Obama names former Bush adviser as cybersecurity chief

Joe Kishore
23 December 2009

On Tuesday, the Obama administration announced the appointment of Howard Schmidt, a former adviser to George W. Bush and executive at Microsoft, as the new White House cybersecurity coordinator.

The post, originally announced in May, was occupied by an acting head who resigned in August. The stated task of Schmidt will be to defend US computer systems—particularly those that run major financial firms and corporations—from being hacked or attacked.

More fundamentally, however, the creation of the new post is part of an increased focus by the US military and state apparatus on computer systems. In foreign policy, this is bound up with Washington's overall aggressive posture. Domestically, it is linked to the growth of domestic spying and efforts to subordinate the Internet to the state.

After the September 11 attacks, Bush appointed Schmidt as vice chair of the President's Critical Infrastructure Protection Board and special adviser on cyberspace security for the White House. Schmidt helped formulate the US National Strategy to Secure CyberSpace. In 2003, he left government to become the vice president and chief information security officer at the online auction company, eBay.

Schmidt's resumé underscores his close ties to the military and intelligence establishment. He served in the Army and Air Force in computer security positions and led a computer forensics team for the FBI at the National Drug Intelligence Center.

Highlighting the concerns of sections of the American ruling class over possible vulnerabilities, the *Wall Street Journal* reported Tuesday that the FBI is investigating a security breach at banking giant Citigroup. The *Journal* wrote that the cyber attack "resulted in a theft of tens of millions of dollars by computer hackers who appear linked to a Russian cyber gang, according to government officials." Citigroup denied that there had been an attack.

The *Journal* commented, "Security officials worry that, beyond stealing money, hackers could try to manipulate or destroy data, wreaking havoc on the banking system."

The military is heavily involved in the cybersecurity project. In the spring—concurrent with Obama's announcement of the cybersecurity post—the Pentagon announced the creation of a new "cyber command." The military has already used offensive cyber weapons, including in Iraq.

According to the *Washington Post*, Schmidt's mission will be "to coordinate cybersecurity policy across the federal government, from military to civilian agencies." He will report to the National Security Council (NSC) and the deputy national security adviser for homeland security and terrorism, John Brennan.

The National Security Council is chaired by the president and includes the vice president, the secretary of state, the secretary of the treasury, the secretary of defense, and the president's national security adviser. The chairman of the joint chiefs of staff is the statutory military adviser to the council and the director of national intelligence is the intelligence adviser. The chief of staff to the president, the counsel to the president, and the assistant to the president for economic policy are also invited to attend NSC meetings.

Schmidt's subordination to Brennan is an indication of the intended role of the new post. According to media reports, the position was the subject of a "turf battle," with White House economic adviser Lawrence Summers arguing that the cybersecurity coordinator should report to him as well. Obama decided against this, however.

© World Socialist Web Site

Brennan himself was initially considered as Obama's director of the Central Intelligence Agency, before he was forced to withdraw due to his support for Bush's policy of "enhanced interrogation" (i.e., torture) and rendition. Brennan is also reportedly one of the major figures who pushed for Obama to agree to immunity for telecommunications companies that participated in the National Security Agency's (NSA) domestic spying program.

There are major threats to democratic rights involved in the government's push for "cybersecurity." The proposed Cybersecurity Act of 2009, presently being considered by Congress, would give the government extraordinary control over the Internet in the event of an "emergency," including the authority to shut down Internet traffic and disconnect critical infrastructure systems.

The act would build on the Cyber Security Enhancement Act of 2002, which gave the FBI expanded powers to collect information on web users from Internet Service Providers.

The question of cybersecurity is also bound up with tensions between the major powers, particularly between the US and Russia and the US and China. The latter two countries are generally cited by the US government as the source of cyber attacks in the United States. Russia has also been blamed by the US for cyber attacks that crippled Georgian web sites during the war between US ally Georgia and Russia in 2008, when Georgia attacked South Ossetia.

The US is aggressively developing offensive cyber warfare capabilities, as evidenced by the creation of the Pentagon "cyber command." Washington has resisted proposals for a treaty banning the offensive use of these weapons, including in current negotiations between the Obama administration and Russia over cybersecurity.

The November 14 edition of the *National Journal* magazine reports that in May 2007: "At the request of his national intelligence director, Bush ordered an NSA cyberattack on the cellular phones and computers that insurgents in Iraq were using to plan roadside bombings… According to a former senior administration official who was present at an Oval Office meeting when the president authorized the attack, the operation helped US forces to commandeer the Iraqi fighters' communications system. With this capability, the Americans could deceive their adversaries with false information, including messages to lead unwitting insurgents into the fire of waiting US soldiers."

Gen. David Petraeus, the commander of US Central Command and the architect of the Iraq "surge" in 2007, is reportedly a strong advocate of cyber warfare.

The *National Journal* noted, "As the White House vets candidates for the 'cyber-czar' post [the post now occupied by Schmidt], the military and intelligence agencies are honing their cyber skills and have already marshaled their forces."

The increasing focus on computer systems in the US is bound up with concerns within the ruling elite that while the American military maintains dominance in its traditional capabilities, it does not have a clear advantage when it comes to information and electronic systems.

In February 2008, then-director of national intelligence under Bush, Michael McConnell, warned, "We assess that nations, including Russia and China, have technical capabilities to target and disrupt" the US information infrastructure.

The Obama administration is attempting to alter this balance of forces as part of its aggressive assertion of military force as a key instrument of US imperialist foreign policy.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact

© World Socialist Web Site