US cybersecurity plan poses new war threats, attacks on democratic rights

Tom Eley
30 May 2009

President Barack Obama announced on Friday the creation of a new "cyber czar" position. The Cybersecurity Coordinator, who is yet to be named, would oversee billions of dollars in funding for developing and coordinating defense of the computer networks that operate the global financial system and domestic transportation and commerce, according to the administration. The position, which Obama said would report directly to him, results from a 60-day "cyberspace policy review" Obama ordered.

Obama's announcement was overshadowed by the US military's imminent creation of a new military "Cyber Command," detailed in a *New York Times* article published Friday. Obama has not even been presented with the military's plan, nor did he mention it directly in his press conference. However, administration sources have said he will sign a classified order or set of directives later this month authorizing the creation of the Cyber Command.

Media accounts indicate that the formation of the parallel domestic and military cyber security agencies was the source of a bitter "turf battle" between and within competing national security and federal domestic agencies.

As a compromise, Obama's domestic Cybersecurity Coordinator would report to both the National Economic Council (NEC), a White House economic advisory group, and the National Security Council, the top-level presidential advisory group that coordinates foreign and military policy, thus ensuring "a balance between homeland security and economic concerns," the *Washington Post* reports. Obama's top economic advisor, Lawrence H. Summers, fought for a dominant role for the NEC so that "efforts to protect private networks do not unduly threaten economic growth."

In his Friday press conference, Obama sought to present the Cybersecurity Coordinator position in the most innocuous terms, referring to the "spyware and malware and spoofing and phishing and botnets." and "cyber thieves" that anyone with access to the Internet confronts. Obama emphasized that the measure would not include "monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans," he said. "Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be—open and free."

But the creation of high-level police agency tasked with overseeing the Internet raises troubling questions. As the *New York Times* notes, it "appears to be part of a significant expansion of the role of the national security apparatus" in the White House.

Meanwhile, legislation working its way through Congress, the so-called Cybersecurity Act of 2009, would grant the US government unprecedented control over the Internet. The bill gives the president unrestricted power to halt Internet traffic, ordering the shutdown of both government and privately owned and operated networks deemed related to "critical infrastructure information systems," merely by declaring a "cybersecurity emergency."

In his remarks, Obama pointed to the threat of cyber terrorism, noting that US "defense and military networks are under constant attack. Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyber attack on our country." He invoked the recent terror attacks on Mumbai, India, where "terrorists...relied not only on guns and grenades but also on GPS and phones using voice-over-the-Internet." Obama also alluded to the possibility of cyberwarfare with a major foe, mentioning Russia by name. "Last

year we had a glimpse of the future face of war," Obama said. "As Russian tanks rolled into Georgia, cyber attacks crippled Georgian government websites."

However, these sorts of threats would most likely not fall under the purview of the Cybersecurity Coordinator, at least based on Obama's explanation of the position. The implication is that these "threats" would be handled by the military-intelligence Cyber Command.

Reports indicate that there is an acrimonious struggle within the national security apparatus over who should oversee the new command. Currently, the National Security Agency (NSA) controls most of the functions that would be associated with cyberwarfare. Created by Democratic President Harry S. Truman in 1952 at the height of the Cold War, the NSA is a spy agency tasked with breaking the codes and signals of foreign entities and encrypting sensitive US government communications. It is overseen by a military figure—either a lieutenant general or vice admiral—and the NSA reports to the Department of Defense.

In March, Rod Beckstrom, the Department of Homeland Security's cyber-security head (Director, National Cybersecurity Center) resigned in protest over the NSA appearing to win out in the struggle over who should "defend" domestic computer networks. In his resignation letter, which was leaked to the press, Beckstrom implied that the Office of Management and Budget had conspired with the NSA to starve his own agency of funding, and raised the threat posed by the NSA overseeing domestic computer-spying operations. "The threat to our democratic processes are significant if all top government network security and monitoring are handled by any one organization (either directly or indirectly)," Beckstrom wrote. "During my term as director we have been unwilling to subjugate the NSCS underneath the NSA."

A *Wall Street Journal* report at the end of April indicated that the head of the Cyber Command would be current NSA chief, General Keith Alexander. Other accounts indicate that the Cyber Command would more likely report at first to the military's Strategic Command, which oversees the nation's nuclear arsenal, according to sources cited in the *New York Times*. And still other sources have said NSA personnel could be moved into a new military command structure under the control of the Pentagon.

In any case, the formation of the Cyber Command raises the threat of the military or the NSA launching operations within the US. Both are currently constitutionally-prohibited from carrying on either military or spy actions within American borders. One anonymous "senior intelligence official," cited in the *Times*, called this "the domestic spying problem writ large."

"These attacks start in other countries, but they know no borders," he said. "So how do you fight them if you can't act both inside and outside the United States?" The answer, implied by the very formation of the Cyber Command, is that the military and spy agencies should disregard the traditional separation of foreign war and espionage, on the one hand, and domestic policing and investigation, on the other.

According to the Defense Department, in 2008 360 million attempts were made to breach its computer networks. It also reported that the Pentagon spent $100 million in the past six months to repair damage done by hackers, most of whom work from Russia and China, it is claimed. In early April the *Wall Street Journal* reported that hackers had penetrated the national electricity grid and even the Pentagon's $300 billion Joint Strike Fighters program.

Yet despite the rhetoric about national defense, comments from administration sources and military figures make clear that motivating the creations of the military cyber defense is its offensive capabilities. "We are not comfortable discussing the question of offensive cyberoperations, but we consider cyberspace a war-fighting domain," said Bryan Whitman, an Obama Pentagon spokesman. "We need to be able to operate within that domain just like on any battlefield, which includes protecting our freedom of movement and preserving our capability to perform in that environment."