The Washington Post

National Security

U.S. investigating potential covert Russian plan to disrupt November elections

By Dana Priest, Ellen Nakashima and Tom Hamburger September 5, 2016

U.S. intelligence and law enforcement agencies are investigating what they see as a broad covert Russian operation in the United States to sow public distrust in the upcoming presidential election and in U.S. political institutions, intelligence and congressional officials said.

The aim is to understand the scope and intent of the Russian campaign, which incorporates cyber-tools to hack systems used in the political process, enhancing Russia's ability to spread disinformation.

The effort to better understand Russia's covert influence operations is being coordinated by James R. Clapper Jr., the director of national intelligence. "This is something of concern for the DNI," said Charles Allen, a former longtime CIA officer who has been briefed on some of these issues. "It is being addressed."

A Russian influence operation in the United States "is something we're looking very closely at," said one senior intelligence official who, like others interviewed, spoke on the condition of anonymity to discuss a sensitive matter. Officials also are examining potential disruptions to the election process, and the FBI has alerted state and local officials to potential cyberthreats.

The official cautioned that the intelligence community is not saying it has "definitive proof" of such tampering, or any Russian plans to do so. "But even the hint of something impacting the security of our election system would be of significant concern," the official said. "It's the key to our democracy, that people have confidence in the election system."

The Kremlin's intent may not be to sway the election in one direction or another, officials said, but to cause chaos and provide propaganda fodder to attack U.S. democracy-building policies around the world, particularly in the countries of the former Soviet Union.

U.S. intelligence officials described the covert influence campaign here as “ambitious” and said it is also designed to counter U.S. leadership and influence in international affairs.

Their comments came just before President Obama and Russian President Vladimir Putin talked privately about cyberspying and other matters on the sidelines of the Group of 20 talks in China. After their meeting Monday, Obama acknowledged tensions over digital espionage and said the United States had strong capability in this area. “Our goal is not to suddenly, in the cyber arena, duplicate the cycle of escalation we saw when it comes to other arms races in the past,” Obama said.

One congressional official, who has been briefed recently on the matter, said “Russian ‘active measures’ or covert influence or manipulation efforts, whether it’s in Eastern Europe or in the United States,” are worrisome.

It “seems to be a global campaign,” the aide said. As a result, the issue has “moved up as a priority” for the intelligence agencies, which include the FBI and the Department of Homeland Security as well as the CIA and the National Security Agency.

Some congressional leaders briefed recently by the intelligence agencies on Russian influence operations in Europe, and how they may serve as a template for activities in the United States, were disturbed by what they heard.

After Senate Minority Leader Harry M. Reid (D-Nev.) ended a secure 30-minute phone briefing given by a top intelligence official recently, he was “deeply shaken,” according to an aide who was with Reid when he left the secure room at the FBI’s Las Vegas office.

The Russian government hack of the Democratic National Committee, disclosed by the DNC in June but not yet officially ascribed by the U.S. government to Russia, and the subsequent release of 20,000 hacked DNC emails by WikiLeaks, shocked officials. Cyber analysts traced its digital markings to known Russian government hacking groups.

“We’ve seen an unprecedented intrusion and an attempt to influence or disrupt our political process,” said Rep. Adam B. Schiff (Calif.), the ranking Democrat on the House Intelligence Committee, speaking about the DNC hack and the WikiLeaks release on the eve of the Democratic convention. The disclosures, which included a number of embarrassing internal emails, forced the resignation of DNC Chairwoman Debbie Wasserman Schultz.

Members of both parties are urging the president to take the Russians to task publicly.

Sen. Ben Sasse (R-Neb.) in a statement urged Obama to publicly name Russia as responsible for the DNC hack and apparent meddling in the electoral process. “Free and legitimate elections are non-negotiable. It’s clear that Russia thinks the reward outweighs any consequences,” he wrote. “That calculation must be changed. . . . This is going to take a cross-domain response — diplomatic, political and economic — that turns the screws on Putin and his cronies.”

Another Republican, Sen. Daniel Coats of Indiana, a member of the Senate Intelligence Committee, said Sunday that if Moscow is indeed trying to influence the U.S. election, “such actions would be an outrageous violation of international rules of

behavior and cannot be tolerated."

Administration officials said they are still weighing their response.

Russia has denied that it carried out any cyber-intrusions in the United States. Putin called the accusations against Russia by U.S. officials and politicians an attempt to "distract the public's attention."

"It doesn't really matter who hacked this data from Mrs. Clinton's campaign headquarters," Putin said in an interview with Bloomberg News, referring to Democratic presidential nominee Hillary Clinton. "The important thing is the content was given to the public."

The Department of Homeland Security has offered local and state election officials help to prevent or deal with Election Day cyber disruptions, including vulnerability scans, regular actionable information and alerts, and access to other tools for improving cybersecurity at the local level. It will also have a cyber team ready at the National Cybersecurity and Communications Integration Center to alert jurisdictions if attacks are detected.

Last month, the FBI issued an unprecedented warning to state election officials urging them to be on the lookout for intrusions into their election systems and to take steps to upgrade security measures across the voting process, including voter registration, voter rolls and election-related websites. The confidential "flash" alert said investigators had detected attempts to penetrate election systems in several states.

Arizona, Illinois and both the Democratic and Republican parties, as well as the DNC, have been the victims of either attempted or successful cyberattacks that FBI agents with expertise in Russian government hacking are investigating.

Federal law enforcement and local election officials say the decentralized nature of the voting process, which is run by states and counties, makes it impossible to ensure a high level of security in each district.

"I have a lot of concern" about this year's election, said Ion Sancho, the longtime supervisor of elections in Leon County, Fla. "America doesn't have its act together." Sancho, who has authorized red-team attacks on his voting system to identify its vulnerabilities, added: "We need a plan."

Sancho and others are particularly concerned about electronic balloting from overseas that travels on vulnerable networks before landing in the United States, and about efforts to use cyberattacks to disrupt vote tabulations being transmitted to state-level offices. Encryption, secure paper backups and secure backup computers are critical, he said.

Tom Hicks, chairman of the U.S. Election Assistance Commission, an agency set up by Congress after the 2000 Florida recount to maintain election integrity, said he is confident that states have sufficient safeguards in place to ward off intrusions. He noted that electronic balloting from overseas is conducted by email, not through online voting machines. The overseas voter "waives their right of privacy" by emailing the ballot, which is tabulated by election officials. The email may still be hacked, but it is not a systemic risk, he said.

Recently, Homeland Security Secretary Jeh Johnson said he favors designating the voting systems used in the country's 9,000 polling places as "critical infrastructure" — in other words, as vital to the nation's safe functioning as nuclear power plants and electrical power grids.

Such a designation could mean increased DHS funding to localities to help ensure that voter registration, ballots and ballot tabulation remain free from interference. But it won't happen before the November elections, federal and local officials said.

Russia has been in the vanguard of a growing global movement to use propaganda on the Internet to influence people and political events, especially since the political revolt in Ukraine, the subsequent annexation of Crimea by Russia, and the imposition of sanctions on Russia by the United States and the European Union.

The Baltic states, Georgia and Ukraine have been subject to Russian cyberattacks and other hidden influence operations meant to disrupt those countries, officials said.

"Our studies show that it is very likely that [the influence] operations are centrally run," said Janis Sarts, director of the NATO Strategic Communications Center of Excellence, a research organization based in Riga, Latvia.

He also said there is "a coordinated effort involving [groups using] Twitter and Facebook and networks of bots to amplify their message. The main themes seem to be orchestrated rather high up in the hierarchy of the Russian state, and then there are individual endeavors by people to exploit specific themes."

Sarts said the Russian propaganda effort has been "successful in exploiting the vulnerabilities within societies." In Western Europe, for instance, such Russian information operations have focused on the politically divisive refugee crisis.

On the eve of a crucial post-
revolution presidential vote in Ukraine in 2014, a digital assault nearly crippled the country's Central Election Commission's website. Pro-Moscow hackers calling themselves the CyberBerkut claimed responsibility, saying they were not state-affiliated, but the authorities in Kiev blamed Moscow. The Russians used a "denial of service" technique, flooding the commission's Web server with a high volume of requests, which was meant to slow down or disable the network.

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties. Follow @nakashimae

Tom Hamburger covers the intersection of money and politics for The Washington Post. Follow @thamburger

This Item Was Found And Cannot Be Explained

RightBrainNews

Here’s Why You Should Never Buy Glasses at Retail Again

GlassesUSA

How To Fix Your Fatigue (Do This Every Day)

EnergyAtAnyAge.com

An Apple engineer designed a sweatshirt that’s disrupting American Manufacturing

American Giant on Business Insider

Psoriatic Arthritis Symptoms: What You Should Know

Yahoo Search

Use Data To Sell Your Home For More

Homelight