The Worm's Aftermath

Computer experts meeting at Fort Meade decide there are no hidden threats to Internet; officials weigh criminal charges against a brilliant hacker

ROBERT T. MORRIS, JR., the apparent source of a "worm" that infected U.S. computer networks in November, is waiting in his parents' home in Arnold, Maryland, for the ax to fall. So far, according to the 23-year-old Cornell grad student, there has been no word from the Federal Bureau of Investigation or from state, local, or college authorities.

Morris up to now has made no comment on his role in the prank that shook the computer world to its foundations (*Science* 11 November, p. 855). "You can talk to [Thomas Guidoboni, a lawyer hired by the Morris family] if you want to," he said when reached by telephone last week. But he implied there is not much to talk about.

Guidoboni, a litigator at the Washington law firm Bonner & O'Connell, says that 70% of his cases involve white-collar crime. "We're still considering whether or not we're going to talk" to the FBI, he says.

The FBI, according to a spokesman in Washington, hopes to have the situation "resolved one way or the other" by the end of the month. Despite the furor, it seems, there may be no prosecution. Officials seem to be waiting for the U.S. Attorney's office to decide whether there is enough evidence to indict under the 1986 federal Computer Fraud and Abuse Act. No one has yet been tried under the law, which was designed chiefly to prevent fraud, although about ten have been prosecuted. The Cornell worm violated both the misdemeanor and felony parts of the law [18 USC 1030 sections a(3) and a(5)], according to a knowledgeable congressional staffer.

Meanwhile, Cornell has begun an inquiry that may lead to action against Morris in a month or two. Its computer science faculty passed a resolution calling the hacker's behavior "deplorable."

FBI agents served two search warrants on Cornell last week, taking away reels of tape and records of Morris's use of a university computer. The school found 200 passwords in Morris's account like those used by the worm. This is circumstantial evidence but perhaps not enough to prove guilt. According to academic computer managers, students accused of wrongdoing often claim that someone else broke into their account and used it. The law is a clumsy tool in such cases; quick administrative action, some universities have found, is more effective.

Immediately after the worm attack, computer wizards and security experts met near Washington, summoned by the National Computer Security Center to discuss what had happened and review whether steps could or should be taken to guard against similar occurrences in the future. The center is part of the secret National Security Agency (NSA) and a sponsor of computer protection research—also the employer of Robert T. Morris, Sr., its chief scientist.

Both father and son are well regarded (or were) by computer programmers. Both graduated from Harvard and both have worked at AT&T Bell Laboratories. The father left the labs in 1986 to work for the government. While at Bell, he helped create the very program (UNIX) that his son attacked over the federal computer links. One of the senior Morris's better known papers, according to Peter Neumann of the Stanford Research Institute, is "UNIX Password Security: A Case History," written with Kenneth Thompson in 1979. It was one of the first to point out the vulnerabilities of UNIX, the kind that were exposed sensationally this fall by Robert Morris, Jr.

It was clear that government and commercial experts were less prepared to deal with the worm invasion than were students.

People at Bell Labs remember the father as exceptionally bright and innovative, and the son as a "nice guy" and a "hard worker." The son was employed at 17, for two summers just following high school graduation, to write codes for internal AT&T use.

On 8 November, computer virus- and worm-fighters gathered at Fort Meade in Maryland, NSA headquarters. Teams from the University of California at Berkeley and the Massachusetts Institute of Technology (MIT) told the meeting the worm held no mystery any longer. Its logic was completely dissected in an extraordinary round-the-clock effort led mainly by students, including an undergraduate at MIT, Mark Eichin. Five days after the attack, they were certain there was no lurking threat, no time bomb hidden in the system. This is one of the greatest security concerns: that a clever programmer could scatter malicious logic through Internet and leave it undetected for months or years.

In this case, the worm was detected within hours because its creator wrote some of its logic backward. He wanted the infection to move subtly, but he miscalculated. Each worm was meant to find a parasitic home and send a signal of success back to a Berkeley computer called "Ernie." Worms were also supposed to detect the presence of their siblings in a computer and avoid infecting a site twice. But here the creator got too bold in his planning. He apparently thought someone might discover the sibling-avoidance signal and use it to fend off the invasion. To overcome this possibility, he instructed each worm that, if rebuffed by a sibling-avoidance signal, it should sit back and roll a 15-sided dice. If the result was positive, which was supposed to happen with a 1-in-15 chance, the worm would attack, no matter what. But, by accident, he reversed the logic and made dice with 14 positive sides. Thus, the chances for reinfection were 14 in 15.

The denouement was classic: the author's ambition apparently led him to reach too far, and a plot that might have been successful had it been more modest came crashing down. The worms infected, reinfected, and multiplied so fast that the whole world learned of them. It remains to be seen how big the failure will be—whether or not the drama will end as a tragedy—for son and father.

The worm fighters at Fort Meade made no earth-shaking recommendations, say attendees at the meeting. But they seemed to agree on several points. One was that the networks themselves were never at risk. Certain computers running a type of UNIX software (Berkeley 4.3) got into trouble. In part, this happened through the carelessness of system managers, some argued. They said that it was irresponsible to use programs with well-known vulnerabilities, and many of UNIX's problems have been known for years.

Second, the academics say, it was clear that government and commercial experts were less prepared to deal with the worm invasion than were students. Sun Microsystems, a company whose workstations were infected by the worm, published a "fix" within 5 days—much longer than Berkeley

and MIT took, but still a record for a private company.

Speakers suggested that the government should set up a central bug-fighting office that could find and remove weaknesses from software and perhaps respond during a crisis. This time, fortunately, the attack was not designed to damage files. Nor did it affect the network, other than to use it as a vector for infection. But next time, the network might not remain intact, and it might be much more difficult to get warnings and repair messages out. In this situation an alternative communication network might be needed. But some doubt the practicality of a central security office, given that the real obstacles exist at the level of the individual user and computer system manager. In the past many have been indifferent to warnings about bugs and reluctant to keep abreast of revisions of the software they use.

There was some concern that the furor might trigger a tightening of access to federal computer networks. Requiring new security passes to get on line, says Jeffrey Schiller of MIT, would be like "posting armed guards at exit ramps on the highway because you're afraid your house will be robbed." It would impede the majority of nonmalicious users and perhaps do little to stop computer vandals. Robert Kahn, one of the founders of ARPAnet, now at the nonprofit Corporation for National Research Initiatives, agrees. The threat, he says, arises not from the openness of the system but from an attitude that tolerates computer hacking.

This thinking has led some computer experts to cry for blood. They argue that the best way to keep the networks open is to punish Morris severely, as an example. This attitude is strong among those who see Harvard's and MIT's computer labs, where Morris spent many hours as an undergraduate, as being full of "hot-rodders." As one critic put it: "This is an example of what I call 'libidinal programming,' " not the work of a serious professional. It reflects a culture of arrogance, he said.

Others look on the case with more tolerance, arguing that it helped focus attention on neglected problems that needed repair. They see little evidence of malicious intent.

Chuck Cole, chief of computer security at the Lawrence Livermore National Laboratory summarized the views expressed at Fort Meade, reflecting what appears to be a consensus: "The strong preponderance of opinion was that there should be punishment. A small fraction said it was a valuable experience." Most agreed, he added, that it would be wrong to "send this guy off to prison. Maybe there should be a fine and a requirement that he do some community service." ■ ELIOT MARSHALL

Soviet-Based Global Foundation Takes Shape

Sakharov is a key player in a group that aims to fund a broad range of peace and environment projects

THE RECENT FORMATION of a private international foundation, the portentously named International Foundation for the Survival and Development of Humanity (IF), marks the first time an entity of its kind has been established in the Soviet Union.

The foundation is headed by Evgeny Velikhov, vice president of the Soviet Academy of Sciences. Jerome D. Wiesner, president emeritus of the Massachusetts Institute of Technology (MIT), is vice president. Plans are to pursue a grand agenda related to "urgent problems of international security, development and environment." The foundation hopes ultimately to raise up to $10 million a year from private sources.

The latest meeting of the executive committee was held in Washington in November during the visit of Andrei Sakharov. Sources say that permission for Sakharov to leave the Soviet Union was a direct consequence of his membership on the board. Approval of the foundation's charter by the Council of Ministers was held up by conflicts over allowing Sakharov to travel, which reportedly were resolved when hardliner Boris Ligachev was "kicked upstairs" to be in charge of agriculture policy. "We refused to come without him [Sakharov]," Velikhov told the *New York Times*. The Council of Ministers approved the foundation in October, guaranteeing it freedom to raise money and pursue its activities in the Soviet Union, and according diplomatic travel and communications privileges to its official representatives.

The idea for the foundation was proposed in February 1987 by Velikhov and Wiesner during an International Forum for a Nuclear-Free World held in Moscow. The group was founded last January.

The IF board is a weighty international roster with representatives from 18 countries. The eight U.S. board members include industrialist Armand Hammer, who has pledged $1 million to the foundation; Apple Computer president John Sculley, who has donated computer equipment; Theodore Hesburgh, president emeritus of Notre Dame University; and former defense secretary Robert S. McNamara. There are six Soviet members including Roald Sagdeev, former director of the Soviet Space Research Institute. The first annual meeting of the board is scheduled to be held in Moscow in January 1989.

The organization has already purchased its own building in Moscow and is run by Rolf Bjoernerstedt from Sweden, a former United Nations assistant secretary general. There will also be an office in Stockholm and one in Washington, headed by William Miller, president of the American Committee on U.S.–Soviet Relations.

The foundation has established committees reflecting its primary areas of interest—on security (headed by board member Frank von Hippel of MIT), human rights (headed by Sakharov), education, development, the environment, and medicine and biology. More than 40 project proposals meeting the foundation's criteria for relevance have been received. These include projects on energy efficiency, the conversion of military resources to civilian uses, verification technologies, Baltic Sea protection, drug and alcohol problems, children's computer camps, African development, and a "socio-psychological survey to investigate mutual stereotypes and prejudices of Soviets and West Germans."

Fund raising is now the immediate priority. As of September, the United States's accounts had $300,000, including donations from the Ploughshares Fund in San Francisco and Rockefeller Family and Associates. The MacArthur Foundation in October donated $150,000 for general expenses. The Carnegie Corporation, whose president David Hamburg is an adviser to IF, has been making in-kind donations and will be participating in specific projects. Carnegie, according to Fritz Mosher, believes it is more appropriate for the IF to get its funding from individuals than from big foundations.

Contributions in the Soviet Union include money from the Soviet Peace Fund. Various other fund-raising approaches are planned such as lotteries and the sale of a record album. Since the foundation is a first in that country, there is said to be a large yet-untapped potential for private donations. ■ CONSTANCE HOLDEN