Assessment, issued in September 1985 as the centerpiece of Congress's attempt to clarify the issues rather than to resolve the debate over Star Wars, reached the conclusion that funding SDI in line with Pentagon plans would mean settling for immature technologies in the early 1990s. Already, SDI has been trimmed back to a point where what was once described as a program limited only by what is technically feasible has been transformed into one constricted by what is fiscally affordable and politically possible.

—IRWIN GOODWIN

Making waves: Poindexter sails into scientific databases

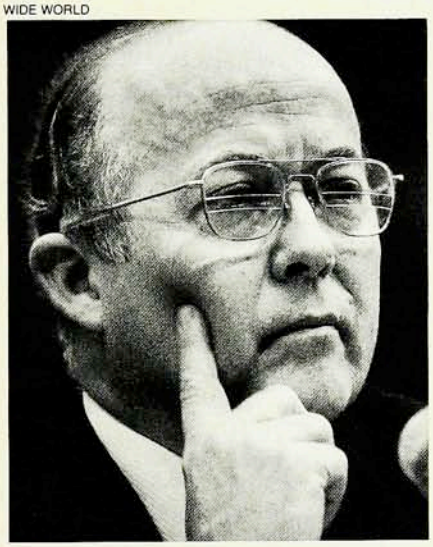
It probably seemed like a great idea, but it confirmed the worst fears of the information industry and the scientific community. Last 29 October, Vice Admiral John M. Poindexter, then President Reagan's national security adviser, issued a policy paper before he left the ship of state over the clandestine Iran–Nicaragua contra affair. The Poindexter paper calls for sweeping new government controls on data and information stored in computer systems and transmitted by electronic communications. The reason for this policy is the fear among many at the White House and on Capitol Hill that a great deal of sensitive but unclassified scientific, technical and even political and economic information is reaching the Soviet bloc.

"Sensitive" data have been defined by the Defense Department for some time as information under its control that is not classified but is subject to export control restrictions. In Poindexter's dictionary the term means "information the disclosure, loss, misuse, alteration or destruction of which could adversely affect national security or other Federal government interests. National security interests are those unclassified matters that relate to national defense or foreign relations.... Other government interests are those related but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the US government by its citizens."

Crackdown. Though scientific and technical research is not on Poindexter's list, it is precisely that subject that has haunted the Reagan Administration since it came to Washington in 1981. When it began cracking down on meetings of science and engineering societies attended by researchers from Warsaw Pact countries or China, tensions increased between scientists and the government. Reagan's Executive Order 12356 of 2 April 1982 sanctioned controls on access to research results beyond the procedures established by every President since Truman. Accordingly, the intelligence groups within the Defense, Commerce and Energy Departments stepped up their activities at open meetings.

A furor followed. In an effort to set a prudent course, a special panel of academics, scientists and industrialists brought together by the National Research Council issued a report, *Scientific Communication and National Security*, concluding that between basic research, which should remain open and unfettered, and classified work there are some sensitive "gray areas" (PHYSICS TODAY, November 1982, page 69). In these, stated the panel, headed by Dale R. Corson, president emeritus of Cornell University, the government might reasonably impose some controls, using contract restrictions in preference to export regulations or security classifications.

WIDE WORLD



POINDEXTER

Directives. While the government continued its practice of restricting reports of research that its authors considered unclassified (PHYSICS TODAY, June 1983, page 41), the President issued two National Security Decision Directives signed a year apart. Both had the effect of strengthening the government's hand in keeping secret any data and information its bureaucrats claimed "could adversely affect the national security."

The first, NSDD 145, issued on 17 September 1984, created a national policy on security for telecommunications and automated information processing systems under a Cabinet-level interdepartmental group that was directed to explore ways of protecting not only government data and information but private or proprietary material in electronic systems. The President's order stated that a "comprehensive and coordinated approach" was required to regulate "information, even if unclassified in isolation, [which] often can reveal highly classified and other sensitive information when taken in aggregate." It directs the Secretary of Defense to take charge of the situation.

The second was NSDD 189, signed by Reagan on 21 September 1985. It sought to calm the troubled waters that the government had stirred up around scientific and technical information. After the government used export control regulations and a 1981 amendment to the Atomic Energy Act to exclude dozens of unclassified papers from some scientific and technical conferences where foreign nationals were present, several professional societies protested the action and a few went so far as to impose a kind of self-censorship (PHYSICS TODAY, November 1985, page 55). NSDD 189 was promulgated to explicitly exempt unclassified "fundamental research" from restraints on communications.

Loophole. Even though it allowed for no shadings between open and classified research, the directive carried a loophole permitting each agency to periodically review all research in progress "for potential classification ... as provided in applicable US statutes." In a covering memorandum to the directive, the President's national security adviser, Robert C. McFarlane at the time, reminded both bureaucrats and researchers, just in case they may have missed the point, that the policy "preserves the ability of the agencies to control unclassified information using legislated authority expressly for that purpose in applicable US statutes."

NSDD 189 marked an uneasy truce in the government's battle to keep scientific and technological secrets. The Poindexter policy paper, with its emphasis on electronic databases and information systems, only slightly changes the course of the battle but renews the war.

Question. The strategy was enunciated to members of the Information

Industry Association by Diane Fountaine, director of the Pentagon's information systems directorate, at their convention in New York on 11 November. "The question is not whether we're going to protect information," Fountaine declared. "The question is, where will the controls be applied?"

Startled by Fountaine's question, IIA members barraged her for an answer. "We were all asking how we could deny access to customers here and abroad and how we could be expected to police the systems," recalls Jack W. Simpson, president of Mead Data Central Inc, operator of LEXIS and NEXIS, leading commercial data banks. "It seemed obvious that her purpose was to let us know the government is serious about limiting the release of information it considers sensitive, even if it's not classified."

What's odd about the way the policy has been disseminated so far is its "fugitive, furtive nature," says Harold Relyea, an expert on government security methods at the Library of Congress's Congressional Research Service. It was never published in the *Federal Record* or announced publicly. The first public inkling of the policy came from Fountaine.

Protection. Fountaine's boss, Donald C. Latham, assistant Defense secretary for command, control, communications and intelligence, is chairman of an interagency group that has been exploring ways to safeguard information in commercial data systems. According to Latham, "sensitive" is not meant to introduce a new category of classification but to indicate that data or information so labeled needs protection of some sort. "This was carefully thought through with lawyers and everybody," he said.

Another database likely to be affected by the policy is SPIN, which indexes and abstracts all journals published by the American Institute of Physics, including those translated from Russian. "There are now dozens of data and information bases that are enormously useful," says Mead Data's Simpson. The Administration's proposed restrictions, he argues, "could inhibit our nation's own research efforts." To Simpson, the new policy appears to give government authorities an open and free hand to restrict any information they deem sensitive—that is, potentially harmful or embarrassing to national defense, foreign policy or possibly government officials.

Before World War II the main object of espionage was to obtain war plans—to find out when and how a prospective enemy intended to attack. During the war the focus changed to cracking codes and battle orders. After the war spying centered on nuclear weapons and delivery systems. In recent years, though, spying has concentrated on acquiring the latest scientific and industrial information with military and economic implications. Since the early 1980s members of the intelligence community, among them Admiral Bobby Inman, former deputy director of the CIA, warned that the lax environment at academic research centers and in high-technology industries offers many opportunities for military or trade rivals to pick up sensitive information or knowhow that could be useful.

Courier. High technology in fact is frequently the courier of such information, the Senate Select Committee on Intelligence reported last October in *Meeting the Espionage Challenge*. This report asserted that damages to the nation's security caused by the theft of advanced technology, incursions into electronic files and other espionage activities "amount to a staggering loss of sensitive information to hostile intelligence services. As an open society, the US already allows its adversaries unfettered access to vast amounts of information that must be shared widely so that our political system can function democratically and the process of free scientific inquiry can be most productive. Our openness gives hostile intelligence services the ability to focus their efforts on those few areas of our government and society where confidentiality is required."

In 1985, often called the "year of the spy" after the Walker case and other, similar episodes exposed the country's security lapses, Congress passed the Intelligence Authorization Act. It requires the executive branch to come to grips with the problem. The Senate select committee found that "the combination of human espionage and sophisticated technical collection has done immense damage to the national security." The committee demanded that government security programs should be strengthened.

Security policies and practices "remain fragmented despite persistent attempts to develop national standards" and, wrote the committee, information security involving computers and telecommunications was vulnerable to secret agents. So, the committee declared, "national security cannot afford much more delay. This is especially true if the current Administration is to leave as a legacy a workable security policy that will not have to be reinvented by each succeeding Administration." Indeed, the report continued, "this country has a long way to go in the development of operations security practices to protect sensitive programs against hostile intelligence collection activities." Among its conclusions, the committee found that the current classification system is "unduly complicated" and "breeds cynicism and confusion in those who create and use classified information."

Paradox. The Senate detected a paradox: The availability of extensive databases and sophisticated search techniques makes it relatively easy for foreign agents or others to piece together bits of information into a fabric that could bear the label "top secret." This is how *The Progressive* magazine was able in 1979 to publish an article decribing how to put together a hydrogen bomb. When the government's case against the magazine came before the US Supreme Court, the editors argued successfully that everything in the article came from open literature, much of the information readily reachable on open library shelves at Los Alamos National Laboratory.

The Pentagon's first targets are certain to be databases at the National Technical Information Service, the Defense Technical Information Center, the Energy Department and NASA. How the new security policy will apply to commercial or scientific databases is not yet certain, largely because neither the State nor Commerce Department is sure about what actions to take and whether such information programs are protected by the First Amendment.

Fuzziness. It is just such uncertainties that cause worries in science and academic circles (see editorial, page 144). Francis Sobieszczyk, who heads the scientific and technical information section for the Pentagon's Office of Research and Advanced Technology, sought to reassure those who fear the worst. "Only our own databases and communications links are affected by the new policy," he said. But Pentagon hard-liners are on record in support of restrictions on databases and information systems they consider sensitive.

How the Poindexter policy affects access to academic supercomputers is also fuzzy. Pentagon authorities say it covers all agencies, including the National Science Foundation, which established five supercomputing centers at universities. But NSF officials argue that the agency has no control over the machines or their output since it turned over ownership. Even so, another interagency panel, under the chairmanship of James F. Decker, deputy director of the Department of Energy's Office of Energy Research, continues its inquiry into the issue. Considering the way the new policy was promulgated, it may take effect before the Decker group presents its report.

—IRWIN GOODWIN □