Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New WH Cyber Strategy Talks Big Game, But Has Big Holes

By **Ben Kochman**

Law360 (October 3, 2018, 8:13 PM EDT) -- The White House's newly unveiled national cybersecurity strategy takes the long-awaited step of adding digital combat to the top of America's foreign policy agenda, but it's unclear how its aggressive rhetoric will play out in practice, former federal officials say.

A 40-page report released by the Trump administration in late September included several ideas that cybersecurity experts in both the public and private sectors have long embraced, including forming an international cyber deterrence initiative to enforce global cybersecurity norms and boosting security requirements for federal contractors.

Other ideas outlined in the report — like its warning that it is authorizing offensive cybersecurity operations and its call to "modernize" federal cybercrime laws — broadly lay out the administration's cyberspace agenda but leave a lot of wiggle room on implementation, the former federal officials told Law360.

“It reads almost like a statement of intent or a set of philosophical priorities. But what we really need to see happen next are tangible steps that the administration is going to propose to bring these aspirations into reality," said April Doss, a partner at Saul Ewing Arnstein & Lehr LLP who formerly served as the National Security Agency's associate general counsel for intelligence law.

The report's warning that the U.S. will "work with partners when appropriate to impose consequences against malicious cyber actors" shows that the Trump White House is rightly adding cybersecurity to its toolbox for dealing with disputes with foreign nations, according to Jonathan Meyer, a partner at Sheppard Mullin Richter & Hampton LLP who served as deputy general counsel for the U.S. Department of Homeland Security during the Obama administration.

The plan warns that "all instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States," including "diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities."

“This is trying to make cyber more like other tools of power in attack and defense that have existed in the kinetic world for many years," Meyer said.

The plan is far from clear on how U.S. officials might approve an offensive cyberattack. The administration has separately said that it repealed an Obama-era directive, Presidential Policy Directive 20, that created a multiagency approval process for approving such a cyberattack.

Cybersecurity experts have warned that any offensive cyber action carries with it serious risks. Once a digital weapon is released into the digital ecosystem, criminal hackers or U.S. adversaries could repurpose it for their own malicious ends.

For instance, cybercriminals in May 2017 used a Microsoft Windows software flaw first discovered by the NSA to launch the global ransomware worm known as WannaCry. That attack locked users out of more than 300,000 computers in 150 countries and temporarily knocked the United Kingdom's public health system offline.

Several major tech firms, including Microsoft Corp., Facebook Inc., HP, Cisco Systems Inc. and Dell, have called on the U.S. government and other major powers to address part of this risk by being more transparent about how they acquire and use cybersecurity flaws found in mass-market products for intelligence operations.

"Certainly, the idea that targets could learn from what we are doing and use it themselves is something that should be considered," said Marcus Christian, a partner at Mayer Brown LLP and former cybercrimes prosecutor at the U.S. Attorney's Office for the Southern District of Florida.

Another risk in both launching and responding to cyberattacks is that such activities are often difficult to attribute to a specific party. Nations the U.S. have accused of ordering recent cyberattacks — North Korea and Russia — invariably deny having anything to do with them. Assembling an international cyber deterrence initiative could help build a consensus around when to publicly call out a country for engaging in digital warfare, and when an offensive response is in order.

"Any decisions on offensive cyber operations need to be informed by a responsible risk analysis that takes into account the potential downsides, including misattribution," said Doss. "It's important for that not to happen in a vacuum and to be viewed in a broader context."

"There may be some cases where taking cyber action is the right answer," she added. "But it should never be the default answer."

Another line in the strategy calling for "modernizing" federal cybercrime laws has cybersecurity lawyers scratching their heads.

The administration says it will work with Congress to "update electronic surveillance and computer crime statutes to enhance law enforcement's capabilities to lawfully gather necessary evidence of criminal activity, disrupt criminal infrastructure through civil injunctions, and impose appropriate consequences upon malicious cyber actors." It does not mention any specific law by name.

"To say that in passing in one sentence leaves a lot of open questions about the scope of how the administration views that issue," said Steve Stransky, senior counsel at Thompson Hine LLP and formerly senior counsel for intelligence law at DHS during the previous administration.

Stransky noted that federal prosecutors already have broad authority under the Computer Fraud and Abuse Act to prosecute any "unauthorized" hacking activity. Recent attempts to revise federal surveillance laws have resulted in a scaling back of law enforcement's abilities, he added, citing 2015's USA Freedom Act that reined in the NSA's collection of bulk telephone records.

The administration could try to boost law enforcement's evidence-gathering methods by proposing legislation requiring service providers to turn over unencrypted data to the government, which would alleviate the issue the FBI refers to as “going dark,” such as when authorities said they were locked out of one of the killer's iPhones in the 2015 mass shooting in San Bernardino, California.

But the White House would likely have a massive fight on its hands if it mounted such an effort from both tech giants, who say building a so-called backdoor into their products would create security concerns, and from privacy advocates, who have cited civil rights issues with the government having such access in places like China.

"The idea of being able to conduct surveillance more easily on some intuitive level makes sense, but how you are going to do that and pass constitutional muster is another question," Christian said.

--Editing by Emily Kokoll and Jill Coffey.