Graphika

BRIEFING FOR THE UNITED STATES SENATE SELECT COMMITTEE ON INTELLIGENCE
Statement of Dr. John W. Kelly, Chief Executive Officer
Washington, DC
August 1, 2018

Chairman Burr, Vice Chairman Warner, members of the committee: Thank you for the opportunity to appear before you today to discuss the weaponization of our social media platforms and the resulting harm to our democracy.

The data now available make it clear that Russian efforts are not directed against one election, one party, or even one country. We are facing a sustained campaign of organized manipulation, a coordinated attack on the trust we place in our institutions and in our media - both social and traditional. These attacks are sophisticated and complex, and the committee's bi-partisan work to untangle and expose them sets a great example for the country.

I am a social scientist, and the CEO of a marketing analytics firm that develops advanced techniques for understanding the flow of information online. My experience with Russian online communities began ten years ago, when I helped lead a research effort at Harvard's Berkman-Klein Center for Internet & Society.[1] In this work, we observed Russia's own online political discussion evolve, from a vigorously free and open forum with a wide variety of organic voices and viewpoints, to a network rife with automated accounts and organized pro-government trolling.

In short, for the past several years, the Russian government has been doing to us what they first did at home and in Eastern Europe a decade ago.

We know this because of indispensable work by a wide range of investigative journalists, academic researchers, NGOs, and grassroots organizations, often conducted at great personal

[1] John Palfrey, Urs Gasser, John Kelly, Karina Alexanyan, Bruce Etling and Rob Faris (2010) *Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization*, Berkman Klein Center for Internet & Society at Harvard University. Available here; Karina Alexanyan, Vladimir Barash, Bruce Etling, Rob Paris, John Palfrey, Urs Gasser, Hal Roberts and John Kelly (2012) *Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere*, Berkman Klein Center for Internet & Society at Harvard University. Available here.

risk. For more than a decade, these groups have documented[2] the playbook used by the Russian government to spread chaos and discord online. These techniques include:

- Crafting fictitious online personas to infiltrate communities
- Infiltrating radical political communities on both sides to enhance their mutual distrust
- Targeting both sides of a country's most divisive issues
- Mixing pop culture references and radical political discourse to influence young minds
- Using bots and trolls for inorganic amplification
- Launching cyber attacks in conjunction with information operations

Again, each one of these features of the Russian government's attack against the American public was first tested and deployed against their own people and then refined to target their chosen enemies abroad.[3]

Thanks to the great work of this committee and to the cooperation of social media platforms, data documenting the Internet Research Agency's US-focused effort in 2016 has now been released to the public. Many dissertations will be written on this data, but today I want to highlight just three points:

First, Russian manipulation did not stop in 2016.

After election day the Russian Government stepped on the gas. Accounts operated by the IRA troll farm became more active after the election, confirming again that the assault on our democratic process is much bigger than the attack on a single election.

Second, they are targeting both sides of our political spectrum simultaneously, both before the 2016 election and right now.

We see from the IRA data how the same Russian organization will use sophisticated false personas and automated amplification, on the left and the right, in an attempt to exploit an already divided political landscape.[4] Our current landscape is particularly vulnerable to these sorts of attacks. In our estimate, today the automated accounts at the far left and far right extremes of the American political spectrum produce as many as 25 to 30 times the number of messages per day on average as genuine political accounts across the mainstream. The extremes are screaming while the majority whispers.

---

[2] *See for instance*: Ivan Sigal (13 October 2017) "Tracking Russian Online Interference Teaches Valuable Lessons on Improving News Quality." Global Voices. Available here.; Max Seddon (June 2, 2014) "Documents Show How Russia's Troll Army Hit America," Buzzfeed News. Available here; Adrian Chen (June 2 2015) "The Agency" New York Times. Available here; Leo G. Stewart, Ahmer Arif, and Kate Starbird. 2018. "Examining Trolls and Polarization with a Retweet Network." ACM, New York, NY, USA, 6 pages. Available here.

[3] Ellen Nakashima (December 25, 2017) "Inside a Russian disinformation campaign in Ukraine in 2014," Washington Post. Available here;

[4] Darren L. Linvill and Patrick L. Warren (2018) "Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building," Clemson University. Working Paper available here.

Third, American media is also being targeted. The IRA persona "Jenna Abrams," which had accounts on multiple platforms, was cited by over 40 US journalists before being unmasked.[5] The Russian activity seeks to turn the normal differences of opinion among Americans into headlines about unbridgeable political divisions. American journalism has a responsibility to harden itself to these manipulations.

The platforms' proactive transparency in these matters will be critical to keeping us ahead of new efforts and tactics, and to informing public debate on how to strengthen our democracy in the face of these threats.

There are significant challenges ahead of us, and unfortunately, knowing the other team's playbook does not mean you are going to win the game. The released data allow us to understand what the IRA did in retrospect. Detecting these efforts before they have already had their intended effect - and agreeing on how to address them - remains a formidable challenge.

On the technological front, our field is making progress on discerning technical markers that distinguish true grassroots movements from fabricated campaigns, and research is yielding methods for detecting manipulations before they gain momentum. It is equally important to keep our values front and center in this work, notably our dedication to freedom of expression and to protecting user privacy.

It will take skilled women and men professionally dedicated to this task and an investment in the development of tools and methods to first catch up, and then stay ahead, in our race to defend America's cyber-social fabric from a new form of Twenty First Century warfare.

Civil society, our media institutions, and the technology sector can only do so much in the face of it: the responsibility also lies with Government to ensure that any state actor eager to manipulate and harass[6] faces consequences for their actions. It's not just bots that are attacking us, and it's not just algorithms that must protect us.

The efforts of this committee represent a tremendous step forward in what will undoubtedly be a long and challenging process, and I commend its leadership, dedication, thoroughness, and bipartisan spirit. Thank you again for the opportunity to participate today.

---

[5] Joseph Cox and Ben Collins (2 November 2017) "Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media and the World." The Daily Beast. Available here.

[6] *See for instance:* Michael Riley, Lauren Etter and Bibhudatta Pradhan (19 July 2018) "A Global Guide to State-Sponsored Trolling." Bloomberg. Available here; Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." Working Paper 2018.1. Oxford, UK: Project on Computational Propaganda. Available here.