December 1989

FBI Law Enforcement Bulletin

Aerial Surveillance

FBI
Law Enforcement Bulletin

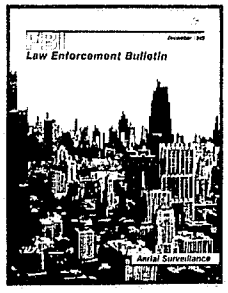
December 1989
Volume 58
Number 12

Page 5

Page 25

Features

Departments



The Cover: The use of aerial surveillance to obtain evidence and recent Supreme Court decisions are addressed in the Legal Digest. See article p. 18.

United States Department of Justice
Federal Bureau of Investigation
Washington, DC 20535

William S. Sessions, Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget.

Published by the Office of Public Affairs, Milt Ahlerich, *Assistant Director*

Editor—Stephen D. Gladis
Managing Editor—Kathryn E. Sulewski
Art Director—John E. Ott
Assistant Editor—Alice S. Cole
Production Manager—Andrew DiRosa

The FBI Law Enforcement Bulletin (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Ave., N.W., Washington, DC 20535. Second-Class postage paid at Washington, DC. Postmaster: Send address changes to Federal Bureau of Investigation, FBI Law Enforcement Bulletin, Washington, DC 20535.

ISSN 0014-5688 **USPS 383-310**

122008

Thefts of Computer Software

By
WILLIAM J. COOK
Assistant U.S. Attorney
Chicago, IL

Between July and September 1987, a Chicago youth attacked AT&T computers at Bell Labs in Illinois and New Jersey, at a NATO missile support site in North Carolina, and at Robbins Air Force Base in Georgia, stealing software worth $1.2 million and causing $174,000 worth of damage.[1]

In October 1988, Scotland Yard arrested an English hacker who had broken into over 200 military, corporate, and university computers in the United States and Europe. The indication was that he planned to extort money from one of the victim corporations.[2]

In November 1988, a college undergraduate planted a computer virus that temporarily disabled 6,000 computers on the U.S. Army research computer network (ARPANET).[3]

As evident by these accounts of computer piracy, computer-aided attacks on Government and corporate networks are becoming more numerous and sophisticated. While estimates vary, computer industry sources indicate that computer-related crime (including software theft) annually costs U.S. companies as much as $555 million per year, with each incident costing approximately $450,000.[4] More importantly, however, the infiltration and theft of computer files is a growing Federal crime problem, since many such actions jeopardize the security and defense of the United States.

This article gives a brief overview of the thefts and illegal export of computer software. It also details steps taken by the U.S. Government to protect national security and defense information with the intent of curtailing and hopefully eliminating the occurrence of such actions in the future.

International Computer Hackers

While most computer attacks are done by hackers who are not agents of a foreign government, the growing attention of Eastern Bloc governments to hackers indicates that these nations clearly recognize the benefits of using them to expose openings in U.S. computer networks.

In March 1989, it was disclosed that West German hackers sponsored by Eastern Bloc intelligence agencies had been systematically searching for classified information on Government computers throughout the United States through a weakness in a computer network at a California university.[5] The following month, Canada expelled 19 Soviet diplomats for wide-ranging espionage operations to obtain Canadian defense contractor information for military and commercial purposes.[6] And in December 1988, a search warrant filed by U.S. Customs agents in Chicago disclosed that a confederate of the Yugoslav Consul-General in Chicago was using a hacker to attack defense contractors by remote access in order to steal computerized information. According to the affidavit, the information obtained by the hacker was subsequently smuggled out of the United States in diplomatic pouches with the help of the Counsel-General.

Public access information and published reports reflect that Soviet efforts to obtain technical information are not an illusion. A

major daily newspaper reported that the Soviet Union was actively fostering hacker-to-hacker ties between the Soviet international computer club and computer firms and hackers in the United States, Britain, and France.[7] Another newspaper account told of the Soviet Union setting up programmers in Hungary and India for the purpose of translating and converting U.S. origin software to the format of Soviet and Warsaw Pact country machines.[8] Then in March 1989, a member of the Soviet military mission in Washington, DC, was arrested and expelled from the United States for attempting to obtain technical information about how U.S. Government classified information is secured in computers.[9]

The Soviet's main targets are U.S. Government agencies, defense contractors, and high-tech companies and are purportedly backed by a $1.5 billion annual "procurement" budget. Further, Soviet satellite countries have become very active in the Soviet high technology procurement effort. For the past several years, Hungarian, Bulgarian, Yugoslavian, and Polish intelligence officers and their agents have participated in the high-tech theft effort, along with agents from Vietnam, North Korea, and India.[10] Also, Cuban and Nicaraguan intelligence officers are using front companies in Panama to obtain U.S. technology.[11]

News accounts suggest that these efforts are successful; 60-70% of the technology is obtained, while 90% of non-classified high technology data is acquired. More than 60% of the stolen technology comes from the United States.[12]

As a result, the U.S. technological "lead" over the Soviets has gone from 10-12 years in 1975 to 4-6 years in 1985.[13] And the savings to the Soviets have been impressive. It has been estimated that in 1978 the Soviet Union saved $22 million in research and development costs by stealing U.S. technology; the following year, they saved $50 million.[14] Between 1976 and 1980, the Soviet aviation industry alone saved $256 million in research and development because of stolen U.S. technology.[15] More significantly, much of the stolen technology is critical to the national security and defense of the United States.

Protecting Technical Data

In 1984, the U.S. Department of Commerce placed expanded export controls on computer software as part of its general protection of technical data deemed vital to the national defense and security of the United States. However, export control in this realm is an enormous challenge since modern technology allows the criminal to steal restricted software stored on Government and corporate computers by remote access from a personal computer anywhere in the world. Literally, international border are destroyed when a telephone line plugs into the computer modem.

Observations

Several observations can be reached from this mosaic. Obviously, U.S. taxpayers are subsidizing the modernization of the Soviet military establishment. And it is more economical for the Soviets to steal U.S. technology than to fund and develop their own research and development capabilities. More importantly, however, the United States needs to do a better job protecting its technology.

As noted previously, in response to the Soviet "tech-threat," the United States and other countries expanded controls on high technology computer software by placing them on the Commodity Control List or Munitions List. Commerce Department and State Department licensing officers require that validated export licenses and end-user assurances are obtained before software named on these lists is exported. Both the Commerce and State Departments routinely call in Defense Department personnel to analyze these export requests.

> ***"Federal agents and computer security professionals must recognize the need for rapid mutual cooperation and communication...."***

Prosecution for illegally exporting computer data and software can be brought under several sections of the U.S. Code.[16] However, before prosecution under these sections can be successful, several areas must be developed in the computer industry and the law enforcement community.

- Corporations should consider placing export control warnings on sensitive software programs, which would clearly assist U.S. efforts to enforce national export laws that require defendants have specific knowledge of export restrictions when exporting computer data.

may be the only evidence of "tech-theft."

- Federal agents and computer security professionals must recognize the need for rapid mutual cooperation and communication, with security professionals providing background information on the attacked computer network and assisting Federal investigations and search warrant efforts.

> ***"... Eastern Bloc governments ... clearly recognize the benefits of using [hackers] to expose openings in U.S. computer networks."***

- Federal agents need to become oriented to the computer industry and computers to overcome computerphobia.
- Corporate and Government hirings must be done with great care when the employees will have access to computer networks or trash from computer centers.
- Computer security specialists and systems administrators must be alert to internal unauthorized access and external hacker attacks and the potential ramifications of such activities. They must also be aware that the modem plug-in on one of their computers could be the international border in the export violation and that computerized log records

Conclusion

It is folly to assume that U.S. industry can continue to make sufficient research and development advances each year to ensure that the United States keeps an edge on Warsaw Pact countries. These countries continue to rob the United States of advanced technological information critical to defense and security of this country. The taxpayers and consumers writing the checks for Government and private sector technological research and development deserve a coordinated Federal law enforcement and computer industry response that recognizes software and computer-related engineering as one of our country's greatest resources. FBI

Footnote

[1]*ComputerWorld*, February 20, 1989.
[2]*Sunday Telegraph*, October 23, 1988.
[3]*The Boston Globe*, November 14, 1988.
[4]*ComputerWorld*, April 3, 1989.
[5]Hamburg Ard Television Network, March 2, 1989; see also, Cliff Stoll, "Stalking the Wiley Hacker," *Communications of the ACM*, May 1988.
[6]*Reuters*, June 28, 1988.
[7]*The Washington Post*, January 2, 1989.
[8]*The New York Times*, January 29, 1988.
[9]*Reuters*, March 9, 1989.
[10]"Soviet Acquisition of Militarily Significant Western Technology: An Update," published by the Central Intelligence Agency, 1985.
[11]*The Los Angeles Times*, November 21, 1988.
[12]Supra note 10.
[13]Ibid.
[14]Ibid.
[15]Ibid.
[16]18 U.S.C. sec. 1029 (fraudulent activity in connection with using accessing devices in interstate commerce); 18 U.S.C. sec. 1030 (remote access with intent to defraud in connection with Federal interest computers and/or Government-owned computers); 18 U.S.C. sec. 1343 (use of interstate communications systems to further a scheme to defraud); 18 U.S.C. sec. 2512 (making, distributing, possessing, and advertising communication interception devices and equipment); 18 U.S.C. sec. 2314 (interstate transportation of stolen property valued at over $5,000); 17 U.S.C. sec. 506 (copyright infringement violations); 22 U.S.C. sec. 2778 (illegal export of Department of Defense controlled software); 18 U.S.C. sec. 793 (espionage, including obtaining and/or copying information concerning telegraph, wireless, or signal station, building, office, research laboratory or stations for a foreign government or to injure the United States); 18 U.S.C. sec. 2701 (unlawful access to electronically stored information); 18 U.S.C. sec. 1362 (malicious mischief involving the willful interference with military communications systems); 18 U.S.C. sec. 1962 (RICO—20 years/$25,000/forfeiture of property for committing two violations of wire fraud and/or transportation of stolen property).