THE WALL STREET JOURNAL.

NATIONAL SECURITY

Debate Deepens Over Response to Cyberattacks

While Some Lawmakers and Policy Makers Call for Counterattacks, Others Cite Difficulty of Targeting Hackers

By **DAMIAN PALETTA** and **DION NISSENBAUM**

Feb. 8, 2015 5:32 p.m. ET

Ashton Carter, President Barack Obama's nominee to be U.S. secretary of defense, told a Senate panel considering his confirmation last week that the U.S. and companies need to improve their defenses, but they should also consider some sort of response to future cyberattacks. *PHOTO: BLOOMBERG NEWS*

WASHINGTON—Several large-scale cyberattacks in recent months have prompted a number of lawmakers and policy makers to call for a more forceful response, including suggestions that the U.S. engage in counterattacks that would disable or limit the culprits' own networks.

But White House officials and some technology security experts remain skeptical that such "offensive" cyberattacks would work, saying they are concerned about the difficulty in targeting specific hackers without causing widespread spillover, among other things.

The debate—playing out in numerous closed-door briefings on Capitol Hill and among federal agencies—has taken on new urgency with the rise in well-executed online attacks against U.S. corporations.

President Barack Obama is expected to meet with business executives in California on Friday to urge them to work more closely with the government to bolster their

READ MORE ON CAPITAL JOURNAL »

- Health Insurer Anthem Didn't Encrypt Data in Theft (http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560?mod=capitaljournalrelatedbox)
- Health Insurer Anthem Hit by Hackers (http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720?mod=capitaljournalrelatedbox)

defenses. His aides have spent weeks drafting a new executive order that would encourage more information sharing between companies and the government about cybersecurity threats.

But the divide within the government on how to respond to future attacks is spilling into public view. Ashton Carter, the White House's nominee for secretary of the Department of Defense, told a Senate panel considering his confirmation last week that the U.S. and companies need to improve their defenses, but they should also consider some sort of response to future cyberattacks.

"We...need to improve our abilities to respond," he said. "And those responses can be in cyberspace or in other ways, but certainly they should include the option to respond in cyberspace."

He said the U.S. should be careful not to reveal the extent of its "capability to respond," so as to deny a "potential aggressor" a way to counter an attack.

Noteworthy cyberattacks in recent months have forced policy makers to rethink their approach. Late last year, the White House alleged that North Korea stole large amounts of data from Sony Pictures Entertainment Inc. Also, the recent theft of personal information from tens of millions of Anthem Inc.'s health-insurance customers may have originated in China, the company has suggested, though law-enforcement officials continue to investigate the breach.

Mr. Obama has labeled the Sony breach "cyber-vandalism," stopping short of calling it an "act of war" that might elicit a more pronounced U.S. response. Determining the culprit of a cyberattack is very difficult because of the sophistication of many hackers, and cybersecurity experts are mostly split on the merits of retaliation, with some saying it could distract companies from doing more to prevent breaches.

"Once the planners and everyone looks [into retaliation], it puts it on an escalation ladder we don't want to be on," said Bob Gourley, a former top technology official at the

Pentagon's Defense Intelligence Agency. "The first thing we need to do is protect our systems. Until we do that, we're almost inviting them to attack, saying 'Come on, take our stuff.'"

Counterattacks could also disable networks used by allies or limit investigators' ability to get to the perpetrators, experts say.

Sen. Angus King (I., Maine), a member of the Senate Intelligence Committee, said he has expressed the need for an aggressive government response to cyberattacks during multiple closed-door congressional briefings, particularly given the breaches at Sony and Anthem.

"I'm wondering if we shouldn't be thinking of strategy that, if a nation-state is behind a cyberattack...they will lose their network," he said in an interview. "Otherwise we are entirely in a defensive posture."

So far, the limited U.S. response to cyberattacks has frustrated some corporate executives. Businesses are largely prohibited by law from a practice known as "hack back," which could either be done to punish a cyberthief or take back information that was stolen from any specific firm. That has left companies relying on the government's response, which so far largely has come in the form of sanctions or criminal indictments.

Pentagon and other U.S. officials have looked at various potential responses, but they have found it difficult to design a uniform strategy. They are debating fundamental questions, a senior defense official said, such as: "What's an act of war? Where does cyber-vandalism stop and warfare begin? We're treading new ground."

The issue came up most recently when hackers briefly took control of U.S. military Twitter and YouTube accounts run by U.S. Central Command. The hackers taunted the U.S. military and posted statements sympathetic to Islamic State militants before the military regained control of the accounts. Pentagon officials dismissed the hacking as "cyber-vandalism" that didn't jeopardize any classified military information.

The incident has also helped shape the debate over how to respond to cyberattacks.

"What is a proportional response?" the official asked. "How do we not only protect our own Department of Defense systems, but also play a role in protection of critical infrastructure and our own cyber systems as a nation."

Though a number of Republicans on Capitol Hill have called for the White House to consider retaliating against hackers, lawmakers from both parties have stopped short of pushing for such responses through legislation.

Rep. Mike McCaul (R., Texas), chairman of the House Committee on Homeland Security, is drafting a bill that would provide incentives to companies to share information with federal agencies working to prevent breaches, while also prod agencies to share more information with companies. His aides said the legislation is still being drafted and could expand after more input from other lawmakers.

—Danny Yadron contributed to this article.

Write to Damian Paletta at damian.paletta@wsj.com and Dion Nissenbaum at dion.nissenbaum@wsj.com