

Opinions

Four steps to fight foreign interference in U.S. elections

By **Mike Rogers and Rick Ledgett** February 14 at 7:38 PM

Mike Rogers, a Republican from Michigan, served in the House from 2001 to 2015 and was chairman of the Intelligence Committee from 2011 to 2015. Rick Ledgett was deputy director of the National Security Agency from 2014 to 2017. Both are members of the Advisory Council of the Alliance for Securing Democracy.

One of the most dangerous misconceptions about the threat of Russian interference in American democracy is that it began and ended with the 2016 presidential election.

Whatever your partisan affiliation, everyone should accept the intelligence community's unanimous conclusion that Russia interfered in the 2016 elections. And similarly, everyone should accept Tuesday's warning from the country's top intelligence chiefs that Russia should be expected to do the same when Americans return to the polls in November.

Election systems differ from state to state and precinct to precinct, but many still have security vulnerabilities that foreign actors — not just the Russians — can exploit. The U.S. government must act to improve security and assure Americans that their votes count.

The government can take many steps to improve its cybersecurity, across the many elements of critical infrastructure and parts of our system that underpin our democratic institutions. But with time running out before the 2018 midterms, the Trump administration and Congress should take four steps immediately.

First, the administration should issue a declaration: “The United States views any foreign attempt to influence our election processes through covert or clandestine means as an attack on the fundamental underpinnings of our system of government. We will not tolerate such activity and reserve the right to respond to such activities.”

We need to establish a clear line that delineates unacceptable behavior and puts others on notice that we will act as needed to defend ourselves. The Trump administration might emulate the actions of our allies France and Germany. In 2017, Jean-Marc Ayrault, France's foreign minister at the time, announced prior to its elections that France would not tolerate any Russian or other foreign interference, a stance adopted by now-President Emmanuel Macron. French government agencies also quickly alerted political parties to the threat of Russian hacking during the campaign. In Germany, the government took a strong stance

against interference, and companies helped raise awareness of Russian meddling by publicly debunking a Russian disinformation campaign that sought to inflame anti-migrant sentiments.

Second, Congress should pass legislation, such as the bipartisan [Secure Elections Act](#), to provide sufficient resources for evaluating the cybersecurity of our states' disparate electoral infrastructure and addressing shortfalls. The Department of Homeland Security's [pledge](#) to complete assessments of states' electoral vulnerabilities by April was a good step. But legislation, particularly with resources attached, can improve upon bureaucratic inefficiencies. Congress should also consider codifying the Obama administration's designation of election systems as critical infrastructure.

Third, the U.S. government should establish an interagency task force to combat foreign attempts to influence our democratic institutions and processes. This task force would be entirely removed from the ongoing investigations into the 2016 elections; instead, it would focus on preventing future attempts to infiltrate and influence our democracy.

Such a task force should combine U.S. policymaking and intelligence communities, including the Departments of Homeland Security, Justice, Commerce, Defense, State and Treasury, as well as relevant intelligence agencies. It should also coordinate with nonpartisan private-sector entities — such as privacy and civil liberty organizations and social media and technology companies — to bring specialized expertise and unique insights. Private companies provide voting machines, aggregate voter data and operate much of the nation's critical infrastructure. Better coordination among these companies and federal and state governments can only improve security.

Finally, the Trump administration should ensure that the U.S. government has the authorities needed to deter foreign actors engaged in malign influence campaigns and cybe roperations against U.S. elections. Countermeasures would include diplomacy, economic tools such as sanctions, covert action and military action. Many of these authorities already exist, but some need further strengthening or clarification to be used in the context of election security.

We are running out of time to defend ourselves from further foreign attempts to influence the vote. Waiting any longer would be an acknowledgment that we are willing to tolerate this national security threat and even permit it to become more dangerous. We hope that the Trump administration and members of Congress on both sides of the aisle see these measures as common-sense, apolitical and in the interests of our country.

Read more:

[Marco Rubio and Chris Van Hollen: Our elections are in danger. Congress must defend them.](#)

[Tom Donilon: Russia will be back. Here's how to hack-proof the next election.](#)

[Paul Waldman: Russia is going to attack our next election. The Trump administration may not even try to stop it.](#)

[Jennifer Rubin: We're defenseless against Russian sabotage in the midterm elections. And Trump's not helping.](#)

[Brian Klaas: The best safeguard against election hacking](#)

 **373 Comments**

