US to rework arms control rule on exporting hacker tools

February 2 2016, byTami Abdollah

In this April 22, 2015 file photo, a presentation is made in the Symantec booth during the RSA Conference in San Francisco. The U.S. government is rewriting a proposal under arms control rules from 20 years ago to make it simpler to export tools related to hacking and surveillance software since they're are also used to secure computer networks. The White House said it supports making cyber intrusion tools available overseas for legitimate cybersecurity activities, according to a letter made public Tuesday, Feb. 2, 2016. (AP Photo/Marcio Jose Sanchez, File)

The U.S. government is rewriting a proposal under arms control rules

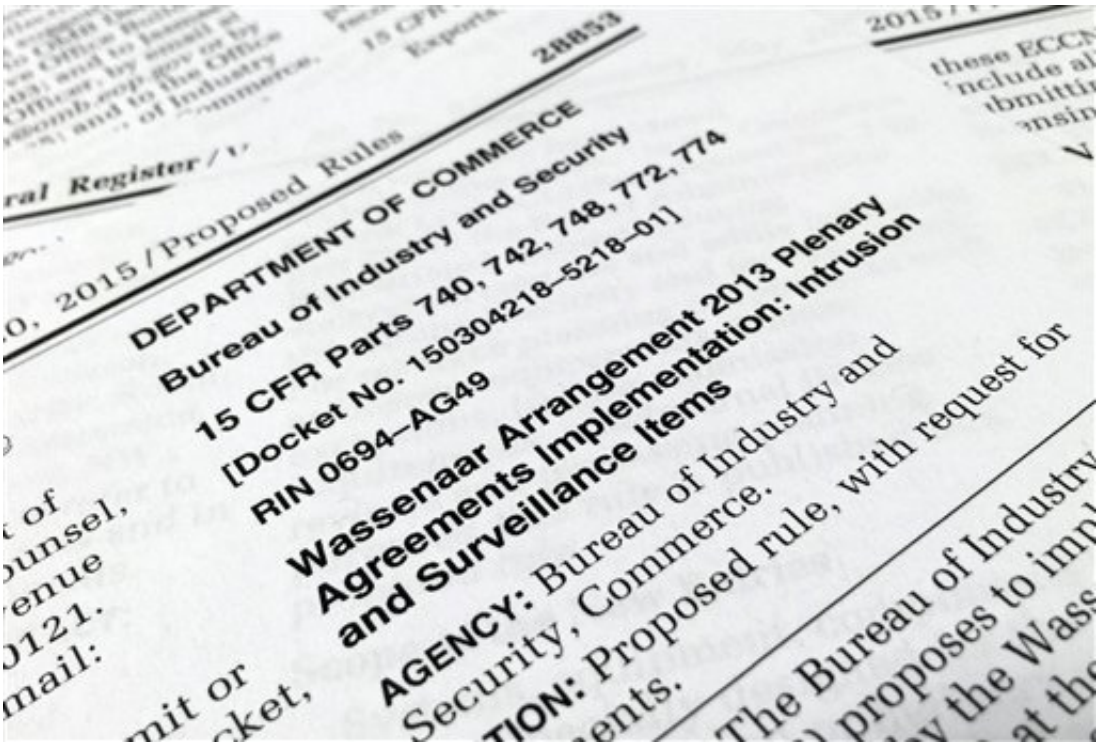
from 20 years ago to make it simpler to export tools related to hacking and surveillance software since they are also used to secure computer networks.

The White House said it supports making cyber intrusion tools available overseas for legitimate cybersecurity activities, according to a letter made public Tuesday.

Industry groups and lawmakers have raised fears that overly broad language aimed at limiting the spread of such hacking tools would have unintended negative consequences for national cybersecurity and research.

As one of the 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 in 2013 to restrict tools related to cyber "intrusion software" that could fall into the hands of repressive regimes.

The Obama administration agrees that "keeping these technologies from illegitimate actors must not come at the expense of legitimate cybersecurity activities," according to a letter from the National Security Council's Senior Director for Legislative Affairs, Caroline Tess. The co-chairman of the Congressional Cybersecurity Caucus, Rep. Jim Langevin, D-RI, made the letter public.



In this photo taken Dec. 22, 2015, a portion of a page from the Federal Register is photographed in Washington on Tuesday, Dec. 22, 2015. The U.S. government is reworking a rule that would determine how, and if, cyber intrusion software, commercially used to test and secure networks, can be transferred to non-Americans after industry groups and lawmakers raised fears that "overly broad" language will have unintended negative consequences for national cyber security and research. As one of the 41 member countries of the longtime Wassenaar Arrangement, which governs the abstruse world of export controls for arms and certain technologies, the United States agreed in 2013 to restrict hacking and surveillance tools or "intrusion software" that could fall into the hands of repressive regimes. The Department of Commerce's Bureau of Industry and Security came out with proposed language, which denied the transfer of "offensive tools," defined as software that uses "zero-day," or unpatched new vulnerabilities, and "rootkit" abilities that allow a person administrator-level access to a system. (AP Photo/Jon Elswick)

Tess said the White House has intensified its discussion with U.S.

officials and industry and that the Commerce Department will not issue a final rule without an additional round of public comment on a revised draft version.

Langevin, however, said in a statement Tuesday that problems with the rule may lie in the language itself, which would require a renegotiation of the 2013 agreement to limit such tools.

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 speedy 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 cyber, "penetration is a defensive action, (testing) how the defenses work," said Jen Ellis, spokeswoman for Rapid7, Inc., which makes a penetration testing tool. "To get to that knowledge you attack yourself, you take offensive action for a defensive purpose. That's a classic example where we can't draw a clear-stock line. They are intentionally and necessarily the same thing."

The Boston, Massachusetts,-based cybersecurity company does business in 90 countries.

The 2013 addition to the arrangement also covers technology used for developing intrusion software, which critics say impacts research. The

U.S. draft rule exempts research in the public domain, but some fixes to vulnerabilities are done privately to avoid giving bad actors insight into a system's flaws.

To transfer intrusion software or information to non-Americans and non-Canadians, companies would have to apply for a license, which can take months.

Symantec Corp. applies for fewer than two dozen export licenses annually and tried to estimate how many it would need under the proposed language, said Cheri McGuire, vice president of global government affairs and cybersecurity policy.

"We stopped counting when we got to 1,000 and we don't even know what the real number would be, because every instance (of information or tool sharing) would require an export license. We're talking thousands upon thousands of licenses just to conduct our business," said McGuire. She called it a bureaucratic nightmare.

The U.S. draft rule provoked nearly 300 comments from cybersecurity professionals, activists and lawmakers, who said it would weaken cybersecurity. The Bureau of Industry and Security is working on new language expected in the first half of the new year. A government spokesman did not return phone calls or email messages from The Associated Press.

"All of our companies agree that providing software to dictators who oppress is wrong," said Craig Albright of the Business Software Alliance, which represents companies including Apple, IBM, Oracle, Dell and Microsoft. But this "sweeps in potentially all of the cybersecurity products that are everyday use and that is an approach that's very scary."