2000-02-29

Cyberwar and Netwar: new modes, old concepts, of conflict

Arquilla, John J; Ronfeldt, David F.

Santa Monica California, Rand Corporation

Excerpt from "Cyber War is Coming", by J. J. Arquilla and D. F. Ronfeldt,
Comparative Strategy, V.12, pp 141-165, 1993
http://hdl.handle.net/10945/39155

Cyberwar and Netwar: New Modes, Old Concepts, of Conflict

John J. Arquilla and David F. Ronfeldt

The information revolution is transforming warfare, contend the authors. No longer will massive, dug-in armies fight bloody attritional battles. Instead small, highly mobile forces, armed with real-time information from satellites and battlefield sensors, will strike with lightening speed in unexpected places. The winner: the side that can exploit information to disperse the fog of war yet enshroud an enemy in it.

Suppose war looked like this: Small numbers of light, highly mobile forces defeat and compel the surrender of large masses of heavily armed, dug-in enemy forces, with little loss of life on either side. Mobile forces can do this because they are well prepared, make room for maneuver, concentrate their firepower rapidly in unexpected places, and have superior command, control and information systems that are decentralized to allow tactical initiatives, yet provide central commanders with unparalleled intelligence and "top sight" for strategic purposes.

Our vision is inspired not so much by the U.S. victory in the Persian Gulf war as by the example of the Mongols of the 13th century. Their "hordes" were almost always outnumbered by their opponents; yet, they conquered and held for over a century the largest continental empire ever seen. The key to Mongol success was their absolute dominance of battlefield information. They struck when and where they deemed appropriate, and their "arrow riders" kept field commanders, often separated by hundreds of miles, in daily communication. Even the Great Khan, sometimes thousands of miles away, was aware of developments in the field within days of their occurrence.

Warfare in the Information Age

Throughout history, military doctrine, organization and strategy have continually undergone profound, technology-driven changes. Industrialization led to attrition warfare by massive armies in World War I. Mechanization led to maneuver predominated by tanks in World War II. The information revolution implies the rise of a mode of warfare in which neither mass nor mobility will decide outcomes; instead, the side that knows more, that can disperse the fog of war yet enshroud an adversary in it, will enjoy decisive advantages.

Sea changes are occurring in how information is collected, stored, processed, communicated and presented, and in how organizations are designed to take advantage of increased information. Information is becoming a strategic resource that may prove as valuable and influential in the postindustrial era as capital and labor have been in the industrial age.

The information revolution sets in motion forces that challenge the design of many institutions. It disrupts and erodes the hierarchies around which institutions are normally designed. It diffuses and redistributes power, often to the benefit of weaker, smaller actors. It crosses borders, redraws the boundaries of offices and responsibilities, and generally compels closed systems to open up.

The information revolution will cause shifts, both in how societies may come into conflict and how their armed forces may wage war. We offer a distinction between what we call netwar--societal-level conflicts waged in part through internetted modes of communications--and cyberwar at the military level.

What Is Netwar?

Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt or damage what a target population knows or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve diplomacy, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks.

Netwar represents a new entry on the spectrum of conflict that spans economic, political, and social, as well as military forms of "war." In contrast to economic wars that target the production and distribution of goods, and political wars that aim at the leadership and institutions of a government, netwars would be distinguished by their targeting of information and communications.

Netwars will take various forms. Some may occur between the governments of rival nation-states. Other kinds of netwar may arise between governments and nonstate actors. For example, netwar may be waged by governments against illicit groups involved in terrorism, proliferation of weapons of mass destruction or drug smuggling. Or it may be waged against the policies of specific governments by advocacy groups--involving, for example, environmental, human-rights or religious issues. The nonstate actors may or may not be associated with nations, and in some cases they may be organized into vast transnational coalitions.

Some netwars will involve military issues, such as nuclear proliferation, drug smuggling and antiterrorism, because of the potential threats they pose to international order and national security.

Netwars are not real wars, traditionally defined. But netwar might be developed into an instrument for trying, early on, to prevent a real war from arising. Deterrence in a chaotic world may become as much a function of one's cyber posture and presence as of one's force posture and presence.

What Is Cyberwar?

Cyberwar refers to conducting military operations according to information-related principles. It means disrupting or destroying information and communications systems. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the "balance of information and knowledge" in one's favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended.

This form of warfare may involve diverse technologies, notably for command and control, for intelligence collection, processing and distribution, for tactical communications, positioning, identifying friend-or-foe, and for "smart" weapons systems, to give but a few examples. It may also involve electronically blinding, jamming, deceiving, overloading and intruding into an adversary's information and communications circuits.

Cyberwar has broad ramifications for military organization and doctrine. Moving to networked structures may require some decentralization of command and control. But decentralization is only part of the picture: The new technology may also provide greater "topsight," a central understanding of the big picture that enhances the management of complexity. This pairing of decentralization with topsight brings the real gains.

Cyberwar may also imply developing new doctrines about the kinds of forces needed, where and how to deploy them, and how to strike the enemy. How and where to position what kinds of computers, sensors, networks and databases may become as important as the question once was for the deployment of bombers and their support functions.

As an innovation in warfare, cyberwar may be to the 21st century what blitzkrieg was to the 20th century. At a minimum, cyberwar represents an extension of the traditional importance of obtaining information in war: having superior command, control, communication and intelligence and trying to locate, read, surprise and deceive the enemy before he does the same to you.

Cyberwar may be to the 21st century what blitzkrieg was to the 20th.

The postmodern battlefield may be fundamentally altered by the information technology revolution, at both the strategic and tactical levels. The increasing breadth and depth of this battlefield and the ever-improving accuracy and destructiveness of even conventional munitions have heightened the importance of information to the point at which dominance in this aspect alone may now yield consistent war-winning advantages to able practitioners.

Networks Versus Hierarchies

From a traditional standpoint, a military is an institution that fields armed forces. The form that all institutions normally take is the hierarchy, and militaries, in particular, depend heavily on hierarchy. Yet, the information revolution is bound to erode hierarchies and redraw the boundaries around which institutions and their offices are normally built.

Mongol attack, 1241. Absolute command of battlefield information.

The Mongols, a classic example of an ancient force that fought according to cyberwar principles, were organized more like a network than a hierarchy. More recently, the combined forces of North Vietnam and the Viet Cong, a relatively minor military power that defeated a great modern power, operated more like a network than an institution. In both cases, the defeated opponents of the Mongols and the Vietnamese were large institutions whose forces were designed to fight set-piece, attritional battles.

Currently, most adversaries that the United States and its allies face in the realm of low-intensity conflict--international terrorists, guerrilla insurgents, drug smuggling cartels, ethnic factions, and racial and tribal gangs--are all organized like networks.

The lesson: Institutions can be defeated by networks, and it may take networks to counter networks. The future may belong to whoever masters the network form.

Excerpted from **Cyber War Is Coming,** by John J. Arquilla and David F. Ronfeldt, in *Comparative Strategy*, Vol. 12, pp. 141-165, 1993.

David Ronfeldt is a senior member of RAND's international policy department. John Arquilla is a consultant.

RAND Research Review Contents

RAND's Home Page