A divided Congress confronts a rising cyberthreat

April 22 2012, By RICHARD LARDNER and DONNA CASSATA , Associated Press

This Sept. 30, 2011 file photo shows a reflection of the Department of Homeland Security logo in the eyeglasses of a cybersecurity analyst at the watch and warning center of the Department of Homeland Security's secretive cyber defense facility in Idaho Falls, Idaho. The center is tasked with protecting the nation's power, water and chemical plants, electrical grid and other facilities from cyber attacks. (AP Photo/Mark J. Terrill, File)

(AP) -- The mysterious caller claimed to be from Microsoft and offered step-by-step instructions to repair damage from a software virus. The electric power companies weren't falling for it.

The caller, who was never traced or identified, helpfully instructed the companies to enable specific features in their computers that actually would have created a trapdoor in their networks. That vulnerability

would have allowed hackers to shut down a plant and thrown thousands of customers into the dark.

The power employees hung up on the caller and ignored the advice.

The incident from February, documented by one of the government's emergency cyber-response teams, shows the persistent threat of electronic attacks and intrusions that could disrupt the country's most critical industries.

The House this coming week will consider legislation to better defend these and other corporate networks from foreign governments, cybercriminals and terrorist groups. But deep divisions over how best to handle the growing problem mean that solutions are a long way off.

Chief among the disputes is the role of the government in protecting the private sector.

The U.S. Chamber of Commerce and other business groups oppose requiring cybersecurity standards. Rules imposed by Washington would increase their costs without reducing their risks, they say.

Obama administration officials and security experts say companies that operate power plants, communication systems, chemical facilities and more should have to meet performance standards to prove they can withstand attacks or recover quickly from them.

The rift echoes the heated debate in Washington over the scope of government and whether new regulations hamper private businesses.

Homeland Security Secretary Janet Napolitano said Friday that without standards for critical industries, there will be gaps that U.S. adversaries can exploit. "That system, which is mostly in private hands, needs to all

come up to a certain baseline level," she said.

The proposed formation of a system that allows U.S. intelligence agencies and the private sector to share information about hackers and the techniques they use to control the inner workings of corporate networks also is contentious.

Civil libertarians and privacy advocates worry that a bill written by the Republican chairman and top Democrat on the House intelligence committee would create a backdoor surveillance system by giving the secretive National Security Agency access to private sector data.

The agency, based at Fort Meade, Md., is in charge of gathering electronic intelligence from foreign governments but is barred from spying on Americans. Army Gen. Keith Alexander, the NSA's director, also heads the Pentagon's Cyber Command, which protects military networks.

"The question is whether this is a cybersecurity bill or an intelligence bill," said Leslie Harris, president of the nonprofit Center for Democracy and Technology. "There is just a fundamental debate over what role the National Security Agency should have in protecting civilian networks."

Intelligence agencies say the bill grants no new power to the NSA or the Defense Department to direct any public or private cybersecurity programs. But committee leaders said they are open to making changes to ease the privacy concerns as long as the alterations don't undermine the goals of the bill.

Businesses including Facebook and the Edison Electric Institute support the bill because it leaves it to individual companies and industries to decide how best to prevent attacks.

House Republicans last week scaled back a separate piece of legislation that would have given the Department of Homeland Security and other federal agencies responsibility for ensuring that critical industries met security performance standards. But those requirements were dropped from the bill during a meeting of the House Homeland Security Committee.

Rep. Jim Langevin, co-chairman of the Congressional Cybersecurity Caucus, said the bill was "gutted" because the House Republican leadership sided with business interests opposed to regulations. "We cannot depend on the good intentions of the owners and operators of infrastructure to secure our networks," said Langevin, D-R.I.

The GOP-led House appears to be heading for a showdown with the Democratic-run Senate over an approach on cybersecurity.

A bill sponsored by Sens. Joe Lieberman, I-Conn., and Susan Collins, R-Maine, would give Homeland Security the authority to establish set security standards. Their bill is backed by the Obama administration but it remains stalled in the Senate.

The legislation faces stiff opposition from senior Senate Republicans.

Arizona's John McCain, the top Republican on the Senate Armed Services Committee, said during a hearing last month that the Homeland Security Department is "probably the most inefficient bureaucracy that I have ever encountered" and is ill-equipped to determine how best to secure the nation's essential infrastructure. McCain has introduced a competing bill.

There is little disagreement over damage from cyberattacks.

China and Russia are the most proficient at cyber-espionage, according

to U.S. officials who last year accused the two countries of being "aggressive and capable collectors of sensitive U.S. economic information and technologies."

Rear Adm. Samuel Cox, Cyber Command's director of intelligence, said U.S. adversaries are developing cyberweapons at a rapid pace. Unlike the traditional tools of war, there is no technological ceiling for cyberweapons that can cause computers to crash or become hijacked remotely and lead to serious economic damage.

"There is no end in sight," Cox said. "It's not like, `Well, they're going to reach a limit as to how bad these things could be.'"

If the House intelligence committee's bill becomes law, companies could get "cyberthreat" information and intelligence from the government that would allow them to identify hackers by their electronic signatures and Internet addresses. With that data, which is collected by the NSA, businesses could block attacks or stop them before they do serious damage. Companies would be encouraged to give the government information about attacks but there is no requirement to do so.

The bill would exempt companies that act "in good faith" from liabilities that might come from protecting their own networks or sharing information with the government.

But one expert on the computer systems that monitor and control power grids, oil refineries and chemical plants said critical industries won't provide federal agencies with much because they don't trust the government. Joe Weiss, a nuclear engineer and managing partner of the consulting firm Applied Control Solutions, said another catch is that few companies do the forensic work necessary to understand why a failure occurred and whether it was an attack or simply a software malfunction.

"What information are you going to share," Weiss said, "when you don't even know you've had a problem?"