Does an extremist's iPhone contain a "cyber pathogen"?

March 5 2016, by Brandon Bailey

This Feb. 23, 2016, file photo shows a New York police officer stands outside the Apple Store on Fifth Avenue while monitoring a demonstration, in New York. San Bernadino District Attorney Michael Ramos suggests in a court filing

that one of the San Bernardino shooters might have used his iPhone, the same one at the heart of Apple's battle with the FBI, to introduce a "lying-dormant cyber pathogen" into the county's computer network. (AP Photo/Julie Jacobson, File)

A local prosecutor has offered an unusual justification for forcing Apple to help hack an iPhone used by a San Bernardino mass killer: The phone might have been "used as a weapon" to introduce malicious software to county computer systems.

San Bernardino County District Attorney Michael Ramos acknowledged to The Associated Press that there's no evidence of malicious software in the county's computer network. But he added, "I wouldn't call it a total hypothetical."

Computer security experts say the prospect is unlikely. By late Friday, the prosecutor's claim had sparked a wave of social media postings, many of which mocked the DA's use of the non-technical term "cyber pathogen" to describe the supposed malware.

Apple has resisted calls to help unlock the phone, arguing that building a software tool to override the phone's security features would render other iPhones vulnerable to criminals and government authorities around the world. Investigators, meanwhile, are eager to see if the phone used by shooter Syed Farook—one issued by Farook's employer, the county health department —contains any useful information about other suspects.

But the idea that Farook might have used the phone to transmit a "lying-dormant cyber pathogen" into county data systems is a new one. Ramos' office, however, cited it in a court filing Thursday among several other

reasons to support the government's position.

"This was a county employee that murdered 14 people and injured 22," Ramos said. "Did he use the county's infrastructure? Did he hack into that infrastructure? I don't know. In order for me to really put that issue to rest, there is one piece of evidence that would absolutely let us know that, and that would be the iPhone."

The argument drew condemnation from one software expert who has signed a brief in support of Apple's position.

"Ramos's statements are not only misleading to the court, but amount to blatant fear mongering," independent software researcher Jonathan Zdziarski wrote in a post on his personal blog .

Other security experts who haven't taken sides also discounted the scenario. "It's definitely possible, technically, but it doesn't seem to me at first glance to be likely," said David Meltzer, a computer security expert and chief research officer at Tripwire, a commercial IT security firm. He said Apple's iPhone operating system is a relatively closed environment that's designed so users can't easily introduce their own programs.

Ramos, meanwhile, said he'd heard about social media posts that mocked the term "cyber pathogen," which is not generally used by tech experts. "When they do that," he said, "they're mocking the victims of this crime, of this horrible terrorist attack."