BROOKINGS

United States House Committee on the Judiciary

Lessons from the Mueller Report, Part II: Bipartisan Perspectives

June 20, 2019

Dr. Alina Polyakova
Director, Global Democracy and Emerging Technology
Fellow, Center on the United States and Europe
Foreign Policy Program
Brookings Institution

Dear Chairman Nadler, Ranking Member Collins, Distinguished Members of the Committee:

It is an honor and privilege to address you today on this important issue. Thank you for inviting me to speak.

The Russian government is engaged in political warfare against the West. Its intent is to undermine trust in democratic institutions, values, and principles, which the Kremlin sees as a threat to its own authoritarian model. The Kremlin's tool-kit of influence is a twenty-first century adaptation of Soviet era "active measures," and includes: disinformation and propaganda campaigns, cyber warfare, political infiltration, and the use of corruption to influence politics.

The Russian operation against the United States, as detailed in the Special Counsel report, fits into a broader pattern of Russian non-kinetic activities—tested, first in foremost, in former Soviet countries, most notably Ukraine. The operation targeting the 2016 U.S. presidential election may be the most prominent case of Russian political warfare against the West, but it has not been the last. Since 2016, Moscow has interfered, in various ways, in France, the United Kingdom, Germany, Montenegro, Spain, and elsewhere.

The Mueller report describes in stunning detail the nature, intent, and inner working of the Russian government's influence operation against the United States before, during, and after the 2016 U.S. presidential elections. To date, the report[1] and the investigation's related indictments from February 2018[2] and July 2018[3] against the Internet Research Agency (IRA) and Russian military intelligence (GRU) provide the most comprehensive assessment of how the Russian strategy evolved over time and how successful the information operations were in targeting and duping Americans. The Mueller report

[1] Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election" (U.S. Department of Justice, Washington, DC, 2019), https://www.justice.gov/storage/report.pdf.
[2] UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC A/K/A MEDIASINTEZ LLC A/K/A GLAVSET LLC A/K/A MIXINFO LLC A/K/A AZIMUT LLC A/K/A NOVINFO LLC et al. 18 U.S.C. §§ 2, 371, 1349, 1028A (2018). https://www.justice.gov/file/1035477/download.
[3] UNITED STATES OF AMERICA v. VIKTOR BORISOVICH NETYKSHO et al. 18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq. (2018). https://www.justice.gov/file/1080281/download.

clearly shows that the Russian information operations were highly adaptive to the political context in the United States, followed a well-thought out strategic plan, involved direction from Russian intelligence, and were incredibly effective in infiltrating American media while influencing public debate around the 2016 election. Their main objective was to undermine trust in the democratic process.

The nature of the Russian attack on the United States

Through various proxies, the Russian government carried out a multi-pronged attack against the United States that aimed to amplify pre-existing divisions in American society, sow distrust in the democratic process, and incite conflict. The campaign involved three distinct elements:[4]

1. An information operation led by the Internet Research Agency (IRA);
2. A cyber hacking operation carried out by the Russian military intelligence agency (GRU); and
3. An infiltration operation of the Trump campaign.

Here, I will focus my comments on the information operations, which began as early as 2014 and resembled a marketing campaign. There were four phases to the information operations. The IRA's first step was to build a network of accounts by creating individual impersonation accounts meant to look like Americans, particularly on Facebook.

Second, the IRA focused on audience growth by creating pages and content that were not necessarily political or even divisive, but simply meant to attract more eyeballs to IRA-controlled pages and accounts. By early 2015, the IRA had turned to audience-building around divisive social issues by creating social media groups and pages posing as U.S. groups and activists, such as "Secured Borders" and "Blacktivist." The IRA's intent from the outset was to use its digital operations to affect real life: as early as 2015, the IRA attempted to organize rallies on divisive social issues.

Third, and once the network had reached a critical mass, the IRA turned explicitly to the U.S. elections around February 2016. The goal was to undermine the Clinton campaign. Instructions (from a redacted source) to the IRA read: "Main idea: use any opportunity to criticize Hillary [Clinton] and the rest (except Sanders and Trump – we support them)" (p. 25). The focus remained primarily on criticizing Clinton until late spring 2016.

In its last step, by the summer of 2016, the IRA began to actively promote then-candidate Donald Trump. At the same time, it aimed to further increase its audience by purchasing advertisements to promote its pages and reaching out via private messages to Facebook users prompting them to organize anti-Clinton rallies. The IRA purchased over 3,500 ads and spent approximately $100,000. In mid-2017, the most popular IRA-controlled group—"United Muslims of America"—had over 300,000 followers.

By the end of the 2016 election, the IRA "had the ability to reach millions of U.S. persons through their social media accounts" on Facebook, Instagram, Twitter, YouTube, and Tumblr, according to the report

[4] Alina Polyakova, "The Next Russian Attack Will Be Far Worse than Bots and Trolls," *Lawfare,* March 20, 2018, https://www.lawfareblog.com/next-russian-attack-will-be-far-worse-bots-and-trolls.

(p. 26). Facebook later estimated that IRA-controlled accounts reached as many as 126 million people,[5] and an additional 1.4 million[6] were reached through Twitter.

The IRA was part of a larger interference project funded by Russian oligarch Yevgeny Prigozhin called "Project Lakhta." The IRA hired specialists for each social media platform, who were given specific instructions on which messages to push, how, and the performance quotas they had to meet. Yet, we still don't know the full scope of the command structure, how far into the Kremlin the decision-making process reached, and how the project continues to be funded today.

A pattern of political warfare against democracies

During Vladimir Putin's tenure, the Russian government has significantly built up its nonconventional warfare capacities, most notably in the information and cyber domains. In particular, digital information warfare is low-cost and high-impact, making it the perfect weapon of a technologically and economically weak power, like Russia.[7] The Russian government has tested these tools first on its own people. It is telling, for example, that the majority of the IRA's 800-900 employees were engaged in Russian language activities. Of those, approximately 80 were working on the "translator project" targeting the United States.[8]

Russian influence operations do not focus on isolated events. Rather, taken as whole, they are at the core of a political strategy—honed in Europe's East and deployed against the West—to weaken democratic institutions, sow discord in societies, and divide the transatlantic alliance. In addition to information operations and cyber-attacks, the Russian government supports, in various ways, far-right political groups and parties in Europe. In May of this year, the head of the Austrian far-right Freedom Party (FPÖ), Heinz-Christian Strache, was forced to resign after a video surfaced showing Strache offering government contracts and a stake in one of Austria's largest newspapers in exchange for Russian support for his party.[9] France's far-right National Front received a loan of approximately $9.8 million in 2014 from a Russian bank, and in 2017, the party's leader and then-presidential candidate, Marine Le Pen, requested an additional $29 million loan from Russia. Italy's League and the Austrian Freedom Party both have formal cooperation agreements with the Kremlin's United Russia party. The U.S. operation thus fits into a broader pattern of influence activities.[10]

A few prominent examples of the pattern of behavior:

---

[5] Mike Isaac and Daisuke Wakabayashi, "Russian Influence Reached 126 Million Through Facebook Alone," *The New York Times*, October 30, 2017, https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.

[6] Christopher Carbone, "1.4 million Twitter users engaged with Russian propaganda during election," *Fox News*, February 1, 2018, https://www.foxnews.com/tech/1-4-million-twitter-users-engaged-with-russian-propaganda-during-election.

[7] Alina Polyakova, "Weapons of the weak: Russia and AI-driven asymmetric warfare," (Washington, DC, United States: Brookings Institution, November 2018), https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

[8] Polina Rusyaeva and Andrey Zakharov, "Расследование РБК: как «фабрика троллей» поработала на выборах в США," RBC, October 17, 2017, https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1; Ben Collins, Gideon Resnick, Spencer Ackerman, "Leaked: Secret Documents From Russia's Election Trolls," The Daily Beast, March 1, 2018, https://www.thedailybeast.com/exclusive-secret-documents-from-russias-election-trolls-leak.

[9] Alina Polyakova, "You Can't Trust the Far Right," *The New York Times,* May 20, 2019, https://www.nytimes.com/2019/05/20/opinion/austria-russia-far-right.html.

[10] Alina Polyakova and Spencer Boyer, "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition," (Washington, DC, United States: Brookings Institution, March 2018), https://www.brookings.edu/wpcontent/uploads/2018/03/fp_20180316_future_political_warfare.pdf.

Ukraine has been the top target of Russian political warfare. Since at least 2004, Russia has consistently interfered in Ukraine's democracy. In 2014, Russia-linked cyber hackers infiltrated Ukraine's central election commission, deleting key files and implanting a virus that would have changed the results of the election in favor of a fringe ultra-nationalist party, Right Sector. A barrage of malware, denial of service attacks, and phishing campaigns bombard Ukraine's critical infrastructure environments on a daily basis. In December 2015, a well-planned and sophisticated attack on Ukraine's electrical grid targeted power distribution centers and left 230,000 residents without power the day before Christmas. The Ukrainian government attributed the attacks to the Russian Advanced Persistent Threat (APT) group "Sandworm." "BlackEnergy," the same Sandworm malware that caused the blackout in Ukraine, has been detected in electric utilities in the United States. The Christmas attack is the worst known cyber-attack on critical infrastructure systems to date.

Russian operations have also targeted Western European democracies. In 2016, in Germany, Russia's Channel One—a Russian state television channel broadcasting into Germany in Russian—initially reported that a Russian-German girl named Lisa, who had been missing for 30 hours, was sexually assaulted by migrants in Berlin. German police quickly determined that the story was false. But it was too late: the story was amplified by German and English-language Russian media (RT and Sputnik), and was widely disseminated on social media, eventually leading to demonstrations against immigrants and Chancellor Merkel. In the end, the story was traced back to a Facebook group and anti-refugee website called "Ayslterror" with Russian links.

Following the U.S. 2016 elections, an online disinformation campaign, #MacronLeaks, targeted the campaign of Emmanuel Macron in the spring of 2017. Russian intelligence agents created bogus Facebook personas in order to spy on then-candidate Macron. In addition, a trove of Macron campaign officials' emails was hacked. Even though the emails were dumped publicly just two days before the elections, during the period when media were no longer allowed to report on the elections in accordance with French law, the Twitter campaign #MacronLeaks reached 47,000 tweets in just 3.5 hours after the initial tweet.

Why Russian political warfare matters

Unlike a conventional military attack, which has direct and often detrimental consequences, a nonconventional threat is not readily felt or seen. Political warfare is purposely opaque, subversive, and thus difficult to attribute. It operates in the "grey zone." Whereas a military strike is akin to a sledgehammer with a physical target, influence operations are more like a slow drip: on its own, a single Facebook ad or a Tweet by a Russian troll-farm worker may not have any impact. But on the whole, and combined with other tools of influence, these operations aim at the core of democratic societies: trust.

Democracies work only as long as citizens trust their democratic institutions to represent their interests. Over time, the slow drip of disinformation starts to burrow a hole in that delicate political contract, eroding democratic discourse and undermining the democratic process. And disinformation campaigns don't stop when the ballot box closes—they are continuous and consistent. We may not feel the effects of such non-kinetic operations immediately or directly, but in the long-term, they present one of the greatest threats to the stability of our democracy.