John Arquilla/David Ronfeldt

Cyberwar Is Coming!*

"Knowledge must become capability."
Carl von Clausewitz, On War

Emergent Modes of Conflict

Suppose that war looked like this: Small numbers of your 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. Your 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 "topsight" for strategic purposes.

For your forces, warfare is no longer primarily a function of who puts the most capital, labor, and technology on the battlefield, but of who has the best information about the battlefield. What distinguishes the victors is their grasp of information–not only from the mundane standpoint of knowing how to find the enemy while keeping it in the dark, but also in doctrinal and organizational terms. The analogy is rather like a chess game where you see the entire board, but your opponent sees only his own pieces; you can win even if he is allowed to start with additional powerful pieces.

We might appear to be extrapolating from the U.S. victory in the Persian Gulf war against Iraq. But our vision is inspired more by the example of the Mongols of the thirteenth 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.

Absent the galvanizing threat that used to be posed by the Soviet Union, domestic political pressures will encourage the United States to make do with a smaller military in the future. The type of war-fighting capability that we envision, which is inspired by the Mongol example, but drawn mainly from our analysis of the information revolution, may allow America to protect itself and its far-flung friends and interests, regardless of the size and strength of our potential future adversaries.

The Advance of Technology and Know-How

Throughout history, military doctrine, organization, and strategy have continually undergone profound changes, owing in part to technological breakthroughs. The Greek phalanx, the combination of gun and sail, the levee en masse, the blitzkrieg, the Strategic Air Command: history is filled with examples in which new weapon, propulsion, communication, and transportation technologies provided a basis for advantageous shifts in doctrine, organization, and strategy that enabled innovators to avoid exhausting attritional battles and pursue instead a form of "decisive" warfare.[1]

Today, a variety of new technologies are again taking hold, and further innovations are on the way. The most enticing include non-nuclear high-explosives, precision-guided munitions, stealth designs for aircraft, tanks, and ships, radio-electronic combat (REC) systems; new electronics for intelligence-gathering, interference, and deception, new information and communications systems that improve command, control, communications and intelligence (C3I) functions, and futuristic designs for space-based weapons and for automated and robotic warfare. In addition, virtual reality systems are being developed for simulation and training. Many of these advances enter into a current notion of a military technology revolution (MTR).[2]

The future of war–specifically the U.S. ability to anticipate and wage war–will be shaped in part by how these technological advances are assessed and adopted. Yet, as military historians frequently warn, technology permeates war but does not govern it. It is not technology per se, but rather the organization of technology, broadly defined, that is important. Russell Weigley describes the situation this way:

"… the technology of war does not consist only of instruments intended primarily for the waging of war. A society's ability to wage war depends on every facet of its technology: its roads, its transport vehicles, its agriculture, its industry, and its methods of organizing its technology. As Van Creveld puts it, 'behind military hardware there is hardware in general, and behind that there is technology as a certain kind of know-how, as a way of looking at the world and coping with its problems.'"[3]

In our view, the technological shift that matches this broad view is the information revolution. This is what will bring the next major shift in the nature of conflict and warfare.

Effects of the Information Revolution

The information revolution reflects the advance of computerized information and communications technologies and related innovations in organization and management theory. 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.[4] Information is becoming a strategic resource that may prove as valuable and influential in the post-industrial era as capital and labor have been in the industrial age.

Advanced information and communications systems, properly applied, can improve the efficiency of many kinds of activities. But improved efficiency is not the only, or even the best, possible effect. The new technology is also having a transforming effect, for it disrupts old ways of thinking and operating, provides capabilities to do things differently, and suggests how some things may be done better if done differently:

"The consequences of new technology can be usefully thought of as first-level, or efficiency, effects and second-level, or social system, effects. The history of previous technologies demonstrates that early in the life of a new technology, people are likely to emphasize the efficiency effects and underestimate or overlook potential social system effects. Advances in networking technologies now make it possible to think of people, as well as databases and processors, as resources on a network.

"Many organizations today are installing electronic networks for first-level efficiency reasons. Executives now beginning to deploy electronic mail and other network applications can

realize efficiency gains such as reduced elapsed time for transactions. If we look beyond efficiency at behavioral and organizational changes, we'll see where the second-level leverage is likely to be. These technologies can change how people spend their time and what and who they know and care about. The full range of payoffs, and the dilemmas, will come from how the technologies affect how people can think and work together–the second-level effects"[5].

The information revolution, in both its technological and non-technological aspects, 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 what may be considered weaker, smaller actors. It crosses borders, and redraws the boundaries of offices and responsibilities. It expands the spatial and temporal horizons that actors should take into account. And thus, it generally compels closed systems to open up. But while this may make life difficult, especially for large, bureaucratic, aging institutions, the institutional form per se is not becoming obsolete. Institutions of all types remain essential to the organization of society. The responsive, capable institutions will adapt their structures and processes to the information age. Many will evolve from traditional hierarchical forms to new, flexible, network-like models of organization. Success will depend on learning to interlace hierarchical and network principles.[6]

Meanwhile, the very changes that trouble institutions–the erosion of hierarchy, etc.–favor the rise of multi-organizational networks. Indeed, the information revolution is strengthening the importance of all forms of networks–social networks, communications networks, etc. The network form is very different from the institutional form. While institutions (large ones, in particular) are traditionally built around hierarchies and aim to act on their own, multi-organizational networks consist of (often small) organizations or parts of institutions that have linked together to act jointly. The information revolution favors the growth of such networks by making it possible for diverse, dispersed actors to communicate, consult, coordinate, and operate together across greater distances, and on the basis of more and better information than ever before.[7]

These points bear directly on the future of the military, and of conflict and warfare more generally.

Both Netwar and Cyberwar Are Likely

The thesis of this thinkpiece is that 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 ideational conflicts waged in part through internetted modes of communication–and "cyberwar" at the military level. These terms are admittedly novel, and better ones may yet be devised.[8] But, for now, they help illuminate a useful distinction, and identify the breadth of ways in which the information revolution may alter the nature of conflict short of war, as well as the context and the conduct of warfare.[9]

While both netwar and cyberwar revolve around information and communications matters, at a deeper level they are forms of war about "knowledge"–about who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries.[10]

Explaining Netwar. Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify 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 public diplomacy measures, 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. Thus, designing a strategy for netwar may mean grouping together from a new perspective a number of measures that have been used before but were viewed separately.

In other words, 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. Like other forms on this spectrum, netwars would be largely non-military, but they could have dimensions that overlap into military war. For example, an economic war may involve trade restrictions, the dumping of goods, the illicit penetration and subversion of businesses and markets in a target country, and the theft of technology–none of which need involve the armed forces. Yet an economic war may also come to include an armed blockade or strategic bombing of economic assets, meaning it has also become a military war. In like manner, a netwar that leads to targeting an enemy's military C3I capabilities turns, at least in part, into what we mean by cyberwar.

Netwar will take various forms, depending on the actors. Some may occur between the governments of rival nation-states. In some respects, the U.S. and Cuban governments are already engaged in a netwar. This is manifested in the activities of Radio and TV Marti on the U.S. side, and on Castro's side by the activities of pro-Cuban support networks around the world.

Other kinds of netwar may arise between governments and non-state actors. For example, these may be waged by governments against illicit groups and organizations involved in terrorism, proliferation of weapons of mass destruction, or drug smuggling. Or, to the contrary, it may be waged against the policies of specific governments by advocacy groups and movements–e.g., regarding environmental, human-rights, or religious issues. The non-state actors may or may not be associated with nations, and in some cases they may be organized into vast transnational networks and coalitions.

Another kind of netwar may occur between rival non-state actors, with governments maneuvering on the sidelines to prevent collateral damage to national interests and perhaps to support one side or another. This is the most speculative kind of netwar, but the elements for it have already appeared, especially among advocacy movements around the world. Some movements are increasingly organizing into cross-border networks and coalitions, identifying more with the development of civil society (even global civil society) than with nation-states, and using advanced information and communications technologies to strengthen their activities. This may well turn out to be the next great frontier for ideological conflict, and netwar may be a prime characteristic.

Most netwars will probably be non-violent, but in the worst cases one could combine the possibilities into some mean low-intensity conflict scenarios. Martin Van Creveld [11] does this when he worries that, "In the future, war will not be waged by armies but by groups whom today we call terrorists, guerrillas, bandits and robbers, but who will undoubtedly hit on more formal titles to describe themselves." In his view, war between states will diminish, and the state may become obsolete as a major form of societal organization. Our views coincide with

many of Van Creveld's, though we do not believe that the state is even potentially obsolete. Rather, it will be transformed by these developments.

Some netwars will involve military issues. Possible issue areas include nuclear proliferation, drug smuggling, and anti-terrorism because of the potential threats they pose to international order and national security interests. Moreover, broader societal trends (e.g., the redefinition of security concepts, the new roles of advocacy groups, the blurring of traditional boundaries between what is military and what is non-military, between what is public and what is private, and between what pertains to the state and what pertains to society) may engage the interests of at least some military offices in some netwar-related activities.

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'sforce posture and presence.

Explaining Cyberwar. Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting, if not destroying, information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, and so forth. 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 C3I, for intelligence collection, processing, and distribution, for tactical communications, positioning, and identification-friend-or-foe (IFF), 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. Yet, cyberwar is not simply a set of measures based on technology. And it should not be confused with past meanings of computerized, automated, robotic, or electronic warfare.

Cyberwar may have broad ramifications for military organization and doctrine. As noted, the literature on the information revolution calls for organizational innovations, so that different parts of an institution function like interconnected networks rather than separate hierarchies. Thus, cyberwar may imply some institutional redesign for a military in both intra- and inter-service areas. Moving to networked structures may require some decentralization of command and control, which may well be resisted in light of earlier views that the new technology would provide greater central control of military operations. 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.[12] Many treatments of organizational redesign laud decentralization; yet decentralization alone is not the key issue. The 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 what and how to strike on the enemy's side. How and where to position what kinds of computers and related sensors, networks, databases, and so forth., may become as important as the question once was for the deployment of bombers and their

support functions. Cyberwar may also have implications for integrating the political and psychological with the military aspects of warfare.

In sum, cyberwar may raise broad issues of military organization and doctrine, as well as strategy, tactics, and weapons design. It may be applicable in low- and high-intensity conflicts, in conventional and non-conventional environments, and for defensive or offensive purposes.

As an innovation in warfare, we anticipate that cyberwar may be to the twenty first century what blitzkrieg was to the twentieth century. Yet, for now, we also believe that the concept is too speculative for precise definition. At a minimum, it represents an extension of the traditional importance of obtaining information in war: having superior C3I and trying to locate, read, surprise, and deceive the enemy before he does the same to you. That remains important no matter what overall strategy is pursued. In this sense, the concept means that information-related factors are more important than ever due to new technologies, but it does not indicate a break with tradition. Indeed, it resembles Thomas Rona's [13] concept of an "information war" that is "intertwined with, and superimposed on, other military operations." Our concept is broader than Rona's, which focused on countermeasures to degrade an enemy's weapons systems while protecting one's own; yet, we believe that this approach to defining cyberwar will ultimately prove too limiting.

In a deeper sense, cyberwar signifies a transformation in the nature of war. This, we believe, will prove to be the better approach to defining cyberwar. Our position is at odds with a view [14] that uses the terms "hyperwar" and "cyberwar" to claim that the key implication of the MTR is the automated battlefield, that future wars will be fought mainly by "brilliant" weapons, robots, and autonomous computers, that man will be subordinate to the machine, and that combat will be unusually fast and laden with stand-off attacks. This view errs in its understanding of the effects of the information revolution, and our own view differs on every point. Cyberwar is about organization as much as technology. It implies new man-machine interfaces that amplify man's capabilities, not a separation of man and machine. In some situations, combat may bewaged fast and from afar, but in many other situations, it may be slow and close-in. New combinations of far and close and fast and slow may be the norm, not one extreme or the other.The post-modern battlefield stands to 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 C3I matters to the point where dominance in this aspect alone may now yield consistent war-winning advantages to able practitioners. Yet cyberwar is a much broader idea than attacking an enemy's C3I systems while improving and defending one's own. In Clausewitz's sense, it is characterized by the effort to turn knowledge into capability.

Indeed, even though its full design and implementation requires advanced technology, cyberwar is not reliant upon advanced technology per se. The continued development of advanced information and communications technologies is crucial for U.S. military capabilities. But cyberwar, whether waged by the United States or other actors, does not necessarily require the presence of advanced technology. The organizational and psychological dimensions may be as important as the technical. Cyberwar may actually be waged with low technology under some circumstances.

Information-related Factors in Military History

Our contention is that netwar and cyberwar represent new (and related) modes of conflict that will be increasingly important in the future. The information revolution implies–indeed, it assures–that a sea-change is occurring in the nature of conflict and warfare. Yet both new modes have many historical antecedents; efforts have been made in the direction of conducting warfare from cyber-like perspectives in the past. Information, communications, and control are enduring concerns of warfighters. There is much historical evidence, tactical and strategic, that attempting to pierce the "fog of war" and envelop one's foe in it has played a continuing role.[15]

In the Second Punic War of the third century B.C., Carthaginian forces under the command of Hannibal routinely stationed observers with mirrors on hilltops, keeping their leader apprised of Roman movements, while the latter remained ignorant of his. Better communications contributed significantly to the ability of Hannibal's forces to win a string of victories over a 16-year period. In the most dramatic example of the use of superior information, Hannibal's relatively small forces were able rise literally from the fog of war at Lake Trasimene to destroy a Roman army more than twice its size.[16]

Another famous, more recent example, occurred during the Napoleonic Wars. The British Royal Navy's undisputed command of the Mediterranean Sea, won at the Battle of the Nile in 1798, cut the strategic sea communications of Bonaparte's expeditionary force in North Africa, leading to its disastrous defeat. The invaders were stranded in Egypt without supplies or their commander, after Napoleon's flight, where they remained until the British came to take them prisoner.

A few years later in the same conflict, Lord Cochrane's lone British frigate was able to put French forces into total confusion along virtually the entire Mediterranean coast of occupied Spain and much of France. The French relied for their communications on a semaphore system to alert their troops to trouble and to tell coastal vessels when they could safely sail. Cochrane raided these signalling stations, then struck spectacularly, often in conjunction with Spanish guerrilla forces, while French communications were disrupted.[17]

Story upon story could be drawn from military history to illuminate the significance of information and communications factors. But this is meant to be only a brief paper to posit the concept of cyberwar. Better we turn directly to an early example, a virtual model of this upcoming mode of warfare.

An Early Example of Cyberwar: The Mongols

Efforts to strike at the enemy's communications and ensure the safety of one's own are found, to varying degrees, throughout history. Yet the Mongol way of warfare, which reached its zenith in the twelfth and thirteenth centuries, may be the closest that anyone has come to waging pure cyberwar (or netwar, for that matter). Examining Mongol military praxis should, therefore, be instructive in developing the foundations for waging war in a like manner in the post-modern world. Use of this example also reinforces the point that cyberwar does not depend on high technology, but rather on how one thinks about conflict and strategic interaction.

At the military level, Mongol doctrine relied for success almost entirely on learning exactly where their enemies were, while keeping their own whereabouts a secret until they attacked. This enabled them, despite a chronic inferiority in numbers, to overthrow the finest, largest armies of Imperial China, Islam, and Christendom.

The simplest way to illustrate their advantage is to suggest an analogy with chess: war against the Mongols resembled playing against an opponent who can hide the dispositions of his pieces, but who can see the placement of both his and yours. Under such conditions, the player with knowledge of both sides' deployments could be expected to triumph with many fewer pieces. Moreover, the addition of even significant forces to the semi-blinded side would generate no requirement for a similar increase on the "sighted" side. (Thus, the similarity is not so much to chess as to its cousin, kriegspiel, in which both players start "blind" to their opponent's position. In our analogy, one player can see through the barrier that is normally placed between the boards of the players.)

So it was with the Mongols. In one of their greatest campaigns, against the mighty Muslim empire of Khwarizm (located approximately on the territory of today's Iran, Iraq, and portions of the Central Asian republics of the former Soviet Union), a Mongol army of some 125,000 toppled a foe whose standing armies amounted to nearly half a million troops, with a similar number of reserves. How could this happen? The answer is that the Mongols identified the linear, forward dispositions of their foes and avoided them. Instead, they worked around the defenders, making a point of waylaying messengers moving between the capital and the "front."

Muhammad Ali Shah, the ruler of Khwarizm, took the silence from the front as a good sign, until one day a messenger, having narrowly escaped a Mongol patrol, made his way into the capital, Samarkand. Muhammad inquired about the news from his army and was told that the frontier was holding. The messenger went on to add, however, that he had observed a large Mongol army but a day's march from the capital. The shah fled and his capital fell swiftly. This news, when given to the frontier armies, led to a general capitulation. Muhammad ended his days in hiding on the island of Abeshkum in the Caspian Sea, where he contracted and died from pleurisy.

The campaign against Khwarizm is typical of the Mongol strategic approach of first blinding an opponent, then striking at his heart (i.e., going for checkmate). Battles were infrequently fought, as they were often unnecessary for achieving war aims. There were times, however, when confrontations could not be avoided. When this happened, the Mongols relied heavily on coordinated operations designed to break down the plans and controls of their opponents. Against the Polish-Prussian coalition forces at the battle of Liegnitz, for example, the Mongols engaged and defeated an army some four times their size. Their success was based on keeping a clear picture of the defending coalition's order of battle, while confusing the opponents as to their own whereabouts. Thus, portions of the Western army chased after small detachments that were simple lures, and ended up in the clutches of the Mongol main force. The Poles and Prussians were defeated piecemeal. Indeed, the Mongols were so sure of their information that they repeatedly used a river crossing during the battle in the intervals between its use by the Poles and Prussians.[18]

What about Mongol advantages in mobility and firepower? Certainly, their ability to move a division some 80 miles per day was superior to other armies, and their horn bows did outrange those of their enemies by 50-100 yards, on average. But neither of thes factors could offset their foesU advantages in fortification technology, and the body armor of Western forces gave them distinct advantages over the Mongols in close combat. Thus, Mongol tactical operations were often significantly stymied by defended cities,[19] and close engagements were exceedingly hard fought, with the Mongols suffering heavily. Indeed, the ferocity and effectiveness of the Prusso-Polish forces at Liegnitz, especially their cavalry, may have deterred the Mongols from continuing their invasion of Europe.[20] At the battle of Hims, the

Mamelukes showed that the forces of Islam could also defeat the Mongols tactically. What neither Islam nor Christendom could do consistently, however, was outwit the Mongols strategically.

Clearly, the key to Mongol success was superior command, control, communication, and intelligence. Scouts and messengers always took along three or four extra horses, tethered, so that they could switch mounts and keep riding when one grew tired. This gave the Mongol horsemen, in relative terms, something approximating an ability to provide real-time intelligence, almost as from a satellite, on the enemy's order of battle and intentions. At the same time, this steppe-version of the "Pony Express" (the Khan called them "Arrow Riders") enabled field generals to keep the high command, often thousands of miles from the theater of war, informed as to all developments within four or five days of their occurrence. For communication between field forces, the Mongols also employed a sophisticated semaphore system that allowed for swift tactical shifts as circumstances demanded. Organizationally, the Mongols emphasized decentralized command in the field, unlike their foes who were generally required to wait for orders from their capitals. Yet by developing a communication system that kept their leadership apprised at all times, the Mongols enjoyed topsight as well as decentralization. The Khan "advanced his armies on a wide front, controlling them with a highly developed system of communication"; that was the secret of his success [21].

In strategic terms, the Mongols aimed first to disrupt an enemy's communications, then to strike at his heart. Unlike Clausewitz, they put little store in the need to destroy enemy forces before advancing. Also, Mongol campaigns were in no way "linear." They struck where they wished, when circumstances were deemed favorable. That their Christian and Muslim foes seldom emulated the Mongol's organizational and communication techniques is to their great discredit. When, finally, the Mamelukes defeated the Mongols attempted invasion of Egypt, it was because they kept track of Mongol movements and were led in the field by their king, Kilawan, who exercised rapid, effective control of his forces in the fluid battle situations that ensued. Also, the Mamelukes, employing carrier pigeons, had developed faster strategic communications than even the Mongols' arrow riders, allowing them to mass troops in time to defend effectively.[22]

As much as they form a paradigm for cyberwar, the Mongols were also adept at netwar. Early in their campaigns, they used terror tactics to weaken resistance. At the outset of any invasion, they broadcast that any city that resisted would be razed and its inhabitants slaughtered. Surrender, on the other hand, would result simply in coming under Mongol suzerainty; this entailed some initial rape and pillage, but thereafter settled into a distracted sort of occupation. As a result, peaceful surrenders were plentiful. In later campaigns, when the Mongols learned that both Christians and Muslims saw them as the dark forces of Gog and Magog, heralding the "end of times," they deliberately cultivated this image. They renamed themselves Tartars, as though they were the minions of "tartarum," the biblical nether world. Later, when it was clear that the world was not ending, the Mongols willingly adopted both Christianity and Islam, whichever eased the burden of captivity for particular peoples. This utilitarian approach to religion impeded the formation of opposing coalitions.

Some analysts have argued that the Mongols represent an early experiment with blitzkrieg.[23] In our view, however, the differences between cyberwar and blitzkrieg are significant, and the Mongols reflect the former more than the latter.

Blitzkrieg, People's War, and Beyond

The relative importance of war against an enemy's command, control, and communications increased with the advent of mechanized warfare. In World War II, the German blitzkrieg doctrine–in some ways a forerunner of cyberwar–made the disruption of enemy communications and control an explicit goal at both the tactical and strategic levels. For example, the availability of radios in all of its tanks provided Germany with a tactical-force multiplier in its long war with the Soviet Union, whose tanks, though more numerous and better built, provided radios only for commanders.[24]

At the strategic level, the destruction of the Soviets' central communications and control site, by capturing Moscow, was a key element of the planning for Operation Barbarossa. But when an opportunity arose during the campaign to win large material gains in the Ukraine, Hitler diverted General Guderian's panzers away from their approach to Moscow, and it was never taken. There would be no "lightning" victory for the Germans, who soon found themselves on the weaker side of a massive attritional struggle, doomed to defeat.[25]

Following WWII, information and communication technologies improved greatly in the major industrialized nations, and the important wars with lessons for cyberwar were between these nations and the underdeveloped ones of the Third World. A comparison of two key conflicts illuminates the growing importance and applicability of cyberwar principles: the one a peoples' war waged by North Vietnam and the Viet Cong in the 1960s and 1970s, and the other recent, more conventional conflict between the American-led coalition and Iraq– illuminates the growing importance and applicability of cyberwar principles.

Both wars represent turning points. In the case of Vietnam, the enemy may have applied cyber principles more effectively than did the United States–not only in military areas, but also where cyberwar cuts into the political and societal dimensions of conflict. In the case of the war against Iraq, the United States did superior work applying cyberwar principles–they were not called that at the time, of course–against an enemy whose organization, doctrine, strategy, and tactics were from a different era.

In the Vietnam war, the United States appeared to have advantages up and down the chain of command and control, from the construction of quantitative indicators and computerized models and databases for analyzing the course of the war in Washington, through field radios for calling in prompt airstrikes, reinforcements, and rescue operations. But the thrall of computerization and quantitative techniques led analysts to overlook the softer, subtler aspects of the war where the enemy was winning. The excellence of U.S. communications capabilities encouraged inappropriate intrusion from above into battles and campaigns best planned and waged within the theater.

While U.S. forces had superior tactical communications, the guerrillas' strategic communications were largely unaffected. Meanwhile, the North Vietnamese and Viet Cong operated on Mao Zedong's doctrine that "command must be centralized for strategical purposes and decentralized for tactical purposes"[26]–a classic combination of topsight and decentralization. The United States, on the other hand, appears to have allowed the timely availability of vast quantities of information at high levels to seduce leadership into maintaining central tactical as well as strategic control, and into believing that they had topsight when they did not.

The Vietnam example illustrates our point that good communications, though they provide necessary conditions, are insufficient to enable one to fight a cyberwar. For this endeavor, a doctrinal view of the overarching importance and value of maintaining one's own

communications, while disabling the adversary's, is requisite. This entails the development of tactics and operational strategies that discard the basic tenets of both set-piece and even traditional maneuver warfighting theories. Neither the grinding attritional approach of Grant nor the explosive thrusts of Guderian will suffice. Instead, radically different models must be considered that focus upon the objective of systemically disorganizing the enemy.

To some extent, the recent American experience in the Gulf War suggests that an increasing sensitivity to cyber principles is taking hold. First, it was made quite clear by President Bush that he had no intention of micro-managing tactical or even operationally strategic actions. This is, in itself, a stark contrast to the classic image of President Johnson poring over maps of North Vietnam, selecting each of the targets to be hit by Operation Rolling Thunder.

The military operations brought significant cyber elements into play, often utilizing them as "force multipliers"[27]. The Apache helicopter strike against Iraqi air defense controls at the war's outset is but one, albeit very important, example. Also, the allied coalition had good knowledge of Iraqi dispositions, while the latter were forced to fight virtually blind. Along these lines, a further example of the force multiplying effect of command of information is provided by the ability of a relatively small (less than 20,000 troops) Marine force afloat to draw away from the landward front and tie down roughly 125,000 Iraqi defenders.

A significant effort was also made to employ netwar principles in the Gulf war. The construction of an international consensus against the Iraqi aggression, backed by the deployment of large, mechanized forces, was intended to persuade Saddam Hussein to retreat. His intransigent behavior suggests that his vision of war was of a prior generation.

An Implication: Institutions Versus Networks

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. Moreover, the information revolution favors organizational network designs. These points were made in the first section of this paper.

This second section leads to related insights, based on a quick review of history. 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, a relatively minor military power that defeated a great modern power–the combined forces of North Vietnam and the Viet Cong–operated in many respects more like a network than an institution; these forces even extended political-support networks abroad. In both cases, the Mongols and the Vietnamese, their defeated opponents were large institutions whose forces were designed to fight set-piece attritional battles.

To this may be added a further set of observations drawn from current events. 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, as well as racial and tribal gangs–are all organized like networks (although their leadership may be quite hierarchical). Perhaps a reason that military (and police) institutions have difficulty engaging in low-intensity conflicts is because they are not meant to be fought by institutions.

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.

Issues for the Future

The implications of a revolutionary technology are often not widely perceived at first. That was true of the tank, the machine gun, and the telephone. For example, with their newly developed, rapid firing mitrailleuse, the French enjoyed a tremendous potential firepower advantage over the Prussians in 1870. Unfortunately, this early version of the machine gun looked more like a fieldpiece instead of a rifle, and it was deployed behind the front with the artillery. Thus, the weapon that would dominate World War I a generation later had almost no effect on the Franco-Prussian conflict. People try to fit new technology into established ways of doing things; it is expected to prove itself in terms of existing standards of efficiency and effectiveness.

It may take time to realize that inserting new technology into old ways may create some new inefficiencies, even as some activities become more efficient. It may take still more time to realize that the activity itself, in both its operational and organizational dimensions, should be restructured, even transformed, in order to realize the full potential of the technology.[28] This pattern is documented in the early histories of the telephone and the electric motor, and is being repeated with computer applications in the business world.

Why should anything different be expected for cyberwar? New information technology applications have begun to transform the business world both operationally and organizationally. The government world is, for the most part, moving slowly in adopting the information technology revolution. One might expect the military world to lag behind both the business and government worlds, partly because of its greater dependence on hierarchical traditions. But in fact, parts of the U.S. military are showing a keen interest in applying the information revolution. As this unfolds, a constant, but often halting, contentious interplay between operational and organizational innovations should be expected.

Growing Awareness of the Information Revolution

An awareness is spreading in some U.S. military circles that the information revolution may transform the nature of warfare. One hears that the MTR implies a period of re-evaluation and experimentation not unlike the one in the 1920s and 1930s that resulted in Germany's breakthrough formulation of the blitzkrieg doctrine. New questions are being asked about how to apply the new technology in innovative ways. For example, one set of arguments holds that the MTR may increasingly enable armed forces to stand off and destroy enemy targets with high precision weapons fired from great distances, including from outer space. But, another set holds that the information revolution may drive conflict and warfare toward the low-intensity end of the scale, giving rise to new forms of close-in combat. Clearly, military analysts and strategists are just beginning to identify the questions and call for the required thinking.

The military, like much of the business world, remains in a stage of installing pieces of the new technology to make specific operations more effective. Indeed, techniques that we presume would be essential to cyberwar may be used to improve the cost-effectiveness of many military operations, no matter what overall strategy is being pursued (even if cyberwar remains unformulated). For example, improved surveillance and intelligence-gathering capabilities that help identify timely opportunities for surprise (to some extent, a purpose of

the new Joint Targeting Network (JTN) can be of service to a traditional attritional warfare strategy. Also, new capabilities for informing the members of a unit in real time about where their comrades are located and what each is doing, as in recent experiments with inter-vehicular information systems (IVIS, may improve the ability to concentrate force as a unit, and maintain that concentration throughout an operation. The list of new techniques that could be mentioned is long and growing.

We favor inquiring methodically into how the information revolution may provide specific new technical capabilities for warfare, regardless of the doctrine and strategy used. We also favor analyzing what kinds of operational and organizational innovations should be considered in light of such capabilities. And we recognize that it is quite another thing to try to leap ahead and propose that cyberwar may be a major part of the answer. But this thinkpiece is not meant to be so methodical; it is meant to be speculative and suggestive, in order to call attention to the possibility of cyberwar as a topic that merits further discussion and research.

Indications and Aspects of Cyberwar

New theoretical ground needs to be broken regarding the information and communications dimensions of war, and the role of "knowledge" in conflict environments. Cyberwar is not merely a new set of operational techniques. It is emerging, in our view, as a new mode of warfare that will call for new approaches to plans and strategies, and new forms of doctrine and organization.

What would a cyberwar look like? Are there different types? What may be the distinctive attributes of cyberwar as a doctrine? Where does cyberwar fit in the history of warfare, and why would it represent a radical shift? What are the requirements and options for preparing for and conducting a cyberwar? Will it enable power to be projected in new ways? What are the roles of organizational and technological factors?— and what other factors (e.g., psychological) should be considered? How could the concept enable one to think better, or at least differently in a useful way, about factors, such as C3I, REC (radio-electronic combat systems), and psywar–that are important but not ordinarily considered together? What measures of effectiveness (MOE) should be used? These kinds of questions–some of which are touched on in this paper–call for examination.

Paradigm Shift. We anticipate that cyberwar, like war in Clausewitz's view, may be a "chameleon." It will be adaptable to varying contexts; it will not represent or impose a single, structured approach. Cyberwar may be fought offensively and defensively, at the strategic or tactical levels. It will span the gamut of intensity, from conflicts waged by heavy mechanized forces across wide theaters, to counterinsurgencies where "the mobility of the boot" may be the prime means of maneuver.

Consider briefly the context of blitzkrieg. This doctrine for offensive operations, based on the close coordination of mobile armored forces and air power, was designed for relatively open terrain and good weather. Its primary asset was speed; swift breakthroughs were sought, and swift follow-ups required to prevent effective defensive ripostes.

"The blitzkrieg is predicated upon the assumption that the opponent's army is a large and complex machine that is geared to fighting along a well-established defensive line. In the machine's rear lies a vulnerable network, which comprises numerous lines of communication, along which supplies as well as information move, and key nodal points at which the various

lines intersect. Destruction of this central nervous system is tantamount to destruction of the army. The principal aim of a blitzkrieg is therefore to effect a strategic penetration. The attacker attempts to pierce the defender's front and then to drive deep into the defender's rear, severing his lines of communication and destroying key junctures in the network."[29]

By comparison, cyberwar takes a different view of what constitutes the "battlefield." Cyberwar depends less on the geographic terrain than on the nature of the electronic "cyberspace,"[30] which should be open to domination through advanced technology applications. Cyberwar benefits from an open radio-electronic spectrum and good atmospheric and other conditions for utilizing that spectrum. Cyberwar may require speedy flows of information and communications, but not necessarily a speedy or heavily armed offense like blitzkrieg. If the opponent is blinded, it can do little against even a slow-moving adversary. How, when, and where to position battlefield computers and related sensors, communications networks, databases, and REC devices may become as important in future wars as the same questions were for tanks or bomber fleets and their supporting equipment in the World War II.

Cyberwar may imply a new view, not only of what constitutes "attack," but also of "defeat." Throughout the era of modern nation-states, beginning about the sixteenth century, attrition has been the main mode of warfare. An enemy's armed forces had to be defeated before objectives could be taken. This lasted for centuries until the grotesque, massive slaughters of World War I led to a search for relief from wars of exhaustion. This in turn led to the development of blitzkrieg, which circumvented the more brutish aspects of attritional war. Yet this maneuver-oriented doctrine still required the destruction of the enemy's forces as the prerequisite to achieving war aims; attritional war had simply been "put on wheels."

Cyberwar may also imply (although we are not sure at this point) that victory can be attained without the need to destroy an opposing force. The Mongol defeat of Khwarizm is the best example of the almost total circumvention and virtual dismemberment of an enemy's forces. It is possible to see in cyberwar an approach to conflict that allows for decisive campaigning without a succession of bloody battles. Cyberwar may thus be developed as a post-industrial doctrine that differs from the industrial-age traditions of attritional warfare. It may even seek to avoid attritional conflict.[31] In the best circumstances, wars may be won by striking at the strategic heart of an opponent's cyber structures, his systems of knowledge, information, and communications.

It is hard to think of any kind of warfare as humane, but a fully articulated cyberwar doctrine might allow the development of a capability to use force not only in ways that minimize the costs to oneself, but which also allow victory to be achieved without the need to maximize the destruction of the enemy. If for no other reason, this potential of cyberwar to lessen war's cruelty demands its careful study and elaboration.

Organizational and Related Strategic Considerations. At the strategic level, cyberwar may imply Mao's military ideal of combining strategic centralization and tactical decentralization. The interplay between these effects is one of the more complex facets of the information revolution. Our preliminary view is that the benefits of decentralization may be enhanced if, to balance the possible loss of centralization, the high command gains topsight, the term mentioned earlier that we currently favor to describe the view of the overall conflict. This term carries with it an implication that temptations to micro-manage will be resisted.

The new technology tends to produce a deluge of information that must be taken in, filtered, and integrated in real time. Informational overload and bottlenecking has long been a vulnerability of centralized, hierarchical structures for command and control.[32] Waging cyberwar may require major innovations in organizational design, in particular a shift from hierarchies to networks. The traditional reliance on hierarchical designs may have to be adapted to network-oriented models to allow greater flexibility, lateral connectivity, and teamwork across institutional boundaries. The traditional emphasis on command and control, a key strength of hierarchy, may have to give way to an emphasis on consultation and coordination, the crucial building blocks of network designs. This may raise transitional concerns about how to maintain institutional traditions, as various parts become networked with other parts (if not with other, outside institutions) in ways that may go "against the grain" of existing hierarchies.

The information revolution has already raised issues for inter- and intra-service linkages, and in the case of coalition warfare, for inter-military linkages. Cyberwar doctrine may require such linkages. It may call for particularly close communication, consultation and coordination between the officers in charge of strategy, plans, and operations, and those in charge of C3I, not to mention units in the field.

Operational and tactical command in cyberwar may be exceptionally demanding. There may be little of the traditional chain of command to evaluate every move and issue each new order. Commanders, from corps to company levels, may be required to operate with great latitude. But if they are allowed to act more autonomously than ever, they may also have to act more as a part of integrated joint operations. Topsight may have to be distributed to facilitate this. Also, the types and composition of units may undergo striking changes. Instead of divisions, brigades and battalions, cyberwar may require the creation of combined-arms task forces from each of the services, something akin to the current Marine Air-Ground Task Force.

There are many historical examples of innovative tinkering with units during wartime, going back to the creation of the Roman maniple as a counter to the phalanx. In modern times, World War II brought the rise of many types of units never before seen. For example, the U.S. Army began using combat commands or teams comprised of artillery-armor-infantry mixes. The German equivalent was the Kampfgruppe. These kinds of units could often fulfill missions for which larger bodies, even corps, had previously failed. The U.S. Navy was also an innovator in this area, creating the task force as its basic operating unit in the Pacific War. Our point here is that what have often been viewed as makeshift wartime organizational adjustments should now be viewed as a peacetime goal of our standing forces, to be achieved before the onset of the next war.

Force Size Considerations. A cyberwar doctrine and accompanying organizational and operational changes may allow for reductions in the overall size of the U.S. armed forces. But if the history of earlier sea-changes in the nature of warfighting is any guide, long-term prospects for significant reductions are problematic. All revolutions in warfare have created advantages that became subject to fairly rapid "wasting," since successful innovations were quickly copied.[33]

If both sides to a future conflict possess substantial cyberwar capabilities, the intensity and complexity of that war may well require more rather than fewer forces. The better trained, more skillful practitioner may prevail, but it is likely that "big battalions" will still be necessary, especially as the relative cyberwar-fighting proficiency of combatants nears parity.

In any case, whether future U.S. forces are larger or smaller, they will surely be configured quite differently.

Operational and Tactical Considerations. Cyberwar may also have radical implications at the operational and tactical levels. Traditionally, military operations have been divisible into categories of "holding and hitting." Part of a force is used to tie down an opponent, freeing other assets for flank and other forms of maneuvering attacks.[34] Tactically, two key aspects of warfighting have been fire and movement. Covering fire allows maneuver, with maneuver units then firing to allow fellow units to move. Fire creates maneuver potential. Tactical advance is viewed as a sort of leapfrogging affair.

Cyberwar may give rise to different, if not opposite, principles. Superior knowledge and control of information are likely to allow for "hitting without holding," strategically, and for tactical maneuvers that create optimal conditions for subsequent fire.

Nuclear Considerations. What of nuclear weapons and cyberwar? Future wars that may involve the United States will probably be non-nuclear, for two reasons. First, the dismantling of the Soviet Union is likely to persist, with further arms reductions making nuclear war highly unlikely. Second, the United States is ill-advised to make nuclear threats against non-nuclear powers.

Besides the lack of central threat and the normative inhibitions against using nuclear forces for coercive purposes, there is also a practical reason for eschewing them in this context: bullying could drive an opponent into the arms of a nuclear protector, or spur proliferation by the threatened party. However, even a successful proliferator will prefer to keep conflicts conventional, as the United States will continue to maintain overwhelming counterforce and countervalue advantages over all nascent nuclear adversaries. Therefore, the likelihood that future wars, even major ones, will be non-nuclear adds all the more reason to make an effort to optimize our capabilities for conventional and unconventional wars by developing a cyberwar doctrine.

In the body of strategic and operational thought surrounding war with weapons of mass destruction, an antecedent of cyberwar is provided. Nuclear counterforce strategies were very much interested in destroying the key communications centers of the opponent, thereby making it impossible for him to command and control far-flung nuclear weapons. The "decapitation" of an opponent's leadership was an inherently cyber principle. The dilemmas of mutual deterrence forced this insight into warfighting to remain in a suspended state for some decades.

Before leaving nuclear issues, we would note an exception in the case of naval warfare. Because the United States enjoys an overwhelming maritime pre-eminence, it is logical that our potential adversaries may seek ways to diminish or extinguish it. Nuclear weapons may thus grow attractive to opponents whose navies are small, if the pursuit of their aims requires nullifying our sealift capabilities. A century ago, the French Jeune Ecole, by developing swift vessels capable of launching a brand new weapon, the torpedo, sought to counter the Royal Navy's power in international affairs. Today, latter-day navalists of continental or minor powers may be driven to seek their own new weapons.[35]

Fortunately, the U.S. Navy has been following a path that elevates the information and communication dimensions of war to high importance. For, at sea, to be located is to become immediately vulnerable to destruction. In fact, naval war may already be arriving at a doctrine

that looks a lot like cyberwar. There may be deep historical reasons for this, in that our naval examples, even from the Napoleonic period, have a strong cyber character.

Suggested Next Steps for Research

Our ideas here are preliminary and tentative and leave many issues to be sorted out for analysis. Yet we are convinced that these are exciting times for rethinking the theory and practice of warfare–and that cyberwar should be one of the subjects of that rethinking. This is based on our assumption that technological and related organizational innovations will continue moving in revolutionary directions.

We suggest case studies to clarify what ought to be taken into account in developing a cyberwar perspective. As noted earlier, these case studies should include the Vietnam and Gulf conflicts. Combined with other materials–e.g., literature reviews, interviews–about the potential effects of the information revolution, such studies may help to identify the theoretical and operational principles for developing a framework that serves not only for analysis, but potentially also for the formulation of a doctrine that may apply from strategic to tactical levels, and to high- and low-intensity levels of conflict. Such studies may also help distinguish between the technological and the non-technological underpinnings of cyberwar.

We suggest analytical exercises to identify what cyberwar, and the different modalities of cyberwar, may look like in the early twenty-first century when the new technologies should be more advanced, reliable, and internetted than at present. These exercises should consider opponents that the United States may face in high- and low-intensity conflicts. The list might include armed forces of the former Soviet Union, North Korea, Iraq, Iran, and Cuba. Cyberwar against a country's command structure may have a special potency when the country is headed by a dictator whose base of national support is narrow.[36] Non-state actors should also be considered as opponents, including some millennialist, terrorist, and criminal (e.g., drug smuggling) organizations that cut across national boundaries. We expect that both cyberwar and netwar may be uniquely suited to fighting non-state actors.

Moreover, we suggest that the exercises consider some potentially unusual opponents and countermeasures. The revolutionary forces of the future may consist increasingly of wide-spread multi-organizational networks that have no particular national identity, claim to arise from civil society, and include aggressive groups and individuals who are keenly adept at using advanced technology for communications, as well as munitions. How will we deal with that? Can cyberwar (not to mention netwar) be developed as an appropriate, effective response? Do formal institutions have so much difficulty combatting informal networks, as noted earlier, that the United States may want to design new kinds of military units and capabilities for engaging in network warfare?

All of the foregoing may lead to requirements for new kinds of net assessments regarding U.S. cyberwar capabilities relative to those of our potential opponents. How much of an advantage does the United States have at present? How long will the advantage persist? Such assessments should compare not only the capabilities of all parties to wage and/or withstand a cyberwar, but also their abilities to learn, identify and work around an opponent's vulnerabilities.

Finally, despite the inherently futuristic tone of this thinkpiece, two dangers are developing in the world that may be countered through the skillful application of netwar and cyberwar techniques. The first comes from the proliferation of weapons of mass destruction. While the

specifics of acquisition and timetables for development of credible, secure arsenals are open to debate, American opposition to proliferation is unquestioned; effective action must be taken now to forestall or prevent it.

The prospects for proliferation in the post-cold war era create a highly appropriate issue area for the application of netwar techniques, since suasion will be much preferred to the use of preventive force[37] in dealing with most nation-state actors (including Germany and Japan, should either ever desire its own nuclear weapons). A netwar designed to dissuade potential proliferators from acquiring such weapons might consist of a "full court press" along the many networks of communication that link us to them, including diplomatic, academic, commercial, journalistic, and private avenues of interconnection. The ideational aspect of the netwar would concentrate on convincing potential proliferators that they have no need for such weapons. Obtaining them would create new enemies and new risks to their survival, while the benefits would be minuscule and fleeting.

The second danger likely to arise in the post-cold war world is to regional security. American defense spending is likely to continue decreasing for at least the next decade. U.S. forces will be drawn down, and overseas deployments curtailed. The number of air wings and carrier battle groups will decrease. Each of these developments spells a lessened American capability to effect successful deterrence against conventional aggression. From South Korea to the South Asian sub-continent, from the Persian Gulf to the Balkans and across the territory of the former Soviet satellites to the Baltic Sea, American forward presence will vary between modest and nonexistent. Indeed, when we consider the likely rise of age-old ideological, religious, ethnic and territorial rivalries, we see a world in which regional deterrence is going to be a problematic practice.

If regional wars are likely, and if American forces will be fewer and farther away from most regions than in the past, then a cyberwar doctrine may help to compensate for problems of distance and small force size. If we are correct about the implications of cyberwar, that traditional force requirements against opponents varying in size and strength no longer hold, then the United States ought to be able to hurl back aggressors when it chooses, even with relatively small forces. General Colin Powell summarizes the essence of this notion succinctly, based on his analysis of the Gulf War:

"A downsized force and a shrinking defense budget result in an increased reliance on technology, which must provide the force multiplier required to ensure a viable military deterrent…. Battlefield information systems became the ally of the warrior. They did much more than provide a service. Personal computers were force multipliers."[38]

While a cyberwar doctrine should provide us with robust war-fighting capabilities against the largest regional aggressors, we must recognize that the small size and (perhaps) unusual look of our forces may have less of an "intimidation effect" on our future adversaries, thereby vitiating crisis and deterrence stability. There are two ways to mitigate this emergent dilemma. First, applying netwar techniques in regions that bear upon our interests may provide early warning signals, and an opportunity to dissuade a potential aggressor as soon as we become aware of his intentions. The second means of shoring up regional deterrence consists of signalling our resolve tacitly. This may involve the deployment or "show" of military force quite early in a crisis, and could even include the exemplary use of our military capabilities.[39] Indeed, if this sort of signalling was aimed at targets suggested by cyberwar doctrine, such as critical communication nodes, the aggressor's capabilities for offensive action might come close to being nil from the outset.

What might a cyberwar against a regional aggressor look like? In most cases, it may well follow a "Pusan-Inchon" pattern.[40] First, the aggressor's "knockout blow" would have to be blunted. Then, American forces would counterattack. The burden of preventing a complete overrun at the outset of a war would surely fall heavily upon the U.S. Air Force and its ability to knock out the attacker's communications and logistics. The details will vary across regions, as some attackers may be more vulnerable to strategic paralysis than others. For example, future Iraqi aggression against the Arabian peninsula would depend on its ability to use a few roads and two bridges across the Tigris River. On the other hand, North Korea has many avenues of advance to the south.

The forces needed to roll back aggression would likely be modest in size. Since the invader will have been blinded by the time U.S. ground forces arrive, the latter will be able to strike where and when they wish. On the Arabian peninsula, for example, even an invading army of a million men would not be able to hold out against an American cyberwar, particularly if a defensive lodgement had been maintained. The attacker, not knowing where the Americans might strike, would have to disperse his forces over a theater measured in many hundreds of kilometers in each direction. American air power would blind him, and destroy his forces attempting to maneuver. Then, counterattacking forces would strike where least expected, destroying the invader's very ability to fight as a cohesive force. As the Mongols defeated an army some ten times their size in the campaign against Khwarizm, so modern cyberwarriors should be able routinely to defeat much larger forces in the field. Of course, details will vary by region. Again, the Korean example would be a bit more complicated, although the lack of strategic depth on that peninsula is more than offset by robust South Korean defensive capabilities.

It seems clear that a cyberwar doctrine will give its able practitioner the capability to defeat conventional regional aggression between nation states decisively, at low cost in blood and treasure. Will it fare as well against unconventional adversaries? This is a crucial question, as many, notably Van Creveld[41], have argued that war is being transformed by non-state actors, and by smaller states that must ever think of new ways to fight and defeat their betters. Thus, crises will likely be characterized by large, well-armed irregular forces, taking maximum advantage of familiar terrain, motivated by religious, ethnic or tribal zeal. Finally, they may move easily within and between the "membranes" of fractionated states.

Cyberwar may not provide a panacea for all conflicts of this type, but it does create a new, useful framework for coping with them. For example, in the former Yugoslavia, where all of the above factors have manifested themselves, the U.S. Army's AirLand Battle, or even Operation Desert Storm, should not be used as models for analysis. These frames of reference lead to thinking that an entire field army (400,000-500,000 troops) is the appropriate tool for decisive warfighting in this environment. Instead, an intervention could easily follow cyberwar's "Pusan-Inchon" approach to regional conflict. For example, indigenous defenders in Bosnia and other areas of the former Yugoslavia could be armed so that they could prevent any sort of overrun (the campaign's "Pusan"). Next, a small combined arms American task force, including no more than a division of ground troops,[42] might strike opportunistically where and when it chose (the "Inchon"). Enemy forces would be easily locatable from the air, from radio intercepts, and by unmanned ground sensors, especially if they try to move or fight. The fact that the aggressors are dispersed makes them easier to defeat in detail. If they concentrate, they fall prey to tremendous American firepower.

The Balkan crisis may prove to be a framing event for future unconventional conflicts. It may also provide an important case for developing cyberwar doctrine in this sort of setting. We note, however, that our assessment does not imply support for intervention in this case.

While the advent of cyberwar enables us to feel more comfortable about the prospects for maintaining regional security in an era likely to be characterized by American force drawdowns and withdrawals, there is another concern associated with this sort of warfighting capability. Should the United States seek out coalition partners when it fights future regional wars? It seems obvious that we should, since both international and domestic political problems are mitigated by the vision of a group of nations marching arm in arm, if not in step, against an aggressor. However, we should be concerned about trying to incorporate other nations' armed forces into a cyberwar campaign. Aside from difficulties with integration, the United States should not be in any hurry to share a new approach, particularly with allies who may have been recruited on an ad hoc basis. It's one thing to take a long-standing ally like Britain into our confidence; Syria is quite another matter. Perhaps this new tension can be resolved by having our allies defend the lodgements, the "Pusans," while we engage in the "Inchons." It is ironic that our ability to fight and win wars in accordance with the principles of the information revolution may require us to withhold our new-found insights, even from our friends and allies.

[1] Delbruck describes warfare as a dual phenomenon: it may be waged with either "exhaustion" or "annihilation" in mind, in: Delbruck, Hans, *History of the Art of War*, 3 vols., Westport, CT, Greenwood Press 1985.

[2] This notion borrows from an earlier Soviet notion of a scientific technology revolution (STR).

[3] Weigley quoting Van Creveld, (1989: 1) in: Weigley, Russell F., *War and the Paradox of Technology* (review of Van Creveld, 1989), International Security, Fall 1989, 192-202.

[4] See Bell, Daniel, "The Social Framework of the Information Society," in: Tom Forester (ed.), The Micro Electronics Revolution: The Complete Guide to the New Technology and Its Impact on Society, The MIT Press, Cambridge, Mass., 1980, pp. 500-549; Beniger, James, The Control Revolution, Cambridge, MA: Harvard University Press, 1986; and Toffler, Alvin, Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century, New York: Bantam Books, 1990.

[5] Sproull, Lee & Kiesler, Sara, *Connections: New Ways of Working in the Networked Organization*, MIT Press, Cambridge 1991.

[6] The literature on these points is vast. Recent additions include: Bankes, Steve, and Carl Builder, The Etiology of European Change, Santa Monica: RAND, 1991; Malone, Thomas W., and John F. Rockart, "Computers, Networks and the Corporation, Scientific American, September 1991, pp. 128-136; Ronfeldt, David, Cyberocracy, Cyberspace, and Cyberology: Political Effects of the Information Revolution, Santa Monica: RAND, 1991; Sproull, Lee & Kiesler, Sara, *Connections: New Ways of Working in the Networked Organization*, MIT Press, Cambridge 1991, and: *computers, Networks and Work*, Scientific American, September 1991, 116-123; Toffler, Alvin, *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, New York: Bantam Books, 1990.

[7] Ronfeldt, *Institutions, Markets, and Networks*, in preparation.

[8] Terms with *cyber-* as the prefix–e.g., cyberspace–are currently in vogue among some visionaries and technologists who are seeking names for new concepts related to the information revolution. The prefix is from the Greek root kybernan, meaning to steer or govern, and a related word kybernetes, meaning pilot, governor, or helmsman. The prefix was introduced by Norbert Wiener in the 1940s in his classic works creating the field of *cybernetics* (which is related to cybernetique, an older French word meaning the art of government). Some readers may object to our additions to the lexicon, but we prefer them to alternative terms like "information warfare," which has been used in some circles to refer to warfare that focuses on C3I capabilities. In our view, a case exists for using the prefix in that it bridges the fields of information and governance better than does any

other available prefix or term. Indeed, kybernan, the root of "cyber-" is also the root of the word "govern" and its extensions. Perhaps rendering the term in German would help. A likely term would be leitenkrieg, which translates loosely as "control warfare" (Our thanks to Denise Quigley for suggesting this term).

[9] We are indebted to Carl Builder for observing that the information revolution may have as much impact on the context as on the conduct of warfare, and that an analyst ought to identify how the context may change before he or she declares how a military's conduct should change.

[10] The difficult term is "information;" defining it remains a key problem of the information revolution. While no current definition is satisfactory, as a rule many analysts subscribe to a hierarchy with data at the bottom, information in the middle, and knowledge at the top (some would add wisdom above that). Like many analysts, we often use the term information (or information-related) to refer collectively to the hierarchy, but sometimes we use the term to mean something more than data but less than knowledge. Finally, one spreading view holds that new information amounts to "any difference that makes a difference."

[11] Van Creveld, Martin, *The Transformation of War*, Free Press, New York 1191, p 197.

[12] The importance of topsight is identified by David Gelernter, who observes: "If you're a software designer and you can't master and subdue monumental complexity, you're dead: your machines don't work. They run for a while and then sputter to a halt, or they never run at all. Hence, 'managing complexity' must be your goal. Or, we can describe exactly the same goal in a more positive light. We can call it the pursuit of topsight. Topsight–an understanding of the big picture is an essential goal of every software builder. It's also the most precious intellectual commodity known to man." (in: *Mirror Worlds, or the Day Software Puts the Universe in a Shoebox ... How It Will Happen and What It Will Mean*, Oxford University Press, New York 1991, 52.

[13] see Rona, Thomas P., *Weapon Systems and Information War*, Boeing Aerospace Co., Seattle, July 1976, 2.

[14] see Arnett, Eric, H., "Welcome to Hyperwar", in: *The Bulletin of the Atomic Scientists*, vol. 48, No. 7, September 1992, 14-21.

[15] Van Creveld puts it this way: "From Plato to NATO, the history of command in war consists essentially of an endless quest for certainty …", in: Van Creveld, Martin, *Command in War*, Cambridge: Harvard Press, 1985, 264

[16] See Caven, Brian, *The Punic Wars*, New York: St. Martin's Press, 1980.

[17] see Brodie, Bernard, A Guide to Naval Strategy, Princeton: Princeton University Press, 1944; Grimble, Ian, The Sea Wolf: The Life of Admiral Cochrane, London: Blond & Briggs, 1978.

[18] James Chambers is the principal reference to Mongol military doctrine for this paper. Jeremiah Curtin translated the original Mongol sagas, rendering them with eloquence and coherence. Harold Lamb remains an important exposition of Genghis Khan's approach to strategy.

[19] Perhaps this is why the Mongols slaughtered besieged forces (and civilian supporters) who resisted their attacks. As word of this brutality spread, fewer cities resisted (a gruesome example of netwar).

[20] Domestic political strife within the Mongol empire also played a part in halting operations.

[21] see Chambers, James, The Devil's Horsemen, New York: Atheneum, 1985.

[22] Kilawan also showed sensitivity to the importance of command and control at the tactical level. At the outset of the battle of Hims, for example, he sent one of his officers, feigning desertion, over to the Mongol commander, Mangku-Temur. When close enough, the Mameluke officer struck Temur in the face with his sword. At the same moment the Mamelukes attacked. The Mongol staff officers, tending to Temur, were thus distracted during the crucial, opening phase of the battle, which contributed to their defeat. See Chambers, James, *The Devil's Horsemen*, New York: Atheneum, 1985, 160-162.

[23] See Liddell Hart, Sir Basil H., *Great Captains Unveiled*, New York, Putnam's 1931, 160-162. His early formulation of armored maneuver warfare mentions the Mongols as a possible model for blitzkrieg.

[24] The memoirs of Heinz Guderian and F.W. von Mellenthin are replete with examples of how radio communication allowed German armor to concentrate fire until a target was destroyed, then shift to a new target. In particular, fire would be initially concentrated on enemy tanks flying command pennants, as the Germans were aware of the radio deficiencies of their foes. Though the Russians were heavily victimized by communication inferiority, even France, with its superior numbers of heavier armed tanks, suffered in 1940 because, while all armor had radios, only command vehicles could transmit. The French also suffered because they deployed their tanks evenly along the front instead of counterconcentrating them. Finally, it is interesting to note that Guderian began his career as a communications officer. See Guderian, Heinz, Panzer Leader, New York: Ballantine Books, Inc., 1972 edn; Mellenthin, F. W. von, Panzer Battles, New York: Ballantine Books, Inc., 1976 edn.

[25] Stolfi contends that the German "right turn" into the Ukraine fatally compromised Hitler's only chance of winning a war with the Soviet Union by striking at the heart of its strategic communications. See Stolfi, R.H.S., Hitler's Panzers East: World War II Reinterpreted, Tulsa: University of Oklahoma Press, 1992.

Liddell Hart refers to the debate over whether to attack Moscow directly, or to destroy Soviet field armies, as the "battle of the theories," which was won by the "proponents of military orthodoxy." See Lidell Hart,Sir Basil H., History of the Second World War, New York: Putnam's, 1970, 175-170.

[26] Mao Zedong bases his theoretical point about guerrilla warfare on his experience in fighting the Japanese who, as the Americans would in Vietnam, focused primarily on the disruption of tactical communications. See: Mao Zedong, trans. by Samuel Griffith, On Guerrilla Warfare, New York: Praeger Books, 1961 edn.

Milton Miles echoes Mao's point in his analysis of the same conflict. See Miles, Milton E., A Different Kind of War, New York: Doubleday, 1968. Thomas E. Lawrence's analysis of the Desert Revolt is also confirmatory. See Lawrence, Thomas E., Seven Pillars of Wisdom, New York: Doubleday, 1938 edn.

[27] Powell, Colin L., "Information-Age Warriors," Byte, July 1992, 370.

[28] See the earlier quotation from Sproull and Kiesler (1991).

[29] Posen, Barry R., The Sources of Military Doctrine, Ithaca: Cornell University Press, 1984, 36.

[30] This is another new term that some visionaries and practitioners have begun using. For example, see Benedikt, Michael, ed., Cyberspace: First Steps, Cambridge: MIT Press, 1991. It comes from the seminal "cyberpunk" science-fiction novel *Neuromancer* by William Gibson (1984). It is the most encompassing of the terms being tried out for naming the new realm of electronic knowledge, information, and communications–parts of which exist in the hardware and software at specific sites, other parts in the transmissions flowing through cables or through air and space. General Powell (1992) nods in this direction by referring to "battlespace" as including an "infosphere."

[31] Chris Bellamy grapples with some of these issues in his analysis of future land warfare. See Bellamy, Chris, The Future of Land Warfare, London: Helm, 1987.

[32] Note that the acclaimed U.S. intelligence in Desert Storm rarely got to the division commanders; for them, every major encounter with the enemy's forces reportedly was a surprise. See Grier, Peter, "The Data Weapon," Government Executive, June 1992, 20-23.

[33] Kenneth N. Waltz considers this phenomenon of "imitation" a major factor in the process of "internal balancing" with which all nations are continually occupied. If a new military innovation is thought to work, all will soon follow the innovator. A good example of this is the abrupt and complete shift of the world's navies from wooden to metal hulls in the wake of the naval experience with ironclads in the American Civil War. See Waltz, Kenneth N., Theory of International Politics, New York: Random House, 1979.

[34] A classic example is the 1944 battle for Normandy. Field Marshal Montgomery's forces tied down the German Seventh Army, allowing General Patton's Third Army to engage in a broad end run of the German defenses.

[35] The authors are grateful to Gordon McCormick for his insights on this topic. Also on this point, see Arnett, Eric H., Gunboat Diplomacy and the Bomb: Nuclear Proliferation and the U.S. Navy, New York: Praeger, 1989.

[36] This last point is inspired by the thinking of RAND colleague Ken Watman.

[37] There is a class of proliferator toward which our reluctance to employ forceful measures will be diminished. Iraq, Iran, North Korea, Libya and Cuba are some of the nations whose threatened acquisition of weapons of mass destruction may justify intervention. The notion that the United States should adopt a doctrine of "selective preventive force" against "outlaw" states is discussed in Arquilla, John, "Nuclear Proliferation: Implications for Conventional Deterrence." In Arquilla and Preston Niblack, eds., American Grand Strategy in the Post-Cold War World, Santa Monica: RAND, 1992.

[38] See Powell, Colin L., "Information-Age Warriors," Byte, July 1992, p 370.

[39] Arquilla discusses this issue in detail. See Arquilla, John, "Louder Than Words: Tacit Communication in International Crises," Political Communication, Vol. 9, 1992, 155-172.

[40] This notion is drawn from the Korean War, where U.S. forces began their involvement by preventing the overrun of the Korean peninsula in the opening months of the war. The Pusan perimeter held a portion of South Korea free, serving as a magnet for North Korean forces. The amphibious counterattack at Inchon, far from the battle fronts, threw the invaders into complete disarray.

[41] Van Creveld, Martin, The Transformation of War, New York: Free Press, 1991.

[42] Kenney and Dugan call for a "Balkan Storm" without employing any American ground forces. We disagree with this approach, rooted as it is in theories of "limited liability" and "air power exceptionalism." Nonetheless, they do identify many of the key types of aerial cyberwar tactics that might be employed, even if their omission of an American ground component would seriously dilute any gains achieved. See Kenney, George and Michael J. Dugan, "Operation Balkan Storm: Here's a Plan," The New York Times, November 29, 1992.