Obama oversees cyber warfare against Iran

Peter Symonds
4 June 2012

A lengthy article in the *New York Times* on June 1 providing details of US/Israeli cyber attacks on Iran has underlined the criminal character of the Obama administration's actions in the Middle East and internationally.

The article confirmed that the US in collaboration with Israel had been responsible for the Stuxnet worm that infected gas centrifuges at Iran's enrichment plant at Natanz. The worm affected the industrial controllers governing the delicate high-speed centrifuges, causing them to spin out of control and self-destruct.

The cyber warfare project, code-named Olympic Games, was begun under the Bush administration, but had failed to achieve significant results by the time Bush left office. "Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. Mr. Obama took Mr. Bush's advice," the *Times* reported.

As another *Times* article detailed last week, President Obama was directly involved in the expanded program of drone assassinations, personally signing off on the strikes on "suspected militants" in Pakistan, Yemen and Somalia. (See: "Obama's role in the selection of drone missile targets")

Obama also personally oversaw the cyber attacks on Iran. "The architects of Olympic Games would meet him in the Situation Room, often with what they called the 'horse blanket', a giant foldout schematic diagram of Iran's nuclear production facilities. Mr. Obama authorised the attacks to continue, and every few weeks—certainly after a major attack—he would get updates and authorise the next step," the article stated.

The cyber attacks were acts of sabotage that destroyed centrifuges and forced Iranian technicians to shut down many more as they tried to work out what was happening. In one of the final attacks before Stuxnet was detected in mid-2010, nearly 1,000 of the 5,000 centrifuges at the Natanz plant were temporarily out of action. According to one US estimate, the project set Iran's enrichment program back by 18 months to two years.

Former CIA chief Michael Hayden told the *Times*: "Previous cyber attacks had effects limited to other computers. This is the first attack of a major nature in which a cyber attack was used to effect physical destruction," rather than just slow down another computer, or steal information from it. "Somebody crossed the Rubicon," he said.

Like its article detailing Obama's involvement in the drone assassinations, the latest *Times* story appears to have been authorised by the White House in order to bolster Obama's militarist credentials in the lead up the November presidential election. The sources included current and former US, European and Israeli officials who were part of the highly classified program.

By their very nature, the cyber attacks were highly provocative and threatened to trigger Iranian retaliation. The publication of the story confirming US and Israeli responsibility will only further inflame tensions in the Persian Gulf prior to negotiations in Moscow on June 18-19 between Iran and the P5+1—the US, Britain, France, China, Russia and Germany.

Iranian officials acknowledged announced last Tuesday that thousands of government and private firms had been infected by a new, sophisticated

computer virus, dubbed Flame, which had been identified by a Russian computer security firm. Unlike the Stuxnet worm, Flame was designed to transform a computer into a virtual spy, sending a full range of data, including video, audio and keyboard strokes to its controller.

Without directly naming the US and Israel, Iranian foreign ministry spokesperson Ramin Mehmanparast said: "It's in the nature of some countries and illegitimate regimes to spread viruses and harm other countries." Iran's computer emergency response team, Maher, linked Flame to an earlier attack involving the Wiper virus that disrupted communications at the country's oil ministry and stole large amounts of data.

Israeli vice prime minister Moshe Yaalon all but admitted his country's involvement in cyber attacks directed at Iran. "Anyone who sees the Iranian threat as a significant threat—it's reasonable that he will take various steps, including these, to harm it," he said, adding: "Israel is blessed as a country rich in advanced technology, and these tools open to us all sorts of possibilities."

The *Times* article makes clear that Israel was heavily involved in developing the Stuxnet worm. American officials, including from the National Security Agency (NSA), worked closely with their Israeli counterparts not only on developing the computer code but finding the means for infiltrating it into the Natanz enrichment plant, which required physical access.

The intimate collaboration of Israeli and American intelligence agencies on the cyber attacks undermines US claims that it was not involved other crimes, including other acts of sabotage and the murder of four Iranian nuclear scientists over the past three years and the attempted assassination of a fifth. The murders have been widely attributed to the Israeli intelligence agency Mossad.

This covert war against Iran, involving sabotage and assassination, is the preparation for even bigger crimes. Both Israel and the US have repeatedly threatened to launch unprovoked military attacks on Iran using the pretext that it is developing, or has the potential to develop, a nuclear weapon. Tehran has repeatedly denied plans to build an atomic bomb.

The virtual breakdown of talks between Iran and the P5+1 grouping in Baghdad last month increases the danger of military conflict. If the new round of negotiations in Moscow in two weeks' time fails, Washington is on a collision course with Tehran. On July 1, harsh new US and European sanctions will come into force that are designed to sharply reduce Iran's much-needed oil exports.

Speaking to NBC News last Wednesday, Israeli Defence Minister Ehud Barak again pressed for tougher measures against Iran, again declaring that "no option" should be off the table including military action. He branded the international talks as "a ritual of self-delusion" that would probably not end Iran's nuclear programs.

Last Friday US Secretary of State Hillary Clinton delivered what amounted to an ultimatum to Tehran to agree to Washington's demands at the Moscow summit. She insisted that Iran had to take "concrete actions", adding that "we will know by the next meeting ... whether Iran is prepared to take those actions." The US is demanding that Iran immediately shut down key aspects of its uranium enrichment program, but is offering little in return.

Obama's direct involvement in cyber sabotage and drone assassinations only underscores the recklessness of US imperialism as it threatens a new war of aggression against Iran.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact