What's government's role in making the Web secure?

September 27 2009, By LOLITA C. BALDOR , Associated Press Writer

FILE - In this July 8, 2009 file photo, an employee of Korea Internet Security Center works at a monitoring room in Seoul, South Korea. There is no kill switch for the Internet, no secret on-off button in an Oval Office drawer. Yet when Congress was exploring ways to secure computer networks, a plan to give the president the power to shut down Internet traffic to Web sites in an emergency set off alarms. Corporate leaders and privacy advocates protested the idea earlier this year, saying the government must not seize control. (AP Photo/Ahn Young-joon, FILE)

(AP) -- There is no kill switch for the Internet, no secret on-off button in an Oval Office drawer.

Yet when a Senate committee was exploring ways to secure computer networks, a provision to give the president the power to shut down Internet traffic to compromised Web sites in an emergency set off alarms.

Corporate leaders and privacy advocates quickly objected, saying the government must not seize control of the Internet.

Lawmakers dropped it, but the debate rages on. How much control should federal authorities have over the Web in a crisis? How much should be left to the private sector? It does own and operate at least 80 percent of the Internet and argues it can do a better job.

"We need to prepare for that digital disaster," said Melissa Hathaway, the former White House cybersecurity adviser. "We need a system to identify, isolate and respond to cyberattacks at the speed of light."

So far at least 18 bills have been introduced as Congress works carefully to give federal authorities the power to protect the country in the event of a massive cyberattack. Lawmakers do not want to violate personal and corporate privacy or squelching innovation. All involved acknowledge it isn't going to be easy.

For most people, the Internet is a public haven for free thought and enterprise. Over time it has become the electronic control panel for much of the world's critical infrastructure. Computer networks today hold government secrets, military weapons specifications, sensitive corporate data, and vast amounts of personal information.

Millions of times a day, hackers, cybercriminals and mercenaries working for governments and private entities are scanning those networks, looking to defraud, disrupt or even destroy.

Just eight years ago, the government ordered planes from the sky in the hours after the Sept. 11 terrorist attacks.

Could or should the president have the same power over the Internet in a digital disaster?

If hackers take over a nuclear plant's control system, should the president order the computer networks shut down? If there's a terrorist attack, should the government knock users off other computer networks to ensure that critical systems stay online? And should the government be able to dictate who companies can hire and what they must do to secure the networks that affect Americans' daily life.

Government officials say the U.S. must improve efforts to share information about cyberthreats with private industry. They also want companies to ensure they are using secure software and hiring qualified workers to run critical systems.

Much like the creation of the Department of Homeland Security, cybersecurity has attracted the interest of a number of House and Senate committees, all hoping to get a piece of the oversight power:

-Bills in the House Homeland Security Committee bills would protect the electric grid and require the department to secure its networks.

-The Senate Homeland Security and Government Reform Committee is writing legislation aimed largely at federal agencies.

-The Senate Commerce, Science and Transportation Committee is working on a bill that promotes public awareness and technical education, raises the planned White House cyberadviser to a Cabinet-level position and calls for professional cyberstandards. An early draft would have given the president the power to shut down compromised federal or critical networks in an emergency.

Bloggers howled that the government was taking over the Internet.

Business leaders protested, and Senate aides reworked the bill. Early versions of the second draft are more vague, giving the president only the authority to "direct the national response" to a cyberthreat.

Committee spokeswoman Jena Longo said the bill "will not empower a government shutdown or takeover of the Internet and any suggestion otherwise is misleading and false."

She said the president has the constitutional authority to protect the American people and direct the response to a crisis - including "securing our national cyberinfrastructure from attack."

Privacy advocates say the government has not proven it can do a better job securing networks than the private sector.

"The government needs to get its own cybersecurity house in order first before it tries to tell the private sector what to do," said Gregory T. Nojeim, senior counsel for the Center for Democracy and Technology.

Nojeim said the Senate Commerce Committee bill appears to leave "tough questions to the president, and that isn't comforting because some presidents will answer those questions in troubling ways."

U.S. officials acknowledge that their networks are scanned or attacked millions of times a day. Spies have breached the electrical grid. In July, hackers simultaneously brought down several U.S. government Web sites and sites in South Korea.

Home computers are targets, too. A study by security software provider McAfee Inc. says as many as 4 million computers are newly infected each month and turned into "botnets" - armies of computers used by someone without their owners' knowledge. As many as 10 percent of the world's computers might be unknowingly infected.

Shutting down a compromised system may sound like a good idea, but "it's not like the Internet has an on-off switch somewhere you can press," said Franck Journoud, manager of information security policy for the Business Software Alliance.

Most industries are federally regulated, so the government should work within those systems to plan for disasters, said Journoud, whose group has met with lawmakers and the White House on cyberpolicies.

Rather than setting minimum standards, business groups say the U.S. should endorse existing voluntary industry ones.

Cyberexperts also argue that when hackers infiltrate a critical network, the solution is not to shut down the system, but to isolate and filter out the offending computer codes.

Private companies are willing and able to protect their systems without government mandates, said Tom Reilly, president of ArcSight, a cybersecurity software company. He said the government should concentrate on protecting critical infrastructure and data privacy, and promote education on cybersecurity.

"People want to know if they are one of the 10 percent of the computers that are infected," he said. "They just don't know what to do. Most people just hope they're one of the other nine."

On the Net:

Senate committees: http://tinyurl.com/2q9q3

House committees: http://www.house.gov/

Center for Democracy and Technology: http://www.cdt.org/

Citation: What's government's role in making the Web secure? (2009, September 27) retrieved 27 April 2024 from https://phys.org/news/2009-09-role-web.html