**Statement Before the**
**Senate Committee on Armed Services**
**Subcommittee on Cybersecurity**

# *"Department of Defense's role in Protecting Democratic Elections"*

A Testimony by:

**Heather A. Conley**

Senior Vice President for Europe, Eurasia, and the Arctic,
and Director, Europe Program
CSIS

**February 13, 2018**

**222 Russell Senate Office Building**

Mr. Chairman, Ranking Member Nelson and distinguished members of the Cybersecurity Subcommittee of the Senate Armed Services Committee, thank you for the invitation to speak before this important subcommittee on a topic that is of utmost importance to the future of the United States and its national security: The essential need to ensure that the American people have complete trust and confidence in the fairness and accuracy of U.S. elections, be they at the local, state or federal level.

I am a professional outlier on this panel for I am not a cyber security expert, but I have spent the last several years at CSIS studying and understanding how malign Russian influence works in Europe, which we have described in detail in our seminal report, *The Kremlin Playbook*.[1] We have studied in detail how Russian economic influence has worked in five European countries (Latvia, Hungary, Slovakia, Bulgaria and Serbia) over a ten-year period to understand how Russia infiltrates a democracy and erodes confidence and credibility in how that democracy works. We have extended our research to include six more European countries (Italy, Austria, the Netherlands, Romania, the Czech Republic and Montenegro) which will culminate in a new report, *The Kremlin Playbook 2*, in early 2019. The Central and Eastern European region has constituted an extensive Russian laboratory for a variety of influence operations for nearly two decades. European governments and citizens have been exposed to a full spectrum of Russian influence tactics that have collapsed weakened governments as well as systemically important financial institutions. Russian influence has fomented societal unrest and altered Western-oriented government policies.

Having said this, I believe Russian influence is less about physical cyber security (although cyberattacks are a useful tool) and more about (dis)information and influence superiority, which is how the Kremlin believes it will maintain its global preeminence as it addresses slow and long-term decline. According to the Czech Security Information Service, it is the Kremlin's goal to convince the average citizen that "everyone is lying," which in turn will "weaken society's will to resist" Russian interests.[2]

Therefore, one of our first lines of defense is to develop a much deeper understanding of and a body of research into how Russia practices its influence operations as well as to study how European countries defend themselves against these ongoing operations. Europe has been at this longer than we have. Our knowledge has atrophied. Our defense and intelligence officials must have the closest possible relationship with our European partners to develop effective and sustainable countermeasures against Russian influence.

Secondly, it needs to be understood that Russian influence does not simply occur in and around a national election; it is a continuous and holistic series of operations that are designed to break the "internal coherence of the enemy system."[3] It is true that elections are the most visible

---

[1] Heather A. Conley and Ruslan Stefanov, *The Kremlin Playbook*, Center for Strategic and International Studies, October 2016, https://www.csis.org/analysis/kremlin-playbook.
[2] Jakub Janda, "How Czech President Miloš Zeman Became Putin's Man," *Observer*, January 26, 2018, http://observer.com/2018/01/how-czech-president-milos-zeman-became-vladimir-putins-man/.
[3] Dimitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," Proliferation Paper no. 54, Institut Français des Relations Internationales, November 30, 2015, https://www.ifri.org/en/publications/enotes/proliferation-papers/cross-domain-coercion-current-russian-art-strategy.

opportunity to harm a democracy when it is at its most vulnerable. We can observe that Russian influence operations and cyber infiltration may accelerate approximately two years prior to an election but this does not mean that Russian operations cease after an election. If anything, they simply adapt their methods to the outcome and alter their strategies to continue to degrade confidence in democratic institutions. Sustained Russian influence operations focus on those issues that are deeply divisive within a society, such as issues related to migration or questions of history or national, racial or religious identity. Today's Russian influence operations, just as their predecessor, Soviet active measures, exploit the weaknesses that are present within a society but they benefit from increasingly sophisticated means amid increasingly confused Western societies that are overwhelmed daily by a growing amount of information.

My contribution to this important discussion is to offer you what I believe European countries have done successfully to combat malign Russian influence and disinformation as well as increase cyber-protection. But before doing this, I will address the questions posed to all the witnesses today.

I do not believe the Department of Defense has a leading role to play in the cyber protection of U.S. elections. This is the purview of the Department of Homeland Security, which has struggled to develop effective policies to protect critical election infrastructure as distrust between the federal government and state as well as local election officials has grown. However, I believe the Department of Defense can play a role that is highly complementary to the work of the Department of Homeland Security by rebuilding trust between state and federal officials, and building knowledge and awareness of the ever-present threat. This will not be easy. State and local election officials are unable to receive classified intelligence briefings. Candidates for office may not have received cybersecurity training or know whom to contact should they become the victim of illicit hacking or an influence operation.

We can learn from the French government about how to combine military and civilian efforts to prevent cyber-destabilization. This month the French Ministry of Defense released its Military Planning Law, which prioritizes cyber risks and seeks to increase cooperation with telecommunication companies to enable them to scan networks for technical clues of ongoing or future cyberattacks. The civilian French Network and Information Security Agency (ANSSI) will provide a list of risk indicators to the Defense Ministry. These risk indicators only focus on technical aspects of security breaches and not on content (which is important to ensure First Amendment protections in the United States). The goal is to enhance early detection. A French white paper was released in conjunction with the planning law which outlined and defined the possible cyberattacks that France could suffer and identifies cyber-protection as a strategic priority.[4] The strategic review of France's cyber defense sets out six main goals: prevention, anticipation, protection, detection, attribution, and reaction.[5] The ANSSI provides cybersecurity

[4] Martin Untersinger, "Cybersécurité : le gouvernement veut mettre les télécoms à la contribution pour détecter les attaques," *Le Monde*, February 8, 2018, http://www.lemonde.fr/pixels/article/2018/02/08/cybersecurite-le-gouvernement-veut-mettre-les-telecoms-a-contribution-pour-detecter-les-attaques_5253808_4408996.html.
[5] Olivier Berger, "Revue stratégique de cyberdéfense : l'Etat et les opérateurs pourront collaborer pour traquer les attaques informatiques," *La Voix du Nord*, February 8, 2018, http://defense.blogs.lavoixdunord.fr/archive/2018/02/08/l-etat-et-les-operateurs-pourront-collaborer-pour-traquer-le-15570.html

awareness-raising seminars to politicians and parties. Could DoD produce something similar in cooperation with DHS?

While there is a role for the Defense Department to play in deploying offensive cyber capabilities should there be an attributable Russian attack on the U.S. election process, it would have to be part of a whole-of-government policy and strategy toward Russian influence operations, which at present the United States government does not have – but urgently needs. Perhaps a more credible policy of deterrence would be for the United States government to notify the Kremlin that future attributable attacks against U.S. elections would force the U.S. to seek to block Russia's access to the Society for Worldwide Interbank Financial Telecommunications (SWIFT). Although the Russian government has developed an alternative system that may mitigate financial disruption internally, it could certainly hamper access to international bank accounts from the Kremlin's very wealthy inner circle – which may have more immediate impact.

There are two additional areas that the Defense Department could explore to enhance disinformation awareness and cyber-protection prior to the 2018 mid-term and 2020 presidential elections. First, it could use its extensive employee and military network to provide timely policy guidance and statements about the threat that Russian influence operations pose to election security. Secretary Mattis and General Dunford should provide extensive public outreach to the defense community about the nature of the threat and how best to counter it to sensitize the DoD community to the threat of Russian influence and misinformation operations in a public service announcement format. Another idea would be to consider engaging the National Guard Bureau to help develop and facilitate training of state and local election officials to enhance cybersecurity awareness and to be able to detect patterns of influence (for example, hacked e-mails surfacing online in conjunction with the spread of false rumors about candidates) in partnership with the Department of Homeland Security. Those National Guard units that have participated in the State Partnership Program (SPP) have served and developed relationships with European partners, and could also be particularly helpful in sharing information about Russian influence operations (U.S. forces serving in these countries have been the recipients of Russian misinformation campaigns) through the State Adjutant Generals who are very well regarded among state and local officials. State Partnership Programs particularly well placed for this would be the Pennsylvania National Guard (Lithuania), the Maryland National Guard (Estonia), the Texas National Guard (the Czech Republic) and the Michigan National Guard (Latvia).[6]

Simply put, the Defense Department must model the bipartisan and fact-based actions, behavior and awareness that will reduce societal division and help bridge the state and federal divide. As one of the most trusted institutions in the United States, the Defense Department must leverage that trust to mitigate malign Russian influence.

[6] See more at "State Partnership Program," National Guard, http://www.nationalguard.mil/Leadership/Joint-Staff/J-5/International-Affairs-Division/State-Partnership-Program/.

Turning now to the European laboratory of Russian cyber-destabilization, there are several important lessons that the 2017 European election cycle has taught us (and that Europeans have learned):

- The necessity of having a paper ballot either as the ballot of record or as a back-up to an electronic ballot. The Dutch and German national elections use paper ballots. The German government has also focused on protecting the software that tallies the election results to ensure that these systems are not vulnerable to cyberattack.
- A unified and all-political party message on what is at stake as well as how to detect and understand Russian influence. The French and German governments were particularly effective at early notification regarding the likelihood of Russian influence and announcing when data breaches occurred. There was sufficient trust in the institutions and their leaders to ensure that a majority of the public took heed of the warning, which reduced the impact of the Russian misinformation campaign.
- French and German media organizations set up fact-checking teams and social media platforms that cooperated with authorities to protect sensitive accounts. The French polling commission went so far as to warn against illegitimate polls coming from Kremlin-affiliated outlets that did not fit legal criteria for accurate polling.[7]
- In Sweden, ahead of the September 2018 elections, the government plans to create a new agency to enhance the public's "psychological defense" against influence by identifying, analyzing and reacting to Russian influence attempts; this would also take place through increased funding for the Swedish intelligence services, and cyber-defense.[8] In January 2018, the Swedish head of security services (Sapo) warned against increased foreign influence operations ahead of the election, citing as examples forged letters of arms deals with Ukraine or fake reports that Muslims had vandalized a church.[9]
- Swedish Prime Minister Löfven plans to convene political parties to share protection and resilience strategies throughout the election process. The media would also take part in some of these meetings to bolster awareness of foreign influence.
- The chief of Sapo has increased information-sharing with European partners, and with other security services to better protect the election process; he argued that despite being a security service, openness was important to inform the public on the threat.[10]
- The Swedish government is also discussing the inclusion of critical thinking skills in primary school curricula, teaching children how to spot fake news. Swedish government authorities have initiated a series of public news literacy activities to

[7] Laura Daniels, "How Russia hacked the French election," *Politico*, April 23, 2017, https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.
[8] Andrew Rettman and Lisbeth Kirk, "Sweden raises alarm on election meddling," January 15, 2018, https://euobserver.com/foreign/140542.
[9] Gordon Corera, "Swedish security chief warning on fake news," January 4, 2018, http://www.bbc.com/news/world-europe-42285332.
[10] *Ibid.*

> help the Swedish public discern how truthful and fact-based information that receive.[11]

The U.S. government has taken none of these positive, proactive steps – to my knowledge. The most proactive work being done in this space is taking place in U.S. think-tanks and universities through independent funding.

If we understood 2016 and 2017 to be exceptional years for all-encompassing Russian influence operations, we must reckon with the fact that 2018 has already witnessed significant Russian influence activities, particularly around the Czech presidential elections. There, in a close second-round election, the opponent (a former president of the Czech Academy of Sciences) of the preferred Russian candidate (outgoing president Milos Zeman) received an onslaught of disinformation during the second and final round of the campaign, from being called a pedophile to a Communist secret police agent who stole intellectual property. Milos Zeman won 51.4% to 48.6%.[12]

We watch with particular concern the upcoming Italian parliamentarian elections (March 4), Montenegro's presidential elections (April 15), Latvian parliamentary elections (September/October), Swedish parliamentary elections (September 8), and Moldovan elections (to be held before April 2019), where Russia has long-standing investments and would potentially seek to influence the outcome of elections in support of the Kremlin's interests. The very same methods that are being deployed to undermine the credibility of these elections are being actively pursued in the United States. This has been recently acknowledged by CIA Director Mike Pompeo.[13] So perhaps the most immediate and important step the Department of Defense could take – in concert with Congress – is to demand a whole-of-government approach to minimize the impact of Russian influence operations in the United States. A disjointed approach by the U.S. government and the daily undermining of the legitimacy of U.S. intelligence and law enforcement agencies does the Kremlin's work far better (and cheaper) than any Russian influence operation could.

---

[11] "A practical approach on how to cope with disinformation," Government of Sweden, October 6, 2017, http://www.government.se/articles/2017/10/a-practical-approach-on-how-to-cope-with-disinformation/.
[12] Marc Santora, "Czech Republic Re-elects Milos Zeman, Populist Leader and Foe of Migrants," *The New York Times*, January 27, 2018, https://www.nytimes.com/2018/01/27/world/europe/czech-election-milos-zeman.html.
[13] Scott Neuman, "CIA Director Has 'Every Expectation' Russia Will Try To Influence Midterm Elections," *NPR*, January 30, 2018, https://www.npr.org/sections/thetwo-way/2018/01/30/581767028/cia-director-has-every-expectation-russia-will-try-to-influence-mid-term-electio.