

US to renegotiate arms control rule for hacking tools

March 1 2016, by Tami Abdollah

The Obama administration plans to renegotiate portions of an international arms control arrangement so it's simpler to export tools related to hacking and surveillance software, since those technologies are also used to secure computer networks, a lawmaker said Monday.

The rare reconsideration of a rule agreed to in 2013 by 41 countries is set to be included on a December agenda by the United States. It makes room to more precisely draft ways 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.

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.

On Monday, the co-chairman of the Congressional Cybersecurity Caucus, Rep. Jim Langevin, D-R.I., issued a statement revealing the administration's decision to ensure countries discuss the removal of language that would broadly sweep up research tools and technology used to create or otherwise support hacking and surveillance software.

"International cybersecurity policy is a new domain, and it is vital that we work together in order to protect our networks from the many threats

they face," Langevin said, applauding the effort thus far.

The White House has said it supports making cyber intrusion tools available overseas for legitimate cybersecurity activities. The White House referred questions Monday to the State and Commerce departments, neither of which responded to requests for comment.

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.

In May, the Commerce Department's Bureau of Industry and Security 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.

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

© 2016 The Associated Press. All rights reserved.

Citation: US to renegotiate arms control rule for hacking tools (2016, March 1) retrieved 9 April 2024 from <https://phys.org/news/2016-03-renegotiate-arms-hacking-tools.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--