Government decodes Kaczynski's diary

John Howard

1997/12/27

SACRAMENTO, Calif. — Driven by secrecy, Theodore Kaczynski kept a cryptic diary for two decades, substituting numbers and mathematical symbols for words and letters.

Prosecutors say the Unabomber suspect's encoded journal is the cornerstone of their case against the mathematics professor-turned-forest recluse. They say it provides a remarkable, step-by-step view of years of wrongdoing — in the defendant's own words. And they intend to have FBI cryptographer Michael Birch lay out his "translation" of the entire document to jurors.

"Although Mr. Birch's expertise is breaking codes, in this case the 'key' to the defendant's code was found in the cabin," the government said in its trial strategy brief. "Therefore, Mr. Birch's expertise will be directed to explaining to the jury how to apply the code to the defendant's coded writings and the admission into evidence of his completed translation."

Earlier, lead prosecutor Robert Cleary said the journal records are "the backbone of the government's case." He said the diary describes in detail the 16 Unabomber attacks from 1978 to 1995 that killed three people and injured 29.

Kaczynski, 55, is charged with using bombs in four attacks He is accused of killing a lobbyist and a computer store owner a decade apart in Sacramento, and maiming a geneticist and a computer professor with Sacramento-postmarked mail bombs in 1993.

Opening statements in the trial are scheduled for Jan. 5. Kaczynski could get the death penalty if convicted. He is charged separately in New Jersey with the third fatality attributed to the Unabomber's 18-year siege.

Unlike the Unabomber manifesto, a 35,000-word treatise that depicts technology as an evil force, the coded diary was never intended to be seen by anyone else.

The diary, written in pencil on several hundred pages of notepaper and several inches thick, includes details of experiments with explosives. It was among 20,000 documents seized from Kaczynski's tiny Montana shack.

The diary contents have not been made public, although Birch's decoded version was given to the defense last year.

Sources familiar with the journal describe it as a sophisticated jumble of numbers, an intricate enigma wrapped in a riddle befitting a Harvard-trained mathematician described by one prospective juror as a "smart weirdo."

But code experts aren't so sure. They believe Kaczynski, who shunned computers and electronic devices in his cabin without electricity, may actually have cloaked the journal in a "hand code" that would have been relatively easy to break, even without the key.

Such codes vary widely, but one basic variety resembles a checkerboard or grid, numbered on the sides, with each square filled randomly with a letter of the alphabet.

The coded message is a string of numbers, which are the coordinates corresponding to the letters in the grid. To read the message, one needs to translate the numbers using the grid, or key. But typically, those numbers may be scrambled using a second code, and even a third, so that the final message is shrouded in layers of secrecy.

Although such a numeric code looks daunting to the lay person, it is no more difficult to crack than the kind of basic substitution ciphers popular in pulp fiction or newspaper word games.

"You may have 'A equals 1', and 'B equals 2,' stuff like that in a numeric code with pencil and paper. Numbers look a little more mysterious and harder, like '39647181.' But it doesn't have anything to do with the complexity of the code. It's totally irrelevant," said David Kahn, an editor at Long Island's Newsday and the author of "The Code Breakers," a seminal work on classical cryptography.

"A checkerboard cipher with nothing else going on is no harder to crack than the simple substitution system used in a newspaper," added James Gillogly, president of the American Cryptogram Association. He is an employee of the Westwood-based Mentat Inc., which develops security software.

Ronald L. Rivest, a professor at the Massachusetts Institute of Technology and a founder of MIT's Cryptography and Information Security Group, agreed.

"When you are dealing in a situation where someone is working by hand with a code, and dealing with pencil and paper, it's not that difficult" to decode, he said.

John Howard
Government decodes Kaczynski's diary
1997/12/27

<www.southcoasttoday.com>