

U.S. data from foreign spies and also spies on other countries' transmissions, is extremely secretive. Nevertheless, in 1985 NSA officials emerged from their vast headquarters at Fort Meade, Md., to urge U.S. companies—including IBM, AT&T and others that deal in high technology—to buy equipment it had designed for scrambling, or encrypting, data. The NSA insisted, however, on managing the “keys” needed to unscramble messages and prohibited the use of its encryption equipment for international communications.

Because of such restrictions, even companies interested in encryption, such as banks, resisted the NSA's overtures, according to Robert H. Courtney, formerly a security analyst at IBM and now a consultant. The NSA, Courtney contends, is too “hopelessly introverted” to understand industry's security concerns, which involve not foreign espionage but fraud and embezzlement. Notwithstanding, according to John M. Richardson of the Institute of Electrical and Electronics Engineers (IEEE), a professional society that helps to set telecommunications standards, many companies worried that if they refused to comply with the NSA's “guidelines,” they would lose Government contracts.

Then in 1986 agents of the Defense Department, the Central Intelligence Agency and the Federal Bureau of Investigation began visiting organizations that manage electronic data bases. The data bases, which transmit data over telephone lines to subscribers' personal computers, included *Chemical Abstracts*, run by the American Chemical Society, and Dialog, a service of the Lockheed Corporation. The Government agents reportedly asked to see lists of subscribers and inquired how access to non-U.S. citizens could be cut off.

In October, 1986, John M. Poindexter, then Reagan's national security adviser, aroused still more concern by issuing a memorandum stating what information the Government considered “sensitive” and therefore subject to regulation. Poindexter included any data related to national defense or foreign relations as well as “economic, human, financial, industrial, agricultural, technological, and law-enforcement information.” “The memo included almost anything you could think of,” says Charles K. Wilbur of the Office of Technology Assessment, who has supervised a major study of data security for Congress.

Concerns over these actions were

aired at hearings chaired by Representative Jack Brooks, head of the House Government Operations Committee, early last year. The American Civil Liberties Union, the American Association for the Advancement of Science, the American Physical Society and many other organizations argued that data controls hurt U.S. research and commerce.

The hearings, in the words of one observer, “turned the tide” against the military's program. Soon after the hearings ended Frank C. Carlucci III, who had replaced Poindexter as Reagan's national security adviser when the Iran-Contra affair erupted, rescinded the increasingly controversial “Poindexter memo.” White House officials later voiced support for a bill, first proposed by Brooks, that makes the National Bureau of Standards, an arm of the Department of the Commerce, responsible for devising security guidelines for civilian information systems. After both the House of Representatives and the Senate had passed the bill, called the Computer Security Act, the presi-

dent signed it into law on January 8.

Yet Pentagon officials, according to one congressional aide, “worked out a deal” with the Senate that may let the NSA keep a hand in the game. As part of the agreement, Senator Lawton M. Chiles declared for the *Congressional Record* that the Computer Security Act applies only to computers and “is not intended in any way to alter the assignment of responsibilities in the area of telecommunications security.”

An aide to Chiles contends the statement was meant to allow the NSA to “save face” rather than to provide it with a semantic loophole. Other observers are disturbed both by the Chiles statement and by the ambiguity of the Computer Security Act itself. Robert L. Park of the American Physical Society maintains, however, that the act will have a positive effect, particularly in combination with the recent departure of two high-ranking officials in the Pentagon's policy office: Richard N. Perle and Fred C. Iklé. “These were the people behind the restrictive policies,” Park says. —J.H.

BIOLOGICAL SCIENCES

Where's Rover?

J Civil Defense *See + The Citizen*
The military loses a fight for control of data—or does it?

At a quiet bill-signing ceremony in the White House in early January, a protracted battle by the Pentagon for control of civilian electronic information systems—particularly those containing scientific and technical data deemed valuable to the Soviet Union—ended in defeat. Perhaps.

The battle officially began in 1984 when President Reagan issued a “national security decision directive” declaring that unclassified but “sensitive” information stored in computers and sent over telecommunications links, both Federal and privately owned, “can become targets for foreign exploitation.” The directive created a committee headed by the National Security Agency, an arm of the Department of Defense, to devise stiffer security standards.

The NSA, which shields classified

in the corresponding place (a larger stuffed dog behind a full-size couch). memory check, the child to retrieve the toy from

eed,” DeLoache says, “the to realize that the model d the room and that, by reg the location of the object the model, he or she could the location of the object l in the room.”

vo-and-a-half-year-olds, ac- to DeLoache, knew they posed to find a toy, but they aware that they had any b- nowing where the toy was looking for it.” As a group arched with little success, ough they were adept at re- rring where the miniature was in the model.

ntrast, the approach of the old- ren highlights “the abrupt na- f the developmental change.” ig a memory game rather than ssing game, they had “nearly rsal” success in finding both ts. With a few months' differ- in age, the three-year-olds were to infer where the toy was hid- from the symbolic relation be- n the model and the room. hy could the younger children