Dumbass US Threatens Conventional Military Response Against Cyber Attacks

by lynx *Monday, Oct 22 2012, 11:45am*
international / prose / post

> There's only one 'minor' problem, the source of expert cyber attacks cannot be traced, so whose chimney is gonna attract the missiles?

The linked article is probably the most lame threat the US has ever made. In the orthodox theatre of war America and it allies can't even claim victory over a bunch of tribals in Afghanistan and Pakistan, what hope have they got fighting sophisticated invisible hackers and digital warriors on the net?

The hysterical US threat actually plays nicely into the hands of hackers who specialise in subterfuge and in creating false leads/targets -- now how would you feel if you were a highly armed military on the receiving end of missile attacks from dumbass Yanks that imagine they have traced a cyber attack to your nation?

This latest development from mental leper, Panetta, is just too perfect, watch out that hackers don't start WWIII -- you incredibly stupid Washington DUNCES!

Report from The Times of Israel follows:

> **White House taking steps to thwart cyberterrorism attacks [in their dreams]**
> by Richard Ladner
>
> WASHINGTON (AP) — A new White House executive order would direct U.S. spy agencies to share the latest intelligence about cyberthreats with companies operating electric grids, water plants, railroads and other vital industries to help protect them from electronic attacks, according to a copy obtained by The Associated Press.
>
> The seven-page draft order, which is being finalized, takes shape as the Obama administration expresses growing concern that Iran could be the first country to use cyberterrorism against the United States. The military is ready to retaliate if the U.S. is hit by cyberweapons, Defense Secretary Leon Panetta said. But the U.S. also is poorly prepared to prevent such an attack, which could damage or knock out critical services

that are part of everyday life.

The White House declined to say when the president will sign the order.

The draft order would put the Department of Homeland Security in charge of organizing an information-sharing network that rapidly distributes sanitized summaries of top-secret intelligence reports about known cyberthreats that identify a specific target. With these warnings, known as tear lines, the owners and operators of essential U.S. businesses would be better able to block potential attackers from gaining access to their computer systems.

An organized, broad-based approach for sharing cyberthreat information gathered by the government is widely viewed as essential for any plan to protect U.S. computer networks from foreign nations, terrorist groups and hackers. Existing efforts to exchange information are narrowly focused on specific industries, such as the finance sector, and have had varying degrees of success.

Yet the order has generated stiff opposition from Republicans lawmakers who view it as a unilateral move that bypasses the legislative authority held by Congress.

Administration officials said the order became necessary after Congress failed this summer to pass cybersecurity legislation, leaving critical infrastructure companies vulnerable to a serious and growing threat. Conflicting bills passed separately by the House and Senate included information-sharing provisions. But efforts to get a final measure through both chambers collapsed over the Republican's concerns that the Senate bill would expand the federal government's regulatory power and increase costs for businesses.

The White House has acknowledged that an order from the president, while legally binding, is not enough. Legislation is needed to make other changes to improve the country's digital defenses. An executive order, for example, cannot offer a company protection from liabilities that might result from a cyberattack on its systems.

The addition of the information-sharing provisions is the most significant change to an earlier draft of the order completed in late August. The new draft, which is not dated, retains a section that requires Homeland Security to identify the vital systems that, if hit by cyberattack, could "reasonably result in a debilitating impact" on national and economic security. Other sections establish a program to encourage companies to adopt voluntary security standards and direct federal agencies to determine whether existing cyber security regulations are adequate.

The draft order directs the department to work with the Pentagon, the National Security Agency, the director of national intelligence and the Justice Department to quickly establish the information-sharing mechanism. Selected employees at critical infrastructure companies would receive security clearances allowing them to receive the information, according to the document. Federal agencies would be required to assess whether the order raises any privacy or civil liberties risks.

To foster a two-way exchange of information, the government would ask businesses to tell the government about cyberthreats or cyberattacks. There would be no requirement to do so.

The NSA has been sharing cyberthreat information on a limited basis with companies that conduct business with the Defense Department. These companies work with sensitive data about weapon systems and technologies and are frequently the targets of cyberspying.

But the loss of valuable information has been eclipsed by fears that an enemy with the proper know-how could cause havoc by sending the computers controlling critical infrastructure systems incorrect commands or infecting them with malicious software. Potential nightmare scenarios include high-speed trains being put on collision courses, blackouts that last days or perhaps even weeks or chemical plants that inadvertently release deadly gases.

Panetta underscored the looming dangers during a speech last week in New York by pointing to the Shamoon virus that destroyed thousands of computer systems owned by Persian Gulf oil and gas companies. Shamoon, which spreads quickly through networked computers and ultimately wipes out files by overwriting them, hit the Saudi Arabian state oil company Aramco and Qatari natural gas producer RasGas.

Panetta did not directly connect Iran to the Aramco and RasGas attacks. But U.S. officials believe hackers based in Iran were behind them.

Shamoon replaced files at Aramco with the image of a burning U.S. flag and rendered more than 30,000 computers useless, Panetta said. The attack on RasGas was similar, he said.

A spokeswoman for the National Security Council, Caitlin Hayden, said the administration is consulting with members of Congress and the private sector as the order is being drafted. But she provided no information on when an order would be signed. “Given the gravity of the threats we face in cyberspace, we want to get this right in addition to getting it done swiftly,” she said.

© 2012 The Associated Press.

http://www.timesofisrael.com/white-house-taking-steps-to-meet-cyberterrorism-attacks/
