

## National Security

# Kremlin trolls burned across the Internet as Washington debated options

---

By **Adam Entous**, **Ellen Nakashima** and **Greg Jaffe** December 25 at 2:14 PM

The first email arrived in the inbox of CounterPunch, a left-leaning American news and opinion website, at 3:26 a.m. — the middle of the day in Moscow.

“Hello, my name is Alice Donovan and I’m a beginner freelance journalist,” read the Feb. 26, 2016, message.

The FBI was tracking Donovan as part of a months-long counterintelligence operation code-named “NorthernNight.” Internal bureau reports described her as a pseudonymous foot soldier in an army of Kremlin-led trolls seeking to undermine America’s democratic institutions.

Her first articles as a freelancer for CounterPunch and at least 10 other online publications weren’t especially political. As the 2016 presidential election heated up, Donovan’s message shifted. Increasingly, she seemed to be doing the Kremlin’s bidding by stoking discontent toward Democratic front-runner Hillary Clinton and touting WikiLeaks, which U.S. officials say was a tool of Russia’s broad influence operation to affect the presidential race.

“There’s no denying the emails that Julian Assange has picked up from inside the Democratic Party are real,” she wrote in August 2016 for a website called We Are Change. “The emails have exposed Hillary Clinton in a major way — and almost no one is reporting on it.”

The events surrounding the FBI’s NorthernNight investigation follow a pattern that repeated for years as the Russian threat was building: U.S. intelligence and law enforcement agencies saw some warning signs of Russian meddling in Europe and later in the United States but never fully grasped the breadth of the Kremlin’s ambitions. Top U.S. policymakers didn’t appreciate the dangers, then scrambled to draw up options to fight back. In the end, big plans died of internal disagreement, a fear of making matters worse or a misguided belief in the resilience of American society and its democratic institutions.

One previously unreported order — a sweeping presidential finding to combat global cyberthreats — prompted U.S. spy agencies to plan a half-dozen specific operations to counter the Russian threat. But one year after those instructions were given, the Trump White House remains divided over whether to act, intelligence officials said.

This account of the United States' piecemeal response to the Russian disinformation threat is based on interviews with dozens of current and former senior U.S. officials at the White House, the Pentagon, the State Department, and U.S. and European intelligence services, as well as NATO representatives and top European diplomats.

The miscalculations and bureaucratic inertia that left the United States vulnerable to Russia's interference in the 2016 presidential election trace back to decisions made at the end of the Cold War, when senior policymakers assumed Moscow would be a partner and largely pulled the United States out of information warfare. When relations soured, officials dismissed Russia as a "third-rate regional power" that would limit its meddling to the fledgling democracies on its periphery.

Senior U.S. officials didn't think Russia would dare shift its focus to the United States.

"I thought our ground was not as fertile," said Antony J. Blinken, President Barack Obama's deputy secretary of state. "We believed that the truth shall set you free, that the truth would prevail. That proved a bit naive."

With the 2018 elections fast approaching, the debate over how to deal with Russia continues. Many in the Trump White House, including the president, play down the effects of Russian interference and complain that the U.S. intelligence report on the 2016 election has been weaponized by Democrats seeking to undermine Trump.

"If it changed one electoral vote, you tell me," said a senior Trump administration official, who, like others, requested anonymity to speak frankly. "The Russians didn't tell Hillary Clinton not to campaign in Wisconsin. Tell me how many votes the Russians changed in Macomb County [in Michigan]. The president is right. The Democrats are using the report to delegitimize the presidency."

Other senior officials in the White House, the intelligence community and the Pentagon have little doubt that the Russians remain focused on meddling in U.S. politics.

"We should have every expectation that what we witnessed last year is not a one-shot deal," said Douglas E. Lute, the former U.S. ambassador to NATO. "The Russians are onto something. They found a weakness, and they will be back in 2018 and 2020 with a more sophisticated and targeted approach."

## **Digital blitz**

The United States and the Soviet Union engaged in an all-out information battle during the Cold War. But the Soviet Union collapsed in 1991, and the Bill Clinton administration and Congress in 1999 shuttered America's preeminent global information agency.

"They thought it was all over and that we'd won the propaganda war," said Joseph D. Duffey, the last director of the U.S. Information Agency, which was charged with influencing foreign populations.

When President Vladimir Putin came to power, Russia began searching for ways to make up for its diminished military. Officials seized on influence campaigns and cyberwarfare as equalizers. Both were cheap, easy to deploy and hard for an open and

networked society such as the United States to defend against.

Early warning signs of the growing Russian disinformation threat included the 2005 launch of RT, the Kremlin-funded TV network, and the 2007 cyberattacks that overwhelmed Estonia's banks, government ministries and newspapers. A year later, the Kremlin launched a digital blitz that temporarily shut down Georgia's broadcasters and defaced the website of its president.

Closer to home for Americans, Russian government trolls in 2012 went after a U.S. ambassador for the first time on social media, inundating his Twitter account with threats.

But for U.S. officials, the real wake-up call came in early 2014 when the Russians annexed Crimea and backed separatists in eastern Ukraine. An intercepted Russian military intelligence report dated February 2014 documented how Moscow created fake personas to spread disinformation on social media to buttress its broader military campaign.

The classified Russian intelligence report, obtained by The Washington Post, offered examples of the messages the fake personas spread. "Brigades of westerners are now on their way to rob and kill us," wrote one operative posing as a Russian-speaking Ukrainian. "Morals have been replaced by thirst for blood and hatred toward anything Russian."

Officials in the GRU, Russia's military intelligence branch, drafted the document as part of an effort to convince Kremlin higher-ups of the campaign's effectiveness. Officials boasted of creating a fake Facebook account they used to send death threats to 14 politicians in southeastern Ukraine.

Five days into the campaign, the GRU said, its fake accounts were garnering 200,000 views a day.

## **Mixing propaganda and fun**

The Ukraine operation offered the Americans their first glimpse of the power of Russia's post-Cold War playbook.

In March 2014, Obama paid a visit to NATO headquarters, where he listened as unnerved allies warned him of the growing Russia threat. Aides wanted to give the president options to push back.

In the White House Situation Room a few weeks later, they pitched him on creating several global channels — in Russian, Mandarin and other languages — that would compete with RT. The proposed American versions would mix entertainment with news programing and pro-Western propaganda.

The president brushed aside the idea as politically impractical.

In the Situation Room that day was Richard Stengel, the undersecretary for public diplomacy at the State Department, who, like Obama, disliked the idea.

"There were all these guys in government who had never created one minute of TV content talking about creating a whole network," said Stengel, the former top editor at Time magazine. "I remember early on telling a friend of mine in TV that people

don't like government content. And he said, 'No, they don't like bad content, and government content sucks.' ”

So Stengel began to look for alternatives to counter the threat. Across Eastern Europe and Ukraine, Russian-language channels mixing entertainment, news and propaganda were spreading the Kremlin's message. Stengel wanted to help pro-Western stations on Russia's periphery steal back audiences from the Russian stations by giving them popular American television shows and movies.

Shortly after Obama nixed the idea of American-funded networks, Stengel traveled to Los Angeles in the hope that a patriotic appeal to Hollywood executives might persuade them to give him some blockbusters free.

Stengel's best bet was Michael M. Lynton, then the chairman of Sony Pictures, who had grown up in the Netherlands and immediately understood what Stengel was trying to do. He recalled how in the 1970s one Dutch political party sponsored episodes of “M.A.S.H.” to portray America as sympathetic to the antiwar movement. A rival party bought the rights to “All in the Family” to send the message that U.S. cities were filled with bigots like Archie Bunker.

But Sony's agreements with broadcasters in the region prevented Lynton from giving away programming. Other studios also turned Stengel away.

Back in Washington, Stengel got Voice of America to launch a round-the-clock Russian-language news broadcast and found a few million dollars to translate PBS documentaries on the Founding Fathers and the American Civil War into Russian for broadcast in eastern Ukraine. He had wanted programing such as “Game of Thrones” but would instead have to settle for the likes of Ken Burns.

“We brought a tiny, little Swiss Army knife to a gunfight,” he said.

## **A counter-disinformation team**

The task of countering what the Russians were doing fell to a few underfunded bureaucrats at the State Department who journeyed to the CIA, the NSA, the Pentagon and the FBI searching for help and finding little.

U.S. intelligence and law enforcement agencies in the aftermath of 9/11 prioritized counterterrorism. They worried about the legal peril of snooping on social media and inadvertently interfering with Americans' communications. The State Department created a small team to tweet messages about Ukraine, but they were vastly outnumbered by the Russian trolls.

Frustrated U.S. officials concluded that the best information on Russia's social media campaign in Ukraine wasn't coming from U.S. intelligence agencies, but from independent researchers. In April 2015, Lawrence Alexander, a 29-year-old self-taught programmer who lived with his parents in Brighton, Britain, received an unexpected Twitter message from a State Department official who reported to Stengel.

“Can you show what [the Russians] are swarming on in real time?” the official, Macon Phillips, asked. “Your work gave me an idea.”

A few months later, Phillips requested an in-person meeting. Alexander, who suffers from a genetic disorder that often leaves him chronically fatigued, wasn't able to make the two-hour trek to the U.S. Embassy in London. So Phillips took the train to Brighton, where Alexander walked him through his research, which was spurred by his alarm over Putin's intervention in Ukraine and his crackdown on gays and journalists.

Phillips's ideas sprang from his work on Obama's first presidential campaign, which used social media analytics to target supporters. One proposal now was to identify "online influencers" who were active on social media spreading Kremlin messages. Phillips wanted to use analytics to target them with U.S. counterarguments.

State Department lawyers, citing the Privacy Act, demanded guarantees that data on Americans using social media wouldn't inadvertently be collected as part of the effort.

The pre-Internet law restricts the collection of data related to the ways Americans exercise their First Amendment rights. The lawyers concluded that it applied to tweets, leaving some State Department officials baffled.

"When you tweet, it's public," said Moira Whelan, a former deputy assistant secretary for digital strategy. "We weren't interested in Americans."

The lawyers' objections couldn't be overcome. The project, which Phillips worked on for more than a year, was dead.

## **Zapping servers**

While Stengel and Phillips were struggling to make do with limited resources, the CIA, at the direction of Obama's top national security advisers, was secretly drafting proposals for covert action.

Russia hawks in the administration wanted far-reaching options that, they argued, would convince Putin that the price he would pay for continued meddling in the politics of neighboring democracies would be "certain and great," said a former official involved in the debate.

One of the covert options that officials discussed called for U.S. spy agencies to create fake websites and personas on social media to fight back against the Kremlin's trolls in Europe. Proponents wanted to spread anti-Kremlin messages, drawing on U.S. intelligence about Russian military activities and government corruption. But others doubted the effectiveness of using the CIA to conduct influence operations against an adversary that operated with far fewer constraints. Or they objected to the idea of U.S. spies even doing counterpropaganda.

James R. Clapper Jr., the top spy in the Obama administration, said in an interview that he didn't think the United States "should emulate the Russians."

Another potential line of attack involved using cyberweapons to take down Russian-controlled websites and zap servers used to control fake Russian personas — measures some officials thought would have little long-term effect or would prompt Russian retaliation.

The covert proposals, which were circulated in 2015 by David S. Cohen, then the CIA's deputy director, divided the administration and intelligence agencies and never reached the national security cabinet or the president for consideration. Cohen declined to comment.

After top White House officials received intelligence in the summer of 2016 about Putin's efforts to help Trump, the deadlocked debate over covert options to counter the Kremlin was revived. Obama was loath to take any action that might prompt the Russians to disrupt voting. So he warned Putin to back off and then watched to see what the Russians would do.

After the election, Obama's advisers moved to finalize a package of retaliatory measures.

Officials briefly considered rushing out an overarching new order, known as a presidential finding, that for the first time since the collapse of the Soviet Union would authorize sweeping covert operations against Russia. But they opted against such a far-reaching approach. Instead, the White House decided on a targeted cyber-response that would make use of an existing presidential finding designed to combat cyberthreats around the world rather than from Russia specifically.

As a supplement to the cyber finding, Obama signed a separate, narrower order, known as a "Memorandum of Notification," which gave the CIA the authority to plan operations against Russia. Senior administration and intelligence officials discussed a half-dozen specific actions, some of which required implants in Russian networks that could be triggered remotely to attack computer systems.

Members of the Obama administration expected that the CIA would need a few weeks or, in some cases, months to finish planning for the proposed operations.

"Those actions were cooked," said a former official. "They had been vetted and agreed to in concept."

Obama left behind a road map. Trump would have to decide whether to implement it.

## **'This is what we live with'**

Before Trump took office, a U.S. government delegation flew to NATO headquarters in Brussels to brief allies on what American intelligence agencies had learned about Russian tactics during the presidential election.

U.S. officials are normally reluctant to share sensitive intelligence with the alliance's main decision-making body. But an exception was made in this case to help "fireproof" all 28 allies in case Russia targeted them next, a senior U.S. official said.

The Obama administration had gone through an agonizing learning curve. The Russians, beginning in 2014, had hacked the State Department and the White House before targeting the Democratic National Committee and other political institutions. By the time U.S. officials came to grips with the threat, it was too late to act. Now they wanted to make sure NATO allies didn't repeat their mistakes.

Jens Stoltenberg, the NATO secretary general, gavelled the closed-door session to order, and the Americans ran through their 30-minute presentation. The Europeans had for years been journeying to Washington to warn senior U.S. officials about Russian meddling in their elections. The Americans had listened politely but didn't seem particularly alarmed by the threat, reflecting a widely held belief inside the U.S. government that its democratic institutions and society weren't nearly as vulnerable as those in Europe.

For the first time since the days after 9/11, the American officials in Brussels sounded overwhelmed and humbled, said a European ambassador in the room.

When the briefers finished, the allies made clear to the Americans that little in the presentation surprised them.

"This is what we've been telling you for some time," the Europeans said, according to Lute, the NATO ambassador. "This is what we live with. Welcome to our lives."

## **Mr. Preemption**

After Trump took office, Russia's army of trolls began to shift their focus within the United States, according to U.S. intelligence reports. Instead of spreading messages to bolster Trump, they returned to their long-held objective of sowing discord in U.S. society and undermining American global influence. Trump's presidency and policies became a Russian disinformation target.

Articles from Donovan and other Kremlin-backed personas slammed the Trump administration for, among other things, supporting "terrorists" and authorizing military strikes that killed children in Syria.

"They are all about disruption," said a former official briefed on the intelligence. "They want a distracted United States that can't counter Vladimir Putin's ambitions."

The dilemma facing the Trump White House was an old one: how to respond.

In the weeks before Trump's inauguration, Brett Holmgren, a top intelligence official in the Obama White House, briefed Ezra Cohen-Watnick, his Trump administration counterpart, on the actions Obama had taken. Holmgren and Cohen-Watnick declined to comment.

Once in the job, Cohen-Watnick sent out memos identifying counterintelligence threats, including Russia's, as his top priority, officials said.

He convened regular meetings in the White House Situation Room at which he pressed counterintelligence officials in other government agencies, including the CIA, to finalize plans for Russia, including those left behind by the Obama team, according to officials in attendance.

By spring, national security adviser H.R. McMaster, senior White House Russia adviser Fiona Hill and Cohen-Watnick began advocating measures to counter Russian disinformation using covert influence and cyber-operations, according to officials.

But, just as in the Obama administration, the most far-reaching ideas ran into obstacles.

McMaster and Tom Bossert, Trump's homeland security adviser, both laid claim to controlling the cyber-portfolio and would sometimes issue conflicting instructions that left policymakers and intelligence officials confused about whose direction to follow.

Obama's 11th-hour actions had cleared the way for spy agencies to conduct cyber-operations to counter the Russian threat. But the CIA still had to finalize the plans, and the Trump White House wanted to review them.

Bossert was more cautious than McMaster about using cyber-tools offensively. His message to the National Security Council staff, a senior White House official said, was: "We have to do our homework. Everybody needs to slow down."

Directing the CIA to conduct covert influence operations was a similarly fraught process. Before the agency could proceed, intelligence officials informed the White House that it would need new authorities from the president.

To Trump officials, the CIA appeared to be more interested in other priorities, such as proposals to target WikiLeaks. The National Security Council and the CIA declined to comment on the covert options.

The policy debates were further complicated by the difficulty of even raising Russian meddling with a president who viewed the subject as an attack on his legitimacy.

In an effort to bring Trump around, officials presented him with evidence of Putin's duplicity and continued interference in U.S. politics. But the president's recent public statements suggest that he continues to believe that he is making progress in building a good relationship with the Russian leader.

This month, Trump noted that Putin, in his end-of-year news conference, had praised Trump's stewardship of the U.S. economy.

"He said very nice things," Trump told reporters.

Putin later called Trump to praise the CIA for providing Russia with intelligence about a suspected terrorist plot in St. Petersburg.

"That's a great thing," Trump said after the second call with the Russian leader, "and the way it's supposed to work."

Even White House officials who take the Russia threat seriously fret that aggressive covert action will just provoke Putin to increase his assault on a vulnerable United States.

"One of the things I've learned over many, many years of looking at Russia and Putin is that he's Mr. Preemption. If he thinks that somebody else is capable of doing something to him, he gets out ahead of it," said a senior administration official. "We have to be extraordinarily careful."



## What's real and not real

The Kremlin has given little indication that it intends to back off its disinformation campaign inside the United States. More than a year after the FBI first identified Alice Donovan as a probable Russian troll, she's still pitching stories to U.S. publications.

In the spring, Donovan's name appeared on articles criticizing Trump's conduct of the war in Syria and defending Russian-backed leader Bashar al-Assad. "U.S.-led coalition airstrike on Assad's troops not accidental," the headline of a May 20 piece on CounterPunch read. Her last piece for CounterPunch, headlined "Civil War in Venezuela," was published Oct. 16.

Other pieces under her byline have been published in recent months at Veterans Today, where Gordon Duff, the site's editor, said he knew nothing about Donovan.

"I don't edit what people do," Duff said. "If it's original, I'll publish it. I don't decide what's real and not real."

At We Are Change, which has also recently published Donovan's work, Luke Rudkowski, one of the site's founders, wondered why the FBI didn't contact his publication with its suspicions.

"I wish we could get information from the FBI so we could understand what's really happening," he said. "I wish they had been more transparent."

The FBI, in keeping with its standard practice in counterintelligence investigations, has kept a close hold on information about Donovan and other suspected Russian personas peddling messages inside the United States.

The bureau does not have the authority to shut down the accounts of suspected trolls housed on U.S. social media companies' platforms.

"We're not the thought police," said one former senior law enforcement official.

The Russians are taking advantage of "seams between our policies, our laws and our bureaucracy," said Austin Branch, a former Defense Department official who specialized in information operations.

The FBI said in a statement that it has employed cyber, criminal and counterintelligence tools to deal with the disinformation threat.

"The FBI takes seriously any attempts to influence U.S. systems and processes," the statement said.

In late November, The Post informed Jeffrey St. Clair, CounterPunch's editor, that the FBI suspects that Donovan is a Russian government persona. St. Clair said in an interview that Donovan's submissions didn't stand out among the 75 or so pitches he receives each day.

On Nov. 30, he sent her an email saying he wanted to discuss her work. When he got no response, St. Clair followed up with a direct message on Twitter, asking her to call him immediately.

On Dec. 5 Donovan finally replied by email: “I do not want to talk to anyone for security reasons.”

St. Clair tapped out a new message, begging her to provide proof — a photograph of her driver’s license or passport — that would show that she was the beginning freelance journalist she claimed to be in her introductory email from 2016.


“It shouldn’t be that difficult to substantiate,” he wrote.


He has yet to receive a response.

*Julie Tate contributed to this report.*

 **7216 Comments**

Adam Entous writes about national security, foreign policy and intelligence for The Post. He joined the newspaper in 2016 after more than 20 years with The Wall Street Journal and Reuters, where he covered the Pentagon, the CIA, the White House and Congress. He covered President George W. Bush for five years after the September 11, 2001, attacks.

Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity, surveillance, counterterrorism and intelligence issues.  Follow @nakashimae

Greg Jaffe is a national security reporter for The Washington Post, where he has been since March 2009. Previously, he covered the White House and the military for The Post.  Follow @GregJaffe

## Share news tips with us confidentially

Do you have information the public should know? Here are some ways you can securely send information and documents to Post journalists.

**[Learn more](#)**





