928 F.2d 504
United States Court of Appeals,
Second Circuit.

UNITED STATES of America, Appellee,
v.
Robert Tappan MORRIS, Defendant–Appellant.

No. 774, Docket 90–1336. | Argued Dec. 4, 1990. | Decided March 7, 1991.

* * *

Opinion

JON O. NEWMAN, Circuit Judge:

This appeal presents two narrow issues of statutory construction concerning a provision Congress recently adopted to strengthen protection against computer crimes. [The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(C)], punishes anyone who intentionally accesses without authorization a category of computers . . . . The issues raised are . . . (2) what satisfies the statutory requirement of "access without authorization."

These questions are raised on an appeal by Robert Tappan Morris from the May 16, 1990, judgment of the District Court for the Northern District of New York (Howard G. Munson, Judge) convicting him, after a jury trial, of violating [18 U.S.C. § 1030(a)(5)(C)]. Morris released into INTERNET, a national computer network, a computer program known as a "worm"[1] that spread and multiplied, eventually causing computers at various educational institutions and military sites to "crash" or cease functioning.

. . . We also find that there was sufficient evidence for the jury to conclude that Morris acted "without authorization" within the meaning of [section 1030(a)(5)(C)]. We therefore affirm.

FACTS

In the fall of 1988, Morris was a first-year graduate student in Cornell University's computer science Ph.D. program. . . .

In October 1988, Morris began work on a computer program, later known as the INTERNET "worm" or "virus." The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered. The tactic he selected was release of a worm into network computers. Morris designed the program to spread across a national network

of computers after being inserted at one computer location connected to the network. Morris released the worm into INTERNET, which is a group of national networks that connect university, governmental, and military computers around the country. The network permits communication and transfer of information between computers on the network.

Morris sought to program the INTERNET worm to spread widely without drawing attention to itself. The worm was supposed to occupy little computer operation time, and thus not interfere with normal use of the computers. Morris programmed the worm to make it difficult to detect and read, so that other programmers would not be able to "kill" the worm easily.

***506** Morris also wanted to ensure that the worm did not copy itself onto a computer that already had a copy. Multiple copies of the worm on a computer would make the worm easier to detect and would bog down the system and ultimately cause the computer to crash. Therefore, Morris designed the worm to "ask" each computer whether it already had a copy of the worm. If it responded "no," then the worm would copy onto the computer; if it responded "yes," the worm would not duplicate. However, Morris was concerned that other programmers could kill the worm by programming their own computers to falsely respond "yes" to the question. To circumvent this protection, Morris programmed the worm to duplicate itself every seventh time it received a "yes" response. As it turned out, Morris underestimated the number of times a computer would be asked the question, and his one-out-of-seven ratio resulted in far more copying than he had anticipated. . . .

Morris identified four ways in which the worm could break into computers on the network[, including vulnerabilities in mail and user directory software, as well as password guessing.]

On November 2, 1988, Morris released the worm from a computer at the Massachusetts Institute of Technology. MIT was selected to disguise the fact that the worm came from Morris at Cornell. Morris soon discovered that the worm was replicating and reinfecting machines at a much faster rate than he had anticipated. Ultimately, many machines at locations around the country either crashed or became "catatonic." When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However, because the network route was clogged, this message did not get through until it was too late. Computers were affected at numerous installations, including leading universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000.

Morris was found guilty, following a jury trial, of violating [18 U.S.C. § 1030(a)(5)(C)].

He was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.

DISCUSSION

* * *

II. The unauthorized access requirement in [section 1030(a)(5)(C)]

[Section 1030(a)(5)(C)] penalizes the conduct of an individual who "intentionally accesses a [protected] computer without authorization." Morris contends that his conduct constituted, at most, "exceeding authorized access" rather than the "unauthorized access" that the subsection punishes. Morris argues that there was insufficient evidence to convict him of "unauthorized access," and that even if the evidence sufficed, he was entitled to have the jury instructed on his "theory of defense."

We assess the sufficiency of the evidence under the traditional standard. Morris was authorized to use computers at Cornell, Harvard, and Berkeley, all of which were on INTERNET. As a result, Morris was authorized to communicate with other computers on the network to send electronic mail. . . , and to find out certain information about the users of other computers ***510**. The question is whether Morris's transmission of his worm constituted exceeding authorized access or accessing without authorization.

* * *

The evidence permitted the jury to conclude that Morris's use of the [mail and directory] features constituted access without authorization. While a case might arise where the use of [mail or directory software] falls within a nebulous area in which the line between accessing without authorization and exceeding authorized access may not be clear, Morris's conduct here falls well within the area of unauthorized access. Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers.

* * *

CONCLUSION

For the foregoing reasons, the judgment of the District Court is affirmed.

Footnotes

[1] In the colorful argot of computers, a "worm" is a program that travels from one computer to another but does not attach itself to the operating system of the computer it "infects." It differs from a "virus," which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer.