the modern age was that the CENTCOM commander, at the outset of the crisis, could gather more intelligence information and more effectively control his forces 7,000 miles away from the theater of operations than from the Saudi MOD. . . . Not only did CENTCOM have to await the build-up of its forces but also the development of a communications infrastructure to fight the war.

the US forces reduced uncertainty, allowing the coalition forces to efficiently destroy a larger Iraqi force in a time-compressed war. In hindsight, the technology used by US forces at the start of the war was a major advantage despite the apparent parity in force numbers; the Iraqi army's edge afforded by defending on its homeland; and the long lines of communication of coalition forces.

Computer and communications systems not only changed the character of war; they also changed the behavior of US military organizations. While using the technology to gain advantage over the enemy, commanders also reshaped the traditional processes by which they planned operations and managed forces in battle. A great deal of analysis is required before we can understand the full extent of the technology employed and how it influenced the course of the war and the management of forces but, as the anecdote above demonstrated, the impact was obvious.

Computers were used for almost every function, including:

- Guiding Tomahawk missiles.
- Maintaining data bases on air and ship movements, personnel and enemy electronic order of battle .

- Contingency war gaming for theater commanders.
- Route planning for aircraft against enemy air defenses.
- Analyzing and filtering intelligence.
- Artillery and air defense management.
- Development of the daily air tasking order (ATO).
- Frequency Management.

Artificial intelligence systems were also used for the first time in support of a war. The Army employed a decision support system called HAWKEYE at VII Corps that assisted in electronic warfare targeting and collection management for combat operations. Another advanced data base was developed by the Army to reduce the planning time for the movement of individual US–based units from several days to a matter of hours by matching unit equipment loads to ship and aircraft capacities.

The management of that deployment could not have been accomplished without computers scheduling the flow; accounting for all supplies and forces; and quickly predicting the resources required. Compare this with the slow build–up in Vietnam, which took several years to develop the infrastructure for 500,000 soldiers.

The command systems employed by the US forces reduced uncertainty, allowing the coalition forces to efficiently destroy a larger Iraqi force in a time–compressed war. In hindsight, the technology used by US forces at the start of the war was a major advantage despite the apparent parity in force numbers; the Iraqi army's edge afforded by defending on its homeland; and the long lines of communication.

Computer networks over satellites, telephone circuits and radio links were essential in tying together the US and coalition partners with critical data and information: tactical and strategic systems gave instantaneous warnings of Iraqi Scud missile launches; provided commanders up–to–date information on the state of the US forces and logistics; and permitted rapid planning of combat operations.

Operational commanders could view the battlefield as never before. US and coalition forces could observe Iraqi elements in near real–time via Joint Surveillance and Target Attack Radar System, AWACS (Airborne Warning and Control System) and advanced unmanned aerial vehicles. Intelligence systems denied, for the most part, the Iraqis the advantage of operational surprise and the use of their homeland to cloak preparations. Nothing remained hidden for long. Unlike Vietnam, much of the intelligence was readily available to tactical and operational forces for exploitation because of a change in attitude by the intelligence community toward supporting front–line commanders and the capability of communications systems to rapidly disseminate information.

These systems promoted "jointness" and unity of command by allowing commanders to share and exploit information, permitting close coordination of operations. The single ATO is a widely stated example of this. Lieutenant General Charles A. Horner, the CENTCOM air component commander, gave credit to automation as the key to successfully developing the highly complex ATO. The integration of Air Force AWACS with Army Patriot missiles and theater–level systems through the use of sophisticated data links also showed how information technology could generate a high level of synergism among the services.

Much of the technology was employed for the first time and, to a large degree, was unanticipated or untried. Major innovations occurred in adapting commercial systems to fill immediate information requirements of commanders, because military technology in this area had not kept up with the computer revolution of the past decade. For example, personal computers with modems sent enormous amounts of record traffic over phone lines far faster than the military message system, which was based on 1960's technology. Staffs scrambled to purchase fax

A soldier from the 51st Signal Battalion makes adjustments to a satellite dish in Saudi Arabia.

Computer networks over satellites, telephone circuits and radio links were essential in tying together the US and coalition partners with critical data and information. . . . Major innovations occurred in adapting commercial systems to fill immediate information requirements of commanders, because military technology in this area had not kept up with the computer revolution of the past decade.

machines, which became mandatory to send graphics such as maps and charts to tactical units. There were just not enough couriers and aircraft to do otherwise.

Other improvisations included the use of mobile satellite ground stations that were leased from commercial operators. The era of the suitcase terminal arrived to handle critical voice and data communications from remote locations. Both commercial and military satellite communications became so essential that major bureaucratic battles were fought over frequency bandwidths and access. These disputes had to be resolved at the joint staff and the Defense Communication Agency levels in the United States.

Use of the Global Positioning System (GPS) reduced the uncertainty of Army commanders in controlling operations in the vast desert west of Kuwait. GPS made up for the lack of accurate maps and absence of terrain features in the Saudi desert and permitted precise coordination of tactical ground forces and aircraft. Most of the GPS receivers were commercial systems bought specifically to support *Desert Storm*. There were 4,500 receivers used during the war. The systems were essential to the famous left hook by the coalition, providing the means for maneuvering the huge force through an uncharted desert. The move surprised the Iraqis, who had thought that the area was unnavigable.

However, the use of computers and data communications brought to the attention of commanders the continuing pathologies, as Martin Van Creveld has called them, of modern command systems—too much data either ignored, misdirected or misjudged for knowledge. Though techniques such as expert systems were used to assist in the analysis of raw data for many wartime planning functions, there was still too much to absorb by commanders and staffs during the fast-paced war. The overwhelming amount of data resulted in blind spots by forcing

Pictures often will not give an accurate look at the damage done to an enemy. (*Left*) Two of four hardened aircraft shelters show evidence of catastrophic destruction. Were Iraqi aircraft located in any of these facilities? Ground forces overrunning apparently intact shelters sometimes found destroyed aircraft inside. (*Below*) A dug-in tank near the Kuwaiti border. Is it still operational? How is the morale of its crew? Has the crew fled?

A controversial example of a "misdirected telescope" was the focus by the intelligence community on imagery–based battle damage assessments used to measure Iraqi strength. The allure of pictures stems from the fact that they are a more concrete form of data than the products from other intelligence collection methods such as enemy prisoner of war debriefs.

organizations to narrow their focus on particular forms of information.

A controversial example of a "misdirected telescope" was the focus by the intelligence community on imagery–based battle damage assessments (BDAs) used to measure Iraqi strength. The allure of pictures stems from the fact that they are a more concrete form of data than the products from other intelligence collection methods such as enemy prisoner of war debriefs. Those products are complex and require sophisticated analysis. However, Horner has stated that "we may have been overly entranced with some forms of intelligence collection" (imagery) to the detriment of other sources of information, which indicated that the Iraqis were far more dissipated than BDA indicated.[2] Pictures are critical to determining the disposition of enemy forces, but they do not reveal the enemy state of mind or morale.

Problems associated with the ATO also illustrate the problem of "information overload." Although the use of the computer allowed for the generation of the ATO and permitted central management of coalition air forces, the product was immense, consisting of a thousand pages of text. The limited time available to read it and plan air operations forced the air wings to concentrate on only the data that specifically applied to them. The air operations planning staffs often were unaware of other missions in the same area that might have affected their plans even though that information was buried in the ATO.

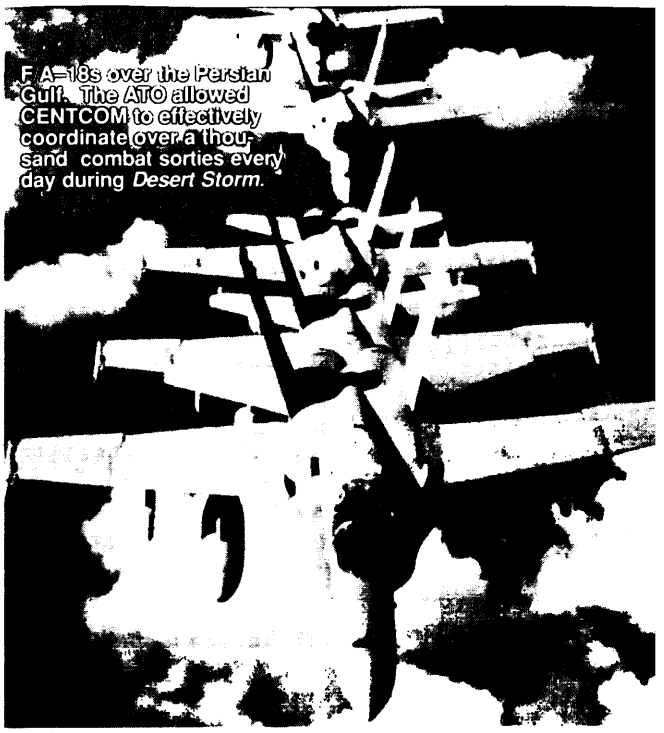
A corollary of this is that critical data did not always go to the appropriate place. From the beginning of the crisis, the routing list for CENTCOM messages grew geometrically. The scale of the operation made it impossible for anyone to know all the organizations that might benefit from any particular piece of data. Additionally, units often created redundant data bases and other applications on computers or retransmitted data that others already possessed. The traditional downward branching flow of information had been corrupted long before the deployment. The complexity of modern war has caused data to become compartmentalized and channeled laterally, based on a variety of needs that undermine the concept of information moving along a chain of command. These needs include security, communication formats and systems, joint service requirements and the cross–linking of many external organizations under the influence, but not necessarily the command, of the theater

commander in chief (CINC).

However, command and decision making, as opposed to strictly information passing, remained hierarchical with a distinct chain from the president to the CINC and to the service components. The lessons of Vietnam were heeded by military commanders paying due respect to the critical importance of organizational structure in command systems, even though the technology made it possible and laid open the temptation to micromanage the war.

Accurate data received by the right people does not necessarily produce the appropriate decisions, even with systems such as HAWKEYE that rely on explicit rules or templates. The actions of the Iraqis and Saddam Hussein often contradicted the opinions of experts because those actions did not fit in with past patterns of behavior and often were irrational. Prior to *Desert Shield*, despite the sophistication of our intelligence information systems, Saddam succeeded in his plan for strategic surprise in his invasion of Kuwait. Fear of surprise after the Iraqi invasion of Kuwait caused intelligence organizations to adopt very conservative approaches to analyzing Iraqi capabilities and intentions. The conservatism had the circular effect of making the agencies focus on the literal forms of information, (for example, imagery), which were incomplete, as discussed above. The result was overly cautious and caveated analyses constructed with incomplete information. As Schwarzkopf told the Senate Armed Services Committee, "We'd still be waiting to start the ground war if the commanders of *Desert Storm* had depended on the national agencies to agree that requirements for beginning the offensive had been met."[3]

The constant demand for automation and the subsequent communications capacity to support it proved again that the demand for information is insatiable in the preparation for and conduct of war. *Desert Storm* showed that the current US communications infrastructure is inadequate for the way commanders intend to fight in the future. The various pipes and spigots of data were either too large or small for each other, causing backups or stoppages. The limitations existed despite the fact that "we put in more communications connectivity [in Saudi Arabia] than we've had in Europe during the past 40 years."[4] The ATO provides another example of this. Although the ATO consisted of text data, it was often carried on floppy disk or in paper copy to ships supporting the air war.



F/A-18s over the Persian Gulf. The ATO allowed CENTCOM to effectively coordinate over a thousand combat sorties every day during *Desert Storm*.

The roles and functions of the other elements of command systems, organizations and procedures must be reexamined carefully in light of new technology. Formal staff structures and procedures have changed little in the last 40 years. . . . During* Desert Storm, *staffs had to improvise new methods and organizations for managing a huge enterprise; [or] they would be overwhelmed.

"A high–ranking Navy communications official said the service tried to circumvent these problems by sending the ATO on circuits designed for record traffic—essentially teletype circuits running at 75 bits per second. These circuits were overwhelmed quickly by the sheer size of the ATO."[5]

High bandwidth computer applications such as imaging are more in demand by staffs because the information produced is less abstract and more readily understood than textual data. Yet, those products cannot be generally supported by the limited capacity of standard military systems.

Dissemination of imagery to tactical forces was delayed during the war because the coalition lacked a distributed communications system capable of handling such high data rates.

The US military was also vulnerable to centralization, not from a decision making standpoint but from the physical placement of key command system facilities. The high demands for communications assets forced theater-level units and staffs to locate closely together to access indigenous systems and share the general support military communications and the logistic infrastructure necessary to maintain and operate them.

Command and decision making, as opposed to strictly information passing, remained hierarchical. . . . The lessons of Vietnam were heeded by military commanders paying due respect to the critical importance of organizational structure in command systems, even though the technology . . . laid open the temptation to micromanage.

Another serious issue was the lack of trained users of the technology in US forces. Most of the computers were user-owned and operated—no special staff existed to develop software, maintain the data or provide quality control. It was not uncommon to see a lone junior enlisted soldier or officer acting as the computer expert on a staff. Unfortunately, the quality of their knowledge of the computer, its application and the data it processed received little scrutiny from superiors, who were just as often ignorant of the limitations of the technology.

Countering these "pathologies" requires our leaders to recognize that computers and communication have changed the behavior of military forces and their command systems. The use of computers on the battlefield is similar to the development of another technology that has changed the American way of war—the helicopter.

Although the helicopter has been used since World War II, it took 40 years to create an environment within the Army to maximize its attack capabilities. The current status of military computers and communications is much like that of the helicopter during the Vietnam War. That war demonstrated that rotary wing aircraft were no longer a marginal factor in fighting the war as they had been in Korea. The experience of Vietnam proved the potential of these systems to leverage military power at the tactical level by introducing rapid mobility for the infantry and giving Army commanders their own dedicated air support in the form of the AH-1 Cobra. However, as explained previously, the helicopter was not a complete weapon until doctrine, procedures and other technology such as sensors were fully integrated.

The successful use of Apache attack helicopters during *Desert Storm* required a tactical concept integrated with AirLand Operations doctrine; a corps of expert operators and commanders trained in their employment; a fully developed logistics support structure; and the right mix of technology on the aircraft itself including weapons, sensors and communications. This synchronization has provided Army commanders with an unmatched responsive and lethal weapon protected by its capability to destroy targets at long range, over the horizon of armor and infantry forces.

The same process must be observed for computers and networks. The roles and functions of the other elements of command systems, organizations and procedures must be reexamined carefully in light of new technology.[6] Formal staff structures and procedures have changed little in the last 40 years. However, during *Desert Storm*, staffs had to improvise new methods and organizations for managing a huge enterprise; otherwise, they would be overwhelmed. These methods often revolved around the use of information technology.

Commanders should encourage innovation but at the same time understand the limits of computer technology. The current system of training the operators and users of computers is a barrier to exploiting and properly understanding the processed data. This is a universal prob-

lem, because information technology has a generational cycle approaching 24 months. If commanders are to have the latest hardware and software, they must have experienced operators and administrators who are constantly retrained. An expert system requires an expert user—one who is knowledgeable of his field, whether logistics, intelligence or operations—who can validate and provide a reality check on the information produced. No software is perfect. The consumers, commanders and staffs (who often are the system operators) must be made aware of the reliability and quality of the products and how best to use them. This is because a single defect does not only influence the performance of one piece of equipment but, more profoundly, human decisions, with broad consequences.

Military leaders must consider the doctrinal implications of computer technology. In light of *Desert Storm*, do the assumptions of AirLand Operations mesh with the reality of the technical means for implementing it? How can computers and communications best be used or improved to support its tenets? How do we protect our command systems while at the same time exploit or destroy our foe's capabilities?

Unlike other countries that orient their defense from their own soil, the United States has been faced with the critical challenge of responding to crises all over an unstable world. Forward basing is becoming less viable for the United States while contingency–based planning for warfighting has become the norm. For future operational and tactical commanders, the requirement to prepare for contingencies will continue the problem confronted by CENTCOM in the beginning of *Desert Shield*—how to establish a flexible command system for an uncertain war.

Military leaders must consider the doctrinal implications of computer technology. . . . Do the assumptions of AirLand Operations mesh with the reality of the technical means for implementing it? How can computers and communications best be used or improved . . . ? How do we protect our command systems while at the same time exploit or destroy our foe's capabilities?

The Gulf War showed that information technology is already a key element in the pursuit of reducing uncertainty. The technology promises to be a decisive tool of command on future battlefields. Lieutenant General Robert H. Ludwig, Air Force deputy chief of staff for command, control, communications and computers, made this clear:

"You have to be a little careful about what you say you learned out of *Desert Storm*. But one lesson I am utterly confident we've learned is that we have become dependent upon information technology. It is now and will continue to be a very significant portion of our military force."[7]

However, commanders must have a realistic understanding of its possibilities and challenges. Finally, as in the case of the helicopter, the US military must develop the appropriate doctrine, training and procedures to extend the technology and fully integrate it within the way we fight.

NOTES

1. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 268.
2. David A. Fulghum, "Desert Storm Highlights Need for Rapid Tactical Intelligence," *Aviation Week & Space Technology* (11 February 1991):18.
3. David A. Fulghum, "Key Military Officials Criticize Intelligence Handling in Gulf War," *Aviation Week & Space Technology* (24 June 1991):83.
4. Bruce D. Nordwall and Philip J. Klass, "Key Desert Storm Technologies Vital to Future Competitiveness," *Aviation Week & Space Technology* (3 June 1991):64. Remark by LTG James S. Cassity Jr., US Air Force.
5. Bob Brewin, "DOD Report Details Success of C3I in Desert Storm," *Federal Computer Week* (29 July 1991):22.
6. Van Creveld, 262.
7. "C4 Chief Tells Lessons of War, Technology and the Bottom Line," *Government Computer News* (5 August 1991):80.

Major Michael R. Macedonia is a Ph.D. candidate in computer science at the Naval Postgraduate School, Monterey, California. He received a B.S. from the US Military Academy and an M.S. from the University of Pittsburgh. He has served in a variety of command and staff positions in mechanized infantry units, as well as with the Systems Engineering Directorate, Joint Electronic Warfare Center, San Antonio, Texas. He was an electronic warfare liaison officer with US Central Command at the start of Operation Desert Shield *and with Joint Task Force* Proven Force *during Operation* Desert Storm.