11

The Flow of Information in Modern Warfare

Jeremy M. Kaplan

INFORMATION HAS ALWAYS BEEN IMPORTANT at the strategic level in warfare, whether to defeat the plans and disrupt the strategic alliances of adversaries as espoused by Sun Tzu,[1] to deliberately mislead enemy spies and make use of a carefully concealed ability to intercept plans—as the allies did in WW II[2]—or to galvanize and maintain public support through the presence of embedded reporters, as the United States did during its 2003 invasion of Iraq.

However, the free and rapid flow of information at the tactical and operational levels is currently causing a revolution in the very nature of warfare—a revolution in which the United States far outpaces the rest of the world. This revolution, while fueled by advancing technology, is heavily driven by the willingness and ability to implement the social and organizational changes needed to use that technology. The United States' recent successes in the use of net-centric information in Afghanistan and Iraq have been a wakeup call to the militaries of the rest of the world, which are now scrambling to join in this revolution.

This chapter focuses on information flow in modern war fighting at the tactical and operational levels—on the needs, issues, and challenges. One of the most fundamental of these challenges, that of protecting an organization from attacks on its information systems, is shared by our

networked society and may require a common commercial/Department of Defense (DoD) solution.

This chapter does not address the global war on terrorism, which may not be a war in the same sense and may be more societal in nature. It also does not address peacekeeping operations and the challenges of rebuilding a society in the face of factionalism and terrorism. While those topics are both current and important, the challenges of tactical and operational combat are likely to continue as long as nations have armed forces.

Information Flows

Although there has been much recent discussion about effects-based operations, modern combat is dominated by information, mobility, and stealth. This is because the extreme lethality of modern precision weapons means that if you can find a target and get the information to an appropriate weapons platform, you can kill it. Thus the challenge has become to find targets quickly and to get information about them to the right weapons platforms in a timely manner. The targets' challenge is to move or hide while finding and directing weapons at you, your sensors, and your weapons platforms.

This is true for engagements across a broad spectrum of domains, from undersea warfare to air defense, ballistic missile defense, and, to a great extent, land combat. It formed the basis of U.S. successes in Afghanistan and Iraq, and it will become increasingly true for the combat engagements of other nations in the future.

Thus emerging U.S. doctrine increasingly stresses net-centricity—a group of operational concepts and technologies for getting the right information to the right users fast enough to give them information superiority over the enemy. These concepts have their roots in the vision of information superiority originally laid out in the Joint Staff's "C4I for the Warrior"[3] and "Joint Vision 2010"[4] in the early to mid-1990s, in many instances in advance of the technologies needed to achieve them.

Net-centric doctrine generally involves the free flow of all the information needed to plan and execute a campaign. This includes the intelligence information on the disposition of the enemy's supporting infrastructure; the logistical information that enables forces to travel light to

theater and be met by the right equipment and supplies at the right locations and times to engage the enemy and continue the fight; the intelligence, surveillance, and reconnaissance (ISR) information that allows a war fighter to know where his enemy is and destroy him before that enemy knows where the war fighter is and can fire or move; and the information to do battle damage assessment, and re-strike insufficiently damaged targets. Finally, it includes the information-handling capabilities that enable forces to collaborate during execution and adjust their plans as the enemy tries to respond.

Networked Information Age

In the industrial age, the information needed to conduct operations flowed down from the top, along the chain of command. Status information on one's own forces and contact information on enemy forces flowed back up. Information flowed through independent or "stovepiped" channels and was often compartmentalized (available only on a need-to-know basis). This slowed planning and caused rigid execution that could not adjust for rapid changes in the disposition of enemy forces.

In the information age, a commander's intent and major resource allocation decisions still flow down from the top, but coordination takes place horizontally on a network that allows everyone engaged in combat, combat planning, and combat support to discover relevant information and collaborate with the other elements needed for the success of the operation. This enables dispersed, massively parallel combat operations at an unheard-of pace. Dispersed war fighters, across echelons, may hear the decision briefings and the commander's intent via networked conferencing and plan in parallel to execute their operations. Logisticians have access to shared databases with current data and understand the competing needs and demands on their resources. Forces self-synchronize their plans for attack and pull the information they need from all available sources. Their operational tempo is increased by globally networked communications that enable coordinated activities and work flows across units and people that are not co-located or even working at the same time.

Networked information flow concepts, like the open posting and pulling of information, are fundamental to hypermodern warfare. They enable organizations (such as supply units) that would not normally have the ability to task assets (such as intelligence, surveillance, and reconnaissance resources) or have access to data to have the ability to search databases (e.g., Web searches of previous reconnaissance imagery) and to locate information no one ever thought to send them because no one ever anticipated their need for that information. DoD has called the concept of open networked information flow "power to the edge," because more people "at the edge" can directly perform mission and mission support, empowered with the information they need, and fewer people are "in the middle," involved with organizing information flows and pushing paper.

Networked Operations

Open information flows and global networks are also driving a decrease in the number of echelons of command needed, and a merging of the strategic, operational, and tactical levels of warfare. An extreme example of this is the ability of a flag officer in the continental United States (CONUS) to direct the flight of an armed Predator unmanned aerial vehicle that is flown by an operator in another part of CONUS and is flying in a theater of operations half a world away.[5]

Globally networked information flows allow some information support units (e.g., some intelligence and logistics personnel) to remain in CONUS and still be effective. This has the added benefit of lowering the footprint in theater (thus fewer forces to support), increasing the speed with which forces can reach theater (fewer forces to transport), and improving the safety of some forces (which do not have to be protected in theater).

Fully networked operations can involve worldwide platforms and people from all four military services working in tandem with analysts from the intelligence community and with the industrial support base and can involve complex operational information flows to and from units around the globe.

To get a feeling for how information flows have changed warfare, first imagine a World War II–era soldier without precision weapons or net-

worked support. He sees a target (perhaps a tank), fires an unguided weapon at it, and probably misses.

Fast-forward in time. Given a precision weapon, the soldier probably hits and does damage if he has the right look angle and enough time to guide the weapon, and if he is not taken out by the enemy's suppressing fire. The soldier's chances of success improve further if he can communicate target information to an airborne platform with a better attack angle, lower vulnerability, and a greater supply of heavier and more powerful precision weapons than the soldier can carry. His chances of success improve still further if he can combine his local target position information (perhaps from a laser rangefinder) with global position information (perhaps from a GPS satellite) and give that to the airborne platform. The likelihood that the target will be hit before it can respond or move improves still further if the soldier can put that information directly into the targeting system of a precision weapon (perhaps a GPS-guided bomb) on board the aircraft—thus making the aircraft merely transportation for the soldier's extended weapon system.

Now imagine doing this across an entire theater, with networked sensors, soldiers, and aircraft designating and attacking hundreds of targets simultaneously, and with a networked, just-in-time, total asset visibility logistics system to supply them. You start to get an inkling of hypermodern, net-centric warfare.

DoD calls the networked information system it is evolving to support these concepts the Global Information Grid. It is composed of sensors and weapons platforms, command and control, communications, and an incredible supporting (and increasingly net-centric) infrastructure.

Issues and Challenges

The movement toward power to the edge through the creation of these net-centric capabilities involves immense questions and challenges that are the subjects of ongoing work. Broadly speaking, are there dangers to the war fighter in overreliance on the net? Will war fighters lose access to essential information or processing functionality at key moments or, still worse, receive information deliberately corrupted by the enemy? Will net-centric forces become vulnerable? As nations increasingly depend

on networks to bring vital information to lighter, more mobile forces, can the networks be made secure? Will necessary information be available, timely, reliable (not tampered with), authentic (from the attributed source), and protected from enemy eyes?

Users always stretch resources to the limit. Will they be able to manage scarce resources to support the most pressing missions in the face of competing demands for networks and networked services (data and processing capabilities)?

Every movement in warfare creates a countermovement. How will the branch of cyberwarfare that attacks net-centric services (the networks, databases, and information processing platforms) evolve? From where (inside or outside the theater of operations) will attacks be launched? How will they be defended?

In addition to these broad challenges, the development of a net-centric force requires that very specific system-of system challenges must be addressed in the areas of interoperability, security, information sharing, and supply chain vulnerabilities.

Interoperability

DoD systems are built in parallel by multiple, independent, and competing developers. While this provides rapid modernization and other competitive advantages, it raises the significant challenge of systems interoperability across the DoD Global Information Grid. This interoperability challenge is a far greater challenge than is faced by Internet users because the complexity of the DoD system of systems is greater, and because DoD often needs a more speedy and reliable service that is protected from threats in a hostile environment.

Security

Greater effectiveness in warfare requires greater sharing, openness, and availability of information. Modern information systems are always in a state of flux (nodes are added, moved, and deleted; new software is installed, and existing software is patched). The heterogeneous Global Information Grid will be modified too frequently for any rigid security certification processes

to be effective. How will we assure that the system has not been compromised? How will we balance the war fighter's need for access to information against the need to protect information systems, information, and sources?

Information Sharing

Warfare in the future will almost certainly involve coalition forces. If the United States wants its coalition partners to be effective and work at its operational tempo, it will have to do more than give them access to selected and screened information—it will have to put them on the DoD net, so that they can determine and access the information they need. This raises immense information protection and assurance issues, especially with coalition partners who are not long-term allies. Will the United States need to protect information about its operations from less trusted partners? Will it need to protect its information sources and methods? Will it need to protect its operating systems, data, combat applications, and combat-support applications from tampering? How can it provide these levels of protection, given the current precarious balance between computer network attack and defense? Should the United States decide, as it has already done in other areas (e.g., in the open publication via the Joint Technical Architecture of the information technology standards used for interoperability) that its military competitive advantage lies in openness, speed, and interoperability, and not in secrecy? Of course, the foregoing discussion applies to coalition partners who are already interoperable with the United States or use systems it supplies. Coalition interoperability faces additional technical challenges if the coalition partners have their own systems and networks built by their own vendors to different sets of standards.

Supply Chain Vulnerabilities

Software and hardware are inherent in all information technology products—from mobile phones to networked computer services. DoD is now a minuscule portion of the information technology market, so future generations of military information systems will come increasingly from industry—which values market share and frequently achieves it through cost-competitive strategies that do not account for potential vulnerabili-

ties. In addition, as software and hardware are increasingly developed globally, can one ever be assured that they are free from designed-in and built-in vulnerabilities? Of course, with the advent of chat, mobile computing, file sharing, the convergence of voice and data, cloud computing, and software agents, information assurance problems will only get worse.

U.S. military strength comes, in good part, from its net-centric doctrine and ability to exploit, both socially and technically, the information revolution: its ability to collect and fuse data; its ability to network-enable services to achieve interoperability; its use of collaborative tools; and its ability to manage networks, information, and information security. As the pace of innovation quickens, it may become increasingly difficult to balance the benefits of adoption of new capabilities against the growing potential risks.

Conclusion

As a final note, society as a whole currently faces and will increasingly have to deal with most of the problems that DoD faces now.[6] Malicious computer hacking, spyware, identity theft, potential sabotage of infrastructure by persons located anywhere in the world—these are just a few of the growing problems of the commercial networked world. Most of our current information assurance problems (especially those arising from viruses, malware, and information attacks) are the result of weaknesses inherent in modern operating systems, computer languages and software, and the Internet protocol suite. Strong economic incentives (e.g., the advantages of being first to market, and the use of embedded freeware to cut development times) encourage software developers to continue these weaknesses. Can current information assurance approaches, with their heavy emphasis on signature recognition, ever provide adequate protection? Will it take a national disaster for us to put significant resources into research and development of a commercially viable and inherently secure architecture for networked computing? The current Internet is the result of an enormous investment made by the federal government, first in DoD and then in NSF-sponsored university research in advance of the current economic incentives. Perhaps it is time to reinvigorate this research program, with an emphasis on inherently secure computing paradigms.

Notes

The views expressed in this chapter are those of the author and do not reflect the official policy or position of the Industrial College of the Armed Forces, National Defense University, the Defense Information Systems Agency, the Department of Defense, or the U.S. government.

1. Griffith, Samuel B., Sun Tzu The Art of War, Oxford University Press, 1971, pp 78.
2. Brown, Anthony Cave, Bodyguard of Lies, Bantam Books, New York 1976.
3. The Joint Chiefs of Staff, 1992.
4. The Joint Chiefs of Staff, 1995.
5. General Tommy Franks, American Soldier, ReganBooks, 2004, pp 288–291.
6. DoD has the most significant expertise in the federal government (and perhaps in the country) in securing heterogeneous networks and computer enclaves from attack. Should DoD have a role in protecting the nation's information infrastructure?