The New York Times

Security Leader Says U.S. Would Retaliate Against Cyberattacks

By Mark Mazzetti and David E. Sanger

March 12, 2013

WASHINGTON — The chief of the military’s newly created Cyber Command told Congress on Tuesday that he is establishing 13 teams of programmers and computer experts who could carry out offensive cyberattacks on foreign nations if the United States were hit with a major attack on its own networks, the first time the Obama administration has publicly admitted to developing such weapons for use in wartime.

“I would like to be clear that this team, this defend-the-nation team, is not a defensive team,” Gen. Keith Alexander, who runs both the National Security Agency and the new Cyber Command, told the House Armed Services Committee. “This is an offensive team that the Defense Department would use to defend the nation if it were attacked in cyberspace. Thirteen of the teams that we’re creating are for that mission alone.”

General Alexander’s testimony came on the same day the nation’s top intelligence official, James R. Clapper Jr., warned Congress that a major cyberattack on the United States could cripple the country’s infrastructure and economy, and suggested that such attacks now pose the most dangerous immediate threat to the United States, even more pressing than an attack by global terrorist networks.

On Monday, Thomas E. Donilon, the national security adviser, demanded that Chinese authorities investigate such attacks and enter talks about new rules governing behavior in cyberspace.

General Alexander has been a major architect of the American strategy on this issue, but until Tuesday he almost always talked about it in defensive terms. He has usually deflected questions about America's offensive capability, and turned them into discussions of how to defend against mounting computer espionage from China and Russia, and the possibility of crippling attacks on utilities, cellphone networks and other infrastructure. He was also a crucial player in the one major computer attack the United States is known to have sponsored in recent years, aimed at Iran's nuclear enrichment plants. He did not discuss that highly classified operation during his open testimony.

Mr. Clapper, the director of national intelligence, told the Senate Intelligence Committee that American spy agencies saw only a "remote chance" in the next two years of a major computer attack on the United States, which he defined as an operation that "would result in long-term, wide-scale disruption of services, such as a regional power outage."

Mr. Clapper appeared with the heads of several other intelligence agencies, including Lt. Gen. Michael T. Flynn of the Defense Intelligence Agency, the F.B.I. director Robert S. Mueller III, and the C.I.A. director John O. Brennan, to present their annual assessment of the threats facing the nation. It was the first time that Mr. Clapper listed cyberattacks first in his presentation to Congress, and the rare occasion since the Sept. 11, 2001, attacks that intelligence officials did not list international terrorism first in the catalog of dangers facing the United States.

"In some cases," Mr. Clapper said in his testimony, "the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks." He said it was unlikely that Russia and China would launch "devastating" cyberattacks against the United States in the near future, but he said foreign spy services had already hacked the computer networks of government agencies, businesses and private companies.

Two specific attacks Mr. Clapper listed, an August 2012 attack against the Saudi oil company Aramco and attacks on American banks and stock exchanges last year, are believed by American intelligence officials to have been the work of Iran.

General Alexander picked up on the same themes in his testimony, saying that he was adding 40 cyber teams, 13 focused on offense and 27 on training and surveillance. When pressed, he said that the best defense hinged on being able to monitor incoming traffic to the United States through private "Internet service providers," which could alert the government, in the milliseconds that electronic messages move, about potentially dangerous attacks. Such surveillance is bound to raise more debate with privacy advocates, who fear government monitoring of the origin and the addressing data on most e-mail messages and other computer exchanges.

Traditional threats occupied much of Mr. Clapper's testimony. American intelligence officials are giving new emphasis to the danger posed by North Korea's nuclear weapons and missile programs, which are said for the first time to "pose a serious threat to the United States" as well as to its East Asian neighbors. North Korea, which recently made a series of belligerent statements after its third nuclear test, has displayed an intercontinental missile that can be moved by road and in December launched a satellite atop a Taepodong-2 launch vehicle, Mr. Clapper's prepared statement noted.

"The rhetoric, while it is propaganda laced, is also an indicator of their attitude and perhaps their intent," Mr. Clapper said during one exchange with a lawmaker, adding that he was concerned that North Korea "could initiate a provocative action against the South."

In his discussion of terrorism, Mr. Clapper noted that while Al Qaeda's core in Pakistan "is probably unable to carry out complex, large-scale attacks in the West," spinoffs still posed a threat. Listed first is the affiliate in Yemen, Al Qaeda in the Arabian Peninsula, which Mr. Clapper said had retained its goal of attacks on United States soil, but he also noted militant groups in six other countries that still threaten local violence.

Mr. Clapper began his remarks by criticizing policy makers for the current budget impasse, saying that the budget cuts known as sequestration will force American spy agencies to make sharp reductions in classified programs and to furlough employees. The classified intelligence budget has ballooned over the past decade, and Mr. Clapper compared the current round of cuts to the period during the 1990s when the end of the cold war led to drastic reductions in the C.I.A.'s budget.

“Unlike more directly observable sequestration impacts, like shorter hours at public parks or longer security lines at airports, the degradation of intelligence will be insidious,” Mr. Clapper said. “It will be gradual and almost invisible unless and until, of course, we have an intelligence failure.”

The threat hearing is the only scheduled occasion each year when the spy chiefs present open testimony to Congress about the dangers facing the United States, and Mr. Clapper did not hide the fact that he is opposed to the annual ritual. President Obama devoted part of his State of the Union address to a pledge of greater transparency with the Congress and the American public, but Mr Clapper, a 71-year-old retired Air Force general, made it clear that he saw few benefits of more public disclosure.

“An open hearing on intelligence matters is something of a contradiction in terms,” he said.

Scott Shane contributed reporting.

A version of this article appears in print on March 13, 2013, on Page A4 of the New York edition with the headline: Security Chief Says Cyberattacks Will Meet With Retaliation