Pentagon forming cyber teams to prevent attacks (Update 2)

March 12 2013, by Richard Lardner

The Defense Department is establishing a series of cyber teams charged with carrying out offensive operations to combat the threat of an electronic assault on the United States that could cause major damage and disruption to the country's vital infrastructure, a senior military official said Tuesday.

Gen. Keith Alexander, the top officer at U.S. Cyber Command, warned during testimony that the potential for an attack against the nation's electric grid and other essential systems is real and more aggressive steps need to be taken by the federal government and the private sector in order to improve digital defenses.

Alexander told the Senate Armed Services Committee that foreign leaders are deterred from launching cyberattacks on the United States because they know such a strike could be traced to its source and would generate a robust response.

But the country is not preventing what Alexander called "low-level harassment of private and public websites, property and information by other states." He did not mention any specific countries, even though the Obama administration is escalating its criticism of cyber thefts by China that have become intolerable to the international community.

Offensive cyber weapons are growing and evolving, Alexander said, and it is only a matter of time before tools developed by other nations wind up in the hands of extremist groups or even individuals who could do

significant harm.

Alexander said 13 cyber teams are being formed for the mission of guarding the nation in cyberspace. He described them as "defend-the-nation" teams but stressed their role would be offensive. In comments to reporters after the hearing, Alexander likened the teams' duties to knocking an incoming missile out of the sky before it hits a target. He also said the teams would work outside the United States, but he did not say where.

He also said another 27 cyber teams are being established to support the military's warfighting commands while others will protect Defense Department's computer systems and data.

But even as Alexander detailed these moves, he pushed lawmakers to pass cybersecurity legislation that would make it easier for the government and the private sector—which controls critical infrastructure such as the electric grid, banking systems, chemical facilities and water treatment systems—to share detailed information about who is getting hacked and what to do about it.

President Barack Obama signed an executive order last month that relies heavily on participation from U.S. industry in creating new voluntary standards for protecting information and expands the government's effort to provide companies with threat data. But the order doesn't do enough to address the threat, administration officials said. Unresolved issues include the legal liability facing companies if they divulge information, and whether companies should be compelled to meet certain security standards.

The general also told the committee that there needs to be a clear consensus on how the nation is organized to protect critical infrastructure from cyberattacks. "It takes a team to operate in

cyberspace," Alexander said. "But at times I think in talking about the team approach, we're not clear on who's in charge when."

Another issue that still needs to be settled is what constitutes an act of war in cyberspace, Alexander said. He does not consider cyberespionage and the theft of a corporation's intellectual property to be acts of war. But Alexander said, "I think you've crossed the line" if the intent is to disrupt or destroy U.S. infrastructure.

Sen. Carl Levin, a Democrat and the committee's chairman, noted that Obama recently issued a classified policy directive to govern cyber operations. The Pentagon also has developed a list of procedures on how to respond in "cyber crisis" situations, he added, and the Pentagon is expected to issue cyber rules of engagement for military commanders.

"The fact that these foundational policy frameworks and planning actions are just now taking shape serves as a stark illustration of how immature and complex this warfare domain remains," Levin said.

Alexander said the private sector maintains varying degrees of security over its computer systems. The financial industry typically is more secure than companies that operate the electric grid. Still, he said, banks are vulnerable to being disrupted by what are called denial of service attacks, a technique that works by overloading a website with traffic.

"The issue that we're weighing is, when does a nuisance become a real problem?" Alexander said. "And when are you prepared to step in for that? And that's the work that, I think, the administration is going through right now in highlighting that."

Alexander's testimony comes a day after Obama's national security adviser called for "serious steps" by China to stop cyber theft that has become intolerable to the international community.

The remarks on Monday by Tom Donilon before the Asia Society in New York underscore the growing concern in Washington over the security risks posed by cyber thefts and intrusions and the economic costs to U.S. businesses.

American companies are being more vocal about cyber theft emanating from China "on a very large scale." He said Beijing "should take serious steps to investigate and put a stop to these activities" and recognize the risk to international trade and to U.S.-China relations.

The Obama administration last month announced new efforts, including a new diplomatic push to discourage intellectual property theft abroad, to fight the growing theft of American trade secrets following the release of a report that linked China's military to the electronic theft of corporate trade secrets and U.S. government data.