Statement of

NINA JANKOWICZ

Woodrow Wilson International Center for Scholars, Kennan Institute

BEFORE THE UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

Concerning

"Election Interference: Ensuring Law Enforcement Is Equipped to Target Those Seeking to Do Harm"

June 12, 2018

Introduction: *Beyond Knee-Jerk Reactions*

Chairman Grassley, Ranking Member Feinstein, and distinguished Members of the Committee: thank you for having me here today. My name is Nina Jankowicz, and I am a Global Fellow within the Kennan Institute at the Woodrow Wilson International Center for Scholars, where my research focuses on Russian disinformation and influence in Eastern Europe and beyond. It is an honor to testify before you this morning on the topic of election interference in the United States and the policy solutions necessary to protect our democratic processes. It is especially heartening to see continued bipartisan interest in this topic, as it is truly one that knows no political party.

Throughout my career, I have worked on the front lines of Russia's information war. I became familiar with Russian disinformation techniques while working on Russia programming at the National Democratic Institute, a frequent target of Russian lies. As a Fulbright Public Policy Fellow in Ukraine, I advised the Ukrainian Foreign Ministry on strategic communications issues and observed the implementation of policies meant to protect Ukraine's information environment. And over the past year, I have spoken with officials countering Russian influence and disinformation across Central and Eastern Europe as I work on a book on the development of modern Russian information warfare tactics and government responses to these critical challenges to the democratic process.

These firsthand experiences and observations have led me to a conclusion that may surprise you: even if the United States Government were to acknowledge the threat posed by Russian influence campaigns today in no uncertain terms, and we were to walk out of the hearing room and secure beyond a shadow of a doubt the country's election infrastructure; even if we hermetically sealed our information environment from inauthentic users and false or misleading information, and if social media companies finally put forth a good faith effort to put users and the security of our democracy first; even then, we would *still* not successfully dispel the threat our democracy faces from malign actors' political influence operations.

If our democratic processes are to remain secure, we must think beyond knee-jerk reactions and punitive measures. The Congress and the U.S. government must put citizens at the heart of our response to disinformation and address the issues that make our society so susceptible to outside influence in the first place.

Moscow's Main Weapon: Ourselves

Over the past few months, as we've learned more about the specifics of Russia's interference in the 2016 US election, some have questioned the Russian operation's "effectiveness" or whether it is "sophisticated" enough for us to care about. Many cite the fact that the potent advertising tools used by the Internet Research Agency are indeed available to all Facebook users.

This is a line of inquiry that privileges the American or Western experience -- as if we in the West are the only countries to have experienced these phenomena -- and dismisses the very actual fears and societal divisions that cause some of our fellow citizens to buy into Russia's tactics. It also misses a key point: **the United States is at risk for further election interference**

today not *only* because of the social media tools that malign actors exploit, but because our society is more fractured than ever.

The 2018 Edelman Trust Barometer measured a 37% decline in trust in US institutions -- government, the media, business, and NGOs -- over a single year,[1] while the Pew Research Center found in December 2017 that only 18% of the population trusts the government in Washington some or most of the time.[2] This trust-deficient environment means that American citizens are looking elsewhere for information.[3] As we saw with the Internet Research Agency's social media campaigns surrounding the 2016 election, Americans of all political stripes were receptive to content of dubious origins and messages.[4] **In short, societal fractures like ours are far more valuable to malign actors than any social media targeting tool. Only solutions with citizens at their heart can truly address these fractures and ensure our society is not left vulnerable to future interference.**

European countries that have been most successful in countering malign influence in their information and electoral environments have in common one key point: their governments recognize they cannot simply fact-check or label their way out of the crises of truth that they face.

Estonia: Outreach to the Disaffected

In Estonia in 2007, the Kremlin exploited tensions between the ethnic Russian population that had remained in Estonia after the country's independence and the native Estonian population. The dominance of Kremlin-controlled Russian language media outlets in Estonia meant that the Russian population was subjected to a constant barrage of antagonizing information, claiming in its historical revisionist narrative that Estonia owed its existence to Soviet troops who "liberated" the capital, Tallinn.[5] In reality, of course, Estonia had suffered under Soviet occupation, but this mattered little to the ethnic Russians who gathered to celebrate Victory Day and other Soviet legacy holidays at the Bronze Soldier, a monument to World War II dead and tomb of the unknown soldier in central Tallinn. Crowds grew, as did tensions between Estonian nationalists and Soviet revisionists who faced off at the monument, only narrowly avoiding physical altercations.

The Estonian government eventually decided to move the statue and associated human remains from the center of Tallinn to a military cemetery on the outskirts of the city. This decision became the latest in a long line of so-called grievances the Russian population were told they had against the Estonian government. Encouraged by the Russian media, riots broke out, destroying

---

[1] Sara Fischer, "Red alert: America suffers record drop in trust; China rises," *Axios*, 22 January 2018.
[2] Pew Research Center, Public Trust in Government 1958-2017.
[3] For more on the trust gap's role in disinformation, see: Nina Jankowicz, "Our Biggest Mistake in Fighting Fake News," *The Washington Post*, 31 March 2017.
[4] For more on the Internet Research Agency's use of social media, see: Nina Jankowicz, "The Top Three Trends We Miss When Discussing Russian Ads," Alliance for Securing Democracy, German Marshall Fund, 15 May 2018.
[5] For more on the Bronze Soldier Crisis, see Kadri Liik, "The Bronze Year of Estonian-Russian Relations," International Centre for Defence Studies, 2007.

much of the center of Tallinn and killing one. Simultaneously, Estonia was hit with a wave of cyber attacks, briefly crippling the country's banking system, government services, and Internet access.

This was Moscow's first attempt to test the disinformation and influence operation tactics we are familiar with today, and social media has only strengthened the Kremlin's ability to more insidiously target and message to receptive audiences organized along societal fissures. Eleven years later, despite the ubiquity of social media, the Kremlin's messaging in Estonia is finding fewer footholds. This is partly a natural process; Russians in Estonia enjoy the economic and social benefits of residence in an EU member state, and are keenly aware of the social, political, and economic realities of life in Russia, due to frequent travel.[6] But addition to beefing up their cyber defenses and expertise, the Estonian government has made a concerted effort to conduct outreach to the ethnic Russian population in Estonia. One of Estonia's leading universities set up a Russian-language outpost in Narva, a border city that is 95% ethnically Russian. The Estonian Ministry of Culture views Russian language programming as a strategic priority,[7] and the government has established a Russian-language TV station to compete with Russian signals. Furthermore, in terms of combatting major instances of cyber attacks and disinformation, the Estonian government believes in early governmental attribution, undermining malign actors through proactive communication.

No Estonian will tell you things are perfect, but they are much better than a decade ago. Most importantly, there is recognition among Estonian government officials and the population *writ large* that these efforts will not yield results overnight, but are a generational investment that will pay dividends in the future.

Ukraine: Beyond Bans

It's not hard to imagine what further damage the Bronze Soldier might have inflicted if social media had been more ubiquitous at the time, as this is a strategy that Russia has expanded upon and pursued in Ukraine since 2014. After Ukrainians overthrew a corrupt Kremlin-aligned government, Moscow illegally annexed the Crimean peninsula and invaded Ukraine's Donbas region. It also launched a parallel assault on Ukraine's information space, flooding social media with fake news claiming the new Ukrainian government was fascist and its election unconstitutional, among many other narratives meant to discredit the post-Maidan authorities.

Civil society groups in Ukraine launched several initiatives to separate fact from fiction, including StopFake, a fact-checking program that was one of the first defensive battalions in the modern information war. The government also undertook a series of initiatives meant to restrict access to Russian media sources, including blocking the Russian social networking sites vKontakte and Odnoklassniki in May 2017. These steps are well-intentioned and make important statements about the information environment and Ukraine's commitment to securing it, but are unlikely to change behavior in the long run. Since the 1970s, psychological research has shown

[6] See Andrew Higgins, "Two Border Cities Share Russian History -- And a Sharp European Divide," *The New York Times*, 9 November 2017.
[7] See "Estonia gets creative about integrating local Russian-speakers," *The Economist*, 10 May 2018.

that repeated untruths are difficult to debunk.[8] According to a study by Columbia University's Andrew Guess, this is even more difficult on social networks such as Twitter, where "false information... overpowers efforts to correct it by a ratio of about three to one."[9] But simply banning access to the websites where false information proliferates is also not a cure-all; while both vKontakte and Odnoklassniki became distinctly less popular in Ukraine, they both remain among the top fifteen most accessed websites. The ban itself has inspired a great deal of criticism from media freedom advocates and fed Russian disinformation that Ukraine is treating Russian speakers unfairly.[10]

Beyond fact-checking and bans, there is a growing demand for media literacy training in Ukraine, where only 23% of the population engage in basic source cross-checking.[11] IREX, an American non-governmental organization, trained 15,000 people in critical thinking, source evaluation and emotional manipulation. As a result, IREX measured a 29% increase in participants who double-check the news they consume. Eighteen months after the end of the program, participants were 13% more likely to correctly identify and critically analyze a fake news story, 25% more likely to self-report checking multiple news sources, and 28% more likely to demonstrate sophisticated knowledge of the news media industry as compared with a control group that had not been trained.[12] Last summer, the Ukrainian Ministry of Education signed a decree prioritizing media literacy in the national curriculum. While Ukraine's battle with Russian information is far from finished, these investments in the country's future will pay dividends in years to come.

Keeping Citizens at the Heart of the American Response to Malign Influence

Citizen-based responses to election interference are not a panacea. They must work in concert with structural and punitive measures, such as securing our election infrastructure and sanctions, designed to protect our institutions. To date, however, the nascent American response has focused on reactive and short-term initiatives rather than those that are proactive and generational. In addition to the stipulations provided in the Honest Ads and Secure Elections Acts, which I support, Congress must pursue and encourage citizens-based solutions in its further interactions and work related to election protection. Below are several ideas for further Congressional exploration with these principles at heart.

Social Media Regulation

Social media companies have so far played "Whack-a-Troll" in responding to Russian disinformation and election interference: researchers uncover posts linked to Russia and social

---

[8] Lynn Hasher, David Goldstein, and Thomas Toppino, "Frequency and the Conference of Referential Validity," *Journal of Verbal Learning and Verbal Behavior,* 16, 107-112, 1977.

[9] Andrew Guess, "Fact-checking on Twitter: An examination of campaign 2014," American Press Institute, 29 April 2015.

[10] Игорь Бурдыга, "Год без "В контакте" и "Одноклассников" в Украине: действуют ли санкции?" Deutsche Welle, 16 May 2018.

[11] Erin Murrock, Joy Amulya, Mehri Druckman and Tetiana Liubyva, "Winning the war on state-sponsored propaganda," IREX, 2018.

[12] *Ibid.*

media firms apologize and remove the content.[13] Unfortunately for both social media users and our democracy, it is extraordinarily easy to create and deploy fake accounts. Furthermore, there is ample evidence of information sharing and even Russian government funding of "alternative" media and fringe organizations abroad. Comparatively, trolls and bots are the least of our worries; how do we account for and stem the amplification of content that looks authentic, but has links to a malign source? These are complex challenges, but educating and empowering social media users will ameliorate them.

- To begin, social media platforms should be required to obtain **informed and meaningful consent from users to terms of service**. Most users have no idea what they are buying into when they sign up to share pictures of their dogs, chat with their friends, or follow the news. This ignorance, as well as emotion, is what Russia exploits through its online influence campaigns. All too often, users are incentivized to blindly click through terms of service that allow their data to be shared with advertisers, be they malign foreign actors or commercial entities. Users should understand the level of microtargeting to which they are being subjected, and understand its costs.

- To that end, **terms of service should be written in plain English and clearly define what content is permissible on platforms**. While platforms have been quick to use Section 230 of the Communications Decency Act to absolve themselves of responsibility for content posted on their platforms, if they are committed to supporting the democratic process, they should consider updating their terms of service to reflect whether disinformation is permissible. Those definitions should be actively enforced, whether they apply to hate speech or disinformation. It would be costly and almost certainly require human content reviewers and the establishment of a complaints and appeals process, but civil discourse and democracy are priceless.

- The steps social media companies have taken to increase advertising transparency are steps in the right direction, but blanket bans and restrictions on political ads are already being clumsily enforced.[14] One potential solution is for platforms or a third party to **establish a online advertising code of conduct that could inform a register of trusted advertisers**, akin to a Better Business Bureau.

- Social media companies have near ubiquitous access to Americans' lives; they should **embrace their role as educators**. Facebook recently announced plans to include media literacy modules at the top of users' news feeds and has taken out full page ads in national newspapers, while Twitter has participated in small-scale media literacy programs. Both platforms should focus on practices that encourage behavior change,

[13] For more on social media's response to foreign and homegrown disinformation, see Nina Jankowicz, "Russian Trolls are Only Part of the Problem," *The New York Times*, 25 January 2018.

[14] Sean Guillory, a Russian history scholar at the University of Pittsburgh with a popular educational podcast about Russia and US foreign policy, was recently denied ads for his podcast because of their "political nature." See Sean Blumenthal, "Facebook's New Ad Disclosures Are Meant to Fight Russian Trolls. A Russian History Podcaster is Paying the Price," *Huffington Post*, 8 June 2018.

rather than simply raising awareness.

Investing in Skills to Support the Democratic Process

The investments that will best protect American democracy for generations to come are decidedly low-tech. They focus not only on empowering Americans to be more savvy consumers of information on and offline, but increasing investments in our collective understanding of civics, as well as in building and repairing critical thought and civil discourse.

- Citizens-based solutions to fighting election interference should be **wider than simply teaching social media users how to recognize online fakes and fact-check**. They should include investments in civics; citizens who better understand how government works are less likely to buy into the falsehoods and conspiracies harmful to democracy. Furthermore, they should be tied to broad-based efforts to increase critical thinking skills and preserve civil discourse. This would assist people in sampling a range of viewpoints to inform their daily lives and the criticism that is healthy for any democracy, while developing greater immunity to conspiratorial versions of the truth. Finally, to avoid politicizing these efforts, they should not be couched in the language of influence operations or a direct response to Russian tactics, but simply an investment in America's future.

- As the United States continues to mount its response to election interference and online influence campaigns, Congress should **encourage cooperation and coordination across government**, particularly between the national security community and departments of education at both the national and state levels. This will promote citizens-based solutions within policy communities that are sometimes detached from the daily concerns of their fellow Americans.

- Finally, these solutions **need not be limited to the halls of schools and universities; adults should also be a target audience** for these skills-building programs. For instance, the United States could launch training programs on digital media literacy and foreign influence for government employees, as countries such as the Czech Republic have done.

Though the issue of malign political influence seems novel and insurmountable, it is one with which our country has always struggled. Even Thomas Jefferson had similar worries, but he, too, recognized the value of investing in American citizens as a holistic response to building a more secure democracy, writing in 1820: "I know of no safe depository of the ultimate powers of the society but the people themselves; and if we think them not enlightened enough to exercise their control with a wholesome discretion, the remedy is not to take it from them, but to inform their discretion by education."

Moscow will continue to attempt to influence our democracy, as it has for decades, and now that the Kremlin has written the playbook for how to do so, other bad actors will undoubtedly imitate Russian tactics. To prepare for these future attacks on democracy – and indeed, even attacks from within – we must think beyond Russia to the key actors in the democratic process: the American people.