Questions for the Record
Senate Select Committee on Intelligence
Foreign Influence Operations and Their Use of Social Media Platforms
August 1, 2018

Submitted by Laura M. Rosenberger

1) So, in 1982, over thirty-five years ago, we had the KGB using active measures in the United States to sow racial discord, try to create problems with NATO, discredit our nuclear modernization, undercut military spending, highlight corruptions, and try to encourage the U.S. to retreat from the world stage. Aren't the themes the KGB used in 1982, similar to those we're seeing the Russian Intelligence Services use on social media in 2018?

The Russian government - through its intelligence services and proxies like the Internet Research Agency (IRA) - manipulates the information ecosystem to attempt to influence American public opinion and undermine U.S. foreign and domestic policy. These influence operations, which include seizing on hot button or divisive political and social issues, seek to accomplish several objectives: amplify and deepen existing polarization in American politics and society in attempt to weaken the institutional and social fabric of the nation; inject pro-Kremlin geopolitical narratives into public discussion and garner sympathy for them from an American audience; and, weaken and distract the United States from its global responsibilities. While some of the specific issues these operations exploit have evolved since the Cold War – for instance, immigration is a newer divisive issue on which these operations play -- overall the Russian government's objectives in conducting these influence operations are consistent with its Soviet predecessors' aims.

In many instances, Russian influence operations seek to accomplish all three of these objectives simultaneously. The Russian social media campaign around the war in Syria provides a good case study. Several IRA-purchased ads on Facebook attempted to influence American public opinion against U.S. military activity, specifically targeting the Trump administration's May 2017 strikes on Syria.[1] Other ads targeted American liberals frustrated with U.S. military actions in Syria by calling for more focus on domestic issues and describing U.S. leaders as "high-powerful warmongers."[2] One ad purchased by the fake IRA page "Blacktivist" targeted

[1] U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 1262," Social Media Advertisements, accessed July 30, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm; U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 3023," Social Media Advertisements, accessed July 30, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm.

[2] U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 2426," Social Media Advertisements, accessed August 20, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm.

African Americans by asking, "How would we feel if another country bombed us for the poisoned water in Flint and for police brutality?"[3] Others emphasized social issues to criticize U.S. actions in Syria, with one ad using anti-war quotes from Martin Luther King Jr to target civil rights supporters.[4] On Google, English-language searches for key events or players in the Syrian conflict – such as the chemical attacks in Douma or the "White Helmets" civilian rescue organization – regularly returned results dominated by overt Kremlin propaganda outlets pushing conspiracy theories, allowing Moscow to insert its narratives directly into public discussion.[5]

These operations use similar tactics around other geopolitical and divisive issues. IRA accounts on Reddit circulated multiple memes discouraging U.S. support for Montenegrin-accession to NATO. Some posts portrayed Montenegrins as free riders, while others painted them as unwilling participants in the alliance.[6] On Twitter, Russian-linked accounts have similarly promoted negative portrayals of Europe in the U.S. and negative portrayals of the U.S. in Europe to undermine transatlantic bonds.[7] IRA accounts on Twitter have also targeted domestic issues by promoting conspiracy theories,[8] amplifying partisan content related to the NFL anthem protests,[9] and exploiting mass shootings to widen divisions over gun control debates.[10]

In all of these cases, the goal is to polarize domestic U.S. debate and manipulate public opinion on key international issues to further the Kremlin's interests. In this way, social media

---

[3] U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 981," Social Media Advertisements, accessed July 26, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm.

[4] U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 1262," Social Media Advertisements, accessed August 20, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm; U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 3023," Social Media Advertisements, accessed August 20, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm.

[5] Bradley Hanlon, "From Nord Stream to Novichok: Kremlin Propaganda on Google's Front Page," Alliance For Securing Democracy, June 14, 2018, https://securingdemocracy.gmfus.org/from-nord-stream-to-novichok-kremlin-propaganda-on-googles-front-page/.

[6] IronhammerConjukelv, "Accession of Countries to NATO: expectations vs. reality," Reddit.com/r/funny/, https://www.reddit.com/r/funny/comments/3q5zpn/accession_of_countries_to_nato_expectations_vs/; and HityndiDutilar, "NATO? No action, talk only," Reddit.com/r/funny, https://www.reddit.com/r/funny/comments/3q5w97/nato_no_action_talk_only/.

[7] Sophie Eisentraut and Bret Schafer, "Russian Infowar Targets Transatlantic Bonds," *Cipher Brief*, March 30, 2018, https://www.thecipherbrief.com/russian-infowar-targets-transatlantic-bonds.

[8] Salvador Hernandez, "Russian Trolls Spread Baseless Conspiracy Theories Like Pizzagate And QAnon After The Election," BuzzFeed, August 15, 2018, https://www.buzzfeednews.com/article/salvadorhernandez/russian-trolls-spread-baseless-conspiracy-theories-like.

[9] Nicole Einbinder, "The Election Is Over, But Russian Disinformation Hasn't Gone Away," *Frontline*, November 1, 2017, https://www.pbs.org/wgbh/frontline/article/the-election-is-over-but-russian-disinformation-hasnt-gone-away/.

[10] @BEEBCLAPTT, "Sheriff Clarke Sounds Off on Vegas Massacre as Liberals Demand Gun Control https://t.co/FB1EnNda8K," Twitter, October 3, 2017, accessed via Oliver Roeder, "Why We're Sharing 3 Million Russian Troll Tweets," FiveThirtyEight, July 31, 2018, https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/.

and the online information space have given Moscow an effective way to supercharge its active measures efforts to reach larger audiences at rapid speed for lower costs.

2) Isn't this Russian social media campaign really just old wine in new bottles, with perhaps a different distributor?

In many ways, the playbook employed by the Russian government is similar to the one used by the Soviet-era KGB. The focus on dividing U.S. society by seizing on polarizing domestic issues, inflaming public discussion to undermine American foreign policy, and driving a wedge between the United States and its allies represent continuity in Moscow's strategy to weaken the United States. But while the playbook is in many ways the same, the tools that can be used to run those plays are very different. Digital platforms allow for manipulation of the entire information ecosystem in new and powerful ways, boosting the reach – and possibly the impact – of the playbook. By combining newer digital tactics like automated and inauthentic social media accounts with more traditional tools like state propaganda outlets, the Kremlin can spread its narratives across the information ecosystem to reach a wider audience than ever before and distort the information space itself. Additionally, the anonymity and reach of social media tools has made information operations cheaper, easier, and likely more effective than pre-digital iterations. In the past, conducting widespread information operations required experienced tradecraft and covert distribution networks. Now, basic cultural and linguistic skills, along with an understanding of trending algorithms, is all that is needed for Russian assets to insert narratives into the information space and watch them go viral.[11] The ability to combine these tactics with other cyber means, including to disseminate hacked material obtained through cyberattacks, also enhances the power of this playbook.

3) To what extent have you looked for and seen Russian activity on this front [to sow racial discord, try to create problems with NATO, discredit our nuclear modernization, undercut military spending, highlight corruptions, and try to encourage the U.S. to retreat from the world stage] on social media?

Inauthentic accounts controlled by Russia's Internet Research Agency (IRA) have attempted to influence U.S. defense policy and alliances through a number of methods. For example, numerous ads purchased by IRA accounts on Facebook sought to undermine U.S. policy on Syria, while IRA accounts on Twitter questioned the United States' nuclear capability[12] and commitment to NATO, including tweets asking why Americans would fight and

[11] Andrew Weisburd and Bret Schafer, "Insinuation and Influence: How the Kremlin Targets Americans Online," Alliance for Securing Democracy, October 16, 2017, https://securingdemocracy.gmfus.org/insinuation-and-influence-how-the-kremlin-targets-americans-online/.

[12] U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 1262," Social Media Advertisements, accessed August 20, 2018, https://democrats-intelligence.house.gov/social-media-

die for "Turkey and their Sharia law."[13] Russian-linked accounts on Twitter have also worked to discredit transatlantic partners in the eyes of each other by painting a negative picture of Europe to American audiences and of the United States to European audiences.[14] And IRA accounts on Reddit discouraged U.S. support for Montenegrin-accession to NATO.[15] While I am not aware of specific examples of Russian activity on social media directly targeting U.S. missile defense deployments or nuclear modernization efforts, such messaging would be consistent with the Kremlin's broader goal of weakening our alliances and influencing U.S. policy on geopolitical issues.

4) What modifications would you recommend to the large social media companies that would enable users to identify the source and potential funding of items posted on social media?

There are a number of measures that social media platforms can implement to help protect users from foreign manipulation. Most of these measures require greater disclosure and transparency. Online information platforms need to supply users with the context necessary to evaluate the information they encounter, including the origin of content and an explanation of why it is being presented to them. To this end, companies should inform users in a clear and approachable manner how and why certain content appears for them. As outlined in the Alliance for Securing Democracy's *Policy Blueprint for Countering Authoritarian Interference in Democracies*, transparency and disclosure of source information are also essential to protecting the integrity of the U.S. political system.[16] Congress could help promote greater transparency by adopting legislation that improves disclosure requirements for online political advertisements so

---

content/social-media-advertisements.htm; U.S. House of Representatives Permanent Select Committee on Intelligence, "2017: Quarter 2, May: Ad ID 3023," Social Media Advertisements, accessed August 20, 2018, https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm.; @RAVENICHOLSON, "Trump questions the US's nuclear arsenal: Here's how the US's nukes compare to Russia's https://t.co/h6KlQ8biha via @BI_Defense," Twitter, December 24, 2016, accessed via Oliver Roeder, "Why We're Sharing 3 Million Russian Troll Tweets," FiveThirtyEight, July 31, 2018, https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/.

[13] @BEEATRWL, "How heartening is it that our sons and daughters are FIGHTING and DYING for Turkey and their Sharia Law? NATO Turâ€¦ https://t.co/eaQ9QaFWiP," Twitter, August 1, 2017, accessed via Oliver Roeder, "Why We're Sharing 3 Million Russian Troll Tweets," FiveThirtyEight, July 31, 2018, https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/.

[14] Sophie Eisentraut and Bret Schafer, "Russian Infowar Targets Transatlantic Bonds," *Cipher Brief*, March 30, 2018, https://www.thecipherbrief.com/russian-infowar-targets-transatlantic-bonds.

[15] IronhammerConjukelv, "Accession of Countries to NATO: expectations vs. reality," Reddit.com/r/funny/, https://www.reddit.com/r/funny/comments/3q5zpn/accession_of_countries_to_nato_expectations_vs/; and HityndiDutilar, "NATO? No action, talk only," Reddit.com/r/funny, https://www.reddit.com/r/funny/comments/3q5w97/nato_no_action_talk_only/.

[16] Jamie Fly, Laura Rosenberger, and David Salvo. Policy Blueprint for Countering Authoritarian Interference in Democracies. June 26, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Policy-Blueprint.pdf

that Americans understand who is funding the political ads they see online, and legislation requiring companies to identify and label automated "bot" accounts.[17]

New mechanisms for data sharing, both between the public and private sectors and among technology companies, are essential for combatting this problem. The U.S. government plays an important role in identifying threat actors of concern, as the intelligence community has important capabilities that allow it to identify both the intentions and behaviors of threat actors. At the same time, social media companies have unique visibility into activity on their platforms – visibility that government analysts often lack. Information sharing mechanisms between the government and social media platforms should facilitate regular communication of developments on these fronts so that both entities are better positioned to identify, deter, and defend against foreign interference. Additionally, given the manner in which interference operations work across the social media ecosystem, tech companies also need mechanisms in order to regularly share threat indicators with one another. And such data should be shared, with appropriate controls for privacy, with independent researchers. Models of sharing mechanisms between the public and private sectors, cross-industry, and with independent experts exist for counter-terrorism, cybersecurity, and financial integrity.[18]

5) Should there be disclaimers on anything other than personal information?

Context about information is critical for consumers to be able to evaluate it. Users should be able to see and understand the origin of information presented to them, whether the information is being spread by an automated account, and why they are being shown that information. Additionally, there are a variety of ways to require authenticity and provide context without compromising anonymity, which is particularly essential for democratic activists who operate in authoritarian states. Another simple step toward empowering users with contextual information is to label automated accounts, which will help people better understand and evaluate the content they interact with. As outlined in the Alliance for Securing Democracy's *Policy Blueprint for Countering Authoritarian Interference in Democracies*, Congress could adopt legislation requiring companies to identify and label automated "bot" accounts.[19]

---

[17] Jamie Fly, Laura Rosenberger, and David Salvo. Policy Blueprint for Countering Authoritarian Interference in Democracies. June 26, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Policy-Blueprint.pdf

[18] One example is the Global Internet Forum to Counter Terrorism (GIFCT), whose goal is to substantially disrupt terrorists' ability to promote terrorism, disseminate violent extremist propaganda, and exploit or glorify real-world acts of violence using our platforms by: employing and leveraging technology; sharing knowledge, information and best practices; and conducting and funding research. https://gifct.org/; The National Cyber Forensics and Training Alliance, is a nonprofit partnership between industry, government, and academia to provide a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cyber crime. http://www.ncfta.net/ ; Two models from the world of financial intelligence are the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) and the United States' FinCEN Exchange.

[19] Jamie Fly, Laura Rosenberger, and David Salvo. Policy Blueprint for Countering Authoritarian Interference in Democracies. June 26, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Policy-Blueprint.pdf

6) Should everything posted on social media have a "tag" that allows users to determine who posted information, even if it was re-posted or shared by another person, so you can always determine the actual source?

Providing users with broader context about the origin of information and why they are seeing it is key to empowering a more discerning and resilient social media culture. As described by Senators Warner and Rubio, "There is really no better defense against Russian aggression on social media than an informed citizenry."[20] Online information platforms should ensure that online content is presented in a manner that relays the origin of the information and why users are seeing the content. Additionally, verifying the authenticity for accounts – while protecting anonymity – and requiring the labeling of automated accounts will help users better understand and evaluate their information environment. Although some platforms have taken steps toward these ends, others have not.

7) What reforms would you recommend to ensure that federal, state and local authorities are not influenced by Russian social media or Internet propaganda?

One of the Kremlin's key objectives with its disinformation campaigns is to cause confusion to slow and undermine the functioning of U.S. institutions. Deception and misdirection are core to its operations to accomplish those objectives. This can include the spread of false or altered documents, as well as the spread of false assertions to undermine U.S. officials' ability to establish a collective truth. No one is entirely immune to covert information manipulation, and it is critical that all Americans scrutinize the sources of their information. The Intelligence Community is well trained at this, and understanding the motivations of sources of information is something that other government officials should be trained on. At a minimum, government employees should be trained to actively verify the sourcing and veracity of information in official material, and should receive up-to-date information from the intelligence community regarding potential nation-state disinformation campaigns. There should also be more formalized partnerships between the various levels of government and the tech platform companies in order to exchange information on foreign attempts to manipulate information online.

8) At the hearing on August 1, 2018, I asked each witness to submit written policy recommendations to the Committee. Specifically, please provide recommendations on the following topics:

[20] Mark Warner and Marco Rubio, "As Trump Meets Putin, We'll Spotlight and Resist Russian Aggression: Warner & Rubio," USA TODAY, July 12, 2018, https://www.usatoday.com/story/opinion/2018/07/12/trump-putin-helsinki-summit-resist-russian-aggression-column/776617002/.

- **Technical solutions, such as requirements to label bot activity or identify inauthentic accounts;**

While I am not a technical expert and defer to such experts on specific recommendations in this area, transparency is a critical principle that should underpin any technical changes. This includes tools to help provide users with more context on the information they are consuming, as well as to label automated accounts. Taking steps to ensure that the algorithms that power these platforms are less vulnerable to manipulation by malicious actors is also critical. Finally, online information platforms should consider the potential utility of hashing as a method or model for identifying and sharing signatures of manipulated or corrupted information.

- **Public initiatives focused on building media literacy;**

Developing media literacy and digital competency programs are key long-term steps to inoculating against the threat of foreign interference. These skills should be taught not only in the classroom, but also through local civil society and non-governmental organizations throughout the country. Some of these organizations are already dedicated to helping Americans better discern sourcing of information, understand why they are seeing it, evaluate whether it may be manipulated, inauthentic, biased, false, or corrupted. These NGOs could partner to conduct public trainings on disinformation and on how to consume news critically; advocate to state and local governments to include media literacy in public education curricula; and devise programs to strengthen civic education, particularly on why democracy matters and why it should be protected against foreign interference. To support these efforts, Congress could establish a fund with pooled public and private resources that would support media and digital literacy education and training throughout the country. This fund could be supported by social media companies as part of their efforts to combat the manipulation of their platforms.[21]

- **Solutions to increase deterrence against foreign manipulation**

Deterrence is essential to securing American democracy against the ongoing threat of foreign interference and preventing adversarial states from conducting future operations. Recent exposure of social media manipulation efforts by Iran,[22] and efforts by China to test these methods, underscore the importance of deterring other authoritarian actors from adopting the Kremlin's playbook.[23] At a basic level, the President of the United States should publicly

---

[21] David Salvo and Brittany Beaulieu, "Ten Legislative Proposals to Defend America Against Foreign Influence Operations," Alliance for Securing Democracy, April 19, 2018, https://securingdemocracy.gmfus.org/ten-legislative-proposals-to-defend-america-against-foreign-influence-operations/.

[22] Casey Michel, "It Turns Out Russia Isn't the Only Country Turning Facebook and Twitter Against Us," *The Washington Post*, August 23, 2018, https://www.washingtonpost.com/news/democracy-post/wp/2018/08/23/it-turns-out-russia-isnt-the-only-country-turning-facebook-and-twitter-against-us/?noredirect=on&utm_term=.019382e8eac7.

[23] Laura Rosenberger, "Foreign Influence Operations and Their Use of Social Media Platforms," Alliance For Securing Democracy, July 31, 2018, https://securingdemocracy.gmfus.org/foreign-influence-operations-and-their-use-of-social-media-platforms/.

articulate a declaratory policy that makes clear the United States considers malign foreign influence operations a national security threat and will respond to them accordingly. Additionally, the Executive Branch should publicly expose and attribute foreign interference efforts as they are discovered – steps by the Department of Justice to adopt such a policy are welcome, and Congress could consider codifying this policy into a mandatory reporting requirement.

To effectively dissuade foreign actors from interfering in our democracy, the U.S. government should tailor its deterrent efforts to most effectively target the interests and weaknesses of foreign regimes while leveraging the United States' relative strengths. In the case of the Russian Federation, the Putin regime is dependent on corrupt financial links between the political leadership, security services, and business for its survival. Inducing behavior change from the Kremlin will require the United States to utilize its relative economic superiority by imposing a broader set of sanctions and reputational costs against individuals and entities that conduct these operations, facilitate corruption, and support authoritarian regimes' destabilizing foreign policy actions.

Additionally, the U.S. should impose reputational costs on authoritarian powers that employ these tools. Vladimir Putin values his standing on the world stage. As such, it is important that Russia not be allowed to reenter normal international fora until Kremlin behavior changes. This is even more relevant for the Chinese Communist Party, which is more sensitive about being exposed for illegal activity and interference operations abroad, as China attempts to sell an alternative model of governance and growth to developing nations.[24] Imposing reputational costs on Beijing must be a pillar of western deterrence strategy.

Finally, the Executive Branch should employ cyber responses as appropriate to respond to cyberattacks and deter future attacks, and consider offensive cyber operations using appropriate authorities to eliminate potential threats.

- **Any additional policy recommendations**

Effectively countering foreign interference will require a whole of society effort, with actions by government, the private sector, and civil society. For a comprehensive set of policy recommendations for securing U.S. democracy against authoritarian interference, please see the Alliance for Securing Democracy's *Policy Blueprint for Countering Authoritarian Interference in Democracies*.[25] A few specific recommendations are worth highlighting specifically with respect to countering online information manipulation.

New mechanisms for data sharing, both between the public and private sectors and among technology companies, are essential for combatting this problem. The U.S. government

[24] Laura Rosenberger and John Garnaut, "The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response," Open Forum, The ASAN Forum, May 8, 2018, http://www.theasanforum.org/the-interferenceoperations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response.

[25] Jamie Fly, Laura Rosenberger, and David Salvo. Policy Blueprint for Countering Authoritarian Interference in Democracies. June 26, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Policy-Blueprint.pdf

plays an important role in identifying threat actors of concern, as the intelligence community has important capabilities that allow it to identify both the intentions and behaviors of threat actors. At the same time, social media companies have unique visibility into activity on their platforms; visibility that government analysts often lack. Information sharing mechanisms between the government and social media platforms should facilitate regular communication of developments on these fronts so that both entities are better positioned to identify, deter, and defend against foreign interference. Additionally, given the manner in which interference operations work across the social media ecosystem, tech companies also need mechanisms in order to regularly share threat indicators with one another. And such data should be shared, with appropriate controls for privacy, with independent researchers. Models of sharing mechanisms between the public and private sectors, cross-industry, and with independent experts exist for counter-terrorism, cybersecurity, and financial integrity.[26]

This is also a transnational problem, and the United States should develop information sharing and coordination mechanisms with its democratic allies and partners across the transatlantic space and around the world. Actions taken by the U.S. government to punish foreign actors for interference will be much more effective if they are executed in coordination with allies. The G7's recent commitment to share information and work with social media companies and internet service providers to prevent foreign interference in elections is a good first step in this direction, and could serve as an impetus for more efficient transatlantic coordination to share threat information and best practices.[27]

Domestically, the United States should also work to develop better coordination and information-sharing across the U.S. government. Appointing a Counter Foreign Interference Coordinator at the National Security Council and establishing a National Hybrid Threat Center at the Office of the Director of National Intelligence would help the U.S. government work across bureaucratic stovepipes in a unified and coordinated way.[28]

---

[26] One example is the Global Internet Forum to Counter Terrorism (GIFCT), whose goal is to substantially disrupt terrorists' ability to promote terrorism, disseminate violent extremist propaganda, and exploit or glorify real-world acts of violence using our platforms by: employing and leveraging technology; sharing knowledge, information and best practices; and conducting and funding research. https://gifct.org/; The National Cyber Forensics and Training Alliance, is a nonprofit partnership between industry, government, and academia to provide a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cyber crime. http://www.ncfta.net/ ; Two models from the world of financial intelligence are the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) and the United States' FinCEN Exchange.

[27] "Charlevoix Commitment on Defending Democracy from Foreign Threats," G7 2018 Charlevoix, June 10, 2018. https://g7.gc.ca/en/official-documents/ charlevoix-commitment-defending-democracy-from-foreign-threats.

[28] A similar concept exists in a bill proposed by Senator Graham and Senator Menendez in August 2018. The ''Defending American Security from Kremlin Aggression Act of 2018'' calls for the establishment of a "National Fusion Center to Respond to Hybrid Threats," which would coordinate analysis and policy implementation across the U.S. government in responding to hybrid threats. Full text here: https://drive.google.com/file/d/12SoqvkJY8yTLSbUYohzYW978ftpKvCCt/view.