Extremist Content and Russian Disinformation Online:
Working with Tech to Find Solutions
Clint Watts
Questions for the Record
Submitted November 7, 2017

QUESTIONS FROM SENATOR FEINSTEIN

My responses are annotated below in blue.

Success of Russian Disinformation

1. You have described social media as providing Russia "cheap, efficient and highly effective access to foreign audiences with plausible deniability of their [Russia's] influence." (Statement for Intelligence Committee Hearing, March 30, 2017)

    a. How did this play out during the 2016 election?
    My observations of Russian influence efforts began in 2014. During that period, I believe the Russian were developing their capabilities to conduct online influence. In 2015, they moved deliberately into the U.S. audience on both the left and right wings of the political spectrum, but some audiences responded to this infiltration to higher degree than others. In 2015, Russia played on social divisions in the U.S. information space to further polarize and amplify animosity, providing a window for them to infiltrate American audiences they would later influence in 2016. Critical to the Russian effort was their hacking and later compromising political targets in the run up to the election. These actions provided the fuel for narratives used to harm then candidate Clinton seeking to reduce her domestic electoral support and depress turnout. The most dangerous aspect of the Russian effort was their push to discredit the integrity of the U.S. election processes by pushing narratives of "Voter Fraud" and "Election Rigging". These claims sought to undermine American faith in democracy and electoral processes – a direct attack by Russia on our country.

    b. According to Facebook, the Research Internet Agency spent $100,000 on over 3,000 ads. With that expenditure, what type of reach do you think Russia achieved?

    I believe these ads were seen by millions of Americans in total. I would add that these ad purchases were one of the smaller efforts Russia conducted on social media to influence the U.S. election. My assessment would be that their operations on Twitter and Facebook in terms of false personas promoting content and engaging in discussions had a much larger influence effect.

    c. What are the key factors that enable Russia's success with social media?

    Russia blends all social media to achieve their objectives. Two factors provide Russia a decisive advantage. First, anonymity allows Russia, regardless of the

social media platform, to hide their hand creating plausible deniability of their influence actions. Second, social media allows Russia to infiltrate U.S. audiences by creating personas that look like and talk like real Americans. This gives Russia the ability to advance their agenda with U.S. audiences that would likely reject overt outreach from the Kremlin.

d. What is the impact of having campaigns or candidates also engaging on these platforms and disseminating divisive messages or disinformation?

Russian influence efforts when combined with political campaign messaging amplifies divisions and animosity between competitors in the information space. This leads to American divisiveness that is often based on false pretenses and results in less political compromise and debate, which are essential in the conduct of a successful, effective democracy.

Notification of Law Enforcement

2. Recently, British parliament's Home Affairs Select Committee released a report finding that social media platforms, such as Facebook, Twitter, and YouTube, failed to remove extremist material posted by banned jihadist and neo-Nazi groups, even when that material was reported. I am working on legislation to require technology companies to report known terrorist activity on their platforms to law enforcement. The provision is modeled after an existing law which requires technology companies to notify authorities about cases of child pornography.

a. What are technology companies doing to prevent this type of activity from occurring on their platforms?

I have not been briefed directly by the social media companies on their policies and procedures. However, from observation, it appears that social media companies are using user reports of terms of service violations to spot extremist content and then assess whether that content should be on the platform.

b. In what ways do you think that technology companies can do more to prevent this type of activity from occurring on their platform?

Social media companies could improve on these methods by employing more threat analysts that understand extremist groups. These threat analysts can help technologists develop machine learning solutions that catch more extremist content in a rapid and more preemptive fashion.

Civil Injunction Authority Related to Terrorism

3. As you know, there is a relentless and growing ISIL recruitment effort through social media platforms. Recruitment is repeatedly identified in nearly all of the 100+ criminal indictments brought by federal authorities during the past two years relating to ISIL. Anwar al-Awlaki is frequently named as one of the inspirational sources in many of these

indictments. I understand that civil injunction authority exists for the Attorney General to obtain orders against those who provide material support to a foreign terrorist organization, as well as to shut down websites from distributing software for spying on people.

a. Do you believe that this type of civil injunction authority could help prevent terrorists and extremists from using tech platforms to commit crimes?

Yes, I believe this injunction will help those working to quell extremist content arising in social media.

Hearing on Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions"
Judiciary Subcommittee on Crime and Terrorism October 31, 2017

QUESTIONS FOR THE RECORD FROM SENATOR WHITEHOUSE

Mr. Clint Watts – Responses in Blue

1) We now know that Russia was able to use disinformation to interfere in our elections in 2016. Why do you think those efforts were successful in this particular context?

There are many reasons that Russia was able to influence the 2016 Presidential election. For a summary of them, I have outlined the major advantages and techniques they used in this article, "How Russia Wins An Election," Clint Watts and Andrew Weisburd, Dec 13, 2016. Available at: https://www.politico.com/magazine/story/2016/12/how-russia-wins-an-election-214524

Three other factors should be of note. First, those investigating Russian hacking of American targets did not understand that hacking was not being used strictly for criminal theft but instead to later be released as *kompromat* on key political targets. This was new from the American perspective.

Second, the U.S. failed to see how Russia's influence system being used overseas might make its way to the U.S. The social media influence campaigns were already being used in the European context and the U.S. didn't seem aware that it could happen here.

Third, U.S. political campaigns wittingly or unwittingly used Russian Active Measures campaigns against other Americans. Each week, more instances of Russian influence accounts and narratives being employed by political campaigns surfaces.

2) Why do social media platforms keep "getting beat" by foreign entities looking to spread hate or disinformation? What is the role of the federal government when it comes to preventing this exploitation of social media platforms?

The greatest vulnerability of social media for foreign influence is account anonymity. There are justifiable reasons why publicly, an account might want to maintain their anonymity. But social media companies need to verify that real humans are behind the accounts. Social media companies must ensure real humans operate accounts in order to thwart social bots and their artificial amplification of content and with regards to extremist groups. Real humans should be held responsible for their extremist content that is being posted online. Twitter could expand its verification process to ensure real humans are on their platform and restore trust to its users.

The federal government should enact legislation to ensure social media advertising by

political campaigns and political action committees meets the same standards as that for television, radio and print advertising.

3) You were involved in the launch of Hamilton 68, a website which tracks Russian propaganda in near-real time and is now working to expose trolls who use Twitter to amplify pro-Russian themes. What main lessons have you learned from tracking this project? Do these lessons lead you to believe that companies can address this problem independently, or is legislation necessary?

In the absence of any U.S. government entity being responsible for detecting and countering Russian influence, I helped launch the Hamilton 68 initiative. We wanted to raise awareness of how Russia does its influence. I think the main lessons are twofold. One, Russia uses social media predominately through the allowable ways any user uses social media. They haven't invented any particular weapon or capability, but instead used the vulnerabilities of social media platforms and the American public to exploit fissures in our country. Second, any and all divisive issue in our country which pulls Americans apart will be exploited by Russian influence. I'd add that Russia may have greater success infiltrating some audiences that others, but ultimately they seek to be in all audiences in the U.S. information space.

I believe legislation should require verification that real humans are operating accounts and can be held accountable for their speech and actions. Second, standards for political advertising observed in other media should be enforced in social media as well.

4) You noted in your testimony that extremist organizations often "radicalize in public and recruit in the dark," using public social media to expose potentially sympathetic individuals to a radicalizing message before moving to more secure channels to make contact and recruit. What can law enforcement do to better prevent extremist organizations from exploiting this pathway?

Law enforcement must not focus on social media monitoring as much as good investigative operations, namely the developing of sources, informants and undercover operations which can provide greater clarity on the recruitment of people in the darker corners of the Internet. I believe, at the federal level, there have been great gains in this area. But for state and local law enforcement, where there are fewer resources and less technical capability, the federal government could be a great help to state and local law enforcement investigations.

Clint Watts – Extremist Content and Russian Disinformation Online
Questions for the Record
Submitted November 7, 2017

QUESTIONS FROM SENATOR COONS

Responses for Clint Watts are noted below in blue

1. Foreign entities will continue to try to use social media to interfere with U.S. elections. What actions would you recommend that the Executive Branch take to combat Russian interference?

I will refer to two previously submitted written testimony for this question. For a whole-of government approach, I will include my statement to the Senate Select Intelligence Committee on 30 March 2017. For methods to develop these capabilities I will include comments from my statement to the Senate Armed Services Sub-committee on 27 April 2017.

From my testimony to the Senate Select Intelligence Committee on 30 March 2017. Available at: https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf.

"The U.S. Can Counter Russia's Modern Active Measures

America can defuse Russia's Active Measures online by undertaking a coordinated and broad range of actions across the U.S. government. Currently, the U.S. ignores, to its own detriment, falsehoods and manipulated truths generated and promoted by Russia's state sponsored media and their associated conspiratorial websites. While many Active Measures claims seem ridiculous, a non-response by the U.S. government introduces doubt and fuels social media conspiracies. The U.S. should generate immediate public refutations to false Russian claims by creating two official government webpages acting as a U.S. government "Snopes" for disarming falsehoods. The U.S. State Department would host a website responding to false claims regarding U.S. policy and operations outside U.S. borders. The U.S. Department of Homeland Security would host a parallel website responding to any and all false claims regarding U.S. policy and operations domestically – a particularly important function in times of emergency where Russian Active Measures have been observed inciting panic.

Criminal investigations bringing hackers to justice will continue to be vital. However, the FBI must take a more proactive role during investigations to analyze what information has been stolen by Russia and then help officials publicly disclose the breach in short order. Anticipating rather than reacting to emerging Russian data dumps through public affairs messaging will help U.S. officials and other American targets of kompromat prepare themselves for future discrediting campaigns.

Russian propaganda sometime peddles false financial stories causing rapid shifts in American company stock prices that hurt consumer and investor confidence and open the way for predatory market manipulation and short selling. At times, U.S. business employees unwittingly engage with Russian social media hecklers and honeypots putting themselves and their companies at risk. The Departments of Treasury and Commerce should immediately undertake an education campaign for U.S. businesses to help them thwart damaging, false claims and train their employees in spotting nefarious social media operations that might compromise their information.

The Department of Homeland Security must continue to improve existing public-private partnerships and expand sharing of cyber trends and technical signatures. This information will be critical in helping citizens and companies prevent the hacking techniques propelling Russian kompromat. Finally, U.S. intelligence agencies have a large role to play in countering Russian Active Measures in the future, but my recommendations in this regard are not well suited for open discussion."

In my previous testimony on 27 April 2017 to the Senate Committee on Armed Services – Subcommittee On Cybersecurity, available at: https://www.armed-services.senate.gov/imo/media/doc/Watts_04-27-17.pdf

"**2) How can the U.S. government counter cyber-enabled influence operations?**

When it comes to America countering cyber-enabled influence operations, when all is said and done, far more is said than done. When the U.S. has done something to date, at best, it has been ineffective, and at worst, it has been counterproductive. Despite spending hundreds of millions of dollars since 9/11, U.S. influence operations have made little or no progress in countering al Qaeda, its spawn the Islamic State or any connected jihadist threat group radicalizing and recruiting via social media.

Policymakers and strategists should take note of this failure before rapidly plunging into an information battle with state sponsored cyber-enabled influence operations coupled with widespread hacking operations – a far more complex threat than any previous terrorist actor we've encountered. Thus far, U.S. cyber influence has been excessively focused on bureaucracy and expensive technology tools - social media monitoring systems that have failed to detect the Arab Spring, the rise of ISIS, the Islamic State's taking of Mosul and most recently Russia's influence of the U.S. election. America will only succeed in countering Russian influence by turning its current approaches upside down, clearly determining what it seeks to achieve with its counter influence strategy and then harnessing top talent empowered rather than shackled by technology.

- **Task –** Witnessing the frightening possibility of Russian interference in the recent U.S. Presidential election, American policy makers have immediately called to counter Russian cyber influence. But the U.S. should take pause in rushing into such efforts. The U.S. and Europe lack a firm understanding of what is currently taking place. The U.S. should begin by clearly mapping out the purpose and scope of Russian cyber influence methods. Second, American politicians, political organizations and government officials must reaffirm their commitment to fact over fiction by regaining the trust of their constituents through accurate communications. They must also end their use of Russian compromat stolen from American citizens' private communications as ammunition in political contests. Third, the U.S. must clearly articulate its policy with regards to the European Union, NATO and immigration, which, at present, mirrors rather than counters that of the Kremlin. Only after these three actions have been completed, can the U.S. government undertake efforts to meet the challenge of Russian information warfare through its agencies as I detailed during my previous testimony.

- **Talent** –Russia's dominance in cyber-enabled influence operations arises not from their employment of sophisticated technology, but through the employment of top talent. Actual humans, not artificial intelligence, achieved Russia's recent success in information warfare. Rather than developing cyber operatives internally, Russia leverages an asymmetric advantage by which they coopt, compromise or coerce components of Russia's cyber criminal underground. Russia deliberately brings select individuals into their ranks, such as those GRU leaders and proxies designated in the 29 December 2016 U.S. sanctions. Others in Russia with access to sophisticated malware, hacking techniques or botnets are compelled to act on behalf of the Kremlin.

  The U.S. has top talent for cyber influence but will be unlikely and unable to leverage it against its adversaries. The U.S. focuses excessively on technologists failing to blend them with needed information campaign tacticians and threat analysts. Even further, U.S. agency attempts to recruit cyber and influence operation personnel excessively focus on security clearances and rudimentary training thus screening out many top picks. Those few that can pass these screening criteria are placed in restrictive information environments deep inside government buildings and limited to a narrow set of tools. The end result is a lesser-qualified cyber-influence cadre with limited capability relying on outside contractors to read, collate and parse open source information from the Internet on their behalf. The majority of the top talent needed for cyber-enabled influence resides in the private sector, has no need for a security clearance, has likely used a controlled substance during their lifetime and can probably work from home easier and more successfully than they could from a government building.

- **Teamwork** – Russia's cyber-enabled influence operations excel because they seamlessly integrate cyber operations, influence efforts, intelligence operatives and diplomats into a cohesive strategy. Russia doesn't obsess over their bureaucracy and employs competing and even overlapping efforts at times to win their objectives.

  Meanwhile, U.S. government counter influence efforts have fallen into the repeated trap of pursuing bureaucratic whole-of-government approaches. Whether it is terror groups or nation states, these approaches assign tangential tasks to competing bureaucratic entities focused on their primary mission more than countering cyber influence. Whole-of-government approaches to countering cyber influence assign no responsible entity with the authority and needed resources to tackle our country's cyber adversaries. Moving forward, a task force led by a single agency must be created to counter the rise of Russian cyber-enabled operations. Threat based analysis rather than data analytics will be essential in meeting the challenge of Russian cyber influence operations. This common operational picture must be shared with a unified task force, not shared piecemeal across a sprawling interagency.

- **Technology** – Over more than a decade, I've repeatedly observed the U.S. buying technology tools in the cyber- influence space for problems they don't fully understand. These tech tool purchases have excessively focused on social media analytical packages producing an incomprehensible array of charts depicting connected dots with different colored lines. Many of these technology products represent nothing more than modern

snake oil for the digital age. They may work well for Internet marketing but routinely muddy the waters for understanding cyber influence and the bad actors hiding amongst social media storm. Detecting cyber influence operations requires the identification of specific needles, amongst stacks of needles hidden in massive haystacks. These needles are cyber hackers and influencers seeking to hide their hand in the social media universe. Based on my experience, the most successful technology for identifying cyber and influence actors comes from talented analysts that first comprehensively identify threat actor intentions and techniques and then build automated applications specifically tailored to detect these actors. The U.S. government should not buy these technical tools nor seek to build expensive, enterprise-wide solutions for cyber-influence analytics that rapidly become outdated and obsolete. Instead, top talent should be allowed to nimbly purchase or rent the latest and best tools on the market for whatever current or emerging social media platforms or hacker malware kits arise.

2. Is legislation necessary to confront the ongoing threat of Russian propaganda and ISIS propaganda on social media platforms?

Yes, social media companies should be required to observe the same standards for political advertising by campaign and political action committees that is required in television, radio and print media. Social media companies must be able to identify the source of advertising to ensure there is no foreign influence on U.S. elections.

3. Social media companies have announced reforms intended to identify fake accounts and pages and increase scrutiny of ad purchases. Do you believe those proposals are sufficient?

The same provisions for political advertising on television and radio should be observed in social media advertising. Most political news and advertising moving forward, regardless of Russian influence, will be seen through social media and not regulating their advertisements will harm the electorate. Social media companies could improve on their methods for detecting false accounts by employing more threat analysts that understand extremist groups. These threat analysts can help technologists develop machine learning solutions that catch more extremist content in a rapid and more preemptive fashion.

4. In your view, are social media companies overly reliant on algorithms and computer intelligence to detect and prevent interference by foreign adversaries?

Yes, social media companies must understand what bad actors might do on their platforms to anticipate rather than react to their ill intentions and erosion of trust and security on their platforms. Algorithms, to this point, can only detect what has been seen before. Thus, hackers, terrorists and Russian influence agents will always have the advantage of a first strike.

5. How do we prevent propaganda from masquerading as real news, while ensuring that we do not infringe upon the First Amendment?

Protection of free speech and freedom of the press is of the utmost importance to our country. Social media companies trying to fact check news will always be overwhelmed.

False information can be produced faster than it can be refuted. I propose instead the development of an independent, non-profit, non-governmental information rating agency that provides a comprehensive rating to news agencies that appears in consumers' news feeds on social media and search engines on the Internet. A full discussion of my recommendation can be found here in this article: Clint Watts and Andrew Weisburd, "Can the Michelin Model Fix Fake News?": https://www.thedailybeast.com/can-the-michelin-model-fix-fake-news.

6. At the hearing, you testified that the United States is "in no way prepared right now for what's going on" with respect to foreign adversaries' interference using social media and violent extremism online.
   a. In terms of foreign adversaries' interference using social media, what are our most exploitable weaknesses? What steps can private companies take to fix them? What can Congress do to address them?

      The greatest weakness of social media for foreign influence is account anonymity. There are justifiable reasons why publicly, an account might want to maintain their public anonymity. But the social media companies need to verify that real humans are behind the accounts on their platform. Social media companies must ensure real humans operate accounts in order to thwart social bots and their artificial amplification of content and with regards to extremist groups. Real humans should be held responsible for their extremist content that is being posted online. Twitter could expand its verification process to ensure real humans are on their platform and restore trust to its users.

   b. In terms of violent extremism online, what are our most exploitable weaknesses? What steps can private companies take to fix them? What can Congress do to address them?

      Same as the answer for 6a. I'd also add that rapid removal and enforcement of banned content is essential and I think social media companies are making great gains in this regard.

7. In January, Senator Gardner and I introduced a bipartisan resolution to establish a Select Committee on Cybersecurity (S.Res. 23), which Senators McCain and Blumenthal have cosponsored. Do you support this bill to create a Select Committee on Cybersecurity? If not, how can it be improved?

   Yes, I believe this a must. U.S. preparedness and legislation is woefully behind where it needs to be and places the country at risk.