



Liberty University
DigitalCommons@Liberty
University

Faculty Publications and Presentations

Helms School of Government


8-1998

Information Warfare: The Computer Revolution is Altering How Future Wars will be Conducted

Stephen R. Bowers

Liberty University, srbowers2@liberty.edu

Follow this and additional works at: http://digitalcommons.liberty.edu/gov_fac_pubs

 Part of the [Other Social and Behavioral Sciences Commons](#), [Political Science Commons](#), and the [Public Affairs, Public Policy and Public Administration Commons](#)

Recommended Citation

Bowers, Stephen R., "Information Warfare: The Computer Revolution is Altering How Future Wars will be Conducted" (1998).

Faculty Publications and Presentations. Paper 80.

http://digitalcommons.liberty.edu/gov_fac_pubs/80

This Article is brought to you for free and open access by the Helms School of Government at DigitalCommons@Liberty University. It has been accepted for inclusion in Faculty Publications and Presentations by an authorized administrator of DigitalCommons@Liberty University. For more information, please contact scholarlycommunication@liberty.edu.

Information Warfare

The Computer Revolution Is Altering How Future Wars Will Be Conducted



For more than a decade, the information revolution, spurred on by the development of advanced computer technology, has had a dramatic impact on every aspect of our lives. Commercial activities, all the way from the world's financial markets to the most basic purchases in stores, are driven by the computer revolution. It is, therefore, not surprising that military operations are equally bound by these technologies which, at first glance, seem so remote from the world of troop movements and combat. But, in fact, these technologies are changing not only society but also our definition of war and the conduct of military operations.

A consideration of some fundamental elements of military affairs—command, control, and communications—reveals the inevitability of this development. Each of these elements is enhanced by the advent of new computer technologies and, at the same time, made more vulnerable by our dependence on them. The role of computer technology has had such a dramatic impact on military operations that the traditional designation of command, control, and communications— C^3 —has been changed to C^4 by the addition of computers.

The technological vulnerabilities of modern society—both its commercial and its military components—are widely recognized. In the military realm, any technology that enhances operations can be used by an adversary to destroy the ability to perform any of the functions essential to survival.

Information warfare (IW) is the term most often used to describe the exploitation of these vulnerabilities. This concept has both old and new usage, a fact that contributes to some misunderstanding today. In its earlier applications, it included psychological operations, electronic warfare, and other military innovations. It has also encompassed the notion of "information dominance" over an enemy—the ability to more quickly and more completely understand battlefield developments. However, in spite of some confusion over terminology, it is possible to identify points of agreement about the impact of our technological vulnerabilities, what constitutes information warfare, and how IW can affect our national security.

There is a clear consensus regarding the dramatic increase in the vulnerability of modern society. Leaders of modern societies recognize that power grids, transportation networks, financial systems, and telephone exchanges are exposed to the threat posed by the almost invisible computer assailants who can touch so many aspects of our lives.

NETWORK VULNERABILITY

Modern warfare, unlike that of past epochs, is "information intensive," meaning the conduct of effective military operations requires a greater accumulation of data than ever before. Today, access to information is just as crucial as possession of petroleum, oil, lubricants, and ammunition.

Studies of allied operations during the Gulf War offer dramatic proof of the degree to which this development has produced a revolution in military strategy. According to a recent analysis, there are hundreds of thousands of "attacks" against military information systems each year and, while almost all of these penetration efforts have been by so-called "hackers," and although nearly all have failed, the few that have been successful raise troubling prospects. Possession of one valid ID and password leads to the exposure of other, presumably better-protected, sites. A breakdown in network security at any point may facilitate access into the entire system.

A computer system's vulnerability is compounded by the fact that attacks against it are likely to be staged from a remote point. Through manipulation of a telephone system and skillful use of a computer, a distant and unseen attacker can cause incalculable damage with little likelihood of being identified. In 1996, for example, an unknown hacker succeeded in shutting down the entire web site for the Environmental Protection Agency.

EVOLVING CONCEPT

The technological revolution that created opportunities for IW has also sown confusion among the military services. The inability to agree on a precise definition reflects difficulty in grasping the full implications of their vulnerability. Consequently, there is uncertainty about what should be considered IW elements, targets, and objectives.

At its inception, there was agreement that information warfare essentially played a tactical role. IW elements such as psychological operations (PSYOP), tactical deception, and electronic warfare were often designed to give military units a short-term advantage—one sufficient to prevail during a single engagement. The tools of the trade included devices designed to inhibit enemy radio communications, thereby disrupting troop movements on the battlefield. In this technologically unsophisticated era, both the mission and the techniques of IW were relatively simple and direct.

The beginnings of a modification to this early IW concept can be traced to the field of business studies, where scholars and practitioners viewed informa-



Stephen Bowers is an associate professor in the Department of Political Science, James Madison University, Harrisonburg, VA.

tion warfare as a device designed for the commercial environment. In the business world, IW was described as a process for gaining and maintaining an advantage over competitors or adversaries. This simple idea has a direct relevance to military operations in which competitive relationships are matters of life and death. Viewed within the military context, information warfare encompasses activities designed to undermine essential information networks upon which nations rely for performance of governmental, military, or commercial operations.

With the incorporation of new technologies, the military now includes the physical destruction of C⁴ assets within its IW definition. This could be accomplished either by conventional means or through the use of the electromagnetic pulse (EMP) generated by nuclear explosions. EMP, of course, can destroy radios and computers for miles around an explosion site. But even when high-value national infrastructure assets became possible targets of IW strikes, IW retained a primarily tactical role—one geared to disrupting enemy communications within an area of operations.

METHODS VS. OBJECTIVES

One common definition of IW refers to it as any malicious act done with computer technology, a phrase which, while true, lacks the precision required for a more comprehensive definition. Yet it does serve a useful purpose by attempting to focus on the methods of IW rather than its objectives.

Recent experience indicates that what may be—within the confines of the most general of definitions—considered information warfare is often more properly regarded as trivial harassment. In an effort to distinguish mere nuisances from activity that poses a serious threat, computer specialists have established three categories for classifying various levels of threats to computer security.

■ **Category One** covers personal attacks, such as the common practice of flooding a person's mailbox with unwanted Internet messages by placing his name on thousands of electronic mailing lists. The irritating result is that the victim loses use of his electronic mail service and is required to take the time to remove his address from the mailing lists.

■ **Category Two** involves industrial attacks against businesses by their "enemies." Tobacco companies are frequent victims of this type of attack. Industrial attacks have the potential of disrupting major corporate operations and could result in devastating economic impacts.

■ **Category Three** involves national attacks—efforts directed against institutions responsible for essential national services. Defense agencies and financial structures are among the most prominent targets of this IW category.

In a contemporary environment in which computer technologies are employed in support of military activities, IW has been expanded to encompass strategic objectives. A recent US military exercise was based on a scenario in which the outcome of a major war in the Middle East hinged on the disruption of power grids, telephone networks, and transportation systems by an invisible adversary who attacked from cyberspace. Categories Two and

Three both involve actions which could elevate IW to a strategic level, possibly determining not only the outcome of a particular battle but also the fate of nations at war.

NATIONAL SECURITY IMPLICATIONS

The evolution of warfighting capabilities demonstrates a central theme: the struggle of nations to project their power more effectively and more affordably than potential adversaries. In evaluating national power, attention is always given to what may be described as synthetic sources of power. The two elements most often cited are military preparedness and industrial capacity. Modern computer systems are relevant in each of these areas, and IW has a direct impact on their performance.

With IW, the weapon is not gunpowder or expensive bombers but rather the ability to get and use information, and to alter it in such a way as to disrupt the enemy's capabilities. IW offers the ability to destroy the coherence of an enemy force by distorting the sensor inputs required for its operation.

Psychological operations are a significant area for introducing IW, especially disinformation. Covert operations are another. Reportedly, one of the techniques employed by the Central Intelligence Agency in combating terrorism involved disrupting international financial activities of supporters of suspected terrorists via computer intervention.

Also, information warfare (by other names) has been an important part of the US mission in Bosnia. Personnel from US PSYOP units have been stationed there since the Dayton agreement was signed.

One of the most significant consequences of recent changes in computerized military activities is that the conventional dichotomy between civilian and military realms has been diminished. Advances in defense technology have required the military to rely upon civilian contractors to develop, operate, and maintain information systems and their related components. The specialized demands of this work have precluded many uniformed personnel with their more general skill levels from performing these highly specialized services. Consequently, on an individual basis, civilian personnel often assume greater military significance than their uniformed counterparts.

As the distinction between uniformed and civilian personnel diminishes, the installation and operation of information systems that serve as force multipliers will enable smaller groups of people to work with deadly consequences in combat situations. Equally significant in an era in which the line between war and peace is increasingly blurred, IW groups can be employed effectively in both situations.

A declaration of war or the advent of open and violent hostilities is no longer a prerequisite for deploying (or employing) military forces. This flexibility in the use of force is consistent with the long-term effort to synchronize the real and psychological effects of various, complementary national force capabilities. In future crises, the various components of national force, including IW capabilities, will be employed as a single weapon. As a result, the conduct of future warfare will be qualitatively different from that of the post-World War II era. ■

