More secrecy on cryptography research

US academics lean towards self-restraint

Washington

Mathematicians and computer scientists in the United States will soon be asked voluntarily to submit papers on cryptography and related research to the National Security Agency before publication, to see if the agency feels they contain anything that should be kept secret.

This precedent-setting system of self-censorship is being proposed by a study group set up last year by the American Council on Education to look at the growing conflict between national security and academic freedom in cryptography research.

The proposal is something of a compromise between the Defense Department's demands for strict legislation to control the publication of research results with potential security implications, and critics who argue that there should be no restriction on the publication of non-classified research.

However, several scientists warned last week that such voluntary self-regulation could lead eventually to demands for a similar approach to research ranging from lasers to integrated circuits.

Tensions between the Defense Department's security agency and sectors of the research community have grown steadily over the past few years. They stem partly from a desire by the agency to limit the spread of knowledge about virtually unbreakable codes — and the insistence of mathematicians that since many difficult mathematical problems can provide the basis for such codes, any restrictions would have a "chilling" effect on research.

Vice-Admiral Bobby Inman, director of the National Security Agency, has argued fiercely that the free publication of research results could inhibit the agency's data-gathering capabilities. Scientists reply that the codes also have important civilian applications — such as the protection of computer data — that justify their wide dissemination.

Last year these tensions rose to the surface when a computer scientist at Massachusetts Institute of Technology, Dr Leonard Adelman, found a grant application to the National Science Foundation had been passed to the National Security Agency. The agency subsequently offered to support part of his research — but on terms which would have given it the right to determine how much should be published.

The incident caused considerable embarrassment to the National Science Foundation — which protested that it had been seeking the views of the security agency on cryptography research applications for several years. It also pointed out that potential conflicts were being studied by the study group of the American Council on Education, set up at the suggestion of the National Security Agency to discuss ways of controlling the distribution of research results acceptable to the scientific community.

After a year's study, the group agreed at a meeting in Washington last week to propose a system leaving responsibility in the hands of scientists and journal editors by setting up a voluntary review system by the security agency.

According to the group's proposals, soon to be circulated in the scientific community, either a scientist or an editor could submit a paper to the agency for comments on whether it contains information considered to be a threat to national security.

If the agency had no objection, the scientist would be free to publish. If it did object, then the scientist could decide not to publish, proceed with publication against National Security Agency advice — or refer the matter to an independent, five-person committee. This would have two individuals named by the security agency, and three picked by the President's science adviser from a list submitted by the National Academy of Sciences.

In principle, officials of the American Council on Education hope that voluntary self-regulation — which would be introduced for a trial period — would avoid the difficulties of new legislation (which could run into constitutional problems over freedom of expression) while meeting the security agency's main concerns.

In practice, getting the system to work will not be easy. The first step will be for the security agency to prepare a guide to the type of research projects it would expect to evaluate. If the list is too broad, agency officials admit they could end up stifling research unnecessarily; yet if it is too narrow, they fear both that they might tip off others about their principal interests, and miss potentially valuable research findings.

There is also likely to be considerable resistance from the scientific community. Only one of the study group's nine members voted against the proposal for self-censorship; this was Dr George Davida of Georgia Institute of Technology, who found a patent application intercepted by the National Security Agency three years ago, and subsequently received a letter threatening consequences if he discussed his research with his colleagues.

Several academics, however, are worried that self-regulation would create a new category of secret research, pointing out that classified research is now banned on many campuses following the anti-war demonstrations of the 1960s.

The study group's proposals are therefore likely to generate considerable heat. But the political tide is now running in its favour and those who protest at the encroachment of security agencies on individual liberties have fewer friends in Congress than in the past. Vice-Admiral Inman has been nominated as deputy director of the Central Intelligence Agency — and remains committed to the desirability of strong government controls over potentially sensitive research.

David Dickson

Committee douches nuclear energy

The British government's 1979 statement on nuclear power, like its predecessors, is a muddle. This is the opinion of the House of Commons Select Committee on Energy, published this week. The committee asks that decisions to build nuclear plants in the 1980s and 1990s should be decided on their merits and not as part of a planned programme.

On economic grounds, the committee is sceptical about the government's programme to build 15 GW of new nuclear plant by 1992. The Central Electricity Generating Board (CEGB) comes in for particularly sharp criticism. The report cites several instances where the board's evidence on costs was misleading. It criticizes the board for basing future costs on early Magnox plants without acknowledging the effects of subsequent inflation on future capital investment, and for comparing the costs of electricity generated by different types of plant by using "highly uncertain variables" such as the average load factor of plant and future fuel and fuel cycle costs.

Most damning is the complaint that the CEGB presented international cost comparisons suggesting that a pressurized water reactor (PWR) would cost 34 per cent more to build in Britain than elsewhere. The committee says that the generating board's estimate of PWR costs are "too perfunctory" and that it is too tolerant of inefficiencies in the British construction industry. Planning permission for the first PWR plant is still to be sought. Subsequent plants will be either PWR or AGR (advanced gas-cooled reactor) depending on cost and performance.

The committee also suggests that the size of the British programme could be cut if CEGB and the South of Scotland Electricity Board reduced their planning margins for the excess capacity needed for plant failure in particularly severe winters. These have crept up to 28 and 73 per cent respectively from about 17 per cent in the

0028-0836/81/080621-02$01.00