Clint Watts

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

Statement Prepared for the U.S. Senate Committee on Commerce, Science and Transportation

"Terrorism and Social Media: Is Big Tech Doing Enough?" – 17 January 2018

Ten years ago, it was al Qaeda in Iraq videos on YouTube. A few years later, al Shabaab's deadly rampages played out on Twitter. Shortly after, Facebook groups and Twitter feeds brought the Islamic State to the world's attention and into the homes of new recruits, before they scurried off to other social media applications like Telegram. And four years ago amongst global jihad's social media storm, I stumbled into Russian influence campaigns, their reboot of an old playbook called "Active Measures", which they've deployed across nearly all social media platforms with devastating effect.

Today, disinformation spread on Facebook propels deadly violence in Myanmar against the minority Ronhingya population.[i] The Duterte regime in the Philippines uses social media groups to suppress domestic political opponents.[ii] LTG H.R. McMaster, our National Security Advisor, noted just last week the Kremlin is again using its cyber influence just across our southern border seeking to push their preferred party and politicians to the forefront in Mexico.[iii]

Social media, at its height, offered a platform for discussion across diverse audiences and led to uprisings usurping dictators during the Arab Spring. But bad actors with motivation, money, manpower and know-how will always come to these information gateways to pursue their objectives. Criminals, terrorists and authoritarians see the Internet and social media as a cost effective open doorway into the very heart of their adversaries. Authoritarians worldwide now recognize the power of the Kremlin's social media manipulation, and if left unchecked, will copy and deploy Russia's playbook against their enemies. Lesser-educated populations around the world predominately arriving in cyberspace via mobile phones will be particularly vulnerable to the social media manipulation of terrorists and authoritarians.

American focus on the Islamic State's social media recruitment or Russian meddling in the 2016 Presidential election overlooks other indicators of damaging activity. American companies have suffered and remain particularly vulnerable to smear campaigns launched by foreign state actors through malicious, false narratives pushed by bogus social media personas. These campaigns can cause serious reputational damage sending stock prices plummeting and decreasing sales.

Beyond just smear campaigns and character assassination, this committee should take seriously the ability of foreign nations to mobilize violence inside the U.S. through an evolution I would call "Anwar Awlaki meets PizzaGate". Just a few years ago, Anwar al-Awlaki, al Qaeda in the Arabian Peninsula's leader of external operations, recognized the power of the Internet to recruit and mobilize terrorists in America to conduct violence in the U.S. homeland. The Islamic State took this to another level with their spokesman abu Muhammad al-Adnani calling on supporters to conduct attacks at home[iv] and then further enabling e-recruits by using a social media battalion to guide plots remotely – connecting with, coaching and directing terrorists in the West to specific targets.[v] A little over a year ago, America saw an individual consume a false conspiracy on the Internet and social media, known as PizzaGate, and then travel to Washington DC to investigate these bogus claims. He arrived at a falsely implicated restaurant and discharged a weapon before being arrested. [vi]

Surely a foreign adversary of the United States sees an opportunity in combining these two scenarios. The greatest concern moving forward might likely be a foreign intelligence service, posing as Americans on social media, infiltrating one or both political extremes in the U.S. and then recruiting unwitting Americans to undertake violence against a target of the foreign power's choosing. Social media companies will be better positioned to stop this potential scenario from occurring than U.S. intelligence or homeland security that are blind to the technical signatures behind this manipulation.

The U.S. government's response to terrorist social media use has been sustained and significant, and their response to state sponsored influence on Americans disjointed and perplexing. In both cases, government officials have pointed to social media companies asking why they would allow their platforms to be used for nefarious purposes.

Social media companies realize the damage of these bad actors far too late. They race to implement policies to prevent the last information attack, but have yet to anticipate the next abuse of their social media platforms by emerging threats seeking to do bad things to good people. In previous testimony to the Senate Homeland Security[vii], Intelligence[viii], Armed Services[ix] and Judiciary[x] committees, I've offered a range of recommendations for how to counter bad actors using social media in the pursuit of violence and nefarious influence. Today, I'll focus and reiterate a few of these recommendations.

The first and most pressing challenge comes in the debate over social media account anonymity and authenticity. Anonymity of social media accounts has in many cases allowed the oppressed and the downtrodden to speak out about injustice. It's given the weak a voice against the strong, powerful, and corrupt. But over time, anonymity has empowered hackers, extremists and authoritarians to inflict harm on the public. Under the veil of anonymity, they spread hate, recruit members and advance divisions in American society.

All people, real humans and their virtual personas, have the right to free speech, but this right to free speech does not permit them to endanger society. Account anonymity today allows nefarious social media personas to shout the online equivalent of “fire” in a movie theater. Bad actors and their fictitious and/or anonymous social media accounts can and have created a threat to public safety. This is not protected free speech and many social media companies offer no method to hold these anonymous personas accountable.

Social media companies can and should protect the public anonymity of account holders if the user chooses, but they must be able to determine a real, authentic person resides behind each persona accountable for their actions on the platform. Some social media companies have advanced better methods to certify account authenticity. However, the current level of authenticity on the Twitter platform is sub-optimal. I’d encourage Twitter to rapidly expand its verification to as many users as possible, as quickly as possible.

Closely connected to the issue of account authenticity is the rise of computational propaganda. The negative effects of social bots far outweigh any benefits. The anonymous, replication of accounts that routinely broadcast high volumes of misinformation can pose a serious risk to public safety and when employed by authoritarians a direct threat to democracy. Social bots should be ceased immediately. For non-automated accounts, 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.

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 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. Some social media companies have already moved in this direction.

I'd note it's unreasonable to think that every social media company can and should hire threat analysts for every possible emerging threat. But a variety of rapid outreach approaches with external social media analysts and threat experts positioned outside social media companies could easily be developed or even be collectively sponsored by social media companies. Several models from counterterrorism and cybersecurity could be adopted by Silicon Valley in this regard.

I've made many other recommendations in the past but will close for now and can elaborate further on them during the question and answer session. In conclusion, some social media companies have done more than others to improve the safety and integrity of their platforms. Others have a lot of work to do to improve their platforms against bad actors. Ultimately, the American consumer will decide whether the benefits of using these services outweigh the risks. Many are walking away from social media applications because they can't trust the information being shared or tolerate the vitriolic user experience. Social media companies should move aggressively to thwart terrorists and authoritarians exploiting their systems not only because its what's best for their users and society, but because it's good for business as well.

[i] Hannah Beech. "Across Myanmar, Denial of Ethnic Cleansing and Loathing of Rohingya." *New York Times.* 24 October 2017. Available at: https://www.nytimes.com/2017/10/24/world/asia/myanmar-rohingya-ethnic-cleansing.html?_r=0.
[ii] Lauren Etter. "What happens when the government uses Facebook as a weapon?" *Bloomberg*. 7 December 2017 Available at: https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook.
[iii] David Alire Garcia and Noe Torres. "Russia meddling in Mexican election: White House aide McMaster." *Reuters.* 7 January 2018. Available at: https://www.reuters.com/article/us-mexico-russia-usa/russia-meddling-in-mexican-election-white-house-aide-mcmaster-idUSKBN1EW0UD.
[iv] Bulos, Nabih. "Islamic State's taunting speech calls for killing civilians." *LA Times*. 22 September 2014. Available at: http://beta.latimes.com/world/middleeast/la-fg-islamic-state-taunts-20140922-story.html.
[v] Rukmini Callimachi, "Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar." *New York Times*. 4 Feb 2017. Available at: https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html?_r=0.
[vi] Grace Hauck. "Pizzagate shooter sentenced to 4 years in prison." *CNN*. 22 June 2017. Available at: http://www.cnn.com/2017/06/22/politics/pizzagate-sentencing/index.html.
[vii] 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/

[viii] 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.

[ix] 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

[x] Clint Watts. “Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions.” Statement prepared for the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism. Available at: https://www.judiciary.senate.gov/download/10-31-17-watts-testimony.