CONGRESS, INTEL & CYBER, STRATEGY & POLICY

CyberCom Chief Alexander Lays Down Cyber Red Line; Destroy A Network, Risk War

By COLIN CLARK
on February 27, 2014 at 4:35 PM

CAPITOL HILL: On the day that China's president took personal charge of his country's new cyber body, pledging to make the People's Republic of China a "cyber power," the outgoing head of America's Cyber Command laid out a clear red line that, if crossed, could lead to war.

"If it destroys government or other networks, I think it would cross that line," Army Gen. Keith Alexander, head of both Cyber Command and the National Security Agency, told the Senate Armed Services Committee today when asked what level of cyber "attack" would potentially cause America to go to war.

The question of what might spark a war in the event of cyber intrusions is extremely sensitive. For most of the last 15 years the United States denied it even possessed offensive cyber capabilities to respond to an attack, although we have had them for at least most of the last decade. Drawing red lines is always a highly sensitive exercise for the military. On the one hand, deterrence requires that potential enemies know we will not tolerate certain behaviors and have a reasonably clear idea of what will happen to them should they cross those lines. On the other hand, strategic

ambiguity is often extremely useful in that it increases the uncertainties a potential enemy faces and must consider before acting. Alexander's comment eliminates some of that ambiguity and appears to be a sign of just how important he and other military leaders believe the threat is and how important imparting a clear message is to those we would deter.

The Chinese government, in particular, regularly probes US networks and engages — as do we — in extensive cyber espionage.

In other news from this morning's hearing, Gen. Alexander reiterated his belief that "we're getting to that stage" when asked if he thought Cyber Command should be elevated to a full combatant command alongside the nine existing COCOMs. Today, it sits underneath Strategic Command. "I think, from an operational consideration that's something they will need to consider in the next year or so," he said. The most important reason for the elevation? "I do get conceded that, in the event of an attack, having a streamlined chain of command is going to be important."

A prime example of the sort of cyber attacks in which America might engage came up at the beginning to the SASC hearing when Chairman Carl Levin asked the head of Strategic Command, Adm. Cecil Haney, about a New York Times story reporting that America has been planning sophisticated cyber attacks on Syrian President Hafez al Assad and his government.

"I assume you were in the middle of those discussions," Levin asked. "Yes sir," replied Haney, appearing to confirm the story.

The final bit of news from the hearing: Haney may have confirmed that the SSBN(X) replacement for the Ohio-class nuclear submarines is funded in the new budget. "We have delayed the Ohio replacement-class submarines to the point that we can no longer delay them," he said.

So as kabuki-like as congressional hearings came become, there are gold nuggets of information we can glean from them. Compare and contrast the Chinese opera that comes out of Beijing. My favorite quote from Xhinua's story about the Chinese president's cyber commitment? "Cyberspace should be made clean and chipper," Xi said. Chipper. Ya can't beat that!

Topics: Adm. Cecil Haney, China, cyber command, cyber warfare, cybersecurity, deterrence, Gen. Keith Alexander, National Security Agency, nsa, offensive cyber warfare, Sen. Carl Levin, Senate Armed Services Committee, Strategic Command