THE BROOKINGS INSTITUTION
The Brookings Cafeteria Podcast
Will Russia hack the 2018 midterms?
October 19, 2018

CONTRIBUTORS

HOST
Fred Dews

ALINA POLYAKOVA
David M. Rubenstein Fellow – Foreign Policy, Center on the United States and Europe

MOLLY REYNOLDS
Fellow – Governance Studies

DEWS: Welcome to another 2018 Midterm Elections edition of The Brookings Cafeteria, the podcast about ideas and the experts who have them. I'm Fred Dews. In 2016, Russia and agents acting on behalf of Russia to spread disinformation through social media and other avenues to disrupt and influence the outcome of the U.S. presidential election.

What is Russia up to in 2018 and what are the latest types of disinformation and cyber threats we need to be paying attention to? To address this and related questions. I'm joined today by Alina Polyakova. She is a David M. Rubenstein Fellow in the Foreign Policy Program's Center on the United States and Europe and an adjunct professor of European Studies at the Paul H Nitze School of Advanced International Studies at Johns Hopkins University. She specializes in European politics, far right populism and nationalism, and Russian foreign policy. Also on today's program, you'll hear another installment of Molly Reynolds take on what's happening in Congress. You can follow the Brookings podcast network on Twitter @policypodcasts to get the latest information about all of our shows and visit us online at Brookings.edu/podcasts. For more analysis from Brookings experts on the upcoming elections. Go to Brookings.edu/2018-midterms. And now on with the interview. Alina, welcome back to the Brookings Cafeteria.

POLYAKOVA: Glad to be back, Fred. Thank you.

DEWS: Well we're facing a midterm election in 2018 and everyone's talking about worrying about what are the Russians going to do? Do you think Russia is going to hack or attack the U.S. midterms?

POLYAKOVA: Yes and No. If we look at what the Russian operation looked like back in 2016, you have to really be honest about it, it wasn't that sophisticated. You know what I mean by that I didn't spend a great deal of money, it primarily involved the social media influence operation. There wasn't massive in scope. I think the biggest concern that most of us following it had was that how vulnerable we turned out to be to a relatively low

level, low cost operation. How much impact it had on our politics, and of course the other piece was the cyber breaches and the attacks on the DNC, the Clinton campaign, and others. But again, those were mainly done through phishing campaigns which are pretty straightforward kinds of operations and the presidential elections are more straightforward. Midterms are so diverse here in the United States. Every locality has a different kind of voting machine. Of course it was a concern that there would be a hack into the voting machines, which are very hackable, but you have to really do a lot of intelligence gathering about the swing districts, understanding their specific systems, so you require a lot more effort to be much more sophisticated and frankly at this point it doesn't seem like the Russians would get much of investing so much more into this kind of operation.

DEWS: I know one question people ask is about voting machines, and you've written a lot about the Russians are focused on hacking what you would call critical infrastructure in the United States, which I guess to mean are water systems and power systems. But even though they might not want to, could they hack into voting machines and change vote totals for a Congressional race, shift 100 votes from candidate X the candidate Y, and is that even possible?

POLYAKOVA: I think technically that is possible. One thing to note is that critical infrastructure now and used to not does refer to our electoral institutions and voting machines and things like that, and we know from a report earlier this year from the Department Homeland Security and FBI, they came out in March that they have detected similar malware that was detected Ukraine during an electrical outage, a cyberattack on the electrical grid. The same malware has been detected on our critical energy infrastructure system, so which includes the things you mentioned like waterways, nuclear, other electrical grids. And we also know most recently from the last indictments they came out in the United States related to Russian cyber-attacks, the anti-doping agencies, and others, these were the seven individuals who were indicted by the United States in

coordination with the Dutch indictments as well around the Skripal operations and other cyber-attack operations. What was revealed there are many companies, including an electrical energy company in Pennsylvania that was the target of some of these attacks.

So we're seeing a lot of probing happening in the voting machines. Again it will be very complicated to do that and frankly you wouldn't have to change votes. I mean this is the big concern that people have but all one would have to do any hostile agent, be that Russia or anyone else is actually delete voter rolls for example that's much easier to do. You can get access to the database, delete people's registration, and somebody shows up to vote and they're not registered. And so they are given a provisional ballot, usually that's what happens. But then to prove that you are the person you say you are on your side of the address you say you reside, you mail in that provisional ballot afterwards. And the way that they double check usually most localities, if you are that person is they go back to the voter rolls. So again, if such operations revealed all you have to do is plant the seed of doubt and mistrust that the elections were not free and fair in some way. You don't really change votes. And that's something that the Russians have realized a long time ago from some of their election interference in places like Ukraine.

DEWS: So it seems like while Russian interest in trying to influence the 2016 election was pretty clear, they didn't want Hillary Clinton to win. It seems like there may not be a clear Russian interest in manipulating the 2018 U.S. midterms in terms of whatever the outcome might be.

POLYAKOVA: Exactly I mean it's unclear what they would get. Which direction would they want to influence you know a district race in Florida, for example, a congressional race anywhere else. Do they actually want more Republicans in the House or more Democrats? Right now we have a bipartisan agreement that Russia needs to be punished for what it has done in terms of cyber-attacks, interference operations. We have seen the Trump administration actually do a lot to impose sanctions and other forms of

punishments on Russia and there is bipartisan support for this. So in fact from Russia's point of view, if it's Democrats or Republicans who control the House or the Senate will not actually significantly change the foreign policy approach from Congress that we've seen develop over time.

DEWS: Well then if Russia doesn't have a clear interest in the outcome the balance of power in Washington and across the country following our midterm elections, do they have a stronger interest in influencing political outcomes in other countries in Western Europe, you mentioned Ukraine or even in Eastern Europe?

POLYAKOVA: Well I think one thing we should think about as well is that the goal of these kinds of influence operations including disinformation, cyber-attacks and the combination of the two and other forms of political warfare is not necessarily to get a specific outcome. Usually that's very difficult to do because elections are dynamic, they're moving and you can't guarantee that you'll get what you want. And we've seen this happen for example in 2004 in Ukraine where the Russians tried to meddle and actually change voter turnout counts to get pro-Russian candidate elected and there was a big uproar that produced the what we called the Orange Revolution, eventually that was a recount, a new election was held, and still the pro-Western candidate was then elected. That didn't work in the way they had expected because they got caught and people were upset about it and there were mass protests and demonstrations.

So it's really difficult to guarantee with an influence operation of your intended outcome be will you actually get, the bigger desire is to just undermine at the edges to just so distrust, to destabilize, to play on the kinds of divisions and polarization that we already have in our societies, and to me, people distrust our institutions just a little bit more. In fact that is what the Russians were doing in 2016 the United States, that's what they've been doing to a lesser extent places like France and Germany throughout the elections in the last two years. And that's what they can do you see doing today. There's still Russian trolls

and bosses still operating on social media, they're still putting out disinformation, is that having an impact? I think that's really difficult to judge for the reasons I said.

DEWS: I do want to come back to kind of remedies for some of the malicious actions that Russia has taken in our systems. Well I want to expand our view from Russia to ask you are there other states other malicious actors out there? I think somebody in the U.S. administration recently suggested that China maybe has an interest in meddling in the 2018 midterms. Is that the case?

POLYAKOVA: Clearly the Kremlin has pioneered some of these techniques and tools by the fact that it was such a low cost, high impact operation especially in the United States, I think has sent a very clear signal to other hostile actors whether it be states like China or Iran and North Korea and also non-state actors like terrorist organizations like ISIS and others, then in fact you can do quite a bit of damage to the political system because our open society is very vulnerable to this kind of interference interventions. So clearly, China has been I think overlooked, but it's also because China is playing a very different game. We see this happening in the United States and also Europe where the Chinese have been for a long time using their economic muscle to gain a foothold and influence in European politics. China is now becoming, increasingly becoming a large stakeholder in European imports for example, they've been buying up Greek ports, and they bought a stake in Europe's largest port in the Netherlands. So it's a much slower moving game, but if the Chinese do decide to get into this high impact, low cost political warfare like the Russians have done, I don't think we're prepared to really deal with that because the Chinese are far more capable, there are far more resources, and they will have far more impact.

DEWS: So back to the US elections just for a moment. Now regardless of Russia's interest in the intensity of their involvement in the elections, do you think that the U.S. government and state and local governments are better prepared now than they were a

couple of years ago to respond to any kind of threat any kind of manipulation of voting systems?

POLYAKOVA: We're prepared in the sense that there's a lot more awareness of this is likely to happen, which I think has been the one positive unintended consequence of what the Russians did in 2016, and now we've had government officials talking about this all the time, making statements, sending warning signs. We've had the Trump administration move in certain policy ways to impose costs on Russia. So I think there's much broader awareness. I don't have to explain to people anymore what disinformation is as much as I used to have to, and I don't have to explain to people the Russians are interested in doing this to us. Sometimes you talk about why that is so clearly the awareness is there in terms of our ability operationally to respond, I think we're still quite behind.

That's actually my primary concern, is that almost two years, well actually more than two years, since we knew the Russian operation began around the 2016 elections that began in 2014 according to Special Counsel indictments, yes all these years later we still haven't really stood up you know a well-resourced, institutional response from the U.S. government, there have been some agency some tools that have been developed, but it's far less than where we need to be. We haven't figured out how to respond to disinformation campaigns which are much more ambiguous to figure out how to respond to, and I don't think we will not lead our population in real way against these kinds of propaganda information attacks. But I think we're at the beginning, and we're moving slowly in that direction. On the technical side, as we were talking about earlier, the voting machines, that infrastructure is incredibly vulnerable.

DEWS: I do want to spend some more time in a few minutes talking about some of those responses that you've suggested. I want to ask one more question about sort of what the U.S. government is doing. I think over the summer. Homeland Security secretary

Kirstjen Nielsen called Russia interference in the U.S. elections a “Category 5 hurricane” and other national security agencies and the U.S. government do seem to take it seriously, but do you think President Trump himself takes the Russian interference seriously?

POLYAKOVA: Well nobody really knows what President Trump thinks or what Mr. Putin thinks for that matter. We know what he says, we know what the administration does, and of course we've seen this gap emerge which is what you're alluding to between the statements and comments and actions of Trump administration officials and Congress who all seem to be on the same page about this red lights flashing, Category 5 hurricane. These kinds of statements are really raising awareness among the public, but of course the president has been more quiet on this, and not just quiet. He's made a lot of positive statements about Mr. Putin about Russia, he's a fine guy, why can’t we all get along. Of course, the Helsinki summit between President Trump and President Putin very clearly I think showed that President Trump was much more willing to buy into the Russian narrative which is deeply problematic. But at the same time, we see the administration moving in one direction and the president either not moving in the direction or staying quiet at this point.

DEWS: So let’s move away from the past and focus on the present and the future. You've called the kinds of disinformation campaigns that Russia ran against the 2016 elections yesterday's game. So if that's yesterday's game, what's tomorrow's game?

POLYAKOVA: That's right. And we're still trying to respond to yesterday's wars, but we should be really thinking about what is going to come at us, because despite what the Russians have been doing now for over a decade in Eastern Europe in terms of these kinds of influence operations, cyber-attacks, propaganda and disinformation, we were completely taken by surprise in the United States in 2016. That's not the case anymore because of some of the awareness raising that I've been talking about. But clearly what's coming at us is that these kinds of information warfare tools are becoming much more

advanced with the advent of emerging technologies like artificial intelligence. I think by now many people are familiar with deep fakes are for example, the certainly wasn't the case about six months ago. Deep fakes are of course manipulated audio or video that is generated to look original, meaning you know you can have President Obama saying whatever you want him to say, he'll sound like President Obama, he looks like President Obama, and you can use any world leader.

DEWS: I have seen one of those of Obama. It's very scary.

POLYAKOVA: Yes, you can't tell the difference between what's real and what's not and these kinds of AI technologies can also generate images of people that don't actually exist and the distribution technologies meaning how quickly this kind of fake content can spread are not really being dealt with by the social media companies who are being manipulated and used to spread this kind of content. I mean so far we really haven't seen Facebook, Twitter, and Google, and YouTube which is owned by Google, do much more than quite superficial fixes. One could say in terms of how they prioritize content or delete certain accounts and things like that, all welcome fixes, but at the end of the day, there is a much deeper ads driven infrastructure that malicious actors like Russia have manipulated before and will continue to manipulate to produce content it's not only impossible to tell from real or fake, but that also targets in a very personalized way, individuals in a customized way. So the same tools that you know Nike will use to sell sneakers to let's say young men between the ages of 17 and 19 who live in the suburbs of Michigan who hold certain political attitudes and who have maybe bought Adidas sneakers in the last year, this exact kind of micro-targeting tools are used to create much more precise disinformation and propaganda. And I've been surprised that we haven't seen more of this because those tools are out there in open source. Russia doesn't have the innovative capabilities to create those tools, but they're out there for them to use. And so I think we're going to see come at us, and again I'm surprised we haven't seen this yet, is much more

sophisticated forms of highly targeted, personalized, customized this information attacks beyond what we've seen the Russians do previously.

DEWS: You've also written about fake Web sites that work together in networks to spread disinformation. Can you explain what that is?

POLYAKOVA: This is sort of an emerging new area of research that so far there hasn't been paid much attention. I think it's difficult to do this kind of work for a variety of reasons. But the way that disinformation in general works is in a few ways. One, you want to put out a piece of content that then is amplified by various entities, so that those can be Twitter bots, trolls on Facebook, and they can also be forms of search engine optimization. So trying to manipulate what appears first in a Google search, for example when you search for Hillary Clinton and Al and Trump or Syria or whatever…

DEWS: You might get an RT or Sputnik story instead of a New York Times story.

POLYAKOVA: And so the question is well, how do people do this how did these hostile actions do this? One potential way to do it is to try to play with the settings and the algorithm. So for example, we learned about a few websites that almost act like zombie websites. So be a website that was a legitimate business at one point those may be gone defunct and then the urinal is up for sale, and the URL gets sold, and then you have dozens of these emerge. So then they start propagating the same cut and paste pro-Kremlin messages, this is happening on energy space for example around Norstrom too which is a Gazprom Russian project in Europe and then these Web sites can then work together to amplify the same message. Why do all this?

Two reasons. We don't know exactly how the Google algorithm prioritizes content, but we do know the two things they look at is has this website been around around for a long time? Is it credible, or is it a fly by night operation that was set up yesterday? Well if it looks like it's been around for a long time, the algorithm says this is more credible. So that's one reason to buy these old URLs that have been around for years. And the other

piece of information that we know the algorithm uses is are other Web sites linking to the content of this website? So then you see this network of Web emerge and it seems like they're trying to do exactly this, is trying to use some of these metrics the algorithm uses Google and others to try to push up certain content, to try to monopolize the narrative. And I would imagine that more and more of this is going to happen as well and that content can of course be amplified through Twitter and Facebook and other efforts like that.

DEWS: So how can governments in Washington and Paris and Berlin and others respond to these emerging tactics to deep fakes in a networked Web sites?

POLYAKOVA: This is an absolutely critical question. And again I think we're years behind from being able to truly answer it. I think clearly from a governmental perspective, we need to invest much more in understanding the implications of emerging technologies, not just artificial intelligence, that's the big one, but also things like block chain and decentralized technologies that we now talk about a lot in the context of crypto currencies, but it's not their only application. All these technologies are dual use, just like we've learned Facebook and Twitter are dual use, but we don't really understand the implications of them for these nonconventional threats, this form of political warfare. We need to invest much more from government in that respect and understand that in my view and in the U.S. government needs to set up a body, an agency that would have intra agency function to coordinate all governmental efforts looking at the implications of artificial intelligence and military, non-military uses. The military side of our government does do that already. We don't know everything about a lot of this work is classified for obvious reasons because it has very clear military implications, but there needs to be much more that's that I think is not being done to understand the full spectrum spanning from military to nonmilitary operations and how technology will transform those operations in the future.

That's step one because you know we talked about China a little earlier and the Chinese have a clear plan as to how they plan to lead on AI technologies by 2030. And it's

a huge amount of investment and they're planning to commit to this, and the U.S. government does not have such a plan. The last time we had an AI strategy was in 2016 the last administration. So I would hope this administration is also focusing on updating that strategy and committing more resources to this kind of work in the future.

DEWS: You've also talked about a whole of society response to these kinds of threats. What is that?

POLYAKOVA: So we mention inoculation earlier in the podcast on this concept of how do you actually get people to be more critical of their information consumption? So you look at a piece of content online and you're not skeptical necessarily. We don't want to be in a world where people believe nothing, right that is a deeply distrustful world. But we also know to be in the world where we are today where we have very low attention spans and we're sharing headlines or other information live without even reading it. We aren't really checking the new sources a lot of times, and so we want to be somewhere that sweet middle where somebody sees something online, their Twitter feed, their Facebook and Google whatever,, and they take a moment to think and do some basic checks, like is this a legitimate organization that I've heard of, if not the content will still be good, does it have editorial board, can I contact them? These things take a couple of seconds, and you know in our fast paced environment many people don't do them. They just look at the headlines and they share them really quickly.

But again the more stuff gets shared, the more there has much broader aggregate effects for how the social media platforms prioritize certain content. And so the actions that we take when we share something on our social media, actually does have profound consequences. And I think that's something that most people don't realize. You ever change. So my friends and that said but it's not really true. There is an underlying kind of backhand to all of this. And so when I say having a whole of society approach, what I mean is that government investment in how I described it into understanding the

implications of these technologies will not be enough. The U.S. model has always been more about letting the private sector Silicon Valley, drive these new developments. But there needs to be much more awareness reason that stemming from civil society as well. Obviously the private sector, the tech companies have a huge responsibility in this. And then of course our government needs to be set up in a slightly different way in making much more responsive to the digital era.

You know we have a government that is set up to fight 20th century threats and we're not the 20th century anymore, the threats look very different. And one example just to wrap up as to what I mean by that that we can look to is the antismoking campaign in the United States. So in the 1950s pregnant women recommended they smoke, doctors gave cigarettes to pregnant women. And now of course, not that far along really in the big scope of human history, smoking is almost outlawed basically in lots and lots of public and private spaces. So how do we go from pregnant women being recommended they smoke to where we are today? Well it took a lot of regulation of big tobacco, it took a lot of civil society groups advocating and activating and mobilizing society to make people more aware by the public health risks. We probably all in schools saw these horrible pictures of dark lungs that been affected by too much smoking. So there's an educational component, and then the end of the day it was the culmination of all these things that produced a really broad societal shift in different understanding of this habit because we were really talking about is how do you change people's behavior?

And to do that it requires a long time, a lot of trial and error, and a generational shift. And we are just at the very, very beginning of this. Twitter on Facebook we've only been around for about 10 years and the antismoking campaign took 65 years. So I think right now we're just starting to figure out what works and what doesn't.

DEWS: And we need to be seeing pictures of our brains on disinformation

POLYAKOVA: If only that was possible!

DEWS: So as the election season continues to unfold, what kinds of research are you doing and what are you going to be looking out for as the elections actually happen and beyond in terms of assessing Russian involvement and disinformation campaigns?

POLYAKOVA: Well I think certainly I'll be keeping an eye out for reports from congressional races. Their experiences with getting hacks, cyber-attacks, phishing attacks. Try to understand the extent, but also the sophistication of these kinds of campaigns. I mean so far there's only been a few congressional campaigns that said they've been targeted as a phishing attack. There's been some breaches in Microsoft for example that Microsoft reported on these and they linked to the Russian intelligence agencies as well. So I've been looking a lot of those things at the election understand the scope of what's really happening. On the other hand, what I'm really concerned with is what we're talking about earlier and what does the future hold. Right. How do we get ahead of this game? You know how do we not get surprised again? So when I'm working on now is exactly trying to understand how countries like Russia will use artificial intelligence tools to create and design far more sophisticated influence campaigns and what we can do about it today. So this is a paper that hopefully publish Brookings the next couple of months they'll looks at the implications of Russian development of technologies for political warfare.

DEWS: All right well we'll look forward to seeing that paper and having you back on the program to talk about it.

POLYAKOVA: Thank you Fred.

DEWS: Alina, thanks for sharing your time and expertise.

POLYAKOVA: It's my pleasure.

DEWS: You can learn more about Alina Polyakova and her research on our website, Brookings.edu and also for more analysis from Brookings experts on the upcoming elections. Go to Brookings.edu/2018-midterms.

Now here's expert Molly Reynolds with her analysis of the shape of the House and

Senate races and what Congress could look like after the midterm elections.

REYNOLDS: Hi this is Molly Reynolds. I'm a Fellow in Governance Studies Program at the Brookings Institution. With the midterm elections just weeks away, the House and Senate are both on recess, with members back in their states and districts. All 435 House members and 35 senators will find themselves on the ballot on November 6th. With the results determining which party controls each chamber for the next two years. By now, the fundamental dynamics at play in the midterms are familiar to many. Democrats enjoy the lead, currently an average of about eight and a half percentage points. On the so-called generic ballot for the house, the poll question where respondents are asked: which party's candidate they would vote for, which party they would prefer to see control Congress. But the generic ballot doesn't tell us much about what the outcome is likely to be in specific races. It does give us a solid overall sense of what to expect in the race for the House.

Other important factors also point towards a favorable environment for Democrats. The president's party almost always loses seats in the House in the midterm elections and presidential approval is an important predictor of how well the out party is likely to do. President Trump remains unpopular with an average of only about 42 percent of respondents indicating they approve of his performance. Democrats then are well positioned to make significant gains in the House of Representatives. If they gain a majority in that chamber on November 6, it will be the first time the party has had a House majority since 2010. More than 40 percent of current House Democrats have never served in the majority, so a change of partisan control of the chamber would usher in a different experience for these members. They'd be serving the chamber where their party gets to set the agenda. That is, decide what bills get considered in committee, and debated and voted on on the floor.

Because Republicans are likely to maintain control of the Senate and will have two

more years of control of the White House even if Democrats do pull off an upset in the Senate, few of these Democratic priorities are likely to advance far in the legislative process. But having the power to set committee agendas would allow Democrats to pursue an aggressive agenda of oversight of the Trump administration.

Indeed, Democrats have already begun to lay out a plan for the kind of investigations they'd pursue. And their priorities wouldn't just be focused on corruption and ethical issues presented by the Trump administration. While things like obtaining Trump's tax returns are likely to be on the table, so are investigations of Trump administration implementation of various federal programs such as actions by the Department of Health and Human Services to undermine the Affordable Care Act. It's not just House Democrats however who are facing significant changes to their caucus after the midterms. House Republicans are too. Regardless of whether the party loses control of the chamber, there are 39 House Republicans not running for re-election this year. This includes eight committee chairs, five of whom would be ineligible to continue to serve in those roles in the next Congress due to House Republican Conference rules that limit members to three terms in committee leadership roles. The conference will also find itself under new leadership. As Speaker of the House Paul Ryan's retiring, and a new leader will succeed him either speaker or minority leader.

The ideological center of gravity in the House Republican Conference is also likely to move to the right after the midterms. Again, regardless of whether Republicans narrowly hold on to their majority. The vulnerable districts that Republicans are likely to lose to Democrats are generally represented by members at the relatively more moderate end of the Republican conference. Consider for example the 20 Republicans who voted against the bill that would have repealed the Affordable Care Act in May 2017. Half of them represent districts that are rated by the Cook Political Report as toss ups, as leaning towards the Democratic candidate, or as likely Democratic pickups. In 2019, then, the

typical member of the Republican conference in the House is likely to be somewhat more conservative than the average member in the current Congress. This could have consequences for everything from selecting a new Republican leader to actually passing legislation.

Even if Democrats gain control of both chambers with a Republican in the White House, we're guaranteed at least two more years of divided government and the governing challenges that come with that. And if Republicans do maintain their majorities in both chambers, the majority in the House is likely to be smaller, even while their majority in the Senate could grow by a few seats. Either of these scenarios would reshuffle power and influence important ways with profound consequences for what was in Congress.

DEWS: “The Brookings Cafeteria” podcast is the product of an amazing team of colleagues, including audio engineer and producer Gaston Reboredo, with assistance from Mark Hoelscher. The producers are Brennan Hoban and Chris McKenna. Bill Finan, Director of the Brookings Institution Press, does the book interviews, and Jessica Pavone and Eric Abalahin provide design and web support. Our interns this semester are Churon Bernier and Tim Madden. Finally, my thanks to Camilla Ramirez and Emily Horne for their guidance and support. “The Brookings Cafeteria” is brought to you by the Brookings Podcast Network, which also produces “Intersections” hosted by Adriana Pita, “5 on 45”, and our events podcasts. E-mail your questions and comments to me at BCP@Brookings.edu. If you have a question for a scholar, include an audio file and I'll play it and the answer on the air. Follow us on Twitter @policypodcasts. You can listen to “The Brookings Cafeteria” in all the usual places. Visit us online at Brookings.edu/podcatsts. Until next time, I'm Fred Dews.