Obama ordered planning for cyberwarfare first strike

Patrick Martin
10 June 2013

The US government is developing detailed plans to attack other countries using cyberwarfare techniques, according to a report Friday in the British daily newspaper *Guardian*. President Obama gave the orders to plan for cyber attacks, including preemptive strikes by the US, in an 18-page directive issued last October and leaked to the newspaper, which published it on its web site.

Presidential Policy Directive 20 defines Offensive Cyber Effects Operations (OCEO), which "can offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."

It continues: "The United States government shall identify potential targets of national importance where OCEO can offer favorable balance of effectiveness and risk as compared with other instruments of national power."

The directive instructs the secretary of defense, the director of national intelligence, and the director of the CIA to "prepare for approval by the president through the National Security Advisor a plan that identifies potential systems, processes and infrastructure against which the United States should establish and maintain OCEO capabilities." Since the deadline for this action is six months after the approval of the directive, which came in October, this plan has presumably already been developed and submitted to the National Security Council.

In relation to foreign targets of cyberwarfare, the directive authorizes actions by US government agencies in circumstances where the identity and nationality of the "adversary" are uncertain. The US government "shall make all reasonable efforts, under circumstances prevailing at the time, to identify the adversary and the ownership and geographic location of the targets and related infrastructure where DCEO or OCEO will be conducted or cyber effects are expected to occur."

Translated into plain language, this means that a US government attack on alleged hackers could target a foreign government or military without definitively identifying them as the source of the hacking. In recent months, the Obama administration and US media, spearheaded by the *New York Times*, have hyped the threat of Chinese hackers, supposedly organized through a Chinese military office in Shanghai, without providing any actual proof of the linkage.

As one of its intelligence sources told the *Guardian*, US complaints about Chinese cyberwarfare efforts were hypocritical: "We hack everyone everywhere. We like to make a distinction between us and the others. But we are in almost every country in the world."

The directive acknowledges that cyber-warfare efforts by the US government may produce "potential unintended or collateral consequences," not only within the targeted countries, but worldwide and in the US itself. These consequences could include "loss of life, significant responsive actions against the United States, significant damage to property, serious adverse US foreign policy consequences, or serious economic impact on the United States."

The directive essentially reiterates the doctrine of preventive warfare, enunciated by George W. Bush in 2002 in the run-up to the invasion of Iraq. Bush declared that the United States had the right to attack other countries, not merely to preempt an impending attack, but to prevent any potential attack at any time in the future—a formula for unlimited worldwide aggression.

Bush himself was giving little more than a rehash of the Nazi doctrine condemned by the Nuremburg

Tribunal after World War II, when a US prosecutor declared that the supreme crime of Hitler's Germany was the "planning, preparation, initiation and waging of a war of aggression," from which all the other crimes, including the Holocaust, ultimately stemmed.

The directive's pro-forma declaration that the "United States Government shall reserve the right to act in accordance with the United States' inherent right of self defense as recognized in international law" cuts no ice, since both the Bush and Obama administrations include such actions as the invasion of countries, bombing, missile strikes and assassinations under the rubric of "self defense."

The directive also discusses possible cyber attacks by the US government against domestic targets inside the country. This raises the prospect that in the event of a political crisis in the US, stemming either from domestic political and social upheaval or mass opposition to war, the US government could shut down the Internet and social media, target specific web sites or carry out other acts of cyber warfare in the name of "national security."

While the document claims that only the president can authorize cyber operations inside the United States, it contains a lengthy section, the longest in the entire executive order, spelling out what it calls "Emergency Cyber Action," which can be taken by the secretary of defense or "a department or agency head with appropriate authorities"—in other words, any top official of the military-intelligence apparatus.

Such actions can be taken if "necessary to mitigate an imminent threat or ongoing attack against US national interests." This would include preventing "significant damage with enduring national impact on the Primary Mission Essential Functions of the United States Government, U.S. critical infrastructure and key resources, or the mission of U.S. military forces…"

The language is so broad that it could easily be applied to a strike by US government employees or workers at any corporation providing services to the military or a government agency, or to workers in telecommunications, utilities, public transportation, or anything else designated as "critical" by the government.

According to the directive, domestic cyber-warfare actions would be coordinated with dozens of federal departments and conducted in accordance with the "National Continuity Policy" document of May 9, 2007.

This is a reference to one of the last versions of the notorious Bush administration planning for "continuity of government," in which plans were made for transferring all federal power to a small cabal of executive branch officials—lodged in Richard Cheney's infamous "undisclosed secure location"—and excluding both the legislative and judicial branches of government.

In other words, from Bush to Obama, from Republican to Democrat, the preparations of the American ruling elite for dictatorial rule continue and accelerate. While nominally justified by the threat of "terrorism" or, in the case of cyber-warfare, the supposed threat of China, the real target of these preparations is the American working class.

In both its plans for worldwide warfare, and its preparations for dictatorship at home, the American ruling class is driven by the mounting social inequality and class antagonisms within the United States.