The Washington Post

National Security

Stuxnet was work of U.S. and Israeli experts, officials say

By Ellen Nakashima and Joby Warrick June 2, 2012

A damaging cyberattack against Iran's nuclear program was the work of U.S. and Israeli experts and proceeded under the secret orders of President Obama, who was eager to slow that nation's apparent progress toward building an atomic bomb without launching a traditional military attack, say current and former U.S. officials.

The origins of the cyberweapon, which outside analysts dubbed Stuxnet after it was inadvertently discovered in 2010, have long been debated, with most experts concluding that the United States and Israel probably collaborated on the effort. The current and former U.S. officials confirmed that long-standing suspicion Friday, after a New York Times report on the program.

The officials, speaking on the condition of anonymity to describe the classified effort code-named Olympic Games, said it was first developed during the George W. Bush administration and was geared toward damaging Iran's nuclear capability gradually while sowing confusion among Iranian scientists about the cause of mishaps at a nuclear plant.

The use of the cyberweapon — malware designed to infiltrate and damage systems run by computers — was supposed to make the Iranians think that their engineers were incapable of running an enrichment facility.

"The idea was to string it out as long as possible," said one participant in the operation. "If you had wholesale destruction right away, then they generally can figure out what happened, and it doesn't look like incompetence."

Even after software security companies discovered Stuxnet loose on the Internet in 2010, causing concern among U.S. officials, Obama secretly ordered the operation continued and authorized the use of several variations of the computer virus.

Overall, the attack destroyed nearly 1,000 of Iran's 6,000 centrifuges — fast-spinning machines that enrich uranium, an essential step toward building an atomic bomb. The National Security Agency developed the

cyberweapon with help of Israel.

Several senior Iranian officials on Friday referred obliquely to the cyberattack in reaffirming Iran's intention to expand its nuclear program.

"Despite all plots and mischievous behavior of the Western countries . . . Iran did not withdrawal one iota from its rights," Kazem Seddiqi, a senior Iranian cleric, said during services at a Tehran University mosque, according to news reports from Iran.

Iran previously has blamed U.S. and Israeli officials and has said its nuclear program is solely for peaceful purposes, such as generating electricity.

White House officials declined to comment on the new details about Stuxnet, and an administration spokesman denied that the material had been leaked for political advantage.

"It's our view, as it is the view of everybody who handles classified information, that information is classified for a reason: that it is kept secret," deputy press secretary Josh Earnest told reporters. "It is intended not to be publicized because publicizing it would pose a threat to our national security."

The revelations come at a particularly sensitive time, as the United States and five other world powers are engaged in talks with Iran on proposed cuts to its nuclear program. Iran has refused to agree to concessions on what it says is its rightful pursuit of peaceful nuclear energy. The next round of negotiations is scheduled for this month in Moscow.

"Effectively the United States has gone to war with Iran and has chosen to do so in this manner because the effects can justify this means," said Rafal Rohozinski, a cyber-expert and principal of the SecDev Group, referring to the slowing of Iran's nuclear program.

"This officially signals the beginning of the cyber arms race in practice and not in theory," Rohozinski said.

In 2006, senior Bush administration officials developed the idea of using a computer worm, with Israeli assistance, to damage Iranian centrifuges at its uranium enrichment plant in Natanz. The concept originated with Gen. James E. Cartwright, who was then head of U.S. Strategic Command, which handles nuclear deterrence, and had a reputation as a cyber-strategist.

"Cartwright's role was describing the art of the possible, having a view or vision," said a former senior official familiar with the program. But "the heavy lifting" was done by NSA Director Keith Alexander, who had "the technical know-how and carried out the actual activity," said the former official.

Olympic Games became a collaborative effort among NSA, the CIA and Israel, current and former officials said. The CIA, under then-Director Michael V. Hayden, lent its covert operation authority to the program.

The CIA and Israelis oversaw the development of plans to gain physical access to the plant. Installing the worm in plant equipment not connected to the Internet depended on spies and unwitting accomplices — engineers, plant technicians — who might connect an infected device to one of the systems, officials said.

The cyberweapon took months of testing and development. It began to show effects in 2008, when centrifuges began spinning at faster-than-normal speeds until sensitive components began to warp and break, participants said.

U.S. officials were concerned when security companies began reporting on the existence of the worm in June 2010.

"It took us a little while to figure out" that the virus had spread, although it was not damaging machines other than those at Natanz, an official said.

Iran replaced the damaged machines and has continued to enrich uranium. Officials said the country's leadership has always assumed that any action destabilizing its government or nuclear program is the work of the United States, Israel or Britain, or some combination, officials said.

"This will certainly play into their fears about what else is out there," said one former intelligence official. "It certainly won't make them eager to get back to the negotiating table."

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties. Follow @nakashimae

Joby Warrick joined the Post's national staff in 1996. He has covered national security, the environment, and the Middle East, and currently writes about terrorism. Follow @jobywarrick