don't have to pad." In marginal cases, however, Relman admits that the art of creative bibliography reading is becoming more complex. "You have to know the journals, and what impact they have on the fields. You have to know the institutions, the people, the meetings. You can quickly sort out the papers that are derivative and not original. With the original, you then have to decide which people are the driving force behind the research and which were the also-rans. It's a ticklish matter."

Since only a few administrators have the time and sophistication to sift through a thick bibliography that at first glance looks promising, problems and misjudgments are probably more common than is ever admitted. A recent example is the case of Elias A. K. Alsabti, a 25-year-old researcher from Jordan who listed 60 papers on his curriculum vitae (*Science*, 27 June 1980). Alsabti had pirated at least seven of his papers and published them in obscure journals. This, however, was unknown to administrators at Baylor College in Houston, where Alsabti was almost accepted into a residency program in neurosurgery—until a researcher who had worked with Alsabti told an administrator at Baylor the details of his academic rise.

Rather than trying to cope with the effects of paper inflation, some researchers have recommended radical steps to prevent the growth of padded bibliographies in the first place. Durack, writing in the 6 April 1978 *New England Journal of Medicine*, says, half-seriously, that the National Institutes of Health should limit the number of papers by each author to five per year, with a stepwise reduction in funding as an automatic penalty for each paper published above five. Other observers, instead of recommending a reliance on bureaucratic sanctions, have called for rigorous self-restraint by researchers.

Since an element of self-deception probably plays a part in the whole process, attempts at restraint may not have much impact. Says one geneticist: "Priority is the rationale that is used for lots of this publishing, for the brief communications. Some people probably believe it. But the cases where somebody is hot on their trail are the exceptions rather than the rule."

Self-restraint is beside the point to some observers. They say there is a good side to paper inflation because it forces administrators and those who judge research careers to dig beneath appearances on a bibliography and discover the truly worthwhile aspects of a research record. But to many others, who are faced with a growing horde of journals filled with fragmented and redundant research, paper inflation represents a time-consuming chore. It may even affect Nobel laureates. At 7:40 one recent morning, *Science* called Watson at Cold Spring Harbor, where he is now the director, and inquired if he would discuss some of the issues involving paper inflation. "I have no time," he said at a brisk clip, and then added, right before he hung up, "My life is too busy." Perhaps he was buried in a stack of journals, struggling to keep up with the literature.—WILLIAM J. BROAD

MIT Committee Seeks Cryptography Policy

Questions of who should do research on cryptography and how results should be disseminated are the first order of business

Within the next 10 years, networks consisting of tens of thousands of computers will connect businesses, corporations, and banks in giant webs, predicts Michael Dertouzos, director of the Laboratory for Computer Science at the Massachusetts Institute of Technology. But the interconnectedness of these computers, which is their very strength, is also their weakness, he says. Unless steps are taken to assure the privacy of computer data and to assure that computer messages can be "signed," it becomes extraordinarily easy to commit crimes and hard to detect them.

Although a number of computer crimes have been reported, many more are not because banks and corporations do not wish to publicize the weaknesses of their systems. And the crimes that are detected, many experts believe, are only the tip of the iceberg. The FBI, aware of this problem, has mounted a major effort to detect computer crimes in the banking industry.

Dertouzos and others at MIT are extremely concerned about the consequences for individuals and for society if computers continue to be connected, as they are now, according to local decisions by individual entrepreneurs. The security of computer data varies greatly and there is no general assurance that data are safe.

Last fall, MIT formed a committee, headed by Dertouzos and called On the Changing Nature of Information, to look into questions of computer security and other matters arising from the proliferation of computer networks. The committee's members include Francis Low and Walter Rosenblith, the current and past provosts of MIT, and John Deutch, the under secretary of energy in the Carter Administration. They also include a computer scientist and lawyer, and professors of political science, philosophy, and management.

As Dertouzos explains, even if a computer is thought of simply as a filing cabinet, the problem of preventing crime is considerable. The very power of the computer can be used to break the defenses of the installation. It is relatively easy to send computer programs between connected machines and to instruct a program to search for, select, and copy data from anywhere in a network. Then the program can be instructed to remove itself without leaving a trace. By analogy, he says, "Consider a network of filing cabinets, connected by subterranean tunnels. Now imagine that agents can crawl through these tunnels, copy anything they want from any of the files, and leave with no signs of their presence. That is one of the situations we are faced with."

Other issues that will arise as computer networks proliferate, the MIT committee predicts, are questions about what types of data should be stored in computers and for how long, how programs can be protected since they can neither be patented nor effectively copyrighted, the extent to which information should be treated as property, and who is liable if a mistake is made, for example in a medical diagnosis that is assisted by a computer. Although the committee intends eventually to address these ques-

0036-8075/81/0313-1139$00.50/0

tions, its first order of business is to recommend MIT policies for conducting research in cryptography—the principal means by which computer data will be protected, if they are protected at all.

For the past few years, MIT computer scientists and mathematicians have been doing research in cryptography. They have been well aware, however, that the National Security Agency (NSA) considers cryptography research to be potentially threatening to the agency's information-gathering and information-protecting mission. It is not clear whether the NSA has any legal means to prevent the publication of research results it considers damaging. One way it may attempt to do so is through the International Traffic in Arms Regulations (ITAR), which restrict the export of sensitive technical data. But these regulations are vague and difficult to interpret. For example, although, according to the ITAR, publications in international journals are considered to be exports, and although the definitions of technical data in the regulations would seem to include descriptions of computer algorithms, it is not certain whether the ITAR restrict the publication of computer algorithms relating to cryptography. The NSA's counsel claims that the ITAR are enforceable, but the Justice Department says they are unconstitutional.

The NSA has so far been pursuing a voluntary approach to clamping down on the open publication of cryptography research. It has encouraged the American Council on Education (ACE), an organization of university administrators, to establish a Public Cryptography Study Group. The group recently recommended that researchers submit papers on cryptography to the NSA for review before publication (*Science*, 20 February 1981, p. 797).

According to Dertouzos, MIT had let the NSA know that it was interested in participating in the cryptography study group, but it was not invited to send a representative to the group's meeting. Dertouzos says that since it was not announced that observers were welcome, it never occurred to him or others at MIT that they could simply show up and participate in the meetings. "That is not the way we are accustomed to doing things," he remarks. Dertouzos believes that his university had something to contribute to the study group because it has worked out its own arrangement to inform the NSA of MIT research on cryptography—an arrangement that does not involve prior restraints on publications.

MIT first became involved with the NSA in 1977 when faculty members Ronald Rivest, Adi Shamir, and Leonard Adleman published a paper describing a new coding scheme. This was the first of a wave of papers on such schemes which, unlike traditional codes, allow for computerized "signatures" of messages. Rivest, Shamir, and Adleman had planned to present their work at a symposium on cryptology at a meeting of the Institute of Electrical and Electronic Engineers (IEEE). They were deterred, however, when an NSA employee, acting on his own, wrote a letter to the IEEE warning that the ITAR might prohibit such a symposium and also might prohibit the distribution of papers on cryptography (*Science*, 30 September 1977, p. 1345). The symposium was held anyway and, on the advice of the MIT lawyers, the MIT group presented its paper. But Rivest said his group still had "some residual uncertainty" about the legality of its presentation.

Dertouzos believes that his university had something to contribute to the study group because it has worked out its own arrangement to inform the NSA of MIT research on cryptography.

Dertouzos, after consulting with MIT lawyers, stopped publication of the Rivest, Shamir, and Adleman paper until the legal situation could be cleared up. Then Dertouzos and Rivest visited the NSA to learn of the agency's concerns. Their discussion led Dertouzos to propose that MIT keep the NSA informed of its research on cryptography by sending the agency prepublication copies of potentially sensitive papers at the same time as the papers are sent to professional colleagues. But, says Dertouzos, "We do *not* say that we will accept a review or decision by the NSA. We send them our papers simply to alert them. We consider our system to be substantially different from the one the ACE cryptography study group recommended." So far the MIT system has worked well. "The NSA has sent back only praise for our work," says Dertouzos.

The legal consequences of publishing results of cryptography research continue to be murky, however. Although MIT decided to resume distributing the 1977 paper by Rivest, Shamir, and Adleman shortly after Dertouzos and Rivest visited the NSA, the university remains concerned about the legal issues in the open publication and distribution of such results. The MIT committee on the changing nature of information has retained lawyers in Boston and in Washington to interpret regulations that may bear on these issues. The committee also is considering various scenarios such as what could happen if an MIT graduate student made a major discovery that not only revealed how to break certain codes but that also had important practical consequences in scheduling theory. What if the student were a foreigner? By this summer, the committee hopes to have developed a set of policies that should clarify how MIT researchers should disseminate the results of their work on cryptography.

The MIT committee members are extremely disturbed by the recommendations of the Public Cryptography Study Group. "There is an aura emerging that the universities have agreed to this sort of review," says Dertouzos. "This university certainly has not. It has neither been consulted nor represented by the ACE."

MIT provost Low also expresses concerns about the public cryptography study group. Prior restraints, even voluntary ones, "pose serious problems for the universities and for society in general," he says. "Many will not do cryptography research and those who do will do so under conditions where they are less productive and their work is less widely disseminated. The prior restraints will impede what we do and will not succeed in keeping secrets," he says.

Asked whether he could conceive of any situation in which cryptographic research by U.S. scientists should not be published, Low first says that he is not an expert in the area but then remarks that this research is international in scope and that many seminal ideas have already been published. He continues, "My impression of cryptography is that the cat is already out of the bag. All you would gain by secrecy is 1 or 2 years of lead time in proliferation. What you would lose is commercial dissemination in a society that is rapidly becoming more computerized."

—GINA BARI KOLATA