U.S. officials in recent weeks have given stark descriptions of the threat to the United States and other countries from cyberattacks and have provided new details on the principles that they say will govern U.S. behavior in responding to the threat.

Separately, officials from more than 60 countries met in Budapest as part of a continuing effort to craft norms for state conduct in cyberspace.

In an Oct. 11 speech in New York City to Business Executives for National Security, Defense Secretary Leon Panetta said the United States faces a real danger of cyberattacks from state and nonstate actors. An attack “could be as destructive as the terrorist attack on 9/11” and “could virtually paralyze the nation,” he said.

He stressed the need to develop offensive capabilities to defend the United States, its allies, and its interests. He said the United States would conduct cyberoperations only “in a manner that is consistent with the policy principles and legal frameworks” to which the Defense Department adheres “for other domains, including the law of armed conflict.”

Some countries do not share the U.S. position that existing international laws should apply to cyberspace. China and Russia have argued that new rules and laws need to be created. In September 2011, the two countries submitted to the UN General Assembly a proposal for a code of conduct in cyberspace. The proposed code calls for states to respect domestic laws and sovereignty and to settle disputes within the framework of the United Nations. (See ACT, November 2011.)

The Defense Department cyberspace strategy released in July 2011 says current international law applies to cyberspace as it does to air, land, sea, and space. Exactly how existing international law fits cyberspace has been the subject of many discussions. In Sept. 18 remarks at a U.S. Cyber Command interagency legal conference in Fort Meade, Maryland, State Department legal adviser Harold Koh clarified several aspects of the U.S. approach.

“[C]yberactivities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force,” he said, and “if the physical consequences of a cyberattack work the kind of physical damage that dropping a bomb or firing a missile would, that cyberattack should equally be considered a use of force.” A U.S. response to cyberactivities would not have to take place in cyberspace as long as the response “meets the requirements of necessity and proportionality,” he said.

Meanwhile, in remarks at an Oct. 4-5 conference in Budapest on cyberspace, British Foreign Secretary William Hague called “for a new international consensus on rules of the road to guide future behavior in cyberspace and to combat the worst abuses of it.”

He made similar remarks at a conference held in London in November 2011, where government officials and members of nongovernmental organizations established a goal of developing norms for state behavior in cyberspace. (See ACT, December 2011.) No specific details were released in Budapest to indicate that the international community had moved closer to that goal.
The Budapest meeting was the first of at least two planned follow-ups to the London conference; the second is scheduled to take place in Seoul in 2013.

In an Oct. 11 interview with Arms Control Today, a U.S. State Department official said the value of the international conferences lies in broadening the topics of the conversation on cyberspace norms and bringing more participants into the conversation.

The United States views the conferences as complementing the ongoing diplomatic discussions over establishing international norms for state behavior in cyberspace in other venues, such as the UN group of governmental experts on information technology, the Organization for Security and Cooperation in Europe, and the regional forums of the Association of Southeast Asian Nations, the official said.

At the Budapest conference, Hague said he did not support the idea of a treaty establishing rules for state conduct in cyberspace, arguing that such a treaty “would be cumbersome to agree, hard to enforce, and too narrow in its focus.”

Hungarian Foreign Minister János Martonyi, who chaired the conference, said in his closing remarks that “existing rules of international law and the traditional norms governing interstate relations apply to cyberspace,” a position seemingly similar to the one expressed by British and U.S. officials.

In an October e-mail exchange with Arms Control Today, Paul Meyer, a former Canadian ambassador to the Conference on Disarmament and a member of a panel at the Budapest conference, said, “One of the issues with the London and subsequent conferences of this type is that there is no ‘deliverable’ beyond the Chairman’s summation under his own authority.”

In his remarks at the conference, Meyer decried “the relative dearth of preventive diplomacy and the apparent dominance of militarized approaches to achieving security in cyberspace.”

Posted: November 2, 2012

Source URL: https://www.armscontrol.org/act/2012_11/US-Officials-Detail-Cyber-Policy