May 30, 2009

Obama Outlines Coordinated Cyber-Security Plan

By DAVID E. SANGER and JOHN MARKOFF

WASHINGTON — President Obama declared Friday that the country's disparate efforts to "deter, prevent, detect and defend" against cyberattacks would now be run out of the White House, but he also promised that he would bar the federal government from regular monitoring of "private-sector networks" and the Internet traffic that has become the backbone of American communications.

Mr. Obama's speech, which was accompanied by the release of a long-awaited new government strategy, was an effort to balance the United States' response to a rising security threat with concerns — echoing back to the debates on wiretapping without warrants in the Bush years — that the government would be regularly dipping into Internet traffic that knew no national boundaries.

One element of the strategy clearly differed from that established by the Bush administration in January 2008. Mr. Obama's approach is described in a 38-page public document being distributed to the public and to companies that are most vulnerable to cyberattack; Mr. Bush's strategy was entirely classified.

But Mr. Obama's policy review was not specific about how he would turn many of the goals into practical realities, and he said nothing about resolving the running turf wars among the Pentagon, the National Security Agency, the Homeland Security Department and other agencies over the conduct of defensive and offensive cyberoperations.

The White House approach appears to place a new "cybersecurity coordinator" over all of those agencies. Mr. Obama did not name the coordinator Friday, but the policy review said that whoever the president selects would be "action officer" inside the White House during cyberattacks, whether they were launched on the United States by hackers or governments.

In an effort to silence critics who have complained that the official will not have sufficient status to cut through the maze of competing federal agencies, Mr. Obama said the new coordinator would have "regular access to me," much like the coordinator for nuclear and conventional threats.

Many computer security executives had been hoping that Mr. Obama's announcement would represent a turning point in the nation's unsuccessful effort to turn back a growing cybercrime epidemic. On Friday, several said that while the president's attention sounded promising, much would depend on whom he chose to fill the role.

James A. Lewis, a director at the Center for Strategic & International Studies, a Washington group that published a bipartisan report last year calling on the president to appoint a cyberczar, said that the White House had now narrowed the list of candidates for the position to fewer than 10, but that choosing the right person would be difficult.

"There aren't a lot of people who have the policy and the strategy skills and the technological knowledge to carry this out," Mr. Lewis said. "If you're talking about missiles and space, there are a lot of people who know policy and technology, but in cyber its such a new field we're talking about a really small gene pool."

For the first time, Mr. Obama also spoke of his own brush with cyberattacks, in the presidential campaign. "Between August and October, hackers gained access to e-mails and a range of campaign files, from policy position papers to travel plans," he said, describing events that were known, though sketchily, at the time.

"It was," he said, "a powerful reminder: in this information age, one of your greatest strengths — in our case, our ability to communicate to a wide range of supporters through the Internet — could also be one of your greatest vulnerabilities."

Mr. Obama's speech delved into technology rarely discussed in the East Room of the White House. He referred to "spyware and malware and spoofing and phishing and botnets," all different approaches to what he called "weapons of mass disruption."

Although the president did not discuss details of the expanding role for the military in offensive and pre-emptive cyberoperations, senior officials said Friday that the Pentagon planned to create a new cybercommand to organize and train for digital war, and to oversee offensive and defensive operations.

A lingering disagreement has been how to coordinate that new command with the work of the National Security Agency, home to most of the government's expertise on computer and network warfare. One plan now under discussion would put the same general in charge of both the new cybercommand and the N.S.A. Currently, the security agency's director is Lt. Gen. Keith B. Alexander, who would be expected to be the leading contender for the new, dual position.

Industry executives were generally supportive of the initiative Mr. Obama announced, but also cautious.

"There was nothing I was disappointed in," said Mark Gerencser, a cybersecurity executive at Booz Allen Hamilton, a consulting firm that deals extensively in the government's cybersecurity strategy.

Mr. Gerencser noted that the United States had separated defense and offense in the cybersecurity arena, while its opponents, including Russia and China, had a more fluid strategy.

"It's like we're playing football and our adversaries are playing soccer," he said.

Thom Shanker contributed reporting from Washington.

This article has been revised to reflect the following correction:

Correction: June 3, 2009
Because of an editing error, an article on Saturday about a new government plan to fight cyberattacks gave an incorrect attribution for a statement about the differences between the strategy of the United States and that of other countries, including Russia and China. It was Mark Gerencser, a cybersecurity executive, who noted that the United States had separated defense and offense in the cybersecurity arena, while other countries had a more fluid strategy. The statement was not by "Mr. Hamilton." (Mr. Gerencser is an executive with Booz Allen Hamilton, a consulting firm that deals extensively in the government's cybersecurity strategy.)