confirmed the relationship between eruptions from the sun and magnetic and density shocks passing through the solar system. These shocks are of more than academic interest, for on Earth they disturb the magnetosphere, often interfering with electronic communications. They can also pose special risks for astronauts and equipment in space. "The Air Force is always interested in this kind of data," one researcher says, "because when something goes funny with a satellite, they want to know if it was the result of a natural event or something done by the Russians."

The Space Environment Services Center in Boulder, Colorado, relied on Solwind for similar reasons. The center makes regular space weather forecasts, reporting on such things as solar wind, radio emissions, and magnetic disturbances. The forecasters checked Solwind data at times in an effort to anticipate magnetic storms arriving from the sun. While the agency has put in a request for a new source of environmental data, says Joseph Hirman, the proposal may take a decade to get through the space bureaucracy. One reason for the delay is that it has become prohibitively expensive to launch new satellites, each of which must prove its worth in a competitive funding environment. Solwind was a hardy and productive gadget that far outlived its expected lifetime.

As for P78–1, it is gone but not forgotten. According to one government official, the satellite has shattered into "in excess of 100 observable pieces." Observable in this case means detectable by radar, being 10 centimeters or more in diameter. U.S. space agencies track more than 4000 bits of debris in orbit, roughly 9 percent of which were created by Russian ASAT tests since 1968. Now an American test has increased the junkpile by 2 percent. The low-orbit pieces will fall and burn up within a few years.

In the meantime, the remains of the satellite pose a certain hazard to anyone or anything wandering into its former neighborhood. Even a 4-millimeter particle can damage a spacecraft, and a 1-millimeter paint chip may be able to puncture an astronaut's space suit. The space shuttle encountered a large paint chip on its seventh mission in 1983 and suffered a damaged window. According to NASA, the malfunctioning electronics boxes recently brought back from Solar Max were peppered with paint-chip impacts. As a result, NASA scientists are asking U.S. and Soviet officials to curb the rapidly growing problem of space pollution from ASAT tests.

Satellite P78–1 thus enters a new era of macabre celebrity, becoming more glamorous in death than in its hard-working life.—**ELIOT MARSHALL**

NSA to Provide Secret Codes

The NSA proposes to supply codes to government agencies and to banks and industries in the private sector; but only the NSA will know how the codes work

The National Security Agency, concerned that the nation's communications security is grossly inadequate, is preparing to expand its role, adding a new dimension to its nature and mission. Rather than concerning itself mainly with breaking foreign codes and supplying codes for the government to use in protecting classified information, the NSA is going to supply codes to anyone who may need them. This includes banks, industries, and others in the private sector. The agency also will be in charge of the cryptographic needs of all government agencies, including agencies such as Health and Human Services, for example, as well as the Department of Defense, which already uses the NSA's codes. In short, says Michael Fleming, who is head of the new industrial relations group at the agency, the NSA will become a service agency.

The impetus for the NSA's new program is its concern that inadequate protection of computers and computer communications in this country contributes to what the agency views as a hemorrhage of U.S. technology to the eavesdropping Soviets.

The way the new program is planned, the NSA will give the code-making algorithms to qualified U.S. companies with appropriate security clearances. These companies will produce the codes in the form of small pieces of hardware. Because these codes are secret, even the users of them will not know how they work. These trusted companies will sell the hardware to U.S. companies or government agencies. The computer chips with the codes on them will be designed to prevent "reverse engineering" so that it will be nearly impossible to examine the chips and figure out the coding algorithms.

The NSA will review the communications security needs of all the government agencies—not just the Department of Defense—and will tell them which codes to purchase. It can only advise the private sector but, says Walter Deeley, who is deputy director for communications security at the NSA, "I will try to identify vulnerabilities. I will tell them where they can be had and how they can be had."

To encode with the NSA's algorithms, each user needs a key in addition to the computer hardware. Keys are individualized—like locks on doors they enable the same basic coding scheme to provide security for a variety of different users. The NSA will supply keys to all government agencies that use the new codes. Of course, anyone who has a key for a particular code can both encode and decode messages with it, but the NSA, says Deeley, will not keep the keys it supplies. "I wouldn't even know where to store them," he says.

Banks and companies in the private sector will be given three choices. They can buy keys, at cost, from the NSA, or they can buy keys from a trusted company, or they can ask the NSA for instructions on how to make their own keys. However, cautions Deeley, "It is not a trivial thing to produce a good key." Those who make their own keys do so at their own risk. The NSA will not vouch for the keys' ability to protect the encrypted information.

As might be expected, the NSA's plans are controversial. Critics are concerned by the increasing power that the NSA is acquiring and with the agency's plans to keep its encryption algorithms secret. Allan Adler, an attorney at the American Civil Liberties Union's Center for National Security Studies in Washington, D.C., remarks, "Putting the NSA in charge ensures a one-dimensional approach. The NSA operates largely in secret and has no feeling for the protection of individual privacy or access to the government's information. The NSA's ex-

pertise is in security. Is that appropriate for the Social Security Administration or for the Securities and Exchange Commission?" Adler also is concerned by the NSA's desire to encode all information that, although unclassified, is, to the agency's mind, sensitive. This includes economic and banking information, for example. "Just what kind of information doesn't have a national security element to it?" Adler asks.

Whitfield Diffie of BNR in Mountain View, California, is concerned by the proposed secrecy of the NSA's algorithms. He would feel more confident advising people to use them, he says, if he knew what they were. Diffie is among the first researchers outside the NSA to study cryptography and is an expert on communications security. Deeley says he has to keep the algorithms secret because "good algorithms are hard to come by." Why publish them, he says, and "give the other side a leg up?" Diffie responds, "I am not particularly persuaded that their algorithms are so fragile and I personally would much rather see publicly available algorithms used."

The NSA's new system would supersede the Data Encryption Standard, or DES, which is widely used both within and outside the government. The NSA feels it cannot continue to endorse the DES.

The DES was published about 10 years ago by the National Bureau of Standards for use by government agencies to protect nonclassified information. The code actually was developed by IBM researchers who consulted with the NSA. The DES is the only unclassified code approved by the NSA and it has taken over the encryption market. Barton O'Brien, who is vice president for sales of RSA Data Security, Inc., estimates that 98 or 99 percent of all the companies that sell encryption equipment in the United States sell the DES. And, says Deeley, "DES is sophisticated. DES is damn good." Although researchers outside the NSA have spent the past decade trying to break the DES, none have succeeded.

But the problem with the DES, according to Deeley, is that it is too popular. It is used by the military, by government agencies, by banks, by corporations. "When you have a standard that you've published and that has been around for a long time and that is now used by everybody and his brother, we get concerned that it has become a sufficiently lucrative target that another government might throw a lot of resources at it," says Deeley. Does that mean that the Soviet Union can break the DES? "I wouldn't bet a plugged nickel on the Soviet Union not breaking it," Deeley responds.

In 1988, the DES is scheduled to be reapproved by the NSA for use through 1993. But, says Deeley, "I won't do it." Instead, the agency will provide its new, secret, algorithms.

Deeley acknowledges that the new computer chips will be designed to prevent reverse engineering but is reluctant to say just how that would be done. "There are a variety of techniques and if you wanted to invest time and money, you could protect chips," he remarks. The chips could be coated with a material that could not be removed without destroying the chips themselves. Or the chips could self-destruct if they are tampered with. Or they could be designed as a puzzle so intricate that it is nearly impossible to reconstruct the encryption algorithms from examining the chips. But it certainly would not be to the NSA's advantage to give away its chip-protection secrets. "Let them play with the chips. Let them dissipate their energies trying to get us," says Deeley.

According to Deeley, the NSA will supply a variety of algorithms as part of its new program, but the exact number is secret. "We will use as few algorithms as possible," he notes. "We will try to provide a very few very good ones."

Despite the qualms of the NSA's critics, it looks like the new program is well under way. Fleming is starting to talk to industry groups about it and he expects to have the first devices next year. So far, he says, the idea has met with enthusiasm. "It's exciting, it really is," he remarks. "There is a lot of interest, a lot of companies are calling us. We're on our way."—**GINA KOLATA**

Another Biotech Board Proposal

In August, the heads of several government agencies accepted a proposal to create a new Biotechnology Science Board that would have broad authority over research and development in genetic engineering (*Science*, 23 August, p. 736). Under the terms of that proposal, the biotech board would have been what amounts to a clone of the National Institutes of Health's Recombinant DNA Advisory Committee (RAC), with the likely potential of usurping most of the RAC's responsibilities. It would have been chartered out of the office of the assistant secretary for health in the Department of Health and Human Services.

Opposition from researchers and others to any administrative move that would undermine the RAC has now resulted in a new, alternative proposal for a biotechnology coordinating committee that would be chartered out of the White House Office of Science and Technology Policy. Instead of having the assistant secretary for health as its head, it would be chaired alternately by the directors of NIH and the National Science Foundation, according to Bernadine Healy, outgoing deputy director of OSTP who presented the new proposal to a meeting of the RAC on 23 September.

The proposed board "will be constituted as an interagency coordinating council," Healy wrote in a letter to Senator Albert Gore (D–Tenn.) who had opposed the previous plan, in large part because it would have undercut the RAC's authority over human gene therapy, an issue to which it has already given a good deal of study. According to an aide to Gore, the Senator is not yet prepared to respond to this second proposal but will once he has had a chance to study it.

The biotech board as currently envisioned would be made up exclusively of government agency officials who would not become engaged in the kinds of detailed analyses of issues that are conducted by the RAC and other agency review committees. Nor would the board's meetings or minutes be open to the public, an aspect of the new proposal that has already raised opposition. However, general reaction to the proposal from people at the RAC meeting can be described as cautiously favorable. "It certainly is an improvement over the Biotechnology Science Board idea," said one observer. Details about the new plan will be released shortly for public comment.

—**BARBARA J. CULLITON**