The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Trump Has Cleared the Way for Russian 'Hacktivities' (Op-ed)

The White House is creating the illusion being proactive on cyber defense. But that alone won't stop Russia from meddling.

By Tinatin Japaridze & Lincoln Mitchell

October 02, 2018



Pablo Martinez Monsivais / AP/ TASS

Over the past two weeks, the Trump Administration has rolled out a flurry of cybersecurity strategies and executive orders, including the latest Cyber Strategy by the Department of Defense and, most notably, the first White House National Cyber Strategy in 15 years. The U.S. government has unveiled what it calls "offensive" and "deterrent" security measures against its cyber adversaries, including Russia. But the devil is in the detail — and details are largely absent from these new documents.

While former U.S. government officials and even political opponents of this administration

have praised the leadership for taking a step forward on the cyber front, many have also criticized the administration for a continued lack of clearly defined roles and responsibilities between U.S. federal agencies on identifying and prioritizing critical functions and missions of federal cybersecurity initiatives. But beyond those directly working on cybersecurity-related matters, this new cyber strategy has drawn almost entirely no attention from the American media and electorate. It is almost as if the Trump administration is reluctant to be seen publicly confronting something that is a much greater threat to national security than, for example, immigration or trade deals, two subjects about which the President never tires of speaking, or Tweeting.

Related article: No, the U.S. Can't Bring Russia to Its Knees (Op-ed)

The pertinent topic of disinformation — a topic that continues to make international headlines — is also largely ignored by the new National and DoD cyber strategies. Neither one of these two documents devotes any significant attention to the U.S. capabilities for battling social media misinformation, an integral component of cybersecurity that would specifically target Russia. And while Russia, alongside Iran, China and North Korea, is mentioned in passing as one of America's primary cyber adversaries posing strategic threats to U.S. prosperity and security, nowhere do we encounter a specific policy directive targeting Moscow for its "hacktivities" against the United States.

Aside from the naming and shaming as a tactic that, along with a number of indirectly related sanctions, has been employed by the United States as a punishment for Russia's actions in the cyberspace, producing a direct response has been placed on the back burner for fear of a possible escalation of bilateral cyber conflict. This means that Russia also faces a lack of clarity on the American position because missing from the strategies is the specification of the "red line," which, if crossed by the adversary, would prompt a direct U.S. response.

The absence of a "red line" can partially be explained by the notion that a rational "red line" would specifically include Russia seeking to change the outcome of an American election, which is precisely what happened in 2016. With that red line already crossed, the ability of the United States to present other red lines that are both plausible and significant is questionable. This is particularly true given that the new White House Cyber Strategy, which was released more than 18 months into the Trump presidency comes on the heels of 18 months of silence from the administration and Republican Congress on efforts to make election related information more secure.

Related article: Putin Hates You? Then Put Less Data Online (Op-ed)

What's more, the White House may be refraining from identifying the specific kinds of cyber operations that the Kremlin would have to conduct against the United States in order for the latter to respond to these actions in a meaningful way for a reason. Some have argued that devising a "red line" could erode deterrence by granting a cyber adversary room for conventional force maneuver without any real repercussions. Whereas others fear that if Russia were to cross the "red line," the United States, forced to respond, would find itself engaged in a full-fledged cyber war with its former Cold War opponent — a war that in a dark

space that knows no physical borders could bleed into digital warfare of global proportions with no real winners. But there is also another possibility, bearing in mind the complex relationship between the United States and Russian Presidents. When it comes to Vladimir Putin and the Kremlin, where, if at all, is that "red line" for Donald Trump?

Since the election of Donald Trump, the U.S. government has struggled to put together a unified cybersecurity policy, but these documents are clearly far from offering a cohesive plan, not in the least in terms of how digital adversaries, such as Russia, should be treated beyond merely taking an aggressive posture on paper. Even in the midst of the Trump Administration's efforts of creating an illusion of progress on America's cyber front by regurgitating the previous administration's strategies, it is likely that Russia will continue to get away with its cyber offensive activities at least for the time being.

Tinatin Japaridze is an M.A. student at Columbia University's Harriman Institute, working on U.S.-Russian relations with a focus on cybersecurity and digital diplomacy.

Lincoln Mitchell is an adjunct associate research scholar at Columbia University's Arnold A. Saltzman Institute for War and Peace Studies who writes about U.S.-Russia relations, American democracy, the former Soviet Union and baseball.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2018/10/02/us-cybersecurity-strategy-offers-russia-no-clarity-a63061