New interest in hacking as threat to security
Michael S. Schmidt

During the five-month period between October and February, there were 86 reported attacks on computer systems in the United States that control critical infrastructure, factories and databases, according to the Department of Homeland Security, compared with 11 over the same period a year ago.

None of the attacks caused significant damage, but they were part of a spike in hacking attacks on networks and computers of all kinds over the same period. The department recorded more than 50,000 incidents since October, about 10,000 more than in the same period a year earlier, with an incident defined as any intrusion or attempted intrusion on a computer network.

The increase has prompted a new interest in cybersecurity on Capitol Hill, where lawmakers are being prodded by the Obama administration to advance legislation that could require new standards at facilities where a breach could cause significant casualties or economic damage.
It is not clear whether the higher numbers were due to increased reporting amid a wave of high-profile hacking, including the arrest last week of several members of the group Anonymous, or an actual increase in attacks.

James A. Lewis, a senior fellow and a specialist in computer security issues at the Center for Strategic and International Studies, a policy group in Washington, said that as hacking awareness had increased, attacks had become more common. He said that the attacks on the nation's infrastructure were particularly jarring.

"Some of this is heightened awareness because everyone is babbling about it," he said of the reported rise in computer attacks. "But much of it is because the technology has improved and the hackers have gotten better and people and countries are probing around more like the Russians and Chinese have."

He added: "We hit rock bottom on this in 2010. Then we hit rock bottom in 2011. And we are still at rock bottom. We were vulnerable before and now we're just more vulnerable. You can destroy physical infrastructure with a cyberattack just like you could with a bomb."

The legislation the administration is pressing Congress to pass would give the federal government greater authority to regulate the security used by companies that run the nation's infrastructure. It would give the Homeland Security Department the authority to enforce minimum standards on companies whose service or product would lead to mass casualties, evacuations or major economic damage if crippled by hackers.

The bill the administration backs is sponsored by Senators Joseph I. Lieberman, independent of Connecticut, and Susan Collins, Republican of Maine. It has bipartisan support, and its prospects appear good. Senator John McCain, Republican of Arizona, is sponsoring a more business-friendly bill that emphasizes the sharing of information and has fewer requirements for companies.

Last week on Capitol Hill, Janet Napolitano, the secretary of Homeland Security; Robert S. Mueller III, the director of the Federal Bureau of Investigation; and Gen. Martin E. Dempsey, the chairman of the Joint Chiefs of Staff, made their pitch to roughly four dozen senators about why they should pass the Lieberman-Collins bill.

At a closed-door briefing, the senators were shown how a power company employee could derail the New York City electrical grid by clicking on an e-mail attachment sent by a hacker, and how an attack during a heat wave could have a cascading impact that would lead to deaths and cost the nation billions of dollars.

"I think General Dempsey said it best when he said that prior to 9/11, there were all kinds of information out there that a catastrophic attack was looming," Ms. Napolitano said in an

interview. "The information on a cyberattack is at that same frequency and intensity and is bubbling at the same level, and we should not wait for an attack in order to do something."

General Dempsey told the senators that he had skipped a meeting of the National Security Council on Iran to attend the briefing because he was so concerned about a cyberattack, according to a person who had been told details of the meeting. A spokesman for General Dempsey said the chairman had "sent his vice chairman to the meeting on Iran so that he could attend the Senate meeting and emphasize his concern about cybersecurity."

"His point was about his presence at the cyber exercise rather than a value judgment on the 'threat,' " the spokesman, Col. David Lapan, said.

Experts say one of the biggest problems is that no part of the government has complete authority over the issue. The Central Intelligence Agency and the National Security Agency give the government intelligence on potential attacks, and the F.B.I. prosecutes hackers who break the law. The Department of Homeland Security receives reports about security breaches but has no authority to compel business to improve their security.

"Nobody does critical infrastructure of the dot-com space where America now relies on faith healing and snake oil for protection," Mr. Lewis said. "The administration wants it to be the Department of Homeland Security, but the department needs additional authorities to be effective."

Fonte: The New York Times, New York, 13 Mar. 2012, Internacional, On-line.

A utilização deste artigo é exclusiva para fins educacionais.