US eyes cyber 'deterrence' to stop hackers (Update)

October 28 2014, by Rob Lever

The US military is looking to flex its muscles in cyberspace as a "deterrence" to hackers eying American targets, the nation's top cyber-warrior said Tuesday.

Admiral Mike Rogers, who heads the Pentagon's Cyber Command as well as the National Security Agency, evoked a policy often put forward for avoiding nuclear warfare, because holding powerful weapons is seen as a deterrent.

Rogers said that as part of his role as the head of Cyber Command, he wants to send a message to potential cyber-attackers that there are consequences for their actions.

"Right now, if you are a nation-state, if you are a group, if you are an individual, my assessment is that most (hackers) come to the conclusion that it is incredibly low-risk, that there is little price to pay for the actions that they are taking," Rogers told a cybersecurity conference at the US Chamber of Commerce in Washington.

"I'm not saying I agree with that but I believe most look at that and in light of that feel that they can be pretty aggressive. That's not in our best interests in the long term as a nation to have that perception. We need to try to change that over time."

Offensive tools in cyberspace

Rogers said the US military has a "legal framework" for the use of any offensive cyber-weapons, noting that a decision to use these tools needs approval from the president and secretary of defense.

But he said US officials are in the midst of discussions on defining offensive military actions in cyberspace and how to implement them.

"What I hope we can develop over time is a set of norms and rules that get us into an area where we can get a better definition of what is acceptable and what is not acceptable (in cyberspace), and even into the idea of deterrence," he told the conference.

The comments came the same day that security researchers, in two separate reports, said the Russian and Chinese governments are likely behind widespread cyber-espionage that has hit targets in the United States and elsewhere.

One team of researchers led by the security firm Novetta Solutions said it identified a hacker group believed to act "on behalf of a Chinese government intelligence apparatus."

A separate report by the security firm FireEye said a long-running effort to hack into US defense contractors, Eastern European governments and European security organizations is "likely sponsored by the Russian government."

The Chinese group, which was dubbed Axiom, "is a well-resourced, disciplined and sophisticated cyber-espionage group operating out of mainland China," Novetta chief executive Peter LaMontagne said in a statement released with the study.

The report said the firms went beyond simply collecting information and cooperated on a "coordinated, effective remediation and disruption" of

the Chinese networks.

"Novetta feels that the unified approach... provides the highest level of visibility and establishes the foundation necessary to effectively counter a threat of this nature," the report said.

Striking back?

Rogers did not specifically comment on Axiom but said he is generally cautious on the use of "cyber-mercenaries" who retaliate against hackers.

"I would urge you to be very careful about going down that road," he told the conference.

"I often get asked this question about 'cyber-mercenaries,'" or private-sector players who seek to take out hacking threats.

"My input to you would be to be very careful about that," Rogers said. "It really potentially opens you up for a whole range of complications."