WASHINGTON — President Obama declared Friday that the country’s disparate efforts to “deter, prevent, detect and defend” against cyber attacks 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 today, which was accompanied by the release of a long-awaited new government strategy, was an effort to balance America’s response to a rising security threat with concerns — echoing back to the warrantless wiretapping debates of the Bush years — that the government would be regularly dipping into Internet traffic that knows no national boundaries.

One element of the strategy clearly differed from the one Bush administration issued in January 2008: Mr. Obama’s approach is described in a 38-page document being distributed to public and to companies that are most vulnerable to cyber attack; 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 between the Pentagon, the National Security Agency, the Homeland Security Department and other agencies over the conduct of defensive and offensive cyber operations.

The White House approach appears to place a new “cybersecurity coordinator” over all of those agencies. He did not name the coordinator on Friday, but the policy review said that whomever the president selects will be “action officer” inside the White House during cyber attacks, whether they are 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, he said the new coordinator would have “regular access to me,” much like the coordinator for nuclear and conventional threats.

For the first time, Mr. Obama also spoke of his own brush with cyber attacks during the Presidential campaign. “Between August and October,” he said, “hackers gained access to e-mails and a range of campaign files, from policy position papers to travel plans,” describing events that were known, though sketchily, at the time.
“It was 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 cyber operations, senior officials said on Friday the Pentagon plans to create a new cyber command 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 cyber command and the N.S.A. Currently, the N.S.A. 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, though cautious, of the initiative announced by Mr. Obama.

“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. He noted that the United States has separated defense and offense in the cybersecurity arena, while its opponents – including Russia and China -- have a more fluid strategy. “It’s like we’re playing football and our adversaries our playing soccer.”

Russell D. Vines, another computer-security expert, said he was pleased that President Obama recognizes the need for a comprehensive strategy. Too many people do not even like to discuss computer security because “it’s kind of like going to the dentist,” Mr. Vines said on Friday in a telephone interview from White Plains, N.Y. “But there’s no going back.”

The president said those who describe the computer-driven era as “a virtual world” are not quite right. “Make no mistake: this world — cyberspace — is a world that we depend on every single day,” he said. “It’s our hardware and our software, our desktops and laptops and cell phones and BlackBerrys, that have become woven into every aspect of our lives.”

“So cyberspace is real,” the president said, “and so are the risks that come with it.”

White House officials say Mr. Obama has not yet been formally presented with the Pentagon plan.

“Waves of cyber thieves trolling for sensitive information” is how President Obama described the vandals of the computer age. Implicit in his remarks was the message that computer hackers
cannot be regarded as mere mischief-makers in a new world where computers are central to the country’s security and prosperity, and the health and happiness of its citizens.

“It’s also clear that we’re not as prepared as we should be, as a government or as a country,” he said, declaring that an uncoordinated, ad hoc approach to cybersecurity will not do.

As for the military cyber command, officials said the president would sign a classified order creating it in the weeks ahead. The development is a recognition that the United States already has a growing number of computer weapons in its arsenal and must prepare strategies for their use — as a deterrent or alongside conventional weapons — in a wide variety of possible future conflicts.

Officials said that in addition to the unclassified strategy paper released by Mr. Obama on Friday to accompany the announcement of the new security position, a classified set of presidential directives is expected to lay out the military’s new responsibilities and how it coordinates its mission with that of the N.S.A., where most of the expertise on digital warfare resides today.

It is still unclear whether the military’s new command or the N.S.A. — or both — will actually conduct this new kind of offensive cyber operations.

The White House has never said whether Mr. Obama embraces the idea that the United States should use cyber weapons, and the public announcement on Friday focused on defensive steps and the government’s acknowledgment that it needs to be better organized to face the threat from foes attacking military, government and commercial online systems.

Defense Secretary Robert M. Gates has pushed for the Pentagon to become better organized to address the security threat.

Initially at least, the new command would focus on organizing the various components and capabilities now scattered across the four armed services.

Officials declined to describe potential offensive operations, but said they now viewed cyberspace as comparable to more traditional battlefields.

“We are not comfortable discussing the question of offensive cyber operations, but we consider cyberspace a war-fighting domain,” said Bryan Whitman, a 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.”

Although Pentagon civilian officials and military officers said the new command was expected to initially be a subordinate headquarters under the military’s Strategic Command, which controls nuclear operations as well as cyber defenses, it could eventually become an independent command.

“No decision has been made,” said Lt. Col. Eric Butterbaugh, a Pentagon spokesman. “Just as the White House has completed its 60-day review of cyberspace policy, likewise, we are looking
at how the department can best organize itself to fill our role in implementing the
administration’s cyber policy.”

The creation of the cyber czar’s office inside the White House appears to be part of a significant expansion of the role of the national security apparatus there. A separate group overseeing domestic security, created by President George W Bush after the Sept. 11 attacks, now resides within the National Security Council. A senior White House official responsible for countering the proliferation of nuclear and unconventional weapons has been given broader authority. Now, cybersecurity will also rank as one of the key threats that Mr. Obama is seeking to coordinate from the White House.

The strategy review Mr. Obama discussed on Friday was completed weeks ago, but delayed because of continuing arguments over the authority of the White House office, and the budgets for the entire effort.

It was kept separate from the military debate over whether the Pentagon or the N.S.A. is best equipped to engage in offensive operations. Part of that debate hinges on the question of how much control should be given to American spy agencies, since they are prohibited from acting on American soil.

“It’s the domestic spying problem writ large,” one senior intelligence official said recently. “These attacks start in other countries, but they know no borders. So how do you fight them if you can’t act both inside and outside the United States?”

*John Markoff contributed reporting from San Francisco and Thom Shanker and David Stout from Washington.*