

Senior Defense official hedges on US involvement in Stuxnet

By [Kim Zetter, wired.com](#) | Published 2 days ago

If you want to see a top Pentagon official squirm, tune into CNBC's cyberwar documentary Thursday night, and watch Deputy Defense Secretary William Lynn face an uncomfortably direct question about the Stuxnet worm.

In *CodeWars: America's Cyber Threat*, correspondent Melissa Lee asks Lynn outright: "Was the US involved in any way in the development of Stuxnet?"

Lynn's response is long enough that an inattentive viewer might not notice that it doesn't answer the question.

"The challenges of Stuxnet, as I said, what it shows you is the difficulty of any, any attribution and it's something that we're still looking at, it's hard to get into any kind of comment on that until we've finished our examination," Lynn replies.

"But sir, I'm not asking you if you think another country was involved," Lee presses. "I'm asking you if the US was involved. If the Department of Defense was involved."

"And this is not something that we're going to be able to answer at this point," Lynn finally says.

The sophisticated Stuxnet worm was released on systems in Iran in June 2009 and again in March and April 2010, and was designed to specifically target programmable logic controllers used in industrial control systems made by Siemens. The worm was programmed to launch its attack only on Siemens systems that had a specific configuration—a configuration believed to exist at Iran's Natanz plant, where weapons-grade uranium is being enriched.

The New York Times reported earlier this year that the United States and Israel had worked in conjunction to create Stuxnet. When Gary Samore, President Obama's chief strategist for combating weapons of mass destruction was asked previously about Stuxnet at a conference, he avoided the question and remarked with a smile: "I'm glad to hear they are having troubles with their centrifuge machines, and the US and its allies are doing everything we can to make it more complicated."

According to the *Times*, in January 2009, former President George Bush authorized a covert program to undermine the electrical and computer systems around Natanz. President Obama was then briefed on the program before he took office and wanted to speed up the plan. Stuxnet is believed to have been part of that plan.

Unfortunately, CNBC doesn't dig any further into questions about the United States' role in Stuxnet. Nor does it explore the implications of what it would mean if the United States was indeed involved in creating and unleashing a powerful piece of malware that could be tweaked and used to attack critical infrastructure systems in the United States and allied countries.

The documentary, which Threat Level viewed prior to broadcast, also makes a number of unsubstantiated claims: that the configuration Stuxnet sought, for example, existed only at Natanz, and that Stuxnet succeeded in significantly sabotaging Natanz's centrifuges. Though centrifuges at Natanz experienced problems, the circumstantial evidence pointing to Stuxnet as the cause is currently incomplete and contradictory. Nonetheless, the piece does a good job of pulling a lot of information together to give an overview of Stuxnet.

The program is not just about Stuxnet, however. It also looks at cybercrime, vulnerabilities in critical infrastructure systems, the broader issue of cyberwarfare, and the wide use in the United States of computer parts made in China that may contain built-in spyware. The documentary covers all these issues well, but makes the oft-repeated mistake of focusing too much attention on the headline-making, low-tech denial-of-service attacks against Estonian websites in 2007, calling them an example of "enemy fire."

Next to Stuxnet, and the United States' possible involvement in it, the Estonian attacks—part of a dispute over the placement of a statue—were child's play.

Photo of William Lynn courtesy CNBC

WIRED