05.09.16

Rounds Will Introduce Bill Requiring Administration to Define a Cyber Act of War

WASHINGTON—U.S. Senator Mike Rounds (R-S.D.), a member of the Senate Armed Services Committee (SASC), today will introduce the *Cyber Act of War Act of 2016*. The *Cyber Act of War Act of 2016* would require the administration to develop a policy to determine whether a cyber-attack constitutes an act of war.

"With the Internet playing a major role in nearly every aspect of our lives, we not only face the threat of losing our personal information online, but we are at risk of having our daily lives interrupted by cyber-attacks that have the ability to cripple our power grid, water supplies and communications networks," said Rounds. "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."

During a February 9, 2016, SASC hearing, Rounds questioned Director of National Intelligence James Clapper, Jr., and Lt. Gen. Vincent Stewart, Director of the Defense Intelligence Agency, about whether it would be helpful to define an act of war in cyber space. Lt. Gen. Stewart responded, "I think it would be extremely helpful to have clear definitions of what constitutes cyber events versus acts of war…if we get much fuller definition of the range of things that occur in cyber space, and then start thinking about the threshold where an attack is catastrophic enough or destructive enough that we define it as an act of war, I think that would be extremely useful." Video of the full exchange is available here.

The *Cyber Act of War Act of 2016* would require that in developing the policy for determining when an action carried out in cyberspace constitutes an act of war against the United States, the administration would be required to consider:

- the ways in which the effects of a cyber-attack may be equivalent to effects of an attack using conventional weapons, for example with regard to physical destruction or casualties; and
- intangible effects of significant scope, intensity or duration.

It would also require the Department of Defense to include this definition in its Law of War Manual.

###

Related Files

Bill, NDAA 2017 Related, Cyber Act of War.pdf