Institute for National Strategic Studies - Strategic Forum

Number 115, June 1997

Defining Information Power

by Dan Kuehl

Conclusions

- All of the various elements and components of national information power, from Command and Control Warfare (C2W) through Military Information Warfare (IW) to Strategic Information Operations (IO) build upon each other to provide the fullest use of information as an element of national power.

- The existing DOD definition of IW is dysfunctional: a better concept is to consider IW as "those offensive and defensive warfighting actions in or via the information environment to control or exploit it."

- The existing DOD definition of IO is also dysfunctional: a better concept is to consider IO as "the range of military and government operations to protect and exploit the information environment."

- Together they provide national information power, "the broadest range of military, governmental and civilian information capabilities that enable national-level exploitation and dominance of the information realm."

Changing Definitions

The seemingly endless series of changes in the official DOD definition of information warfare-a different one in each of the three years the School of Information Warfare & Strategy has existed-reflects the lack of conceptual certainty about what IW is and where it fits into the range of elements of national power. The fact that there is no universally-accepted understanding of IW is certainly no surprise, given its newness; for comparison, ask a group of military officers to define "strategic airpower" or "maneuver warfare" and you'll get a variety of answers, even though these have been exercised for most of this century. The intent of this paper is to suggest an approach that leads to an understanding of not just IW, but how it fits into the full range of national information power.

Command and Control Warfare: C2W

The Joint Chiefs of Staff published the Memoran-dum of Policy (MOP) 30 in March 1993, defining and establishing guidelines for Command and Control Warfare, or C2W, which is perhaps best understood as the "strategy that implements IW on the battlefield." This is IWOs basic building block, its foundation in a sense, and it incorporates a range of operations the military understands quite well.

The five elements or pillars of C2W are Psychological Operations (PSYOP), Operational Security (OPSEC), Deception, Electronic Warfare (EW), and physical destruction of vital C2 nodes. Because the first three of these have been recognizable elements of warfare since biblical times, the question that immediately comes to mind is "what"s new about C2W?" The answer involves several words, including "stovepipes," "synergies," and "integration."

Stovepipe activities have largely been conducted by small and isolated groups of little known and frequently less well-regarded specialists, so there was little coordinated effort to integrate them into a unified whole and build on the synergies between them. This approach forfeited much of the advantage that could have been gained by integrating these operations, such as the relationship between psychological operations, deception, and operational security. The fundamental intent of MOP 30 (rescinded in early 1997) and now Joint Pub 3-13.1, "Joint Doctrine for C2W," is to break down the stovepipes and integrate the various elements of C2W so that their synergies and relationships can be magnified.

One of the hallmarks of C2W is that it can be conducted in any or all of the different warfighting environments-land, sea, air, outer space, even cyberspace-by any or all of the military services. The objective of C2W is the incapacitation of the enemy's military C2 function, by operations against the enemy's C2 target set and the protection of one's own. The targets can be physical: such as a command center, communications switching system, or planning cell; or cognitive: such as the morale and fighting spirit of the enemy forces, or the enemy commander's knowledge of friendly forces. Methods vary from the application of traditional instruments or weapons: such as leaflets, radio broadcasts, or high explosives; to the use of radically new technologies: such as anti-satellite weaponry or even the internet.

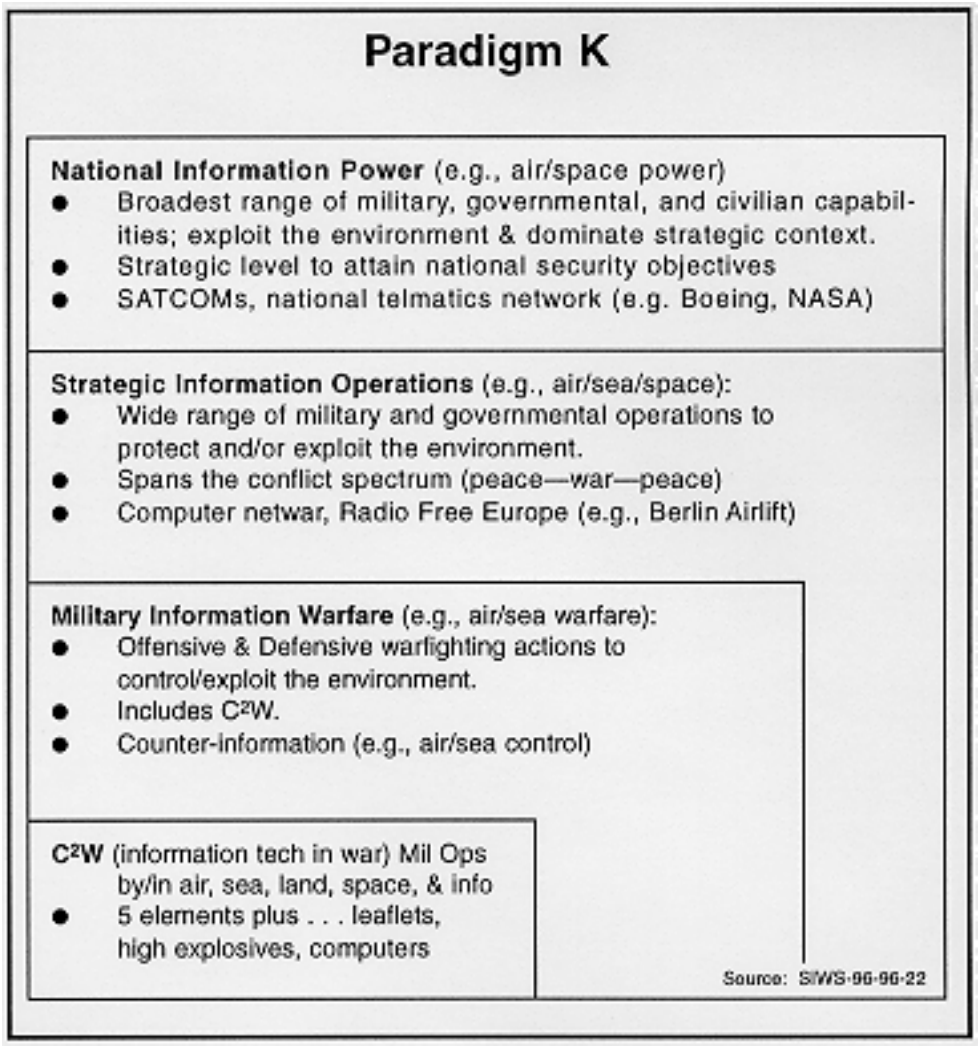
Military Information Warfare

The greatest difficulty facing the development of IW today is not technological but conceptual, because there is no common understanding or acceptance of what constitutes IW. The seemingly continuous DOD thrash over defining IW has yielded a series of definitions that have grown increasingly useless and perhaps even disuseful. The latest definition, "Information Operations conducted during time of crisis or conflict to achieve specific objectives over a specific adversary or adversaries," which was established by DOD Directive 3600.1, signed on 9 December 1996-after more than a year of coordination, rewriting, recoordination, and wrangling over its content-is hardly enlightening even to the members of the IW community who know what "information operations" are.

Some concepts of IW are so broad they essentially make all other human activities subsets of IW, while others reduce IW to little more than an umbrella for a series of separate activities. Neither approach is accurate or conducive to a better understanding of IW. Information Warfare, however, should not be complicated: it is offensive and defensive warfighting actions in or via the information environment to control and exploit that realm. The obvious parallel to other forms of warfare, such as air or maritime warfare, helps to clarify what constitutes IW. The suggested definition helps to clarify that IW is a military activity conducted during wartime and carried out in or via the information environment.

Which leaves open the question: what kinds of activities or operations constitute military information warfare? Because C2W is a subset or component of IW all of its elements comprise IW in the same sense that close air support is a component element of air warfare, or that anti-submarine warfare is part of war at sea. So how is IW different from C2W? A major aspect of IW is the effort to seize and maintain control of the information environment, which leads to what the DOD calls information superiority or information dominance. This concept is not part of C2W.

The Air Force, in its visionary white paper "Cornerstones of Information Warfare," incorporates "counter-information operations" as part of the effort to gain and maintain control of the information environment-"control" meaning the ability to use the environment for our purposes and deny it to our adversary. The parallel to the Air Force's doctrinal belief in "counterair operations" as part of the effort to gain and maintain control of the air is both unmistakable and very useful. The destruction of a communications switching center, for example, whether by an airstrike, a special operations team, or a malicious computer code modification is information warfare because the objective is to gain control of the information environment. These examples, of course, could also be defined as aerial warfare or special operations.



One of the conceptual problems to be faced is the realization that the urge to place activities into artificial pigeonholes or categories can be counterproductive to better understanding the relationship between goals or missions and the methods used to reach or complete them. Information as an environment may be a difficult concept to grasp, but there is no arguing that there is a physical environment to which information is uniquely related: cyberspace. Cyberspace is that place where computers, communications systems, and those devices that operate via radiated energy in the electromagnetic spectrum meet and interact. A radar or radio jammer is an IW device; implanted computer code that affects an adversary's computer system via a "logic bomb" is an IW device; and a videotape altered via computer "morphing" to influence an adversary's political stability is an IW device. Note the synergies between IW and other forms of warfare. As cited previously: disabling an enemy air defense computer with either a bomb or a virus can be both air and information warfare, given the means employed and the effect sought.

Strategic Information Operations

The current DOD definition of Information Operations, "Actions taken to access and/or affect adversary information and information systems while defending one's own information and information systems" is only marginally more descriptive than the definition of IW. The military is not the only branch of government that uses information for strategic purposes, and solely during wartime. A larger concept is needed incorporating the other governmental actors that engage in information operations for strategic

purposes. This concept, "strategic information operations," is defined as those military and governmental operations that protect and exploit the information environment to attain strategic objectives. This highlights the fact that competition and conflict in the global information environment is a constant affair not contained within the narrow confines of "wartime." The information struggle, which a previous version of the National Security Strategy called the "worldwide war of ideas," goes on during peacetime and crisis as well as war, and it involves a far broader range of actors than armed military forces. The airpower analogy cited previously works here as well.

One of airpower's greatest strategic successes came through the exercise of strategic airlift during the 1948-49 Berlin Blockade, an operation conducted during peacetime without any aerial combat. A prime example of a strategic information operation was that multi-year effort to influence the populace of not only the Iron Curtain countries but the USSR itself via Radio Free Europe and its associated programs. Another, which did occur during wartime, was the successful effort by the British in the opening days of World War I to dredge up from the bottom of the North Sea the underwater telegraph cables that connected Germany to the outside world. This strategic information operation not only cut Germany's military C3 links to its forces worldwide (at sea and in its colonies) but also-and more importantly-meant that the neutral countries of the world, most especially the United States, saw the war through London's filter. These two examples clearly highlight the use of information for strategic political objectives.

Strategic information operations thus differ from military information warfare in two important ways: IO spans the conflict spectrum from peace to war and back to peace, and it involves all elements of the national government, not solely the military. These are important considerations precisely because the effort and coordination needed to engage the entire panoply of governmental organs is a particularly difficult and sensitive affair. Associating the word "war" with the gathering and dissemination of information has been a stumbling block in gaining understanding and acceptance of the concepts surrounding information warfare. An information-intensive non-military organization such as the Voice of America may be uncomfortable with the concept of information warfare, yet see an important role for itself in strategic information operations.

National Information Power

The exercise of national power in the information environment does not rest solely with the national government, whether through its military or civil organs. The reason for this is that national information power is the broadest range of military, governmental and civilian information capabilities that enable national-level exploitation and dominance of the information environment. It is at this level that information power operates with economic, military, diplomatic, technological, and other forms of national power to provide national leadership with the fullest range of power capabilities to use in attaining national strategic objectives. None of these forms of power function in a vacuum-all are synergistically related to the other forms: the art of statecraft rests in how one integrates them. Perhaps the key word in this definition of information power is capabilities, for it is in the judicious weighing of the military, governmental and civilian components of information power that the potential emerges to blend and use them to achieve national strategic objectives.

The airpower analogy once again is useful, for at the national strategic level American airpower is more than bombers or fighters; it also includes, for example, the American aviation industry-which is the world's largest, an enormous contributor to a positive balance of trade, and the provider of untold thousands of jobs. This is even more true of information power, for the revolution in information technologies is being driven by the civil sector, not the government or military. The civilian component of national information power thus includes such diverse elements as our telematics infrastructure, Less than two decades old, telematics is the marriage of advanced telecommunications systems and computerized databases and networks. It is the world of the storage, transmission, manipulation and dissemination of electronic digital information and includes satellite communications systems, the microprocessor ("chip") production industry, and software developers and producers. Other, less obvious elements, such as the computer science departments of our colleges and universities, or even the news media, make important contributions to national information power by demonstrating to the world the strength and robustness of a society whose governmental organs are open to constant scrutiny and inspection. The United States' ability to exercise power and influence people, organizations and governments through the information environment is dependent upon the collective contributions of its information infrastructure. This is the paradigm of national information power.

Dr. Daniel Kuehl is a professor of Information Warfare in the School of Information Warfare and Strategy at NDU. For more information contact Dr. Kuehl at (202) 685-2257 or e-mail at kuehld@ndu.edu.

The Strategic Forum provides summaries of work by members and guests of the Institute for National Strategic Studies and the National Defense University faculty. These include reports of original research, synopses of seminars and conferences,the results of unclassified war games, and digests of remarks by distinguished speakers.

Editor in Chief - Hans Binnendijk

Editor - Jonathan W. PierceNOTE

| Return to Top | Return to Strategic Forum Index | Return to Publications Home Page |

Return to NDU Homepage
INSS Homepage