Shunning Cryptocensorship

A panel advising the National Science Foundation (NSF) about support of cryptological research has registered opposition to prior restraints, voluntary or otherwise, on publication of academic research in this field.

The panel's report expands the controversy over relations between NSF and the National Security Agency (NSA) in respect to their roles in cryptological research. NSA is a Defense Department agency responsible for gathering and protecting communications intelligence. NSA officials claim that open dissemination of some academic research in this field could damage U.S. security interests.

The new report, endorsed by NSF's Mathematics and Computer Science Advisory Committee, takes specific exception to a recommendation by a study group established by the American Council on Education (*Science*, 20 February, p. 797). The ACE group advocated that researchers accept a system of voluntary prepublication review of research papers in cryptography for possible security classification. Such a system, the new report states, is "unnecessary, unprecedented, and likely to cause damage to the ability and willingness of American research scientists to stay at the forefront of research in public sector uses of cryptography."

As an alternative, the NSF panel recommends that researchers notify federal agencies of results that might be security-sensitive but leave the initiative in respect to classification to the agencies. John Guttag, Massachusetts Institute of Technology computer science professor and chairman of the NSF advisory panel that drafted the report, said, "What we're recommending is that people send their papers in for information and allow NSA to set things in motion legally if necessary [to classify material]." Furnishing material "for information is different from submitting it for approval," he said.

The report and its recommendations were endorsed, with some modifications, by the advisory committee at a meeting on 29 May, but exact phrasing of some sections, including that on the handling of potentially classifiable research, must still be refined.

Citing a significant "point of disagreement" with NSF, the report objects to possible tightening of NSF requirements for researchers reporting progress on cryptology research funded by the foundation. The panel's report says that "any attempt to change the de facto policy by imposing more rigorous reporting requirements, either in general or on a particular group of researchers, should be considered to be a significant change in policy," and researchers should be fully consulted.

Guttag, whose own research field is not cryptology, said that his panel reacted vigorously against the ACE group's recommendations on prepublication review largely because the ACE group appeared to concentrate on military and diplomatic uses of cryptography and pay little attention to its rapidly growing importance in the public sector. In recommending against prior restraints on publication, the NSF advisory committee expressed the view that such a system does not have a consensus of the scientific community behind it.

The new report also urges NSF to continue to support cryptological research and encourage other agencies besides NSA to support such research.

In a concluding section, the report expresses the committee's view that the controversy over cryptological research is "just the tip of the iceberg" and that similar controversies will soon affect other fields. Most of their recommendations "have as their implicit goal promoting the clean separation of the procedures for funding and otherwise promoting basic research from the procedures for handling national security and other nonscientific considerations."

The report, which reflects attitudes in NSF's academic research constituency, is intended to assist the NSF leadership in amplifying NSF policy on cryptological research. The NSF will have to coordinate that policy with NSA, which is conducting a similar policy-formulating effort, and may have some differing views.—JOHN WALSH

er), one by high-frequency radio, and one by ultrahigh-frequency radio. Later, low-frequency radio was added, and plans are under way to install satellite ground stations. Even with this redundancy, however, there is some doubt by the military about getting the message through. Asked about the EMP threat, one Pentagon official who deals with Minuteman capabilities on a day-to-day basis said: "It may take hours, and we might have to send runners with handwritten messages, but somehow the message will get out." It is commonly assumed that of all the U.S. strategic forces, Minuteman missiles have the most reliable command channels.

Since a nuclear test in space is unlikely, debate between hawks and doves may remain deadlocked.

Hawks think it is possible to add enough hardening and new technology to make the U.S. military invulnerable to EMP, and thus able to fight any kind of conflict. Doves say this is improbable and that the current situation will reign for the foreseeable future. At best, as Steinbruner testified before Congress in 1979 (*6*), "enough protection can probably be provided to plant serious uncertainty in the mind of an attacker contemplating a strategy based on electromagnetic pulse effects. Feasible protection is likely to fall well short, however, of what would be required to have unquestionable assurance that strategic invulnerability had been achieved." Saying essentially the same thing about the deterrent aspects of the communications situation today is Gerald P. Dinneen, the top Pentagon specialist during the Carter Administration on communications issues: "Since there is a great deal of uncertainty about EMP, and most of the information has been derived from simulations, it is unlikely that the Soviets would take a chance."

However, just as there is uncertainty about the degree of destruction that EMP would cause, so too is there uncertainty about the Soviets, who might decide that the risk is worth taking. After all, executing an EMP attack would be simplicity itself. The United States is frequently crossed by picture-taking Cosmos series satellites that orbit at a height of 200 to 450 kilometers above the

0036-8075/81/0612-1250$00.50/0