US fails to renegotiate arms control rule for hacking tools

December 19 2016, by Tami Abdollah

The Obama administration has failed to renegotiate portions of an international arms control arrangement to make it easier to export tools related to hacking and surveillance software—technologies that can be exploited by bad actors, but are also used to secure computer networks.

The rare U.S. move to push for revisions to a 2013 rule was derailed earlier this month at an annual meeting in Vienna, where officials from 41 countries that signed onto it were meeting. That leaves it up to President-elect Donald Trump's administration whether the U.S. will seek revisions again next year.

U.S. officials had wanted more precise language to control the spread of such hacking tools without the unintended negative consequences for national cybersecurity and research that industry groups and lawmakers have complained about for months. Critics have argued that the current language, while well meaning, broadly sweeps up research tools and technologies used to create or otherwise support hacking and surveillance software.

Rep. Jim Langevin, D-R.I., said in a statement Monday that he is "deeply disappointment" by the plenary's decision and hoped the incoming administration will continue the effort. Langevin co-chairs the Congressional Cybersecurity Caucus.

"U.S. cybersecurity and that of our allies will be imperiled if companies and researchers are not able to quickly share defensive tools," said

Langevin, who co-chairs of the Congressional Cybersecurity Caucus.

The White House referred questions Monday to the State and Commerce departments, neither of which responded to requests for comment.

As one of those 41 member countries of the 1996 Wassenaar Arrangement, which governs the highly technical world of export controls for arms and certain technologies, the United States agreed to restrict tools related to cyber "intrusion software" that could fall into the hands of repressive regimes.

The voluntary arrangement relies on unanimous agreement to abide by its rules on export controls for hundreds of items, including arms such as tanks or military aircraft and "dual-use" technologies such as advanced radar that can be used for both peaceful and military means.

The failed effort was a "bummer" said Katie Moussouris, CEO and founder of Luta Security who was part of this year's Wassenaar delegation as a U.S. industry expert.

"If anybody understands how quickly you need to respond to a fire, this would essentially impede the internet's firefighters if it was left in place," Moussouris said. But she also noted that such work involving an international body also can take time and finding precise language is critical.

The plenary did agree to tighten up language essentially specifying that the rule should apply to attacker code used to command and control malware, not regular computer defense tools that might have been caught in the rule, Moussouris said.

Efforts to come up with a workable U.S. rule have highlighted the difficulty of applying the export controls restricting physical items to a

virtual world that relies on the free flow of information for network security. Many companies operate in multiple countries and routinely employ foreign nationals who test their own corporate networks across borders.

The difficulties with the rule came to light in May 2015 after the Commerce Department's Bureau of Industry and Security began working on its rule to abide by the arrangement and proposed denying the transfer of offensive tools—defined as software that uses "zero-day" exploits, or unpatched new vulnerabilities, and "rootkit" abilities that allow a person administrator-level access to a system.

Because in the cyber world testing a network often requires determining first how to exploit it and attempting to do so.

"Exploit code today is relatively routinely shared for purposes of security research and identifying and mitigating security vulnerabilities," said Harley Geiger, director of public policy for Boston-based Rapid7, Inc., a cybersecurity company which makes software that can test for network vulnerability.

Geiger said the rule could require security researchers to obtain an export license when sharing across borders—a process that can take months.