Written by Yaron Vorona
Thursday, 24 January 2013 00:00

In an address last year, Harold Hongju Koh, Legal Advisor to the U.S. Department of State asserted that a cyber attack can be considered to be an act of war, and reserves the right to respond with force.

Excerpt:

Question 3: Do cyber activities ever constitute a use of force?

Answer 3: Yes. Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law. In analyzing whether a cyber operation would constitute a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes. Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.

Question 4: May a State ever respond to a computer network attack by exercising a right of national self-defense?

Answer 4: Yes. A State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof. As the United States affirmed in its 2011 International Strategy for Cyberspace, "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."

Read More