Clint Watts

- **Robert A. Fox Fellow, Foreign Policy Research Institute**
- **Non-Resident Fellow, Alliance For Securing Democracy, German Marshall Fund of the United States**
- **Senior Fellow, Center for Cyber and Homeland Security, the George Washington University**

Statement Prepared for the U.S. Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism

"Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions" – 31 October 2017

A decade ago, al Qaeda in Iraq littered YouTube with violent videos. A few years later, Twitter became a playground for al Shabaab's violent tirades in Somalia and the devastating Westgate shopping mall attack in Kenya. During this same period, I watched from my laptop and cell phone as thousands of young men and women used Facebook, Twitter and later Telegram to join ISIS, helping pave their way to becoming the Islamic State and executing never before seen terrorist attacks on many continents. During that social media research, I encountered Russian influence efforts. In the nearly four years since, I've watched as they've employed social media at a master level to perpetrate the largest and most successful information attack in world history – a campaign that continues to harm our country even today.

Every few years social media becomes the playground for bad actors - criminals then terrorists and now authoritarians - who exploit the vulnerabilities of these information systems and our nation's civil liberties and freedoms to harm our country. Terrorists' social media use has been acute and violent, but now authoritarians have taken it to the next level using social media more subtly to do something far more dangerous – destroy our democracy from the inside out through information campaigns designed to pit Americans against each other.

With features like account anonymity, unlimited audience access, low cost technology tools, plausible deniability – social media provides Russia an unprecedented opportunity to execute their dark arts of manipulation and subversion known as Active Measures. Russia has conducted the most successful influence operation to date by infiltrating, steering and now coordinating like-minded audiences across the Western world to subvert democratic governance. The rapid spread of Russian disinformation enflames electoral divisions and employs indigenous American audiences to support the Kremlin's foreign policy of breaking all unions and alliances that challenge their rise. The Kremlin disinformation playbook will also be adopted authoritarians, dark political campaigns and unregulated global corporations who will use this type of social media manipulation to influence weaker countries, harm less educated, vulnerable populations and mire business challengers.

Social media companies consistently struggle as bad actors repeatedly exploit the seams in their systems. Each social media company has uncovered some piece of Russia's social media influence campaign but no one company alone can fully comprehend the extent of Kremlin operations. As they conduct investigations into their data, they'll each detect only those accounts where the Kremlin failed to hide its hand, seeing only the tip of the iceberg floating above the social media sea upon which they float.

Within the Kremlin's playbook, each social media platform serves a function, a role in an interlocking social media ecosystem where Russia infiltrates, engages, influences and manipulates targeted American audiences. Russia's Active Measures in social media and those nefarious dark campaigns emerging in the future will need five complementary social media functions to conduct effective full spectrum social media influence campaigns: reconnaissance, hosting, placement, propagation, and saturation.

Social media ***reconnaissance***, knowing the target audience, is the first hurdle for effectively infiltrating and influencing an audience. Twitter provides openly available and robust data on communities, and once analyzed, leads to deeper dives into key influencers and adversaries ripe for targeting. A quick jump to Facebook offers incredible insights into key targets' personal and social relationships and wider audience preferences. In parallel, LinkedIn reconnaissance outlines organizational hierarchies and work history. In sum, these platforms help bad actors orchestrate enticing tailored influence packages cognizant of each audience members' professional and personal details.

During the Cold War, creating news outlets and hosting content able to reach global audiences presented a challenge to Soviet Active Measures. But the Kremlin was probably the first to learn how RT, their state sponsored news outlet, could reach a larger audience via social media. ***Hosting*** on YouTube rather than broadcasting via satellite television, RT obscured the Russian source of their content and spread it to foreign audiences through subtler social media distribution via reporters, producers and like-minded supporters. Most Americans don't regularly watch RT, but many Americans have now seen their YouTube content. Views and clicks on their overt content provides essential audience data. This data can potentially be used by the Kremlin to hone targeted advertisements on other social media platforms or covert community infiltration through false personas.

Sowing doubt amongst electorates, leveraging conspiracies undermining confidence in democracy and smearing Kremlin challengers requires the placement of forgeries. For decades during the Cold War, the KGB's Active Measures operations created thousands of forgeries and distributed them to news outlets scattered throughout the world. Creating and placing these forgeries proved time consuming and the return on investment, if seen at all, took years to achieve. Today, anonymous sites rife with conspiracy theories, such as 4Chan and Reddit, offer unlimited options for ***placement*** of digital forgeries that drive Kremlin narratives. Graphics, memes & documents litter these discussion boards providing ammunition for Kremlin narratives and kompromat. Anonymous posts of the Kremlin's design or those generated by the target audiences power smear campaigns and falsehoods that tarnish confidence in America

and trust in democratic institutions. These anonymous placements proliferate to unwitting Americans or may be used by witting Russian agents as bogus evidence to support conspiracies, enrage and mobilize American audiences and target Kremlin foes. These placements quickly proliferate to other social media platforms where they're used to support anti-government narratives or enflame social divisions in America.

Successful, social media influence relies on ***propagation*** – the ability to spread narratives and themes to audiences far and wide. Twitter provides the single best method to quickly move stories to target audiences and introduce Kremlin narratives into the mainstream media. Should a Russian theme, narrative from their state sponsored outlets or kompromat hacked from a Kremlin foe garner a response from mainstream media outlets then organic audience engagement will naturally further Russian aims and mask Kremlin influence. Even further, Twitter offers unprecedented opportunities for employing computational propaganda via social bots. Social bots create thousands of false accounts that can simultaneously broadcast hashtags and topics thousands of times advancing Russian narratives into the trending topics on Twitter. Trending stories routinely generate mainstream media stories across print, radio and television news and migrate to the social media feeds of target audience members.

Beyond Russia, computational propaganda's attributes of replication, volume and repetition creates dangerous side effects for American audiences. Social bots can be tailored to replicate the appearance and speech of the target audience making unwitting observers more likely to engage with and believe the falsehoods they spread. What people see first and what they see the most is what they are most likely to believe. Social bots play on this psychology broadcasting at such high volumes that it makes falsehoods appear more credible. As social bots repeat falsehoods, they often drown out fact-based stories or overpower refutations of their conspiracies. Employment of social bots and fake personas allows the Kremlin to inject narratives into the feeds of key American influencers. Top government officials, political campaigns, news reporters and producers can easily be duped into unwittingly furthering Russian Active Measures in America. Those speaking out against the Kremlin are challenged by social media sweatshops and automated accounts attacking their credibility, harming their reputation and diminishing their influence amongst American policymakers.

The final component of social media influence is ***saturation***. Content shared and discussed by friends and families is more likely to be trusted than information presented by outsiders or unknown media outlets. Facebook groups, pages and personas offer Russian influence a method for spreading overt and covert content from all social media platforms directly into American discussions. Saturating the audience with divisive content designed to enrage competing poles of the U.S. electorate leads to the amplification of political and social divisions and erodes constituent faith in democracy. Russia can even use Facebook to recruit target audience members for creating and distributing propaganda, orchestrate protests and rallies or potentially incite violence – all without Americans knowing the Kremlin's involvement.

In summary, Russia employs all social media in concert to achieve its influence. As a hypothetical example, an anonymous forgery placed on 4Chan can be discussed by Kremlin

Twitter accounts who then amplify those discussions with social bots. Then, a Russian state sponsored outlet on YouTube reports on the Twitter discussion. The YouTube news story is then pushed into Facebook communities, amplified through ads or promoted amongst bogus groups. Each social media company will see but a part of the Kremlin's efforts. Unless all of the social media companies share their data, no one can fully comprehend the scope of Russia's manipulation and the degree of their impact. Russia is the first to successfully integrate the entire social media ecosystem, but they assuredly won't be the last.

Social media companies must move to deal with Russian disinformation, but also look beyond to the much larger and more ominous problem of misinformation. Some analysts have concluded fake news outperformed mainstream news in the lead up to the 2016 election.[1] The recent tragedy in Las Vegas saw an innocent man falsely labeled the gunman on social media where bogus attribution stories quickly trended to the top of Facebook feeds and Google searches.[2] More startling in just the past few weeks has been the ethnic divisions and resulting violence in Myanmar stemming from misinformation disseminated via Facebook.[3]

In previous testimony to the Senate Select Committee on Intelligence[4], the Senate Armed Services Subcommittee on Cybersecurity[5], and the Senate Committee on Homeland Security and Government Affairs[6], I proposed several policies and actions the U.S. government could pursue to thwart al Qaeda, the Islamic State and Russian Active Measures in social media. I'd offer some additional recommendations for federal legislation and policy as well as some thoughts for social media companies.

Federal laws governing attribution of political ads and solicitations in television, radio and print should immediately be extended to social media advertising conducted by political campaigns and political action committees. Social media political advertising will continue to grow in every election cycle and U.S. citizens must know the source of the information they consume in any medium – print, radio, television or social media.

Social media companies must assist in protecting the integrity of democratic principles, institutions and processes - the very governance systems that have provided them the freedoms and free markets to flourish. Users should be provided information on the source of all advertisements brought into their social media feeds. Account anonymity in public provides some benefits to society, but social media companies must work immediately to confirm real humans operate accounts. The negative effects of social bots far outweigh any benefits that come from the anonymous, replication of accounts that broadcast high volumes of misinformation. Reasonable limits on the number of posts any account can make during an hour, day or week should be developed. Even further, human verification systems (CAPTCHA) should be employed by all social media companies to reduce automated broadcasting.

Social media companies continue to get beat in part because they rely too heavily on technologists and technical detection to catch bad actors. Artificial intelligence and machine learning will greatly assist in cleaning up nefarious activity, but will for the near future, fail to detect that which hasn't been seen before. Threat intelligence proactively anticipating how bad

actors will use social media platforms to advance their cause must be used to generate behavioral indicators that inform technical detection. Those that understand the intentions and actions of criminals, terrorists and authoritarians must work alongside technologists to sustain the integrity of social media platforms. This has become an effective, improved and common practice in cyber security efforts to deter hackers, but to date, I've not seen a social media company routinely and successfully employ this approach. As an example, the Alliance for Securing Democracy's Hamilton 68 and Artikel 38 dashboards use this exact approach to diagnose the Kremlin's influence efforts via social media and raise awareness for the public.[7]

Social media companies and search engines will continue to grow as the most prominent distributors of news and information worldwide. Yet, time and again, falsehoods have outpaced truth, and fiction has outpaced facts resulting in a grave disservice to Americans. I admire those social media companies that have begun working to fact check news articles in the wake of last year's election. These efforts should continue but will be inadequate for stopping the 'fake news' epidemic plaguing their systems.

Stopping the false information artillery barrage landing on social media users comes only when those outlets distributing bogus stories are silenced – silence the guns and the barrage will end. I propose "nutrition labels" for information outlets, a rating icon for news producing outlets displayed next to their news links in social media feeds and search engines.[8] The icon would provide users an assessment of the news outlet's ratio of fact versus fiction and reporting versus opinion. The opt-out rating system would not infringe freedom of speech or freedom of press, but would inform users as to the veracity of content and its disposition. Users wanting to consume information from outlets with a poor rating wouldn't be prohibited, and if they are misled about the truth they have only themselves to blame. The information consumer reports agency producing the rating would reside outside the social media companies, have no contact with the government and should be a non-profit entity. The public would benefit from collective rating systems as top performing outlets focused on facts and reporting would likely garner more views over time. In contrast, pop-up conspiracy outlets promoting falsehoods would receive fewer views, less advertising clicks and shares over time hopefully reducing their distribution and squelching their falsehoods. Cumulatively, the public, mainstream media and social media companies all benefit from the rating system without restricting or regulating individual freedoms.

It's been more than a year since my colleagues and I described in writing how the Russian disinformation system attacked our American democracy.[9] We've all learned considerably more since then about the Kremlin's campaigns, witnessed their move to France and Germany and now watch as the world worst regimes duplicate their methods. Yet our country remains stalled in observation, halted by deliberation and with each day more divided by manipulative forces coming from afar. The U.S. government, social media companies, and democracies around the world don't have any more time to wait. In conclusion, civil wars don't start with gunshots, they start with words. America's war with itself has already begun. We all must act now on the social media battlefield to quell information rebellions that can quickly lead to violent confrontations and easily transform us into the Divided States of America.

[1] Craig Silverman. "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook," *Buzzfeed News,* 16 November 2016. Available at: https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.pk37kJVDgG#.pl38yQq90A

[2] Sam Levin. "Facebook and Google promote politicized fake news about Las Vegas shooter," *The Guardian,* 2 October 2017. Available at: https://www.theguardian.com/us-news/2017/oct/02/las-vegas-shooting-facebook-google-fake-news-shooter

[3] Megan Specia and Paul Mozur. " A War Of Words Puts Facebook at the Center of Myanmar's Rohingya Crisis." *The New York Times.* 27 October 2017. Available at: https://www.nytimes.com/2017/10/27/world/asia/myanmar-government-facebook-rohingya.html

[4] Clint Watts. "Disinformation: A Primer In Russian Active Measures and Influence Campaigns." Statement prepared for the Senate Select Committee on Intelligence, 30 March 2017. Available at: https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf.

[5] Clint Watts. "Cyber-enabled Information Operations." Statement prepared for the Senate Committee on the Armed Services, Subcommittee on Cybersecurity, 27 April 2017. Available at: https://www.armed-services.senate.gov/download/watts_04-27-17

[6] Clint Watts. "Terror in Europe: Safeguarding U.S. Citizens at Home and Abroad." Statement prepared for the Senate Committee on Homeland Security and Government Affairs, 5 April 2016. Available at: https://www.fpri.org/article/2016/04/terror-europe-safeguarding-u-s-citizens-home-abroad/

[7] See the Alliance for Securing Democracy for the Hamilton 68 and Artikel 38 Russian propaganda tracking efforts at this link: http://securingdemocracy.gmfus.org/

[8] Clint Watts and Andrew Weisburd. "Can the Michelin Model Fix Fake News?" *The Daily Beast.* 22 January 2017. Available at: https://www.thedailybeast.com/can-the-michelin-model-fix-fake-news

[9] Andrew Weisburd, Clint Watts and J.M. Berger. "Trolling For Trump: How Russia Is Trying To Destroy Our Democracy." *War On The Rocks.* 6 November 2016. Available at: https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/