Bloomberg

China, Iran Boost Cyber Attacks on U.S., Lawmaker Says

By Eric Engleman - Feb 14, 2013

China and Iran are intensifying cyber assaults against the U.S., the head of the House Intelligence Committee said as he pressed for legislation to encourage companies to share information on hacker threats.

China's cyber espionage effort targeting U.S. industrial secrets "has grown exponentially both in terms of its volume and damage it's doing to our economic future," the intelligence panel's chairman, Mike Rogers, said at a hearing yesterday. "We have no practical deterrents in place today."

In a separate report on cyber risks to government computers, the Government Accountability Office said yesterday that cybersecurity incidents reported by U.S. agencies increased almost ninefold, to 48,562 in fiscal 2012 from 5,503 in 2006.

The incidents have "placed sensitive information at risk, with potentially serious impacts on federal and military operations; critical infrastructure; and the confidentiality, integrity, and availability of sensitive government, private sector, and personal information," the report said.

The GAO report found continuing weaknesses in the government's ability to assess cybersecurity risks and develop effective controls.

The Homeland Security Department has made "incremental progress" in coordinating the federal response to cyber incidents, while challenges remain in disseminating information among federal agencies and critical-infrastructure owners, and developing analysis and warning capability, the report said.

House Bill

Rogers, a Michigan Republican, and the committee's top Democrat, C.A. "Dutch" Ruppersberger of Maryland, reintroduced a bill on Feb. 13 to give legal protection for companies that share cyber threat information with each other and the government.

The bill passed the House last year but failed to advance in the Senate after President Barack Obama's

administration threatened a veto, saying the measure didn't go far enough to boost cyber defenses and failed to protect privacy of consumer data.

Obama issued an executive order this week directing the government to develop voluntary cyber standards for companies operating vital assets such as power grids and railway systems. It also instructs U.S. agencies to share more threat information with industry.

Cybersecurity has gained renewed attention in recent weeks with revelations about a security breach of a U.S. Federal Reserve website, intrusions at the New York Times and other news organizations attributed to Chinese hackers, and a wave of attacks on websites of U.S. banks.

'Inevitable' Breach

"It is reasonable to assume that, if an advanced attacker targets your company, a breach is inevitable," Kevin Mandia, chief executive officer of Mandiant Corp., an Alexandria, Virginia-based threat detection company that has investigated intrusions at the Times and Washington Post, said at the congressional hearing yesterday.

"That surprises many people, but it is the undeniable truth, and a direct result of the gap between our ability to defend ourselves and our adversaries' ability to circumvent those defenses," Mandia said.

Referring to the denial-of-service attacks against banks, Rogers said that in discussions with the private sector, "I heard nothing to dissuade me from the conclusion that the Iranian government is behind these attacks."

"You begin to see a pattern of steady, asymmetric, and often lethal Iranian attacks on the United States and our interests," Rogers said.

Sharing Information

Companies lack strong legal protections for sharing and receiving cyber threat information as well as guidance on how such information-sharing may be treated under antitrust laws, which hinders exchange of threat data within and across industries, John Engler, president of the Business Roundtable, an association of U.S. chief executive officers, said at the hearing.

The American Civil Liberties Union and other digital-rights groups renewed criticism of the Rogers-Ruppersberger bill, saying it allows companies to share sensitive personal information with the government, including military agencies. Rogers said his bill has "strong restrictions and safeguards" to protect privacy.

Caitlin Hayden, a White House spokeswoman, declined to comment on the bill, saying the administration doesn't want to prejudge the legislative process before a bill is ready for a vote.

Information-sharing improvements are essential and must include "proper privacy and civil liberties protections, reinforce the appropriate roles of civilian and intelligence agencies, and include targeted liability protections," Hayden said in an e-mail.

To contact the reporter on this story: Eric Engleman in Washington at eengleman1@bloomberg.net

To contact the editor responsible for this story: Bernard Kohn at bkohn2@bloomberg.net