Clint Watts
• Robert A. Fox Fellow, Foreign Policy Research Institute
• Senior Fellow, Center for Cyber and Homeland Security, the George Washington University

Statement Prepared for the U.S. Senate Committee on Armed Services – Subcommittee On Cybersecurity

"Cyber-enabled Information Operations" - 27 April 2017

Mr. Chairman, Members of the Committee. Thank you for inviting me today and for furthering the discussion of cyber-enabled influence. My remarks today will further expand on my previous testimony to the Senate Select Committee on Intelligence on 30 March 2017 where I detailed the research Andrew Weisburd, J.M. Berger and I published regarding Russian attempts to harm our democracy via social media influence. I'll add further to this discussion and will also provide my perspective having worked on cyber-enabled influence operations and supporting programs for the U.S. government dating back to 2005. Having served in these Western counterterrorism programs, I believe there are many lessons we should learn from and not repeat in future efforts to fight and win America's information wars.

1) How does Russian nation state influence via social media differ from other influence efforts on social media?

As I discussed on March 30, 2017, Russia, over the past three years, has conducted the most successful influence campaign in history using the Internet and more importantly social media to access and manipulate foreign audiences. Russia and other nation states are not the only influencers in social media. Profiteers pushing false or salacious stories for ad revenue, political campaigns running advertisements and satirists looking for laughs also seek to influence audiences during elections, but their online behavior manifests differently from that of Russia. Russia's hacking may be covert, but their employment of compromat ultimately reveals their overt influence campaigns. Furthermore, Russian influence performs a full range of actions to achieve their objectives that distinguish them from other influence efforts.[1]

- ***Create, Push, Share, Discuss, Challenge (CPSDC) - Effective State Sponsors Do All Of These In The Influence Space, Others Do Only Some***
    - ***Create*** - Russia uses their state sponsored media outlets and associated conspiratorial websites to ***create*** propaganda across political, social, financial and calamitous message themes. This content, much of which is fake news or manipulated truths, provides information missiles tailored for specific portions of an electorate they seek to influence. More importantly, Russia's hacking and theft of secrets provides the nuclear fuel for information atomic bombs delivered by their state sponsored media outlets and covert personas. This information fuels not only their state sponsored outlets but arms the click-bait content development of profiteers and political parties who further amplify Russia's narratives amongst Western voters.
    - ***Push*** – Unlike other fake news dissemination, Russia synchronizes the ***push*** of their propaganda across multiple outlets and personas. Using sockpuppets and automated bots appearing to be stationed around the world, Russia simultaneously amplifies narratives in such a way to grab mainstream media attention. Many other social media bots push false and misleading stories for profit or politics but their patterns lack the synchronization and repeated delivery of pro-Russian content and usually follow rather than lead in the dissemination of Russian conspiracies.
    - ***Share*** - Like-minded supporters, aggregators (gray accounts) and covert personas (black accounts) ***share*** coordinated pushes of Russian propaganda with key nodes on a one-to-one or one-to-many basis. This coordinated sharing seeks to further amplify and cement influential content and their themes amongst a targeted set of voters. Their sharing often involves content appealing to either the left or right side of the political spectrum as well as any anti-government or social issue. This widespread targeting often varies from profiteers and political propagandists that seek a high rate of consumption across a narrow set of themes designed for a more narrow target audience.
    - ***Discuss*** – Russian overt supporters and covert accounts, unlike other digital influence efforts, ***discuss*** Russian themes over an enduring period driving the preferred message deep into their target audience. This collaborative discussion amongst unwitting Americans makes seemingly improbable false information more believable. Comparatively, bots and campaigns from profiteers, satirists and political propagandists more frequently appear as "fire-and-forget" messaging operations.

- ***Challenge*** – Heated social media debates during election season have been and will remain commonplace. But Russian influence operations directly ***challenge*** their adversaries for unnaturally long periods and at peculiar intervals. Russian covert personas heckle and push chosen themes against political opponents, media personalities and subject matter experts to erode target audience support for Russian adversaries and their political positions. These challenges sometimes provide the Kremlin the added benefit of diminishing Russian opponent social media use. Other social media influence efforts will not go to such lengths as this well resourced, fully committed Advanced Persistent Threat (APT).

- **Full Spectrum Influence Operations: Synchronization of White, Gray and Black Efforts** – Russian cyber enabled influence operations demonstrate never before seen synchronization of Active Measures. Content created by white outlets (RT and Sputnik News) promoting the release of compromising material will magically generate manipulated truths and falsehoods from conspiratorial websites promoting Russian foreign policy positions, Kremlin preferred candidates or attacking Russian opponents. Hackers, hecklers and honeypots rapidly extend these information campaigns amongst foreign audiences. As a comparison, the full spectrum synchronization, scale, repetition and speed of Russia's cyber-enabled information operations far outperform the Islamic State's recently successful terrorism propaganda campaigns or any other electoral campaign seen to date.

- **Cyber-enabled Influence Thrives When Paired with Physical Actors and Their Actions –** American obsession with social media has overlooked the real world actors assisting Russian influence operations in cyber space, specifically "Useful Idiots", "Fellow Travellers" and "Agent Provocateurs".
  - **"Useful Idiots"** - Meddling in the U.S. and now European elections has been accentuated by Russian cultivation and exploitation of "***Useful Idiots***" – a Soviet era term referring to unwitting American politicians, political groups and government representatives who further amplify Russian influence amongst Western populaces by utilizing Russian compromat and resulting themes.
  - **"Fellow Travellers"** - In some cases, Russia has curried the favor of "***Fellow Travellers***" – a Soviet term referring to individuals ideologically sympathetic to Russia's anti-EU, anti-NATO and anti-immigration ideology. A cast of alternative right characters across Europe and

America now openly push Russia's agenda both on-the-ground and online accelerating the spread of Russia's cyber-enabled influence operations.

- **"Agent Provocateurs"** - Ever more dangerous may be Russia's renewed placement and use of "Agent Provocateurs" – Russian agents or manipulated political supporters who commit or entice others to commit illegal, surreptitious acts to discredit opponent political groups and power falsehoods in cyber space. Shots fired in a Washington, D.C. pizza parlor by an American who fell victim to a fake news campaign called #PizzaGate demonstrate the potential for cyber-enabled influence to result in real world consequences. While this campaign cannot be directly linked to Russia, the Kremlin currently has the capability to foment, amplify, and through covert social media accounts, encourage Americans to undertake actions either knowingly or unknowingly as Agent Provocatuers.

- Each of these actors assists Russia's online efforts to divide Western electorates across political, social and ethnic lines while maintaining a degree of "plausible deniability" with regards to Kremlin interventions. In general, Russian influence operations targeting closer to Moscow and further from Washington, D.C. will utilize greater quantities and more advanced levels of human operatives to power cyber-influence operations. Russia's Crimean campaign and their links to an attempted coup in Montenegro demonstrate the blend of real world and cyber influence they can utilize to win over target audiences. The physical station or promotion of gray media outlets and overt Russian supporters in Eastern Europe were essential to their influence of the U.S. Presidential election and sustaining "plausible deniability". It's important to note that America is not immune to infiltration either, physically or virtually. In addition to the Cold War history of Soviet agents recruiting Americans for Active Measures purposes, the recently released dossier gathered by ex MI6 agent Chris Steele alleges on page 8 that Russia used, "Russian émigré & associated offensive cyber operatives in U.S." during their recent campaign to influence the U.S. election. While still unverified, if true, employment of such agents of influence in the U.S. would provide further plausible deniability and provocation capability for Russian cyber-enabled influence operations.

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 – a methodology prioritizing Task, Talent, Teamwork and Technology in that order.

- **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 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 will 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 entity must be created to counter the rise of Russian cyber-enabled operations.

- **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 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.

3. What can the public and private sector do to counter influence operations?

I've already outlined my recommendations for U.S. government actions to thwart Russia's Active Measures online in my previous testimony on 30 March 2017. Social media companies and mainstream media outlets must restore the integrity of information by reaffirming the purity of their systems. In the roughly one month since I last testified however, the private sector has made significant advances in this regard. Facebook has led the way, continuing their efforts to reduce fake news distribution and removing up to 30,000 false accounts from its system just this past week. Google has added a fact checking function to their search engine for news stories and further refined its search algorithm to sideline false and misleading information. Wikipedia launched a crowd-funded effort to fight fake news this week. The key remaining private

sector participant is Twitter, as their platform remains an critical networking and dissemination vector for cyber-enabled influence operations. Their participation in fighting fake news and nefarious cyber influence will be essential. I hope they will follow the efforts of other social media platforms as their identification and elimination of fake news spreading bots and false accounts may provide a critical block to Russian manipulation and influence of the upcoming French and German elections.

In conclusion, my colleagues and I identified, tracked and traced the rise of Russian influence operations on social media with home computers and some credit cards. While cyber-influence operations may appear highly technical in execution, they are very human in design and implementation. Technology and money will not be the challenge for America in countering Russia's online Active Measures; it will be humans and the bureaucracies America has created that prevent our country from employing its most talented cyber savants against the greatest enemies to our democracy.