Center for Strategic and International Studies

"Press Briefing: Potential Election Interference Ahead of the November Elections"

CSIS Experts:
James Andrew Lewis,
Senior Vice President,
CSIS

William A. Carter,
Deputy Director and Fellow, Technology Policy Program,
CSIS

Heather A. Conley,
Senior Vice President for Europe, Eurasia, and the Arctic; and Director, Europe Program, CSIS

Suzanne Spaulding,
Senior Adviser for~~,~~ Homeland Security~~, Program and~~ International Security Program,
CSIS

Moderator:
Colm Quinn,
Director of New Media and Audience Development,
CSIS

Location: CSIS Headquarters, Washington, D.C.

Time: 3:00 p.m. EDT
Date: Wednesday, October 17, 2018

Transcript By
Superior Transcriptions LLC

COLM QUINN: OK, folks, I think with that it's about 3:00 p.m., so I think we'll begin.

Brief introductions first. My name is Colm Quinn. I'm in the External Relations Department here at CSIS.

Speaking today in order will be Jim Lewis, who is a senior vice president and also directs our Technology Policy Program here at CSIS. To his immediate left is Will Carter, who's a fellow and deputy director of Technology Policy Program here, followed by Suzanne Spaulding, who's a senior adviser for Homeland Security and our International Security Program here. And finally speaking will be Heather Conley, who is a senior vice president for Europe, Eurasia, and the Arctic, and also our Europe Program director.

Just a few housekeeping items before we begin. Do please speak into the mics when you're asking your questions. We also have people calling in on our conference line, so just making sure everything is picked up; also very important to use those microphones because we will be putting a transcript together of this directly after this event concludes, so just to make sure that everything is recorded.

So that's everything I have. And without further ado, I will hand over to Dr. Lewis.

JAMES ANDREW LEWIS: Thanks, Colm.

So I'm going to talk about a general overview and about the administration remarks about Russia, China, and Iran. Will, to my left here, will talk about domestic preparations and the work at the states. Suzanne will talk about DHS and some of the threats we face. And finally, Heather will talk about what she sees the Russians as up to, where she believes the risks are from there.

So there's been a lot of studies since 2016 on how to improve election security. We're doing two or three ourselves. And so that's why I thought this might be useful. But the environment is very different than it was in 2016. People know about the foreign interference. They know about fake news. The social-media companies are on the spot to try and deal with the problem. And the states have put – as you'll hear from Will, the states have put a lot of efforts into hardening their system. So the tricks that we saw in 2016 probably won't work as well this time. We are in a much better place than we were then.

Russia is still the leading problem in terms of interference, and Heather will tell you about their efforts to do reconnaissance on voter registration and the electoral machinery. One of the things that we have been looking at here at CSIS is if there are people, foreign powers, who intend to interfere in our elections, will they do it now or will they save their best tricks for 2020? We all have different views. I kind of vote for 2020.

We know from a variety of sources that both China and Iran studied the 2016 Russian effort to see what they could learn from it, if they could duplicate it. And so both of them have campaigns that are at least looking at how you could interfere with the American elections.

For the Chinese, I think this is part of a larger global-influence campaign intended to improve China's image and to increase its soft power. It's not only in the U.S. It's in other countries. But the

most effective techniques for the Chinese have been to organize students and businessmen in protest groups and to use their market access as a way to shape opinion. We have not seen the same kind of messaging that the Russians undertook.

Iran's efforts are crude. And they appear to be more designed for the Arab street than for a U.S. population. So while the Iranians have thought about interfering in the U.S. election, they have not put that much work into designing an effective program. The biggest gap in our policy is that we still have not done enough to discourage Russia and others from trying again. What would be useful would be a clear statement from the administration that there will be consequences for any foreign power that interferes or tries to interfere in our election.

As I said, with all the work, our electoral systems are in much better shape than they were in 2016. Is the election threat overrated? Not really. There's a lot of people who would like to do us harm. But what is underrated is our ability to defeat it. We have strong institutions and our democracy is strong. I think with the lessons of 2016 before us, we will do better this time.

Will.

WILLIAM A. CARTER: Thank you, Jim. So we undertook a project over the last few – we undertook a project over the last few months to better understand the cyberthreats to U.S. elections, and also some of the work that's been put in in the last two years to harden our infrastructure and our systems. One of the first things that we did was put out a survey of the cybersecurity experts in our network to better understand the types of threats that they were most concerned about. Unsurprisingly, over 80 percent identify Russia as the number-one threat to U.S. elections. But it was interesting to see that the vast majority of our experts agreed that the real threat we need to worry about is influence operations and information operations. Direct cyber threats to core election infrastructures were not as high on their list.

And I think that reflects in part some of the defenses that have been put in place, both before and after the 2016 election. Importantly, in the last two years a number of measures have been put in place using $380 million of funding under the Help America Vote Act passed by Congress, as well as state funding, that will be in place ahead of the 2018 elections. More than $40 million has been earmarked for new security measures in advance of 2018, including seven states using that funding to expand post-election audits, twenty states conducting security assessments and implementing cybersecurity upgrades across their systems before November, 14 states upgrading voting systems and replacing voting machines, five states that have earmarked dedicated funds to replace voter registration systems and e-poll books, 13 states that have earmarked more than a million dollars for advanced cybersecurity training for their 2018 election staff.

And 44 states participated in a recent DHS three-day exercise to help them to understand how to coordinate incident response and information sharing in the event of an attack on our election systems. I'm going to let Suzanne talk a little bit more about DHS's efforts. And finally, and this I think is really important, all 50 states are now members of the MS-ISAC. And 548 state and local election organizations are now members of the election infrastructure ISAC. And in fact, over 1,000 organizations are participation informally in the election information sharing network. So in terms of understanding the threats that are out there, the types of attacks that people are seeing, the information flow is a lot stronger than it was.

Finally, much more is being done in advance of the 2020 election. Half of the experts in our survey agreed with our assessment that Russia is going to save their best tricks for 2020. And almost $200 million has been earmarked for specific security measures. Over 100 (million dollars) for upgrading voting machines and secure vote tallies across 42 states. Fifty-two million dollars to significantly upgrade or replace voter registration systems in 29 states. And almost $3 million has been dedicated for election night reporting systems.

There's still more that needs to be done. Many states have ambitious plans that they would like to implement but haven't been able to locate the funding to do everything that they want to do to secure their election systems. Many states and local organizations are not leveraging partnership opportunities with the FBI, DHS, and private organizations like Cloudflare, Jigsaw, Microsoft, Synack, Akamai, and others that have offered pro bono help to secure election systems ahead of 2018.

And finally, we need to keep in mind that credibility is as important as accuracy in elections. And that means not just securing the voting systems and voter registration systems that could directly affect the outcome of the election, but also ensuring that campaigns and election-night reporting systems are secure, so that our votes are the results of elections and the candidates that are running have credibility in the eyes of the voters.

With that, Suzanne?

SUZANNE SPAULDING: All right. Thanks, Will.

So I think we have made significant progress since I was at the Department of Homeland Security as the undersecretary responsible for cybersecurity and infrastructure protection. We designated, of course – at the very end of our time, we designated election infrastructure – I prefer to say recognized election infrastructure – as critical infrastructure. We made the formal recognition that it fit the definition of being of significance to the nation. And as a result of that a number of things happened, including institutionalizing/regularizing mechanisms for interaction with the state and local officials.

So they established the Federal, State, Local, Territorial, and Tribal Coordinating Committee (sic; Council), the FSLTTGCC, which is terrific. (Laughter.) Or you can – yeah, a lot of fun to say. Or you can call it the GCC, the Government Coordinating Council. And that's for the feds and the state and local election officials to come together on a regular basis, and establish their priorities and strategies and ways in which they can help each other, in addition to the information sharing.

And then, in addition, a Private Sector Coordinating Council, so the Sector Coordinating Council, which is primarily, actually, the vendors and the folks who produce the infrastructure that the elections use. That's an important place, also, for those folks to come together, and to come together with government officials.

And then, as Will mentioned, of course, they set up the Election ISAC, the Information Sharing and Analysis Center, which is located, you know, as part of the sub-sector to the Multi-State ISAC, which is a long-established information sharing and analysis group made up of all the 50 states and their key IT defense officials. And they have a seat on the operations floor at DHS, of the NCCIC, the National Cybersecurity and Communications Integration Center. There is a seat there for the MS-ISAC, just as there is for some of the private sector ISACs – electricity, et cetera. And so they get –

they have the opportunity to get real-time visibility, the same visibility that DHS cyber analysts get, and now there is this subset for elections.

They are providing more clearances for state and local election officials, although I will say I think we are never going to clear our way out of the cybersecurity challenge. And so I think they continue to put, as we did when I was there, a tremendous emphasis on getting information at an unclassified level so that it can be shared more broadly. But they are – but there was concern among some of the state and local election officials that they didn't have access because they didn't have clearances, so they are working on getting them clearances.

So government has done a lot. DHS certainly has done a lot to secure the election infrastructure from cyber – malicious cyber activity.

And civil society has also stepped in. I've been working with folks up at Harvard, at the Belfer Center, the Defending Digital – Defending Digital Democracy Project, which has worked with state and local election officials to produce tabletop exercises, campaign playbook, a state and election officials playbook, both of those written for non-technical officials, senior officials to understand the cyber risks that they face and basic steps to take to address them; and a communications annex, which as we know is increasingly important.

But as we understood even in 2016, in the runup to the elections, as we saw the malicious activity around voter-registration databases, the biggest concern, as has been stated, is really about undermining public confidence in the credibility of the outcome of the election. And that's what we were worried would happen with their – with Russia's access to voter-registration databases, that they would remove names, change names, do things that would otherwise cause significant disruptions on Election Day and cause people to wonder about the validity of the outcome.

And so we understand that in countering that, a key is making sure that you can restore or maintain public confidence and that's where, really, paper ballots and the audits become so important. Because all of the cyber steps that you'll put in place, nothing is a hundred percent guaranteed, and so you want to be able to go in after the fact and be able to tell what if anything happened. And in virtually every case, what you'll be trying to do is reassure the public that nothing did happen. So that's critically important.

Finally, and this is where we'll segue into Heather's presentation, I think it's really important that we understand that the influence operations, which is what we are really critically concerned about, are not just about elections.

After the election in 2016, there was a lot of talk about the Russians will be back in 2018 and we now know they never left and that this started long before the elections and will continue – continues to this day and that it is really a broader campaign to undermine democracy, including other democratic institutions. And the project that I'm working on here at CSIS is looking at how they are working to undermine public confidence in the justice system, so it goes beyond elections.

HEATHER A. CONLEY: Great. Suzanne, thank you so much.

I thought I would begin with a quote actually from Secretary Mattis, who said last month there is no doubt that they, Russia, has transferred money and are also conducting broader influence campaigns. Now, Secretary Mattis was in Skopje prior to the Macedonia referendum to change its

name. But I think it helps to understand that this contest continues on in Europe and in the United States.

Just to echo some themes that Suzanne has noted, this is about the credibility and integrity of the U.S. election process, but it's so critical to understand that Russian malign influence is a continuous and holistic operation. It does not end, but it does have – I think there is a – there is a level of intensity that begins one to two years before a major national election or a parliamentary election in the case of Europe and then there is a post-election cycle that looks at what worked, what didn't work, how does that adapt – necessarily adapt those techniques. So it's very important, again to reinforce it is a never-ending process. You can't say after an election, whew, we got through that. It's a continuous sense.

I think I have taken a great deal of instruction from watching how the French responded to the 2017 French presidential election and the Russian cyberattacks on President Macron's campaign. And I think for me, it's been a helpful way the French Network and Information Security Agency has sort of six steps of how you think about protecting elections. The first three steps: to prevent, to anticipate and to protect. And if I use that as sort of the guidance, in 2016 the U.S. was not where we wanted to be in either preventing, anticipatory or protecting. But I think as you've heard, very significant steps have been made in those three areas.

The other three areas where I think we're going to continue to have to do much more work is detection, attribution and reaction. And those are the other three steps. And in the detection, the auditing process, understanding what has happened, what has occurred to continue to provide future protection, but it is that ability to, with clarity, attribute who and what is happening. And that in our political conversation has not been as clear as it should be on a bipartisan basis for clarity of attribution.

And then there's been a much delayed reaction. If in fact the behavior has been detected, it has been attributed to an actor, then what is the policy response by the United States government? In 2016, we had a delayed response to that. There is now an effort to be preemptive. And legislation that Senator Marco Rubio and Senator Chris Van Hollen have put forward, the DETER Act, which is an effort to establish clearly what would happen if an actor would in fact interfere with U.S. elections. And it's unknowable if that would have a deterrent effect just having that legislation being proposed, but we do need to think about defining thresholds and declaring our policy and what would happen and then, of course, following through on that – on that declaratory policy.

As I look forward through the lens of Russia, I think what we're going to anticipate is a lot of what we call below-threshold activity, that which would not rise to the level of invoking any very strong reaction to that. I think they will continue to test new approaches on disinformation and influence operation. That is where they have concentrated their activities and where it is the least cost and the most successful.

I think it will continue to look more American and less Russian. And I think this is where some of the work that just now – we're seeing really, because of the data analysis of the 2016 social-media inputs, whether that's Facebook, Twitter, and others, we're seeing where it is focusing on identifying affinity groups, understanding whether that would be law-enforcement groups, which is another credibility-destroying effort – the military, religious organizations, that these unwittingly are being used to promote disinformation and malign influence.

I think this will also be a testing and a probing of the most divisive issues for the country. Russian malign influence seeks to exploit weaknesses and amplify divisions in our society. They don't

create the divisions, but they amplify them. And they are an equal-opportunity amplification. They will work both sides of the division to see who can be more volatile and more divisive into society.

And so what we anticipate – and we hope we're not surprised on the down side; you cannot discount that – but I think we're going to continue to see testing and probing of new methods, new themes, new issues. This will, in fact, be preparatory for those themes and organizations that seem to have efficacy in the lead-up to the 2020 presidential election.

And just to give you a comparison, it was last year – as many of us were preparing for Russia's military exercise in the west, Zapad, we were all very focused and anticipating that this would be something very significant. We almost over-anticipated. The exercise was sort of normal or what we would anticipate. And in some ways that was our own catch, because the Kremlin was very quick to say, what were you – here you go; you were saying we would do something, and yet we did not.

So I think this is where we have to think very clearly about making sure we don't over-respond or overreact to something that may not be there, but be very confident that we have the ability to push back and to detect this behavior and hopefully build confidence amongst the American people that we have adequately prepared for this ongoing challenge.

And with that, Colm, over to you.

MR. QUINN: Thank you so much, Heather.

Thank you, everyone, for giving your comments.

I will now turn to questions. Just, if you could, name yourself and your outlet when you ask a question; make it easier to find yourself later on. And so if anyone has any, please raise your hands. And we also have people on the phone as well. We can come to you once we've come to the room.

Yes, sir.

Q: Hi. Paul Handley from AFP.

There's been some lack of clarity on how much – how much attempt there have been to interference with systems on the cyber side. I have the same question for influence ops. But could you talk about that? There were some reports at Congress today, the result of which wasn't clear; other various reports. What are they trying to do? And how does it compare with last time, 2016?

MS. SPAULDING: So the confusion is understandable, because, on the one hand, we have public statements saying we haven't seen any concerted efforts to, you know, interfere with the election. On the other hand, we did – we've seen these reports about an increase in reporting coming in from the states about cyber activity.

I think – based on the comments that have been made from DHS publicly, I think what's happened is what you would expect when you put sensors in place. So as the states have stepped up to cooperate with DHS, they have put systems – they have deployed tools that the state and local folks are using that are allowing them to detect more of the activity than they were able to detect in the past. They are also reporting more of that activity than they were before to the feds, to DHS.

And so we saw the same thing when we – when we deployed technology to the various civilian departments and agencies to detect suspicious activity. We knew that the first reports would be very alarming, because suddenly you were getting greater visibility. It doesn't mean that the actual level of activity has increased. So what may be seeing is simply better detection of the same level of activity. And in fact, some of the state and local officials have said just that.

MR. CARTER: I would add that I think a similar phenomenon is happening on the campaign side. So greater awareness among campaigns of cybersecurity issues and of Russian efforts to target campaigns for – primarily for doxxing purposes – has led to more campaigns discovering anomalous activity, reporting anomalous activity, and chasing it down. So there's definitely been many reports of activity targeting campaigns in this election. And I don't necessarily think that that reflects a greater volume of attacks overall, but it's certainly kind of greater awareness. And I think take that as a positive sign. We're catching it more, and we're becoming more active in responding.

MS. SPAULDING (?): Do you want to define doxxing?

MR. CARTER: Oh, yes. And doxxing is the kind of selective releasing of documents that are stolen from a campaign. So, for example, some of what we saw targeting the DNC and the Clinton campaign in 2016, among others.

MR. LEWIS: We have a pretty good idea of what the timeline looks like, and there's two thresholds. The first is, will people try and interfere with the voting process itself by interfering with voter registration rules or reporting or accounts. That will happen on Election Day, right? The other would be the influence operations. These usually occur two to three weeks out, if they're to have any effect. So we're at the magic moment, if people are going to launch something. And that's something to watch. That's one reason why the next week or so might be really critical for whether the Russians – who are the primary actors – whether they actually release something.

It's going to be hard to get the same level of effect in a series of state and local races that you get for a national race, right? So there's not going to be the one big bang we saw in 2016 or that they tried to have in France. But we're at the – we're at the timeline now. If they're going to do something, it will happen pretty soon.

Q: Can I just follow up? Do you know of any successful interruptions or invasions in cyberspace, state and local campaign this time around?

MR. CARTER: So there have been some confirmed reports of them targeting campaigns. Most of the confirmed reports, just given the timeline, are from the primaries, including some, for example, DDoS attacks against some candidates around high-profile events and debates.

MS. SPAULDING (?): A DDoS attack is?

MR. CARTER: A DDoS attack, a distributed – a distributed disruption of service attack. Basically, blocking people from getting access to their campaign websites to find out more about who they are.

MS. SPAULDING (?): Or to give them money.

MR. CARTER: What? Yes. Or to give them money.

Q: That was mainly around the primaries?

MR. CARTER: Most of the ones that are now confirmed. The ones that I was thinking of, including one of the DDoS attacks that was reported, happened during the California primaries.

MR. LEWIS: That's why we think this might be a test run for them. 2018 will be testing, because reconnaissance and low-level stuff, but no big actions. So 2018 might be the preparation for 2020.

MS. SPAULDING: Which isn't to say that we aren't seeing any influence operations out there that are – that involve the elections. Certainly we've seen Hamilton 68, which tracks social media accounts that are either affiliated with Russia or known to be really pushing Russian narratives, for example, highlighting "walk away" – hashtag #WalkAway, which is trying to get people to be so disgusted with the process that they opt out.

MS. CONLEY: And this was, in fact – I offered the Macedonia. It's voter suppression, voter confusion, misdirecting, this polling place is closed. That could be where misinformation could be part of the suppressing voter turnout.

MR. LEWIS: But compared to the level of activity in 2016, we are not at the same level of activity in 2018. And that is something we're trying to figure out why. Is it they're saving their best tricks? It's because they've already set the fire and they don't need to do more? Or is it that they are worried about something? But we're not at the level we saw in 2016.

Q: Yeah. Shaun Waterman, a freelance reporter.

Two questions. First of all, there was an issue with the vendors and their attitude to security research and cybersecurity generally. They didn't seem to believe in it. Is that – you know, can you talk a little bit about what you found, William, in that – in that regard?

And, for Suzanne and anybody else, you know, a lot of conversation has focused around the states and the attitude of the states and what DHS is doing with the states. But, you know, on the ground, the polling is actually run by the counties. The counties count the votes. I mean, is there a gap there? Is there a capability gap or an information-sharing gap between the – you know, at that level?

MR. CARTER: So I think a big part of the issue that a lot of the vendors had with some of the coverage, the vulnerability research and some of the big demos – for example, the DEFCON Hacking Village – were that they created unrealistic circumstances which made the systems seem far more vulnerable than they were and didn't reflect the real threats that these companies are genuinely worried about and that they invest a lot of money in trying to manage. And so, you know, I don't think it's general opposition to or skepticism of cybersecurity or cybersecurity research, but there were some objections to the way that it was being done. All of the companies – and this goes beyond the election systems vendors – many companies across many industries take issue with public disclosure of vulnerabilities that they haven't had an opportunity to patch. That's another practice that's been of concern.

But I do think, at the end of the day, all of the major vendors that are working – that are providing election systems in the United States have gotten the message that security of these systems

is a higher priority than it has been, and I think it's an area where they are going to be investing and where they have been investing. And they take issue with some of the tactics that have been used in some of these kind of, you know, grand displays of vulnerability, but that doesn't mean that they don't believe in research and they don't want to know where these vulnerabilities are so that they can address them.

MS. SPAULDING: And on the counties, it's a really good point, and it's one of the reasons that I actually use all the letters in FSLTTGCC, because it's Federal, State, Local, Territorial, Tribal Government Coordinating Council. And so it does include – I mean, it's open to local officials in addition to state officials.

The Homeland Security secretary talks about 90 state and local entities that are, you know, very much engaged with the department. But that still, even if you assume that, you know, only 40 of those are states and, you know, 50 are counties, that still leaves out an awful lot of local jurisdictions.

The assistance to those folks is going to be filtered largely through the National Association of Secretaries of State and the secretaries themselves. So the elections are run through the secretaries of states' offices, and they're very aware, obviously, of all of the local elements of those elections, and they have those mechanisms and those communications in place.

The tabletop exercises that I referenced included the – you know, from the precinct captains to the poll workers, up to the secretaries of state and the, you know, senior government officials. So there is an awareness and a – and folks who are looking at this are factoring in the roles all the way through the system.

But is there a capacity gap? Absolutely. I mean, there's just no way around that. You have to acknowledge that they don't have the resources. It's much like local campaigns, where the IT person – you know, there's probably no CISO. There's no, you know, chief information security officer for a campaign. There may be an IT person, but they're also the person who's putting signs up and licking envelopes and has a day job. So yes.

MR. LEWIS: Just on the county point, too, it's worth thinking about that the Russians were probably surprised in 2016 about the decentralized nature of the American electoral system, and that helped a lot, you know. It's hard to hack thousands of different systems.

But what we're looking for now is a more sophisticated approach would target some key electoral districts, either for House or Senate races. We haven't seen that. One of the questions is will they, you know, in the last minutes try and influence these key races? They're not going to go after every race in the country. This is not going to be a replay of 2016. But they might – there's no evidence yet, but if they thought about it they might go after some of the key races. That's something to watch for.

Q: Hi. I'm Ann Kaupet (ph) for the French radio.

Talking about targeting, I just wanted a clarification about how many states still don't have paper ballots. And do you think they will be more targeted than the other? As you said, it's more political, that maybe it's easier when you don't have paper ballots to check.

MR. CARTER: Sure. So 14 states have no paper trail for some of their voters. Five states have no paper trail for all of their voters.

But a few things. One, I think we have to keep in mind that it's not just about a paper trail, it's about actually doing the audits, and particularly risk-limiting audience, that are conscious of the risk that you're trying to manage. That's something that is a broader problem across the states, and even states that have the paper ballot trail to actually do these audits aren't necessarily doing them or doing them as well as they could.

But the other thing is a number of these states are actually already taking action to replace these systems. So, for example, Virginia is replacing their paperless voting systems out of the 2018 election. And by 2020, 39 states will have voter-verified paper trail for all of their – all of their votes; another 11 will have partial coverage, with the goal of reaching full coverage. And so that bring us to 50.

So I think it's a problem that is recognized and, you know, there is action being taken, but the big challenge is going to be funding the replacement of all of those machines funding the management of all of those paper ballots, and funding risk-limiting audits to make use of that audit trail.

Q: Hi. I'm Jun (sp) with the South China Morning Post.

I think both President Trump and Vice President Pence mentioned at some point in the past few months that China has been proactively interfering with the midterm elections in the United States, and just now Dr. Lewis brought up the point that, you know, China has been studying, you know, Russia's approaches to interfere with the 2016 elections. So my question is, do you guys think China has the capability to do that? Or are there – are there signs or evidence so far to support those comments made by Trump and Pence? Thank you.

MR. LEWIS: So there's a consensus within the intelligence community that China and Iran are studying Russian activities in 2016 and interested in finding ways to duplicate them. The Iranian efforts, as I have said, have been relatively crude.

Chinese efforts are more interesting. We have not seen them do the kind of hack and release activities that the Russians used so successfully in 2016. There's probably one or two test cases, one test case in Taiwan of an influence operation that looks like a Chinese test. If you look at Australia, New Zealand, and Canada, you can see a much more active campaign. But there's a general view in the U.S. that China is trying to figure out, on top of its larger influence campaign – you know, the full-page ads in The Des Moines Register – well, that's politics, not Russia-style interference. But there's a sense that the Chinese are trying to see if that's, one, something they can do; and, two, worth doing. So there's no doubt there.

And I asked exactly the same question; I was like, oh, you guys are just saying this to obfuscate. And the answer is, no, we're really seeing it from all three countries.

Q: Speaking of the president's comments – Rob Pegoraro. I write for Yahoo Finance and The Parallax.

You've spoken a lot about keeping people's confidence in the system, but for the past two years the president has been scoffing at the idea that Russia did anything and that it helped him in any way, and literally telling his supporters don't believe what you see and hear. Much of his party, like the

chairman of the House Intelligence Committee, seem to have bought into that. How does that complicate this confidence-building pull?

MS. CONLEY: Well, it really hampers sending a unified and clear message to the American people to be vigilant, to make sure they understand and how to be discerning readers of their news and their Twitter feeds and Facebook. This is where, again, we look towards Europe, that have had some very successful examples. Sweden and news literacy. And you really do need a whole of government approach to this. I think you have a more unified effort amongst the various departments that are charged with both protecting this and identifying it. But you are absolutely correct. When we do not have a unified message in Congress and in the administration it gets very confusing for voters, who I'm sure are already very confused about what is true and what is not true. So this is why, I think, we all feel that there has not been the best effort put forward in this strong, clear, unified, whole-of-government message on Russian malign influence.

MR. LEWIS: One of the best – one of the best things we could do would be to have a coherent Russian policy. And we don't have that. And one of the best things we could do would be to come up with a credible deterrent policy. And there's been work on that, but I think it's the need for coherence and credibility that will be the things that are most effective in protecting us.

MS. SPAULDING: And of course, it goes beyond just the unified messaging to a whole-of-government strategy and plan of action. And that requires—there's a formal interagency mechanism that helps to produce that, where White House-led, you know, convening of interagency folks at various levels, working its way up from assistant secretary of state deputies to principals, develops – everybody brings to the table what they can – what their insights are, what capabilities, resources, tools they have to counter it, and a plan is put together. And I think there are some statements coming out of the White House, just in the last few weeks, that maybe there has been an interagency meeting along those lines. But it would be the first in this administration, I think, interagency meeting specifically to look at foreign influence efforts, and particularly Russian influence efforts, and begin to develop a unified plan.

MR. CARTER: I think that it's encouraging to see that a growing number of states can have a very kind of factual debate about improving their election systems, where things like election security were viewed as a proxy for efforts to manipulate, you know, relative voter turnout or access to the polls in the past. There's still some of that. And we've seen in some states the defeat of legislation that would strengthen electoral systems' security, because there is concern that it's being used as a proxy for political ends. But I do think that if more smart people come out and talk about the risks that we're facing, and the more that it's become a mainstream conversation, the more it is pushing these state legislatures in particular to start passing the legislation to authorize and fund more security measures.

MR. LEWIS: Also – you know, we also don't want to give the Russians too much credit. I mean, they were very active in 2016. They definitely violated American sovereignty. But it's not sure to me how effective they actually were. They took existing divisions and amplified and accelerated them. But let's not give them too much credit for doing basically an expanded effort at their traditional influence operations.

Q: Hi. There have been – there have been a few stalled efforts in Congress in terms of election security legislation, such as the Secure Elections Act which has been stalled in the Senate Rules Committee. Has anyone on the panel heard about any movement on that? And if not, is there anything more that can be added to that to get more majority support for that bill?

MR. LEWIS: Well, I think we're in the descent phase when it comes to the election, so probably nothing will happen until after November 8th. I mean, that's always the safe bet on any issue. What people are looking at now is where – what the defenses we have now are what we are going to have to use. They are more than adequate. But we need to increase our efforts for 2020. And I think that will be the focus. So next Congress will probably pick this up and we'll see more.

MR. CARTER: On some of the legislation that's been debated, I think a couple of the issues that are not going to go away, one is cost. And, you know, anything that is putting a significant amount of money into anything is difficult to get through Congress for one reason or another.

And a second is the – I think so much is just frozen around the midterms right now. If we see in 2018 significant campaigns to target core election infrastructures, I think that would provide a lot of support to folks in Congress who are trying to push legislation on this. If we don't see a lot of activity, it might be a little bit more difficult for them to sell that narrative going into 2020. But also, keep in mind, if we see changes in control of a chamber, that could also have significant implications for what's moving and where there's interest in pushing legislation forward.

Q: Thank you. Jeff Seldin from VOA.

You mentioned earlier some of the Russian influence campaigns targeting affinity groups like law enforcement, the military. Wondering, what did you see during 2016 targeting groups like that? And what have you been seeing in the runup to this election?

MS. CONLEY: So, again, this is mostly anecdotal. I study more European methods and approaches. I think we saw, again, testing out of new – it looked more Russian, it was very clearly marked, it was a little clumsy efforts. And I think what we've seen is evolution where it is now looking much more as it originates from American organizations. And again, this is where in the amplification, what we've seen – and, Will, I may ask you to have that great example.

We've seen this in the German experience a little bit more where it's the use of getting a broad group of diverse interests together as a chat group, they're sharing innocuous pictures and then over time the pictures start being interspersed with some light political messaging about immigrants or something like that, and then it starts – it starts identifying the key voices within these broader groups. They are American voices. It provides them with more – the pictures leave, it's more political messaging, and then they have captured hundreds of thousands of voices within these larger groups and then they start messaging very divisive issues.

So is that Russian? It was sort of organized by that. But by the end of it, it is amplified by Americans on the views that they have. And that's what's going to be harder and harder to discern what is truly a Russian attempt at malign influence, or is this just creating and amplifying divisions?

And, Will, maybe you have a more specific view on that German example.

But it's a – it's a nice way of saying this is where we have to have organizations very aware. And I'm very worried about religious organizations. We are seeing a prevalent use of Russian malign influence with the Orthodox church across the Western Balkans and Central Europe. There is no tool that is not potentially abused. And if you're not prepared to think about that, you could be very susceptible and unwitting to something being part of. And you – even law enforcement has been

caught up and they had no idea what was behind this organization. So it's getting quite less Russian, more American and harder and harder to detect what it is.

MR. CARTER: I think the one thing I would add to that, the example that Heather was talking about was an example that there was a great study done of a campaign during the German election. What I – what I think was interesting about that was Heather talked a lot about the very important issue of them manipulating existing identity groups and turning them against each other. But what was interesting about that particular campaign was they created a group that previously had not identified itself as a group and tied them together into a self-identified grouping of people who shared a political vision. And as Heather mentioned, the initial contours of the group were they were sharing these images, they were from all different political stripes, demographic backgrounds, and they were tied together into a political entity.

And so I think, in addition to exploiting groups that already exist, creating identities that can be put into conflict with each other is the next kind of evolution, I think, of Russia's tactics in this area. And it complicates things so much because it's going to be hard to anticipate and hard to counter.

MS. SPAULDING: And as you can gather from the frequent references to using photographs, you know, we've focused so heavily on Facebook and Twitter and Google and, of course, this is using Instagram often to create and perpetuate and grow these affinity groups. The law enforcement in particular, of course, what we've seen is the Blue Lives Matter, that particularly what goes viral, we know, is messages that appeal to emotion. And so we've seen messages that are targeting – that are targeted to anger, create anger in these law-enforcement affinity groups, for example.

MR. LEWIS: I got to talk to someone affiliated with the 2016 effort. And it was really interesting, because he said, you know, his goal is to get clicks on the website. His goal is to get people to look at the story. We all have that goal. And he said the things – what he found is that the stories that were lead-ins, good lead-ins for getting attention, were violence, sex, health, and retirement. And he would look – you know, and I was, like – so the first thing I said is, well, geez, maybe we should do that here.

You know, there's a very careful study of what is effective. One of the problems we have now is it's a little late for this kind of influence campaign, right. If they were going to do it, they would have started months ago. But the Russians are good at identifying themes that they know are of interest to Americans and are vulnerabilities to Americans. They didn't invent racism. We did that ourselves. But they know how to exploit it.

Q: Hi. Brendan Bordelon from National Journal.

I want to talk a little bit about the tech platforms, sort of their policies in the lead-up to the election. You know, obviously you said if they're going to do anything, James, he said that this is sort of the magic moment.

Do you feel that the platforms – I mean, not just Facebook and Twitter, but sort of all the Instagram and all the other ones – are they doing enough to take down fraudulent accounts, accounts that are suspected of being tied to the Russians or the Chinese or the Iranians? Do there need to be additional policies in that space? And, if so, obviously we've been talking about legislating in that area. Is that something that you guys think is needed, or do you think the platforms sort of have this under control, not just in the lead-up to this election but in 2020 as well?

MR. LEWIS: It might be best to say the platforms are moving in the right direction and they're not there yet. But they are – you know, two years ago they would have said, not our problem. We're just a platform. You know, we don't control things. And they don't say that anymore.

The dilemma with a regulatory policy or with legislation is the linkage to freedom of speech. And so it's very difficult for the U.S. And I think this was intentional, at least on the part of the Russians. It's difficult for us to regulate constraints on speech. And so the problem will fall to the companies, and they probably – they're doing more, but they need to do more yet.

And a friend of mine once said Twitter is going to – pardon me – Facebook is going to end up having to hire 30,000 editors. The companies will have to take responsibility for what's on their networks. They're starting to do that, but they can do more.

MR. CARTER: Some of the companies are also investing in – I think there are the 30,000 human editors going through content, but I think some of the tools that the companies are investing in now are going to be a really important part of this. It can't be a manual solution. And I think the companies relate to the party, as with everyone else. And so we're a little bit behind the curve in trying to come back.

But doing things like – you know, in the example that Heather gave, the Russians were experimenting with different types of network theory. How do you create a group out of a group that does not really identify itself as such? Now the companies are starting to do the opposite. They're saying how do we identify patterns of malicious activity across what appear to be unconnected accounts? How do we identify some of these tactics that we see and then prevent them from being replicated at scale? And I think a lot of that is going to be done with artificial intelligence. A lot of that's going to be done with behavioral modeling. But that's going to be an important piece as well.

MR. LEWIS: And two precedents, just if you're interested – the Child Online Pornography Act, COPA, and the Digital Millennium Copyright Act, DMCA. These are things that remove content that is deemed to be inappropriate. And it's largely automated, as Will said. We know how to do this. We just haven't built the tools for political content. And that's probably the task for the next couple of years.

Q: And just one quick follow-up. How important is it to get most of those tools set up before 2020? And do you think that's feasible?

MR. LEWIS: Well, yes, it's feasible. A lot will depend – one of the reasons I think we need to take a deep breath about the midterm elections is, you know, if nothing happens – and that's one possible outcome – if nothing dramatic happens, then we don't want to say, oh, gosh, well, we fixed that; we can go home now. No, there has to be a lot of – a lot of effort to come up with these across the board. And I don't think it'll just be the U.S. pushing this. When you look at German hate speech laws – German hate speech laws, at the European Union, there will be a desire to see the big global platforms do a better job at policing themselves when it comes to political speech.

MS. SPAULDING: But I do think that in the context of political speech, unlike some other contexts that Jim has mentioned, you're less likely to see removal than transparency. That's a much, you know, safer ground when you're talking about political speech. And then what will be interesting

is to see whether Americans care when they're told that this is – this event, this rally you're being invited to is being sponsored by Russia, for example.

MR. CARTER: I think, to your question about 2020, I think a lot of the companies know they need to have a better toolkit, and one that they can explain to people and show as an effort by 2020. The one thing I would say is, we will be prepared for 2016 tactics in 2020. Whether we are prepared for 2020 tactics in 2020 I think is another question. But as we continue to iterate on this, because the problem is not going away, I think we will get better. And the platforms will get better. And we'll get better at anticipating where our adversaries are going to go. But it'll take time.

Q: Just to clarify a little bit on what we might see between now and Election Day, Jim, I know you said that we're sort of in a magic hour, but I know there's been some influence campaigns. I think Suzanne mentioned the #WalkAway stuff and trying to get people to be – throw up their hands and be fed up with politics. But, you know, will we know what we see between now and Election Day? I mean, how obvious is it? How obvious will it be that something is happening? And how will we identify it or react to it quickly enough over the next three weeks?

MR. LEWIS: Well, that is sort of the million-dollar question because we are much more aware of these tactics than we were in 2016. On the other hand, the other side has become much more skillful at hiding their tracks. So it is kind of a race. Will we be able to detect these things? Will we be able to counter them? Or will they be able to hide? And right now, it looks like we're a little bit ahead of the curve, but I don't think any of us would feel comfortable saying that victory is nigh, right? So it's very much a race.

MS. SPAULDING: And, again, it's not as though we're in this weird pause where we're not seeing any activity. We're seeing Russian influence operations every single day – whether they're fanning the flames of divisiveness around Kavanaugh, around Mollie Tibbetts' murder, around a whole range of issues, that they are out there every day fanning the flames. And whether that ties into a strategy that is – that they think is connected to the elections or not, you know, that's part of what we don't know at this point. But, again, it's not as though they're silent.

Q: And I guess, does it – strategically, do we think that it matters to them if it plays into the elections? I mean, if the Russians' main goal is simply to disrupt our democracy and make us sort of tear ourselves apart, does a specific electoral result actually matter to their efforts? And I guess, if we can, contrast that with what we think might be happening from China. Does their effort strategically differ from what we think the Russian efforts might be aimed at?

MR. LEWIS: Suzanne has to go to The Atlantic Council, so it's not disgust with your question. (Laughter.)

So the Russian goal has always been to disrupt. The Chinese goal has always been to build up China's image and influence. So very different goals. Very different strategies. The Russians did not seek to do much more than create dissention, doubt, uncertainty in the American public. And they've been remarkably successful. So I think we'll see them continue to try that. But China's goals are very different. I don't think – one of the things that we – I think some of us worry about is, we don't want to build defenses against 2016 because our opponents are not dumb. They are not going to do the same thing. They'll try something different. It's getting a little late if they're going to interfere with this. And they may be saving their best tricks for 2020.

But the goals for Russia and China are very different, and that affects their strategies. The Chinese have not undertaken the kind of influence operations that we've seen the Russians do that are covert, that are aimed at creating fake news, that are exploiting dissention. Their goal is to build a very positive image of China, to put out news. The most remarkable success is probably everyone in the room thinks that China's rise is inevitable. It's not, but that's been a success for their influence campaign. So very different goals, very different outcomes and very different tactics so far.

MS. CONLEY: So just what I'm watching for, I mean, I think this is where we just – we're going to have to be monitoring this, anything that happens between 48 and 24 hours before and, for me, looking at voter suppression, voter confusion, something there.

The other thing I'm looking at is, exactly to your point, the day after the midterm election, how is Russia repositioning its messaging amplification based on outcome? We saw that – we saw this after 2016 as well. If they're repositioning immediately, what are the new issues that a divisive, how do I – so that's going to be, I think, very instructive. They're going to wait to see what happens, as we are.

And then I think once we can get some of the data and analysis, really focusing on those swing counties that we know for 2020. Was there any interest in areas that we should be particularly focused on? Because I think as we understand our national races, it does come down to a very – a handful of counties, potentially. And would there be some early experimentation in this cycle that would bear fruit in 2020? So those are just simply – again, I have no idea and, you know, nothing may be impactful, but those are some of the things that I'm watching for.

MR. CARTER: So one thing I would add to that is, unfortunately, if you look at the states and counties that have the most competitive races this year, a lot of them are the ones that have the weakest cybersecurity protections in place. So there was a study recently done that graded all of the states on their cybersecurity preparedness for the election. The average grade nationwide was a C minus, so that's a lovely starting point, but the average grade for the seven states that have toss-up Senate races was an F. And so I think we will be keeping an eye on what the Russians do if they try to take advantage of the vulnerabilities in these particularly competitive areas to access voter registration systems, poke around on vote counting or Election Night reporting. Those will all be things to watch for sure.

Q: Who did that study?

MR. CARTER: Center for American Progress.

MR. QUINN: All right, guys. I want to take these final questions. I'm also just conscious of the people on the phone.

Laura, could you just open up our question line as well?

OPERATOR: OK. Thank you.

(Gives queuing instructions.)

And we do have a question from the line of Joseph Marks with NextGov.

Please go ahead.

Q: Hi. Thanks for doing this.

The Homeland Security Department has talked about running a kind of national online chat room on Election Day, but has not provided many details yet. Has anyone been invited to this? Do you know anything about what's going to happen, who's going to be on, what they're going to be doing, et cetera?

MR. LEWIS: No. That one probably would have been better for Suzanne, who has since left. I don't think any of us have been invited. If we find out more, we can get back to you.

Q: Thanks very much.

OPERATOR: OK, thank you.

And back to you, Mr. Quinn.

MR. QUINN: All right. Thank you, Laura.

All right.

Q: Yeah. So we've talked a lot about the potential 24-, 48-hour window before the election, messing with voter registration, confusion and particularly targeting some of the close races. My question is, particularly in the case of the Russians, who is that designed to benefit? You know, obviously in 2016, there was a lot of talk about the Russians working to elect President Trump. Are we going to see Russian efforts largely – if there are Russian efforts – largely leaning towards electing Republicans? Because obviously, they have the one track where they just want to divide. But if they're going to be going into voter rolls, sowing confusion, it seems to me like they'd be wanting to work for a particular candidate or party and I wonder if you guys have any thoughts on that.

MS. CONLEY: So I still maintain that the exact goal is to discredit democracy and credibility into the institutions, make everyone walk away. And that's certainly been very true of some of the malign influence in Europe as well; just you don't care anymore, you're not – and then you're more susceptible to those who may support Russian interests.

So I honestly do not believe this is about – particularly in the midterm, where it's a not a presidential where there's very defined policy approaches to Russia or to areas of their interest. This is about just sowing discord, division, complete distrust. So I think that's really the hallmark. When you get into a presidential moment, then it's obviously shaping candidates and perspectives that would be in support of the Kremlin's aspirations. And there would be a more purposeful effort, I think, in finding – and this would be true as I look at leaders across Europe, those that have a pro-Kremlin perspective do get their support, Matteo Salvini in Italy and others. You can see that working more clearly.

Q: I was just wondering if the – does – the diversity of voting system in the U.S. makes it easier or harder to attack? Like, how does that play?

MR. CARTER: So this is – this is a point that often gets brought up. And I personally am very skeptical of it because if you say the diversity of U.S. voting systems makes it difficult to attack, that's true in the sense that if you wanted to manipulate every vote, or every vote count or every state, that

would be extremely difficult to do. But the reality is that it's a relatively small number of counties and even precincts that really determine the outcome of elections in this country. So if you are looking at a midterm election, if I can manipulate a few key counties in just the seven states that have Senate tossup races, I could determine, you know, the balance in the Senate. In the House, I think there's 29 races that are currently listed as tossups. Many of those are in counties that have all paperless voting machines which a lot of legitimate concerns have been raised about.

You know, so diversity provides protection from massive, pervasive attacks. But for an adversary who really understands our system and who's able to identify those points, the key – that's not a real protection. And that's why we need to have strong baseline cybersecurity practices that we implement consistently across the country. We can't let some states fall behind, we can't let some localities fall behind because you don't need to hit everyone in order to have an impact.

MR. LEWIS: Well, I'm sure it was very disappointing for them in 2016 because they probably thought, you know, there's some office like the Federal Electoral Commission or somebody that has THE vote or THE control. And to come and find, no, you've got 3,000 counties, it's very hard to strike multiple targets simultaneously. And so then, if you were going to do this, you would look for chokepoints. You would look for the key counties, as Will has mentioned, or you'd look for core technologies, so interfering with state-level voter registration to cause lines and delays in voting.

But that's a line they haven't crossed yet, and it's a bigger line. Influence operations and poking around the electoral system and leaking documents, that's Russian practice that we've seen for more than a decade, starting in Russia. But to actually try and interfere with the vote tallies is a line they haven't crossed.

So I'm a little skeptical that they'll do it, even with our sort of fuzzy message. That might be seen as risky, even by this Kremlin.

MR. QUINN: OK. I think that puts us at the end of the briefing. I just want to thank Heather, Suzanne, Will, and Jim for joining us today and for giving us their thoughts. Thank you all for coming. Thanks for those joining us on the phone, too.

There will be a transcript of this discussion sent out later today, so please take a look at your inboxes for that. If for any reason you didn't get the invite to this briefing, please come up to me, let me know, and we'll trade information. And, yes, if you need any follow-ups over the course of leading up to the midterms, you can contact myself, Colm Quinn, my colleague Emma Colbran, and of course our Chief Communications Office Andrew Schwartz.

Thank you all for coming and thank you guys again. Thanks.

(END)