The US Army War College Quarterly: Parameters

Volume 28
Number 3 *Parameters Autumn 1998*

Article 10

8-13-1998

Military Theory and Information Warfare

Ryan Henry

C. Edward Peartree

Recommended Citation
Ryan Henry & C. E. Peartree, "Military Theory and Information Warfare," *Parameters* 28, no. 3 (1998), doi:10.55540/0031-1723.1895.

Military Theory and Information Warfare

RYAN HENRY and C. EDWARD PEARTREE

From *Parameters*, Autumn 1998, pp. 121-35.

> "To conquer the command of the air means victory; to be beaten in the air means defeat and acceptance of whatever terms the enemy may be pleased to impose." -- Giulio Douhet[1]

The effect of technology on warfare often has colored the predictions of theorists, elevating to eternal truths what we discover in retrospect to have been passing historical epochs. Free of the context of the 1920s, Douhet seems dazzled by the revolutionary possibilities of air power. He cannot be criticized for not anticipating anti-aircraft radar and surface-to-air missiles, nor were he and his contemporaries alert to the continued success of low-tech, ground-based asymmetric strategies of determined, resilient adversaries. But one word--Vietnam--provides a corrective to his assertions. Air power has had a tremendous effect on warfare, but it simply has not lived up to Douhet's prediction that it would be the decisive factor in all future conflicts.

Current interest in information warfare and the manifold effects of the information revolution on the conduct of war cause many to proclaim a revolution in warfare. Evangelists of information warfare, like forerunner evangelists of air power, sea power, and artillery, risk losing sight of historical context and the continuities of conflict. We are once again faced with a genuine technological revolution which seems to offer an entirely new mode of warfare, one that advocates insist will supplant existing modes. Thus military theorists and defense planners are once again challenged to use new technologies for the competitive advantages they may offer on the battlefield, while bearing in mind their limitations.

This article reviews the effects of information technologies on military theory, tempered by insights into the consequences of previous technological revolutions. Issues emerge that are independent of any technology or international security environment. They include an appraisal of the ability of contemporary analysts and theorists to challenge promises of unprecedented change, and an examination of the theoretical implications of the so-called "revolution in military affairs." Related issues include the need to avoid being dazzled by the new technologies (while not exaggerating their significance) and at the same time appreciating the extraordinary near-term advantages and capabilities they afford. Finally there is the matter of balance. We must use the technologies to advantage, neither misapplying them in haste nor hesitating until we miss the opportunities they represent.

Technology, Society, and War

The enormous popularity of *The Third Wave* and *War and Anti-War* has given currency to the notion that historical epochs--and the wars that go with them--are characterized by revolutionary technological breakthroughs that cause "waves" of socioeconomic change.[2] According to the authors of those texts, Alvin and Heidi Toffler, the first (agrarian) wave was characterized by animal domestication and agricultural cultivation; the second (industrial) wave by mechanization, mass production, and the division of labor; and the emerging third (information) wave by digitization, computers, and information technologies.

While the Tofflers' thesis is less than perfect,[3] they are generally correct with respect to the goals of warfare imposed by the prevailing socioeconomic frameworks of the various epochs. Successful pre-industrial war was generally predicated on the seizure of territorial assets, control of them, or both. Successful industrial age war was about reducing the means of production and out-manufacturing one's opponent--dubbed *schlachtmaterial* by the Germans

during World War I. If the analogy holds, the advance guard of Pentagon theorists and defense analysts contends, future wars will be waged for control of data, information, and knowledge assets.

Weapons of war also reflect the dominant aspects of each era's socioeconomic paradigm. Rifled arms, iron-clad ships, machine guns, tanks, and aircraft depict the evolution of industrial age war. The precision-guided munition, popularly known as the "smart bomb," heralds for some the weaponry of the information age. The deeper expression of any age, however, can generally be found in the organization and culture of the warfighting community. Some propose that hierarchical command structures and ponderous military-industrial bureaucracies, created to fit industrial age needs, must now give way to the decentralized, "flattened" business network of the information age. The success of businesses that have adapted to the new world of networked computing, communications, and data processing--and the failure of those that have not--seem to the Pentagon's reform-minded Young Turks to be compelling arguments in favor of introducing commercial processes and procedures into the military.

But there are liabilities associated with moving too rapidly to reengineer the force around new technologies without first considering interests and risks. A view that is too techno-centric risks revisiting such flawed experiments as the Army's Pentomic division of the 1950s, the 280mm atomic cannon, the flying jeep, and the jet-pack-powered infantryman. The appearance of new weapons and new technologies has sometimes caused military leaders and theorists to make errors in judgment, misreading the meaning of the new technology and producing poor returns on the investment, whether on the battlefield or in the view of history.[4]

Technology and Military Theory

Some attribute current interest in Sun Tzu, the Chinese strategist and philosopher of war, to the advent of the information age and its military subset, "information war." This may seem curious, for Sun Tzu lived some 2500 years before the invention of the computer, the fiber-optic cable, or the orbital satellite. What appeals to many current military writers is Sun Tzu's simple, aphoristic approach to warfare based on the principles of superior intelligence, deception, and knowledge of the mind of one's enemy. Current theorists therefore conclude that the new mode of warfare ushered in by the information revolution will have sweeping effects on the conduct of war in the near future. Precision weapons will be directed at the enemy's decisive point(s) at the critical moment through "information superiority." Superiority, in turn, will occur through space, near-space, and ground-based sensing technologies that will transmit attack instructions in real time via a "system of systems" that links all parts of the battlespace. Some even predict that the new technologies will penetrate, if not lift, the fog of war.

The more radical of the theorists predict that information warfare will not only provide dominant awareness of the battlespace; it will also allow us to manipulate, exploit, or disable enemy information systems electronically. The intent here evidently is to knock an enemy senseless--literally--and leave him at the mercy not only of conventional kinetic attack, but of psychological operations aimed at controlling his perceptions and decisionmaking abilities. Public opinion is to be shaped, leaders will be cut off from citizens, and the mind of the enemy will be directly penetrated and his strategy defeated. In the ideal case all this will occur bloodlessly, fulfilling Sun Tzu's goal of victory without battle. At least that's the theory.

Unlike Sun Tzu, whose timelessness owes much to his lack of tactical or technical advice, most military theorists of the past 500 years have based their work on either specific technologies or scientific assumptions peculiar to the prevailing thinking of their age. This may seem axiomatic, but it is worth considering--given the fact that many of them sought enduring wisdom in their work. Machiavelli, whose insights into military character and the importance of political motives in war prefigures the thinking of Clausewitz, deemphasized the technical aspects of warfare. His exception, however, seems to prove the rule. The theorists that followed him--continuing to this day--demonstrate a predilection for technical fixes.

. The renaissance and the emergence of the scientific revolutions of the 16th and 17th centuries stimulated a fascination with the machine which extended beyond the realm of science and technology proper into the culture and, inevitably, into the making of war. Engineers and mathematicians, among them Galileo and Niccolo Tartaglia, attempted to develop ballistic equations that would refine the blunt and unpredictable force of artillery. Advocates of artillery, which had become progressively more effective starting in the 15th century, believed that it would dominate

all wars in the future, sweeping away the age of cavalry and diminishing the importance of the foot soldier.

. The preeminent military theorist of the 17th century was an engineer, Sebastien le Prestre de Vauban, the master of siegecraft and fortification. Vauban produced no theoretical writings on the nature of war or the integration of new technical innovations into strategy. A technologist, he was concerned only with the creation of plans and formulae for the successful attack of enemy fortresses and the protection of one's own. The study of war in this age of science and reason had become detached from theoretical underpinnings. It used a purely quantitative means of analysis to focus on tools and methods of applying them.

. The tradition of "scientific" war reached its theoretical apogee during the Industrial Revolution in the writing of Baron Antoine Henri de Jomini. Jomini, who served as Chief of Staff to Marshall Ney, analyzed Napoleon's campaigns in a search for the unchanging principles and practices of war. He believed that quasi-mathematical concepts dictated the proper organization of military formations, and the direction and size of attack at the "decisive point." War was, for Jomini, reducible to propositions that were universally true and universally applicable across the spectrum of military conflict, much as any natural compound could be smelted into its elemental nature and thus understood. And despite his embrace of scientific principles, Jomini's decline as an enduring military thinker was due in large measure to his neglect of specific technological innovations. Rifled arms, high-explosive shells, machine guns, and later mobile armor and air power rendered his supposedly immutable rules about "interior lines" and the geometry of the battlefield highly dubious.

. Carl von Clausewitz, Jomini's 19th-century rival, has held up well by comparison. He, like Sun Tzu and Machiavelli, focused less on military technology or contemporary intellectual fads (like Jomini's Newtonianism), and more on war as an eternal human phenomenon, not rational but capricious, not reducible but complex . . . in short, a human activity.[5] He rejected quantitative analysis and scientific formulae in favor of philosophical insights. Clausewitz's concept of "friction" as inherent in war, his belief that in every battle and in every war there is a "culminating point," and his insistence upon recognizing the passionate, violent nature of conflict are not bound to any age. Unlike most of the technical theorists, Clausewitz was mainly concerned with the ultimate goals of conflict. Thus his insistence on the political nature of war and the oft-quoted aphorism that war is "an act of force to compel our enemy to do our will."[6]

. Alfred Thayer Mahan, the prophet of sea power in the late 19th century, was concerned with grand strategy, specifically that of the United States in its development as a world power. Mahan's views on the importance of geography, trading economies, and styles of government are clouded by his obsessive promotion of sea power to the neglect of land power. The new technology of the steam gunship and a selective reading of military history convinced him of the absolute primacy of sea power in ensuring the commercial and military success of nations, and caused him to dismiss the importance of railways and the growing significance of motor transport on land.[7] Nor did he pay much attention to the development of torpedoes and submarines, which promised to make armored capital ships vulnerable to attack.[8] Like his strategic inspiration, Jomini, he continued to insist on permanent scientific principles of naval strategy which would remain unchanged regardless of technical alterations to the equation.

Some may recall that even Clausewitz wrote extensively of tactics and operations. Who has studied his chapters on "Attack of Convoys" or "Defense of Swamps"? These sections of *On War* are seldom read and justifiably so; wed to their particular time and place, they are now of mere historical interest and largely irrelevant to the making of modern war. So we tend to overlook his neglect of sea power, as egregious in a sense as is Mahan's ignoring land power, because of Clausewitz's transcendent insights. Mahan, captured by a long-gone technological moment and the zeitgeist of a forgotten age, does not appeal today because he lacks Clausewitz's reach and depth.

. Air Marshal Giulio Douhet was the last great military techno-prophet before the advent of nuclear weapons (which produced their own generation of influential strategic thinkers) and before the current crop of information warfare theorists. Even before World War I, Douhet saw the potential of aviation as a transformational technology in war. His mature writings, from the 1920s, predicted the emergence of air power as the dominant realm of war and the aerial bomber as the predominant tool:

> The brutal but inescapable conclusion that we must draw is this: in the face of the technical development of aviation today, in case of war the strongest army we can deploy in the Alps and strongest navy we can dispose on our seas will prove no effective defense against the determined efforts of the enemy to bomb our cities.[9]

Douhet anticipated rapid strikes by aerial bombers that would devastate defenseless cities, causing terrified societies and demoralized national governments to capitulate before any counterattack could be mounted. Defenses against air power were bound to fail; they were a waste of resources, he said, based on what he had seen during World War I. Armies and navies, ponderous and surface bound, were virtually useless because wars were likely to be won or lost in the air before fleets could be put to sea or armies mobilized. He tells us unequivocally:

> If I may be so bold, I have mathematical certainty that the future will confirm my assertion that aerial warfare will be the most important element in future wars, and that in consequence not only will the importance of the Independent Air Force rapidly increase, but the importance of the army and navy will decrease in proportion.[10]

Mathematical certainty?

Information Warfare: Prelude to Revolution

The revolution in information technology, from the transistor through widespread digitization toward global socioeconomic revolution via deeply networked communications, has profoundly influenced analysts and planners in and out of uniform. It has also produced a cottage industry in information warfare concepts, studies, and proposals as the military attempts to understand, derive principles and theories for, and apply the new technologies. The frequently confusing nature of these products stems from three principle sources: the rapidity of technological change; the very nature of information and information technology, which blurs distinctions between civil and military use and targets; and uncertainty about the nature of information warfare itself.[11] As with the air power revolution, new and apparently revolutionary information technologies promise an immense effect on the conduct of war. And as with air power, theorists are emerging to wrestle with the nature of information age war, seeking clues as to how it might change the shape of conflict in general.

The Persian Gulf War afforded the average American his first (albeit filtered) glimpse of the future of warfare. Millions were treated to precision-guided bombs annihilating targets in downtown Baghdad, learned of satellite uplinks from the battlefield that provided real-time connectivity, and applauded the ability of stealth aircraft to ensure aerial dominance. These outcomes were enabled by battlefield tracking and targeting systems that allowed American forces to identify and attack targets well beyond the line of sight, by advanced aerial reconnaissance from airborne warning and control systems (AWACS) and from joint surveillance and target attack radar systems (JSTARS), and by space-based satellite sensors. The latter provided highly accurate battlefield information to combatants, tightening decision cycles and dramatically accelerating the tempo of combat. Everyone seemed to understand that something was different about this "videogame war"; there was much more to the spectacle than the immediacy of Vietnam's television war 20 years earlier.

Since Desert Storm there have been orders-of-magnitude improvements in technological capabilities. For example, the system used by Gulf War commanders to transmit messages could move 2400 bits of information per second. The current commercially developed and operated Global Broadcast System transmits 23 million bits per second into Bosnia. A message that took more than an hour to send in 1991 can now be sent in less than a second.[12] The challenge for the US military and for political leaders has been to keep up with the pace of change in information technologies generated by innovations in the commercial, not defense, market and driven by consumer, not warfighter, demand. The convergence of digitized information, computers, networks, cellular communications, satellites, precision munitions, and data fusion technologies has translated into quantifiable improvements in volumes of data exchanged, experimental concepts, and testbed programs.

The idea of an information-based military technical revolution is reflected in increased understanding of what is happening on the battlefield and improved ability to apply destructive force when and where we want to. These

capabilities are built upon specific technologies, such as improvements in sensors carried on advanced AWACS and JSTARS, unoccupied aerial vehicles, or electro-optical satellites with one-foot image resolution and wide-area coverage. Others include intelligent fusion of data products by combining artificial intelligence with "knowledge bases" to process, manipulate, and tailor information for specific user needs; "sensor to shooter" couplings (automatic target recognition capabilities are not far off); and integrated, high-speed, high-capacity battlefield communications capabilities via the aforementioned Global Broadcast System (GBS) and the Global Command and Control System (GCCS), both of which are designed to provide the right information to the right user at the right time and place.

Mastery of information and information processes leads naturally to increases in precision and lethality. The quest for battlespace omniscience can improve tracking and targeting capabilities, aggravating the adversary's problem of finding sanctuary. What can be seen, in the parlance of military analysts, can be hit; with these new information technologies, nearly everything that is not hidden can be seen and is therefore vulnerable. The current revolution in information technologies promises military leaders an extraordinary extension of previous battlespace awareness, information dissemination capabilities, and ubiquitous "smart" weapons. Together they offer the ability to know what is happening, what is important, where the points of maximum leverage are, and connection to the means to apply force at those points, all on a vastly compressed time scale.

To appreciate the magnitude of these changes, recall that as recently as the 1970s reconnaissance was conducted by manned aircraft or ground patrols. Both called in data that were plotted on maps for analysis by intelligence experts. Hours at best, more likely days or weeks, could elapse before critical information was sufficiently processed to be forwarded to planes in the air or soldiers in the field. In Panama in 1989 things had still not changed substantially. Today, digital 3-D map representations could provide a complete picture of the battlespace to every friendly combatant, updated as events occur. Satellite imagery, or live video from an unoccupied aerial vehicle (UAV) equipped with a digital camera, is potentially available in real-time to a soldier in the field via a ruggedized laptop computer and a global positioning system (GPS) receiver. The soldier and his comrades could then synchronize their actions with the flow of battle, unaided by the traditional hierarchical and bureaucratic command and control system.

Automatic target recognition systems currently in prototype may eventually remove most of the middlemen in such an environment, directing long-range precision strikes as soon as information is received from the sensor. All this is perceived to occur without human intervention. If these concepts mature, decision cycles for commanders and soldiers would be both compressed and enriched, accelerating the tempo of warfighting, demanding more initiative-based, decentralized decisionmaking, reducing personnel in the field and on the staff, and eliminating much of the noise, error, and viscosity normally inserted by human links. These communications and intelligence-gathering advantages also would be available during any non-combat operation in which our 21st-century forces might participate: humanitarian, peace enforcement, or support of domestic authorities.

Given the seemingly decisive comparative advantage which information technologies offer the possessor, the intrinsic value of data and information would seem to be on the rise. The Gulf War suggested how new awareness and faster targeting capabilities relative to adversary capabilities could translate into a smashingly decisive victory in the field. Therefore, the new technologies--highly sophisticated and integrated, vulnerable to both kinetic and electronic disruption--will themselves become objects of war. Hence the enthusiasm for information warfare.

While intelligence and operations security have always been important in wartime, and lines of communications have always been targets, current thinking establishes the preeminence of "information superiority." According to the Joint Chiefs of Staff publication *Joint Vision 2010*: "We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[13] So by announcing that the sine qua non for success in future conflicts is "information superiority," we have defined new vulnerabilities and targets for the attack and for the defense.

Battlefield employment, exploitation, and targeting, and protection of the means of gaining and maintaining superiority, presently define the conventional range of the information warfare spectrum. The various Pentagon permutations--command and control warfare (C2W); command, control, communications and intelligence (C3I); command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR)--describe the realm of traditional warfare. They are reflected in the addition of new information technologies to units trained for

traditional force-on-force combat. The popular image is that of a soldier with a wearable computer and a GPS terminal, calling in long-range precision strikes. But beyond this image, and to many the more revolutionary and important aspect of information warfare, are the vulnerabilities of national and military infrastructures that rely on a host of modern automation and information technologies.

The information revolution is driven by the changes that information technologies are creating as they are integrated into the cultural, economic, and civic life of society. Essential national infrastructures such as telecommunications, transportation, electrical power, emergency services, and food, water, and fuel distribution are dependent on digital, software-based systems that are controlled through networked, publicly accessible communications interfaces. International commercial and financial transactions are increasingly dependent on electronic networks. It has been estimated that 62 million Americans now use the Internet to communicate, bank, shop, and do business.[14]

Public switched networks on which essential public and commercial infrastructures depend have shown themselves vulnerable to penetration, disruption, and manipulation. Furthermore, a combination of cost concerns and the superiority of established commercial systems has created a situation in which an estimated 95 percent of all military communications travel over commercial systems. With the recent completion of an accord on telecommunications deregulation, these networks become subject to foreign ownership and control. In these changes lie the concerns that America, the most sophisticated, highly networked information age economy and society, has become vulnerable to an "electronic Pearl Harbor."

From Technology to Theory and Doctrine: Competing Concepts of Information Warfare

Definitions of information warfare are abundant and protean. The most recent Department of Defense definition describes information warfare (IW) as "information operations (IO) conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[15] According to the Joint Chiefs of Staff,

> IW can be waged in wartime within and beyond the traditional military battlefield. As a subset of IW, command and control warfare (C2W) is an application of IW in military operations that specifically attacks and defends the C2 target set. However, the capabilities and disciplines employed in C2W (psychological operations [PSYOP], deception, operations security, and electronic warfare) as well as other less traditional ones focused on information systems can be employed to achieve IW objectives that are outside the C2 target set.[16]

This attempt to define the information-based revolution for national security policymakers and warfighters is multilayered, a bit confusing, and apparently deliberately vague. Agreeing that IW is a field with the potential for great effect, perhaps the linchpin of a revolution in military affairs, questions still abound about how it will affect military culture and future conflicts. While issues of integration remain problematic, the spectrum of possibilities may be laid out as follows. At the most incremental level of change, there are those who would overlay new and near-future technologies on current military systems. Such an effort can be seen in the "digital battlefield" of the US Army's "Force XXI," and the robust, highly detailed Department of Defense "Advanced Battlespace Information System."[17] These programs perceive information technology as a powerful force multiplier for kinetic warfare that would not in itself be substantially changed from the heyday of industrial age war.

Others have suggested that the nascent information-based revolution in military affairs will eventually make possible radical reform of military organizations and tactical doctrines while still operating within the traditional parameters of warfare--dominating an adversary on a physical battlefield. Such approaches can be found in the "Army After Next" project, the Marine Corps' "Sea Dragon" concept, the Navy's "Forward . . . from the Sea," and the Air Force's "New World Vistas." The concept was developed most fully in 1996 through the Defense Science Board's "Summer Study on Tactics and Technology for 21st Century Military Superiority." The report envisioned restructuring US ground forces into small "distributed combat cells" rather than hefty battalions and divisions, their warfighting power multiplied by sensors, robotic systems, precision logistics, and the ability to call in long-range precision firepower from land, sea, or air. All of these changes were of course predicated on a robust information infrastructure.[18]

Finally, where science fiction meets science fact, there is the emerging concept of "cyberwar": conflict in the purely

digital realm consisting of remote attacks on critical information nodes, links, and databases to disrupt, exploit, disable, or deny service. Information warfare of this sort would also include deception and psychological operations at a much higher level of subtlety and effectiveness than expected in conventional operations, given the manipulability of digital information. Combinations of all of the foregoing concepts appear in multiple-fence-straddling positions such as the one established above by the Joint Staff.

Theories of Information Warfare

So what do the theorists expect in a future adapted to the emerging information age? The answer presently seems to be faith in the future of information technologies to produce revolutionary changes in military affairs and the conduct of war.

. John Arquilla and David Ronfeldt, two of the first and best, have produced a number of intellectually rich articles, most of them examining the twin concepts of "cyberwar" and "netwar."[19] In their view, cyberwar refers to an information-enriched style of future military conflict in which the struggle for information dominance holds the key to victory. Netwar, the more heady form of future conflict, refers to inter-societal contests of perceptions and national messages. Arquilla and Ronfeldt are well known for their comparison of information warfare to the "decapitation" techniques employed during the 13th century by the Mongols, who used superior speed and lines of communication to control numerically superior enemies located over a wide area. In this context, cyberwar would allow a network of decentralized information warriors to achieve decisive, bloodless victory--a sort of post-industrial blitzkrieg--by directly targeting an adversary's information "nerve centers." Netwar in theory could prevent real wars (or cyberwars) by allowing for deterrent posturing and for control over potential adversaries' perceptions.

. Another group of theorists--George Stein, Richard Szafranski, and Owen Jensen--are associated with the Air University at Maxwell Air Force Base in Alabama. Much of their theoretical work has appeared in *Airpower Journal*, a hotbed of discussion of information warfare. In general this group maintains that the highest potential of information warfare is as a new realm of conflict in which information (or knowledge) itself is both the center of gravity and the principal weapon. This type of futuristic conflict would occur in a transformed environment; weapon platforms as we now know them would be outmoded. No digitized battlefield, no info-tech applique on existing systems, but something fundamentally different.

To paraphrase their ideas, information warfare would assume an autonomous role in "information campaigns" far beyond its application as a force multiplier in more linear military evolutions. Emerging information technologies might allow us to battle the mind of the enemy via customized propaganda, morphing reality into a fictive universe which we serve up through diversified information networks. These theorists suggest that information warfare, not unlike Arquilla and Ronfeldt's concept of netwar, would be a high-tech, more sophisticated form of psychological operations and propaganda, directed at mass or niche audiences. They conclude that technology will be used to control an opponent through strategic information dominance: tailoring his information content to suit our interests, conditioning his knowledge and understanding of the situation, ideally without his awareness.[20] As defined by the Maxwell school, information warfare seems to be the functional equivalent of conventional concepts of strategic air power.[21]

. Martin Libicki, a standard-setter on the subject of information warfare who has worked harder than most to bridge the gap between ideas and action, has suggested that information may ultimately prove to be a universal deterrent to war because of the global transparency that it will foster. He suggests that a network of satellites, and of air, ground, and sea-based sensors, will ring the earth, affording a God's eye view of the world and all its activities. A global information infrastructure will link users of this information, ensuring a sort of universal awareness of military and other activity. Under such conditions, any border incursions or sudden mobilization would be sensed and could be thwarted immediately, ostensibly by exposing and threatening the would-be aggressor. Were the aggressor to persist, the international community would only have to dam up the aggressor's bitstreams and the information flows essential to his war effort, economy, and national infrastructures. Such procedures would (ideally) curb his ambitions without firing a shot.[22]

These authors are exploring new ways of thinking about war and warfare in an era of change. They are to be commended for attempting to expand the intellectual horizons of often parochial, hide-bound military and civilian bureaucracies. The assumptions of many of these theorists, however, are highly dependent on the technological innovations of the moment. Even emphasizing as some do, recalling Sun Tzu, that the real object of information warfare is the human mind, the visions they present are unattainable without the array of new and emerging technologies assumed to be part of a fully netted information age world.

Our ability to combat or deter adversaries using cyberspace tools is predicated on their being as reliant on information technologies as we are. Threatening to cut off a hostile neighbor's bitstreams will be credible only if two conditions are met. The first is that he is largely dependent upon them for survival; the second is that we have the ability to turn them off. Little of value will be accomplished by niche-casting propaganda at a nation that lacks satellite television or an Internet connection. As recently as 1997, it has been suggested, half the world's population had never even made a telephone call. Similarly, strategic psychological operations, no matter how overwhelming and sophisticated technologically, are likely to be far more effective in a democracy than in the authoritarian states that currently present many of our most significant security threats: Iran, Iraq, Libya, and North Korea. In fact, it is interesting that such a strategy would appeal to an American theorist because it is our highly democratic, media-saturated, and technologically sophisticated society that is most vulnerable to a counterattack.

Some information warfare theorists have attempted to shield themselves from accusations of technological determinism by suggesting that we need not follow slavishly the technology wave. Rather, we should use our imaginations to determine what we want it do for us and then develop the technology to fit those needs. This ignores the fact that technology development, much like the formulation of strategy and tactics, is a coevolutionary process. New technologies emerge to either exploit or compensate for weaknesses in existing technologies. Inventing a theory of information warfare risks falling victim to the kinds of fallacies that Douhet encountered. Unable to see the future, he imagined one based on linear projections of extant technologies. Unable or unwilling to imagine counter-air defenses, or the limitations of strategic bombing in the face of a determined foe, he saw only a pristine view of air power, conducting operations with impunity against helpless, terror-stricken citizens.

Technology and the Current Revolution in Military Affairs

Technology-driven changes in military affairs are transient, sometimes eclipsed in less than a generation, and the competitive advantages that they offer are increasingly fleeting. Andrew Krepinevich, one of the leading thinkers in this area, has identified ten technology "revolutions" from the advent of infantry warfare to the birth of nuclear weapons.[23] Steven Metz and James Kievit of the US Army War College have divided military "revolutions" into major and minor forms. The first are mostly technology driven and malleable; the others ride on broader socioeconomic "waves."[24] It is clear that specific technologies have sometimes had significant effects on the conduct of warfare; gunpowder, internal combustion engines, breech-loading mechanisms, radio, and radar are among the most memorable. But war remains essentially what it has been for centuries: Clausewitz's "act of force to compel our enemy to do our will."

In a century that began with active cavalry regiments and ends with nuclear arms, stealth aircraft, and theories of information warfare, progress has been continuous and evolutionary. In Machiavelli's time, improvements in artillery led enthusiasts to predict that it would supplant all other tools of war. Five hundred years later, artillery is still improving, and it still plays a subordinate role in combat operations. So perhaps it is too much to expect truly revolutionary new technologies to lead to fundamental changes in the forms and functions of conflict.

The German blitzkrieg is sometimes offered as a compelling example of creative minds deriving a competitive edge over adversaries by astute application of technology to the problems of land warfare. The Germans combined armor, radio communications, and tactical air support to remarkable effect in Poland, the low countries, and France during 1939-40. But once others had an opportunity to analyze their techniques and methods, the edge was lost. As the Germans later drove into Soviet territory, their logistics train was stretched beyond endurance and the army, in effect, became "de-modernized." The blitzkrieg--material intensive and dependent on frequent resupply to maintain communications, mobility, and combined arms capabilities--fell apart, and the war in the east degenerated into a slow, brutal contest of attrition.[25] The benefits of technological edges can be fleeting indeed.

The 1997 "Army After Next" winter wargame, which featured a face-off between the United States and a peer competitor, began with two surprises: a laser attack on US space-based satellite reconnaissance, GPS, and communications capabilities, followed closely by a nuclear electro-magnetic pulse burst in space. The combined effects of these unexpected initiatives reduced by 50 percent the military information infrastructure on which most of our new weapon systems are dependent.

Predictions about the effects of technology are almost always erroneous, even when the technology involved justifies the designation "revolutionary." The airplane, an unprecedented technological breakthrough which added a new dimension to the battlespace, repeatedly has been shown to be insufficient in and of itself to transform war. Contrary to Douhet's assertions, command of the air has certainly not made armies and navies obsolete. And as Michael Howard has pointed out, when the Allies bombed the cities of Germany toward the end of World War II and the conduct of strategic air war most closely approached Douhet's vision, it not only failed to force the enemy to capitulate, but actually hardened resistance.[26]

Clausewitz reminds us that the human elements of war are extraordinarily difficult to gauge. If necessity is the mother of invention, asymmetric tactics, strategy, or technological countermeasures will always upset the best laid technology-based plans. Nuclear weapons were supposed to make conventional arms obsolete and totally revolutionize warfare. Massive retaliation, the Eisenhower-era strategy for their deployment, ignored conventional capabilities only to find that the will to use weapons of mass destruction was lacking. Dirty little wars on the periphery continued and guerrillas flourished, despite our fearsome nuclear arsenal and the threat of certain annihilation we wielded. Our bluff was called in Korea and later in Vietnam, and the nukes remained holstered. Soldiers at the dusk of the industrial age faced the same mud and mayhem that had confronted their counterparts during the Napoleonic wars at its dawn.

Technological advantages in war have generally proven ephemeral; neither can a technology-driven theory of war or strategy for war hold sway for very long. Nor do old weapons necessarily go out of style--new tools are just added to the box. Technology-driven revolutions in military affairs entail the reorganization of forces and doctrine around those new technologies. Anyone who believes that the nature and rate of change qualify for designation as "revolutionary" should read their mandate carefully and proceed cautiously. It is important to grasp the functional significance of technological innovations; it is equally important that risks and vulnerabilities--the stuff of strategy--remain foremost in assessing their political and military implications. The most durable military theory focuses less on the latest technology and more on the infinite complexity of the user.

NOTES

1. Giulio Douhet, *Command of the Air*, trans. Dino Ferrari (New York: Coward-McCann, 1942), p. 28.

2. Alvin Toffler, *The Third Wave* (New York: Bantam Books, 1991); Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (New York: Warner Books, 1995).

3. Where, for example, do the Tofflers place the trading states of late medieval Europe and the Renaissance that flourished long before the Industrial Revolution, yet whose wealth and power had nothing to do with agriculture or territorial assets?

4. For an excellent overview of a failed, technology driven RMA of an earlier era, see A. J. Bacevich, *The Pentomic Era: The U.S. Army between Korea and Vietnam* (Washington: National Defense Univ. Press, 1986).

5. An intriguing and thoughtful application of current "complexity theory" thinking to Clausewitz can be found in Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security*, 17 (Winter 1992-1993), 59-90.

6. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton Univ. Press, 1976), p. 75.

7. Margaret Sprout, "Mahan: Evangelist of Sea Power," in *Makers of Modern Strategy*, ed. Edward Mead Earle

(Princeton, N.J.: Princeton Univ. Press, 1941), p. 424.

8. Ibid., pp. 428-29, 435.

9. Douhet, p. 10.

10. Ibid., p. 91.

11. There are a profusion of definitions scattered across popular literature and documents of military doctrine. For the evolution of the Department of Defense definition of information warfare, see William H. J. Manthorpe, "From the Editor," *Defense Intelligence Journal*, 5 (Spring 1996), 8-9; for an excellent tour of the various modalities of information warfare, see Martin C. Libicki, *What is Information Warfare?* (Washington: National Defense Univ. Press, 1995).

12. Jim Katzaman, "Short Path to the Future," Air Force News Service, 13 September 1996.

13. Department of Defense, Joint Chiefs of Staff, *Joint Vision 2010* (Washington: Department of Defense, 1996), p. 16.

14. US Department of Commerce, "The Emerging Digital Economy," May 1998, http://www.ecommerce.gov/emerging/htm, ch. 2, "Building Out the Internet."

15. Department of Defense, Department of Defense Directive 3600.1, "Information Operations" (Washington: Department of Defense, 9 December 1996), p. 1-1.

16. Department of Defense, Joint Chiefs of Staff, "Information Warfare: A Strategy for Peace . . . The Decisive Edge in War" (Washington: Department of Defense, 1996), p. 6.

17. Department of Defense, Joint Chiefs of Staff and Office of the Secretary of Defense, Final Report of the Advanced Battlespace Information System (ABIS) Task Force, vol. I-VI (Washington: Department of Defense, May 1996).

18. Department of Defense, Defense Science Board, "Summer Study Task for on Tactics and Technology for 21st Century Military Superiority, Final Report" (Washington: Department of Defense, 1996).

19. See John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, 12 (April-June 1993), 141-65; and Arquilla and Ronfeldt, "Information, Power and Grand Strategy: In Athena's Camp," in *The Information Revolution and National Security*, ed. Stuart J. D. Schwartzstein (Washington: Center for Strategic and International Studies, 1996).

20. George Stein, "Information Warfare," *Airpower Journal*, 9 (Spring 1995), 34-35; see also Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal*, 9 (Spring 1995), 58-59, 62.

21. Stein, pp. 38-39.

22. Martin Libicki, "The Emerging Primacy of Information," *Orbis*, 40 (Spring 1996), 261-76.

23. Andrew Krepinevich, "Cavalry to Computer: the Pattern of Military Revolutions," *The National Interest*, No. 37 (Fall 1994), pp. 30-42.

24. Steven Metz and James Kievit, *Strategy and the Revolution in Military Affairs: From Theory to Policy* (Carlisle Barracks, Pa.: US Army War College, Strategic Studies Institute, 1995).

25. Omer Bartov, *Hitler's Army* (Oxford, Eng.: Oxford Univ. Press, 1992).

26. Michael Howard, *War in European History* (Oxford, Eng.: Oxford Univ. Press, 1976), p. 130.

Captain Ryan Henry (USN, Ret.) is Vice President for advanced planning and strategy with Science Applications International Corporation and was formerly a senior fellow in the Political-Military Studies program at the Center for Strategic and International Studies (CSIS). His career has included experience as a combat commander (including 83 combat flights during Desert Storm), defense analyst, experimental test pilot, Senate staffer, and researcher. A graduate of the US Naval Academy, he has master's degrees in aeronautical systems, systems management, national security resourcing, and public administration, and he is completing his Ph.D. dissertation in public policy.

C. Edward Peartree is with the Office of Strategic Policy and Negotiations, Bureau of Political-Military Affairs, US Department of State. He was formerly a research associate in the Political-Military Studies program at CSIS, where he worked on a multiyear study of information warfare and the effects of the information revolution on national and international security, and he is a contributing author to *Air and Space Power in the New Millennium* (CSIS Press, 1997). He is a graduate of Johns Hopkins University and holds an M.A. from George Washington University's Elliott School of International Affairs. As with all *Parameters* articles, the views expressed here are the authors' and not necessarily those of the Department of State or any other agency of the US government.

A version of this article appeared in *The Information Revolution and International Security* (CSIS Press, 1998), edited by Ryan Henry and C. Edward Peartree.

Reviewed 13 August 1998. Please send comments or corrections to carl_Parameters@conus.army.mil