Source: http://federalnewsradio.com/cybersecurity/2016/05/senator-wants-definition-cyber-act-war/

Senator wants definition on cyber act of war

By Scott Maucione (http://federalnewsradio.com/author/scott-maucione/) | @smaucioneWFED (https://twitter.com/smaucioneWFED)
May 9, 2016 1:31 pm

The United States is constantly attacked in the cyber realm, but when do those attacks mean war?

Sen. Mike Rounds (R-S.D.) is trying to find an answer to that question in a new bill (http://www.rounds.senate.gov/imo/media/doc/Bill,%20NDAA%202017%20Related,%20Cyber%20Act%20of%20War.pdf) introduced May 9.

The Cyber Act of War Act of 2016 would require the President to develop a policy to determine whether a cyber attack constitutes an act of war.

Sen. Mike Rounds (R-S.D.)

The proposal is an extension of a battle fought between the Obama administration and the Senate Armed Service Committee late last year over the White House's lack of cyber deterrence policy.

The bill requires the White House to compare how a cyber attack may be equivalent to conventional weapons in destruction of causalities when evaluating the attack as an act of war.

"Cyber attacks on our critical infrastructure are capable of impacting our entire economy and causing significant destruction. This legislation would require the executive branch to define which of these actions constitute a cyber act of war, which would allow our military to be better able to respond to cyber-attacks and deter bad actors from attempting to attack us in the first place," Rounds said in a May 9 statement.

The bill must first make it through the Senate Armed Services Committee before being considered by the Senate as a whole.

Federal News Radio contacted the committee about its intentions for the bill, but did not receive a response in time for publication.

The bill comes as attacks on critical infrastructure in the United States are on the rise. The Industrial Control System Cyber Emergency Response Team reported 295 cyber incidents involving critical infrastructure in 2015, that's compared to 245 in 2014.

In December, the Obama administration released a cyber deterrence policy (http://federalnewsradio.com/cybersecurity/2015/12/white-house-finally-acquiesces-congress-cyber-deterrence-policy/) outlining how the U.S. will respond to cyber attacks from malicious actors.

It explains how the Defense Department would pursue law enforcement measures, sanction malicious cyber actors, conduct offensive and defensive cyber operations and use military force to respond to cyber attacks.

The policy goes further in saying it is in the United States' interest to assist other countries in building the capacity to combat cybercrime.

Even before the White House released the policy, DoD maintained it had mechanisms to properly deal with cyber attacks.

During a Sept. 29, 2015, Senate Armed Services Committee hearing, Deputy Defense Secretary Bob Work said DoD does have a cyber strategy (http://federalnewsradio.com/defense/2014/10/dod-to-be-more-transparent-about-strategy-to-deter-cyber-attacks/), but not a policy per se.

"That does not mean if we had an attack tonight that we do not have the structure in place right now with the national security team to get together to try and understand who caused the attack, to understand what the implications of the attack were and what response we should take," Work said. "Those are in place right now."

Some senators were not impressed by the deterrence policy, however.

The policy is "wholly-lacking any new information about the administration's plan to integrate ends, ways, and means to meaningfully deter attacks in cyber space. It mostly reiterates steps taken and pronouncements made over the past few years, all of which we know have failed to deter our adversaries or decrease the vulnerability of our nation in cyber space," Senate Armed Services Chairman John McCain (R-Ariz.) said in a statement.

Rounds' bill may force the administration to further define or at least be more transparent about its cyber policies.