Obama administration claims power to authorize pre-emptive cyberwar strikes

Joseph Kishore
5 February 2013

The Obama administration has concluded that the president can authorize pre-emptive cyberwar attacks, according to a secret legal review prepared by the US government. The move is part of efforts to expand the ability of the American military to use new technologies to carry out acts of aggression—with Iran and China the most immediate targets.

The discussions within the administration were reported by the *New York Times* in an article published on Monday.

While invariably couched in the language of "defense," the Pentagon's cyberwarfare plans are part of an array of offensive capabilities—in addition to and alongside economic sanctions, global spying, drone assassination strikes and more traditional military actions.

According to the *Times*, the administration's legal review concludes that the president "has the broad power to order a pre-emptive strike if the United States detects credible evidence of a major digital attack looming from abroad." The newspaper also reports on new policies "that will govern how intelligence agencies can carry out searches of faraway computer networks for signs of potential attack on the United States and, if the president approves, attack adversaries by injecting them with destructive code—even if there is no declared war."

The doctrine of pre-emptive war was adopted by the Bush administration for the purpose of justifying military aggression against any country deemed an existent or even potential threat to the United States. The *Times* notes in an aside, "Pre-emption has always been a disputed legal concept," citing the invasion of Iraq in 2003 on the fraudulent pretext of that country's possession of "weapons of mass destruction." Such disputes have evidently been swept aside by the Obama administration.

The importance of cyberwarfare has expanded with the increasing reliance on computer networks for the delivery of basic services. A cyber attack could take down power plants, hospitals, transportation systems or other critical infrastructure, potentially leading to economic devastation and widespread casualties.

According to the *Times*, decisions to authorize cyberwarfare will generally be made by the president himself. "One senior American official said that officials quickly determined that the cyberweapons were so powerful that—like nuclear weapons—they should be unleashed only on the direct orders of the commander in chief."

China is a particular target of current or potential cyberwarfare carried out by the US. Seeing China as a principal economic and geopolitical competitor, the Obama administration has organized a "pivot" to Asia and the Pacific to focus military resources in the region.

The *Times* quotes Richard Falkenrath of the Council on Foreign Relations: "While this is all described in neutral terms—what are we going to do about cyber attacks—the underlying question is, 'What are we going to do about China?'"

The report comes only days after a number of newspapers—including the *Washington Post*, the *Wall Street Journal* and the *Times* itself—announced that they had been the target of hacking attacks by individuals in China, which the *Times*, in particular, sought to link to the Chinese government.

The most significant act of cyberwar to date, however, came not from China, but from the United States and Israel, and was directed at Iran's nuclear program. It was revealed last year that the two countries were behind the creation of the Stuxnet virus, which infected Iranian networks in June 2010. The US

military operation, dubbed Operation Olympic Games, began under Bush and was continued under Obama.

As with drone assassinations, Obama personally directed the cyber attack on Iran from the Situation Room, receiving updates on a regular basis.

Stuxnet was accompanied by the release of the Flame malware virus, also jointly developed by the US and Israel, first discovered in 2012. While originally produced to monitor Iranian government computers, the Flame virus escaped into the general population, infecting thousands of computers.

What has been disclosed publicly is only a small indication of what is already being carried out. “This is about preparing the battlefield for another type of covert action,” one former high-ranking US intelligence official told the *Washington Post* in June 2012, around the time that the Flame virus was first discovered. “Cyber-collection against the Iranian program is way further down the road than this.”

The *Times* quotes one administration official as declaring, “There are levels of cyberwarfare that are far more aggressive than anything that has been used or recommended to be done.”

Cyber actions are being coordinated by Cyber Command, originally set up under the authority of the Obama administration in 2010. It is led by General Keith Alexander, who is also the head of the National Security Agency, the military’s main spy agency. The NSA maintains vast databases of communications, foreign and domestic.

According to an article in the *Washington Post* last week, the military recently approved a fivefold increase in the number of personnel in the Cyber Command, from 900 to 4,900. The newspaper writes that the move is “part of an effort to turn an organization that has focused largely on defensive measures into the equivalent of an Internet-era fighting force.”

Heavily involved in developing the Obama administration’s policy on cyberwarfare is John Brennan. Obama’s pick to head the CIA, Brennan has played a central role in defending and institutionalizing the administration’s policy of extra-judicial drone assassination, including of American citizens.

The recent actions are part of a broader campaign. In mid-October of last year, Obama signed an executive order expanding military authority to carry out cyber attacks and redefine as “defensive” actions that would previously have been considered acts of aggression—such as the cutting off of computer networks.

Around the same time, Defense Secretary Leon Panetta gave a bellicose speech in which he warned of a “cyber Pearl Harbor.” A cyber attack on the US could “cause physical destruction and the loss of life” and “paralyze and shock the nation and create a new profound sense of vulnerability,” he said.

Panetta’s speech aimed both at justifying an expansion of cyberwar capabilities and preparing the ground for military action using the pretext of a cyber attack on the US.

In addition to plans for aggressive war abroad, the expansion of military cyberwarfare poses immense dangers to the democratic rights of the American people, as the administration moves to expand government control over the Internet and create the basis for military intervention and oversight within the United States.

The cyberwar plans include procedures for military action within the United States. According to the *Times*, the military “would become involved in cases of a major cyberattack within the United States” under certain conditions, with Panetta describing “the ‘red line’ [to justify such actions] in the vaguest of terms—as a ‘cyber 9/11.’”