

If this is cyber war, possible U.S responses are limited

By Pauline Jelinek, Associated Press 07/10/09

WASHINGTON (AP) -- A lot of people are saying this is cyber war. But if the Internet attack on U.S. Web sites was an assault by North Korea or some other foreign government, what good responses are in America's arsenal?

"The short answer is probably 'Not a heck of a lot,'" says James Lewis, a senior fellow at the Center for Strategic and International Studies.

Defense and cyber analysts said Thursday that chances are high that very little eventually will be done to whoever orchestrated several days of attacks against Web sites including the White House and Pentagon as well as sites in South Korea. That's largely because the investigation is unlikely to figure out who did it.

But even if it's determined that another nation was behind the attacks, the possible responses are hardly warlike: trade sanctions, diplomatic protests or a complaint before the United Nations.

"You could eject an attache, recall your ambassador and throw out their ambassador," Lewis said. That's not possible with North Korea, he noted of a main suspect in the attacks, since Pyongyang doesn't have an embassy in the U.S.

But war? Military action? No one is talking about that. Any punishment needs to fit the crime, analysts said, and this doesn't meet the threshold of an act of war.

"I don't think this kind of attack merits the use of force," said Kristin Lord, national security expert at the Center for a New American Security.

"It's annoying, a little embarrassing, but it's not a big deal," Lewis said, meaning that no major damage was done.

But others think retaliation might be called for, strong enough to send a stiff message, perhaps even a similar dose of the U.S. military's secret offensive cyber capability.

U.S. officials routinely refuse to talk about either computer defenses or computer attacks America might have launched. But U.S. offensive cyber retaliation could range from a passive intrusion such as listening in on a foe's communications to an attack that cripples an enemy's air defense systems to clear the way for a bomber attack.

A counterstrike on an attacker's computer network could be launched, Lewis said, but it would be extremely difficult.

"This is a gray area," said Stewart Baker, who worked on cyber security at the Department of Homeland Security. "But if you know that the North Koreans were doing this, then at a minimum I would have thought you'd be entitled to do the same thing to them to show that you didn't like it."

If the attacks caused harm to anyone "you get more serious, and start thinking and talking about it as an act of

war or at least state-sponsored violence," said Michael O'Hanlon, a defense analysts at the Brookings Institution.

Though the recent computer attacks are considered by many cyber experts to be little more than a nuisance to public Web sites, the incident raised anew old criticism that the U.S. government's policies on cyber warfare are shrouded in secrecy, ill-formed and require broad public debate.

"There's a lot of thinking that needs to be done about how to respond to attacks like this and what the threshold is for responding to cyber attacks, with other means, whether they be economic sanctions or even military force," Lord said.

The assault involved more than 100,000 "zombie" computers, used by someone without their owners' knowledge and linked together in a network known as a "botnet." Most of those computers were in South Korea, but others were in Japan, China, the U.S. and possibly other countries.

"If you shoot back at the computers that actually launched the attack, then you're hitting third parties who probably don't even know they were involved," Lewis said.

"And if you go out over the networks to strike back at Pyongyang, how can you be sure you're not accidentally going to also take down Japan at the same time?"

Said Lewis: "You could end up shooting the wrong guy."

COMMENT ON THIS ARTICLE IN THE FORUM

© 2009 BY NATIONAL JOURNAL GROUP, INC. ALL RIGHTS RESERVED