NATIONAL DEFENSE UNIVERSITY
STRATEGIC FORUM
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

Number 105, March 1997

Joint Information Warfare

An Information-Age Paradigm for Jointness

by Dan Kuehl

Conclusions

- Current concepts of "jointness" that focus on integrating the operations of DOD's four military Services are too narrow for Information Warfare and Information Operations (IW/IO).
- National information power and the broad needs of national security in the dynamics of the information age necessitate a more inclusive understanding of what is meant by "joint".
- "Joint IW/IO" must incorporate the actions and involvement of numerous non-DOD organizations and activities, to include elements of the private sector. Although their actions will not be directed by DOD, active elements in Joint IW/IO must at least coordinate their actions, even if that coordination is informal, in order to be effective.
- This concept of "Joint IW/IO" should be reflected in DOD policy and military doctrines

Jointness and the Information Age

The passage of the Goldwater-Nichols Act in 1986 generated a new emphasis on "jointness". Current concepts of jointness and joint operations are defined as "activities, operations, organizations, etc., in which elements of more than one Service [emphasis added] of the same nation participate." The blending of the operations and capabilities of the military Services, however, is no longer sufficient for information warfare/information operations (IW/IO) and the needs of national security in the information age. The impacts and implications of the information revolution are so widespread that they necessitate a broader, more inclusive concept incorporating all of the various elements of national information power.

The Services and Information Warfare

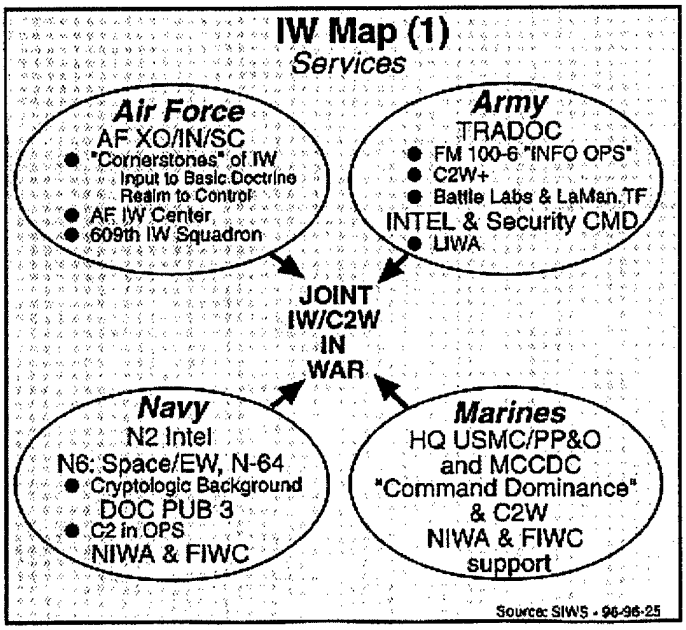
All of the Services are responding in some manner to the challenges of the information age and the imperatives of information warfare. The Marines, while uncertain about the broader theories of IW, are deeply involved in exploring the means by which they can attain "command dominance" over their adversaries. While acknowledging and leveraging the recent dramatic technological advances in information and communication systems, the Marines' focus is clearly on the human dimension of conflict, with the objective of maximizing human and operational flexibility instead of relying on

technology to minimize friction.

The Army, also cautious about the broader theories of IO, has no such qualms about the technological opportunities of the future, and the Army's vision for the next century, incorporated in "Force XXI" and based on digitization of the battlefield, is heavily, perhaps critically, dependent on the technologies of the information age. The Army is investigating the means and implications of these concepts and capabilities, and its Land Information Warfare Activity **(LIWA)**, located at Fort Belvoir and associated with its Intelligence and Security Command **(INSCOM)**, is one of the Army's focal points for this effort. Another is its Training and Doctrine Command **(TRADOC)** at Fort Monroe, which recently issued the Army's first doctrinal manual in this area, Field Manual (FM) 100-6, "Information Operations." (The exact meaning of "information operations" varies according to the user, and while the term is used by DOD, the Army, and the Air Force, it means something different to all three.)

The Navy has possibly more personnel engaged in "nuts and bolts" IW/IO than any other Service and has (perhaps more than any other Service) for decades practiced some of the elements of Command and Control Warfare (C2W), defined as "the military strategy that implements information warfare on the battlefield." While still exploring the broader ramifications of IO, the Navy is exercising and practicing IW/C2W increasingly in its daily operations. While the Naval Information Warfare Activity (NIWA) at Fort Meade is a geographical reflection of the Navy's long history of cryptology, the Fleet Information Warfare Center (FIWC) at Little Creek Amphibious Base near Norfolk and Atlantic Fleet HQ, and its several branches around the country, are heavily involved in developing and refining concepts for fleet IW/C2W operations.

The Air Force has taken dramatic steps, both organizationally and doctrinally, to move into information age warfare. In 1993 the Air Force established its Information Warfare Center around what had been its Electronic Warfare Center, and the newly-activated **609th IW Squadron** is the first unit dedicated to an operational IW mission. The Air Force's white paper "Cornerstones of IW", published over the signatures of Dr. Sheila Widnall, Secretary of the Air Force, and General Ron Fogleman, Chief of Staff, expresses the broadest view of IW of any of the Services, stating information is a "realm" to be dominated in a manner alike to air or space. Evolving doctrinal concepts speak to the need to integrate Air Force

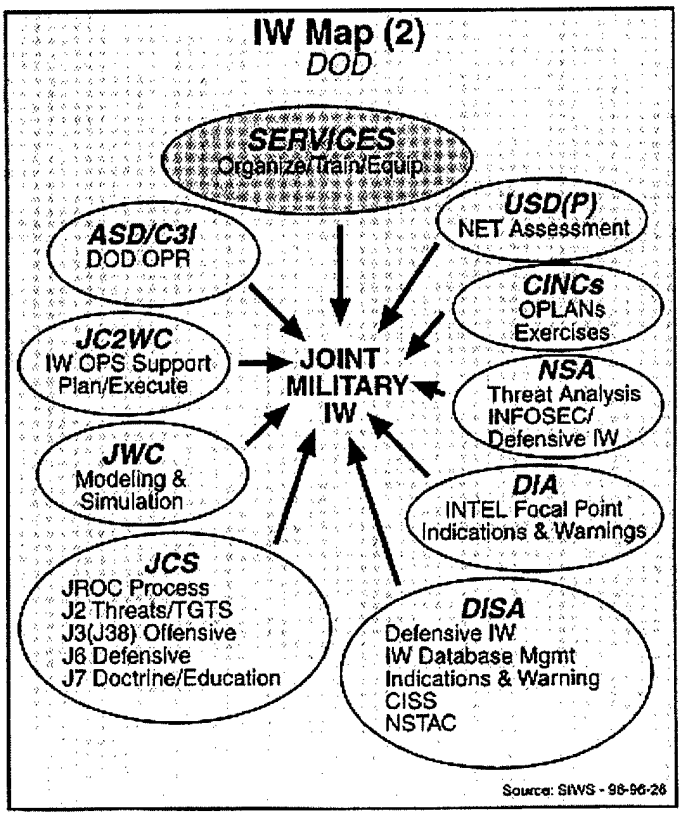


operations across three realms-air, space and information-in order to attain superiority and freedom of action in each. Joint information warfare involves integrating and coordinating IW across the doctrinal, organizational, and conceptual differences of the four Services.

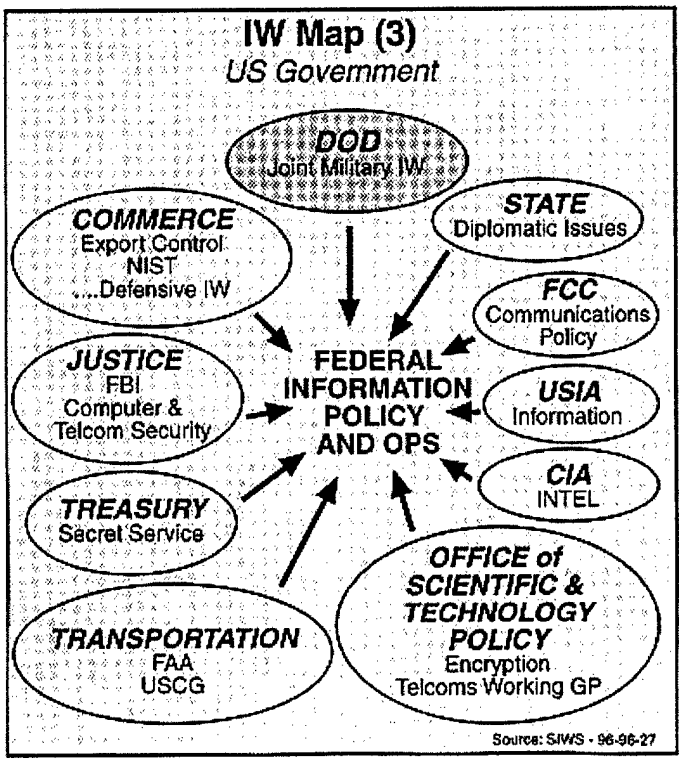
IW in the Department of Defense

Any discussion of IW that does not take into account the capabilities, responsibilities, and operations of a myriad of DOD organizations and agencies apart and aside from the four Services, however, is incomplete. The most immediately apparent are those that respond directly to the Chairman of the Joint Chiefs of Staff or through the Joint Staff, or are in the direct chain of operational command through the Unified Commands ("theater CINCs"). The CINCs are the most obvious players, because they are charged with the responsibility of planning for and conducting IW, and the Chairman issued detailed guidance in the early 1996 issue of CJCS Instruction 3210.1, "Joint IW Policy."

The Unified Commands are exploring means to integrate information warfare into their plans and operations; indeed, some see it as a centerpiece of their future mission. The Unified Commands are jointness personified, as is the organization charged with supporting their IW/C2W efforts, the Joint C2W Center (**JC2WC**, or "jake-wick"), collocated with the Air Force Information Warfare Center at Kelly AFB. Information warfare in the real world simply is not possible without these elements of the joint force. Other members of the joint community also contribute to our IW capability. The Joint Warfighting Analysis Center, Joint Doctrine Center, and Joint Warfighting Center, for example, all have a role in shaping our IW capability, as do the elements of the Joint Staff such as J-6 or J-3, which serves as the OPR for joint IW/IO matters.



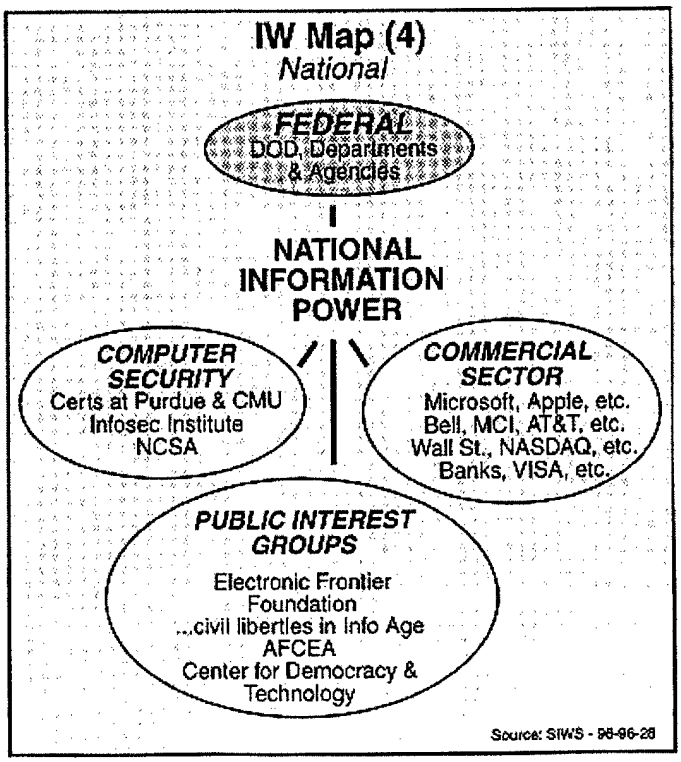
However, several DOD organizations outside of the JCS structure are also critical to our national IW/IO capability. The Defense Information Services Agency **(DISA)** manages DOD communications systems and is critical in the effort to provide information assurance and security to DOD communications. DISA, through the National Communications System **(NCS)**, provides the DOD's interface with the National Strategic Telecommunications Advisory Council **(NSTAC)**, which is comprised of the chief executives of the nation's largest telecommunications firms who provide the President with strategic advice on matters relating to telematics (the marriage of telecommunications and computer networks) and information policy. The Defense Intelligence Agency is the internal DOD focal point for intelligence matters relating to IW, while the National Security Agency is a key player in the effort to analyze the threat and provide information security and defensive IW/IO. Any discussion of national information power and security must take into account the responsibilities and capabilities of these DOD agencies. No discussion of "joint IW" would be complete without them. A comprehensive approach to joint IW, therefore, requires coordinating the activities and policies of several Joint and DOD elements as well as the Services.



IW in the Federal Government

But, the new paradigm of information warfare is unsettling for traditional DOD warriors, because from a national security perspective several other elements of the federal government are crucially important to the use of information for national security, the development of national information power, and the conduct of IW in its broadest sense. The Central Intelligence Agency is the focal point for national security intelligence. This not only includes potential IW/IO threats to national capabilities, systems and infrastructures but also the explosively expanding world of "open source intelligence", and the CIA is wisely and aggressively looking at ways to incorporate this new and technologically-driven source of information into its processes and databases. Another key provider of American information power is the United States Information Agency (USIA), and although its staffers would bristle if told they were involved in IW, the use of information as a weapon in the "contest of ideas" and the worldwide nurturing of democracy clearly fits into a larger and more inclusive view of IW.

One might wonder what role the Justice Department has in IW, but Justice is one of the core members of the President's Commission on Critical Infrastructure Protection, established in mid-1996 with President Clinton's Executive Order 13010, and the **FBI** is conducting an ever-increasing number of investigations into computer crime and cybernetic espionage. The Bureau has an active program



underway in computer and telecommunications security. If a DOD or other federal computer system suffers a break-in or intrusion, the FBI will almost certainly be one of the first agencies called. Another organization that at first glance might seem miscast in the IW arena is the Secret Service, but one of their critical responsibilities is security of the currency, which tasks them with protecting the electronic funds transfer systems upon which our national economy is becoming increasingly dependent. The Commerce Department's *Office of Export Control and National Institute for Standards and Technology* ***(NIST),*** and the President's Office of Scientific and Technology Policy (an autonomous element not associated with a Cabinet office), and the Office of Management and Budget are involved with issues such as electronic data encryption or national information infrastructure policy. These might not seem like national security issues to a traditional warrior, but similar issues are becoming increasingly important to areas such as technology exports, terrorism, and the war on drugs, all of which have some degree of current military interest or involvement. Most other federal agencies-*Energy, FEMA, Transportation,* and more-also increasingly rely on the smooth and uninterrupted flow of electronic digital information to carry out their functions and thus have interest and involvement in national information power. Thus, the paradigm of joint IW/IO must incorporate not only the Services but the Joint, DOD, and Federal communities as well.

National Information Power

The paradigm of joint information power has a broad and troubling perspective for the traditional concept of "jointness". The "defense" of cyberspace (that place where computers and electronic telecommunications systems connect and interact, a field of study known as "telematics") is being waged in part by entities such as the computer emergency response teams **(CERTs)** at universities such as Purdue or Carnegie Mellon. Information age "warriors" are trained not by military drill instructors but by computer science departments around the country. Educational organizations such as the *National Computer Security Association and the Infosec Institute* also play a role. Myriad **public interest groups**

represent all points of the political and social compass, from the National Military Intelligence Association and the Armed Forces Communications & Electronics Association, to the Center for Democracy and Technology, and the Electronic Frontier Foundation. They all help shape and set the political terrain and social context for the ongoing evolution of information age security issues.

Finally, and certainly not least, there is the commercial sector, because the issues involved in information age security would be meaningless without the activities, advances, and involvement of Microsoft, AT&T, NASDAQ, Citibank, etc. The information revolution is, at heart, not a military revolution but a commercial, cultural and technological one, albeit with extremely important impact on and implications for the uniformed military. Neither the Services nor DOD are leading this revolution; rather they are running fast to merely stay abreast of the changes in technology and society.

Summary

National security in the information age and the development and exercise of the information component of national power requires a new paradigm of jointness that incorporates and synchronizes the policies and activities of all the players in the information realm. The development and exercise of national information power spans the organizational spectrum from the members in a military IW unit to the leadership of the largest information-related corporations and commercial entities. Although the DOD cannot direct these widespread activities, the paradigm of Joint IW/IO must of necessity encompass military, governmental, and private sector organizations and actions. This will require changes, both organizational and cultural, that will allow discussion and coordination of activities, even if the coordination is informal and non-directive. Perhaps the recent formation of the President's *Commission on Critical Infrastructure Protection* presents a baseline model for the integration of federal and private sector concepts and activities. Within the military Services, doctrines for IW/IO must take into account the dual nature of information power and help to set a mindset that sees the civil sector as a partner in the new paradigm of information age jointness. Without such a paradigm, information age national security increasingly will become a chimera towards which we will strive but find unattainable.

Dr. Daniel Kuehl is a professor of Information Warfare in the School of Information Warfare and Strategy at NDU. For more information call 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 Research and Publications|

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Joint Information Warfare: An Information-Age Paradigm for Jointness

B. DATE Report Downloaded From the Internet: 09/26/01

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **National Defense University Press**
Institute for National Strategic Studies
Washington, DC 20001

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/26/01**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.