The Washington Post

Opinions

Russia never stopped its cyberattacks on the United States

By Michael Morell and Mike Rogers December 25, 2017

Michael Morell is a former deputy director and twice acting director of the Central Intelligence Agency from 2010 to 2013. Mike Rogers, a Republican from Michigan, served in the House from 2001 to 2015 and was chairman of the Intelligence Committee from 2010 to 2015. Both are on the advisory council for the Alliance for Securing Democracy.

Every first-year international-relations student learns about the importance of deterrence: It prevented a Soviet invasion of Western Europe during the height of the Cold War. It prevented North Korea from invading South Korea in the same time frame. Today, it keeps Iran from starting a hot war in the Middle East or other nations from initiating cyberattacks against our infrastructure.

And yet, the United States has failed to establish deterrence in the aftermath of Russia's interference in the 2016 election. We know we failed because Russia continues to aggressively employ the most significant aspect of its 2016 tool kit: the use of social media as a platform to disseminate propaganda designed to weaken our nation.

There is a perception among the media and general public that Russia ended its social-media operations following last year's election and that we need worry only about future elections. But that perception is wrong. Russia's information operations in the United States continued after the election and they continue to this day.

This should alarm everyone — Republicans, Democrats and independents alike. Foreign governments, overtly or covertly, should not be allowed to play with our democracy.

Russia's information operations tactics since the election are more numerous than can be listed here. But to get a sense of the breadth of Russian activity, consider the messaging spread by Kremlin-oriented accounts on Twitter, which cybersecurity and disinformation experts have tracked as part of the German Marshall Fund's Alliance for Securing Democracy.

In a single week this month, Moscow used these accounts to discredit the FBI after it was revealed that an agent had been demoted for sending anti-Donald Trump texts; to attack ABC News for an erroneous report involving President Trump and Michael Flynn, the former national security adviser; to critique the Obama administration for allegedly "green lighting" the

communication between Flynn and then-Russian Ambassador Sergey Kislyak; and to warn about violence by immigrants after a jury acquitted an undocumented Mexican accused of murdering a San Francisco woman.

This continues a pattern of similar activity over the past year. Russian operatives have frequently targeted Republican politicians who have been critical of Trump, including Sen. Jeff Flake (Ariz.), Sen. Lindsey O. Graham (S.C.) and Sen. Bob Corker (Tenn.). In September, they also attacked Sen. John McCain (Ariz.) after his decisive "no" vote against the Republican health-care bill.

And in mid-November, after Keurig pulled its advertising from Sean Hannity's Fox News show for comments the host made defending Alabama Senate candidate Roy Moore, the Russians used their social media accounts to urge a boycott of the company. For two days, #boycottkeurig was the most used hashtag among Kremlin-influenced Twitter accounts. This was a Russian attack on a U.S. company and on our economy.

More troublingly, other countries are beginning to follow Russia's lead on social media, according to research provided by the Alliance for Securing Democracy. The Chinese are doing so in Taiwan, where 75 percent of the population consumes media from a Japanese instant messaging app called LINE — a hotbed for fake news, much of it from China. Some of the messages pushed by Beijing — including one incorrectly saying that the Taiwan government was planning to regulate Buddhist and Taoist temples — have resulted in large protests in Taipei. And Turkey is starting to use social media to try to influence European policy debates, specifically by targeting the large Turkish diaspora in Europe.

While those information operations have not yet reached the United States, they most certainly will. Russia's use of social media as a political weapon will continue, and more countries will follow suit — until deterrence is established.

The sanctions that the Obama administration and Congress put in place in the aftermath of the 2016 election are steps in the right direction, but they were not significant enough to check Russian President Vladimir Putin. True deterrence requires policies that prevent adversaries from achieving their objectives while imposing significant costs on their regimes. So far, we have done neither.

Read more here:

The Post's View: Another cyberattack alarm is going off

Nicholas Weaver: 'Wannacry' havoc was just the beginning

Chris Stewart: It's time to install a deterrence plan

David Ignatius: The cyberwar has begun