THE BROOKINGS INSTITUTION

BROOKINGS CAFETERIA: Protecting American elections from foreign interference

Friday, August 2, 2019

PARTICIPANTS:

Host:

FRED DEWS
Managing Editor, Podcasts and Digital Products
The Brookings Institution

Guest:

DARRELL WEST
Vice President and Director
The Brookings Institution

(Music)

DEWS: Welcome to the Brookings Cafeteria, the podcast about ideas and the experts who have them. I'm Fred Dews.

In June, FBI Director Christopher Wray testified to the Senate Judiciary Committee that "the Russians are absolutely intent on trying to interfere with our elections." And just recently the State Intelligence Committee issued a bipartisan report finding that governments at all levels are unprepared to combat a Russian attack on U.S. election infrastructure. Meanwhile, Senate Majority Leader Mitch McConnell has refused to allow a vote on House-passed bill on election security, calling such efforts partisan and pointing to the steps the Trump Administration has already taken to bolster election security.

To discuss these issues, I am joined today in the Brookings podcast network studio by Darrell West, the Vice President and Director of Governance Studies and Founding Director of the Center for Technology Innovation here at Brookings.

His program is heading up a series that examines the threats to our elections from cyberspace, foreign interference, disinformation campaigns, and more. You can follow the Brookings podcast network on Twitter @PolicyPodcasts to get information about links to all of our shows, including Dollar and Sense, the Brookings trade podcast, the Current, and our events podcast. If you like the show, please go to Apple podcasts and leave us a review. It helps others find it.

And now, on with the interview.

Darrell, welcome back to the Brookings Cafeteria.

WEST: Thank you, Fred. It's nice to be with you.

DEWS: It's nice to have you back in the studio.

So we're talking about election security. First, what do you make of Senator McConnell's refusal to bring election security bills to the Senate that were passed by the Democratic controlled House, claiming that democrats are trying to give themselves a political benefit?

WEST: I mean, it is mystifying to me why the senate has not acted on this, because there is a clear threat, especially from Russia, but possibly from other countries as well. We know the Russians engaged in a lot of disinformation in our 2016 presidential campaign, they did the same thing in the 2018 congressional race. This year, they've intervened in a number of European contests. And so there's no doubt that as we head into 2020 that the threat is very real.

And when you look at the measures that were passed by the House, these are not really contentious partisan initiatives. So, for example, they just want to provide additional funding to the states so the states can beef up their election infrastructure. That's not very controversial. They want to provide technical expertise to the states so that they have better access to information on how to counter disinformation and hacking. There is a provision asking states to develop a paper back up of their electronic machines, so if there is any controversy, we can go back and actually see what actually happened. And there's a provision to add sanctions to foreign governments or foreign agents that interfere in our elections.

These bills have a bipartisan sponsor, so it really does not make any sense for the Senate not to act on this and it's important that they take this issue seriously.

DEWS: Well, one claim that Senator McConnell and others have made is that since elections are administered by state and local governments, the federal government

shouldn't have a role and that these bills give too much of a role to the federal government. What do you make of that argument?

WEST: I mean the Senate Majority Leader is correct that under our system states and localities administer American elections. They set up the voting machines in the precincts and actually run the elections, but it's not true that the federal government plays no role. Historically the federal government has provided funding to the states to upgrade their equipment, they provided technical expertise to the states because most states don't have a lot of cybersecurity expertise. It's a relatively new topic and a new kind of threat that has come up. And this is exactly the area where the federal government can be very helpful to the states.

So I don't think the states' right argument really is a good justification for the Senate not to act on this issue.

DEWS: And it strikes me that we're talking in many ways about a national level election when we're talking about the election of the president, senators who are elected to serve in the federal government, and so on.

WEST: Absolutely. I mean, there is a national stake in having elections that have strong integrity, that people respect the outcome, there are no questions about the legitimacy of what happened in that race. And especially now, just given all of our contentiousness, it's really important to get the election process right.

DEWS: I mentioned in my introduction that your program, Governance Studies, is heading up a series called "Cybersecurity and Election Interference." Can you talk about what that series is all about?

WEST: We launched a series because of the major worries about the risk of

election interference in the 2020 race. So we know that there are major problems here, there are many social divisions in the United States based on race, gender, geography, lifestyle, and a lot of other dimensions. And the Russians already have demonstrated a capability to use disinformation to try and exploit those differences and pit whites against African Americans and other sorts of things.

I'm worried, given our national contentiousness, whether if there is interference in this election will people view the outcome as fair, because in any democratic system it's really important that the elections result be seen as fair, that it's accepted by people. I mean the whole legitimacy of the system really depends on that. And given Russia's past behavior and their likely future behavior, this is something we need to worry about.

So we developed this series just to look at the various potential problems, but also to try and suggest some solutions to deal with those issues.

DEWS: One of the authors in the series is Elaine Kamarck, a Senior Fellow in Governance Studies. She has a short piece on the history of campaign dirty tricks, and I'll quote from it. She writes "Every dirty trick that was possible before the internet is possible today. The biggest difference is that they are cheaper, faster, and easier to hide."

Can you comment on that idea?

WEST: Elaine is 100 percent accurate in that comment. It's certainly the case that dirty tricks in elections are nothing new. You can go back decades and centuries and find many example of this, but Elaine is correct in noting that in a digital world it is cheaper, faster, and easier to undertake a lot of these types of efforts. And so what I like about her piece -- and I definitely recommend it to your listeners -- is (1) she puts some of our current problems in historic context, which I think with technology it's important because a lot of

people think digital technology is new and so therefore all the problems associated are new and we've never dealt with this before, and that's not the case. The digital world does create some new stresses and some new risk, and so we need to be cognizant of how dirty tricks may play out differently in a digital world and to take steps to address them.

DEWS: In your piece you talk about what you call the new disinformation risks as we approach 2020. What are some of those new risks?

WEST: Well, there are so many new technologies that can be used for good purposes but also could be put to nefarious purposes as well. So we have to be careful in looking at some of these technologies, like fake videos, the misuse of social media to spread disinformation or outright falsehoods. I think particularly in the 2020 election where we have a lot of female candidates and minority candidates, it's possible to doctor images and/or videos to make it look like someone has done something really bad, or to put them in a compromising position, or to make it look like they should not be taken seriously as a presidential candidate.

So I think the growing diversity of America and the fact that some of these tools can be used for really nefarious purposes, we have to worry about how technology could end up distorting the 2020 election.

DEWS: Well, I want to probe a little bit more deeply into some of the ways in which this disinformation can influence the outcome of an election. So, for example, can votes that I go and cast at my local polling station, can that be changed remotely.

There are ways in which outside actors could change the voting process as well as the voting outcomes. So, for example, you mentioned this Senate Intelligence Committee report that just came out quite recently. They found that the Russians had actually

penetrated the voter databases in all 50 of the U.S. states. And what that means and the reason that is important is like when you show up at the ballot box and you want to cast your vote, the first thing the registrar does is to check to see if your name is on the list. And so if they can go into the databases, they could change your name, they could take your name out of the database, they could change your address, and basically make it difficult for you to actually cast your ballot. So that is certainly very threatening.

In terms of changing actual votes, that's a little more challenging because most states actually keep their voting equipment off the internet for security reasons, like they don't want someone to be able to directly in real time affect the results. But, still, after the votes are tabulated, they are electronically sent to the Board of Elections in each of the 50 states. So there's a potential for mischief there in the sense of taking down networks, hacking into those results. So there are several different ways that people with bad intentions could disrupt our elections.

DEWS: Yeah, I want to follow up on that. And, again, back to the example of I'm casting a ballot at my polling station and somehow my registration data got messed up and then they said that we can't find you, you're not a registered voter. I think I would have the wherewithal, me personally, to do what I needed to do to get an affidavit, whatever procedure I could use, on the spot to validate who I am and to be able to cast at least a provisional ballot. But it seems to me that a lot of voters in American would not be able to do that, they wouldn't know they could do that, they may only have one hour to take off from their job to do that, and that was the only chance they had, and they'll leave. And so instead of changing a vote, it's disrupted, as you said, the voting process. That could be one of the intents of these malicious interventions in our elections, right?

WEST: That is absolutely correct. The goal is really just to mess up the process, slow the process down. So many states, as you point out, do have a way for people to cast a provisional ballot if, for example, their name isn't in the voter database but they argue, you know, it actually is and they're voting at the right address.

But think about if that started to happen in large numbers, how it would slow down the process, how it would lengthen the lines. A number of states already have cut back the number of polling places within their states. So in past elections we've seen people having to wait one, two, three hours or more in order to vote. If there are these types of disruptions, those delays could turn into two, four, or six hour delays. And of course a lot of people are not going to want to stand in line that long, they're not going to vote.

So even just by disrupting the process and/or slowing down the act of voting, that could cause enormous problems for our election.

DEWS: One of the other issues that comes up in this series of papers is political polarization. Can you talk about how does political polarization influence the effectiveness of digital disinformation? That is without such severe polarization between political parties, between ideologies in America, would this disinformation be as effective?

WEST: The problem in the digital world and in a polarized digital world is that disinformation becomes more believable when people are sharply divided from one another. Like one of the hallmarks of our era -- and I wrote a book about this entitled "Divided Politics" -- is people are divided on all sorts of different dimensions, by party, by ideology, by geography, by educational levels, by income, and by a lifestyle and in today's world people increasingly define opponents as enemies. We question each other's motives. Like if you support President Trump and I do not support and I do not support

him, it's easy for me to think poorly of you and to cast dispersions on your character, your intelligence, and everything else.

So in a polarized world, when social media starts to spread fake information about one of the opponents, it may be more likely and easier for me to believe that false information because it might confirm what I already think about that individual. And so the combination of the polarization and the ease of information dissemination in a digital world, that makes for a very toxic combination.

So it's not that this is the first time we've been at risk of disinformation, but in a polarized world disinformation becomes even more problematic.

DEWS: An upcoming guest on this show who is going to talk about a similar issue, deep fake videos, has also drawn out this issue of political polarization in reference to deep fake videos, and you reference it too in your piece for the cybersecurity election interference series. Can you extend a little bit more into this issue of deep fake videos, what they're all about, and some of the things that you're most worried about?

WEST: I mean deep fake videos are highly problematic right now because you can do this either with images and pictures or videos themselves. You can actually doctor the image to put somebody next to somebody who is toxic or deeply unpopular and then engage in guilt by association by saying, you know, this candidate hangs out with this really bad person, so therefore we should think negatively about them. You could put somebody in a compromising position, again through a photo or through a video, you can doctor images in ways that would cast doubts on the character of particular individuals.

You know, we saw a recent example with Speaker Pelosi where someone basically slowed down the video to make her look old, bumbling, and out of touch. And so, you

know, this is the type of thing that when images and videos are doctored in that way and then spread very quickly over social media, people may reach negative conclusions about somebody just based on that video, even if the video is completely false.

DEWS: So we're talking about ways to bolster the integrity of America's electoral system, to protect people's right to vote, to protect the voting process itself. And we hear time and again President Trump and others claiming "serious voter fraud" that took place he claims in California with as he claims 1 million illegal votes cast. Other republican officials, like Mitch McConnell, discount the threat from foreign entities to our electoral system despite what the Senate committee has said, despite what our intelligence community has said. They point to fraud in voter registration in voting.

How do you respond to that focus?

WEST: I mean in general, cybersecurity should not be a partisan issue. This is not an issue where republicans and democrats should be fighting, because both have the same stake in wanting an election process that is fair, open, and transparent, and that people widely accept the legitimacy, both of the process and the outcome. And if we reach a point where republicans and democrats are reaching different conclusions on that, that is very risky from the standpoint of democracy in general.

So I think the question of voter fraud and fraud in voter registration, there have been academic organizations that have looked at this, there are nonprofit organizations that have studied it in detail, they have never documented examples of widespread fraud or fraud that actually influenced the way an election turned out. You know, there have been cases of individual fraud, kind of on a one to one basis, small groups of people, and so on, but in an electorate, a national electorate, of well over 100 million voters, like there's

no evidence, as Trump claimed, that a million people voted illegally in California. So there's just no empirical evidence that supports that claim.

DEWS: let's move on to solutions as we wrap up the conversation. You with Raj Gambhir have a piece in the series that talks about specific solutions. You mentioned some of the specific policy measures that the House and some Senate bills also have, and you might mention Margaret Taylor has some analysis from what some European countries have done in response to Russian interference in their electoral process.

Can you walk us through some of the solutions and some of the lessons we might learn from abroad?

WEST: I mean there are things that governments can do, that people can do to protect themselves and that the news media should do to make sure we have a fair and open election. So on the government front -- and again these are reforms that come from bipartisan legislation, it's already passed the House, there's not been a vote schedule in the Senate on these things, but it's basically about providing more money for states and localities so they can upgrade their equipment, so we can make sure that we protect our election infrastructure, so that we have the proper cybersecurity protections, so the Russians, the Chinese, the North Koreans, the Iranians, the Saudis, or other people cannot hack into our system and disrupt the election.

So those are all things where the government can provide funding, they can provide technical expertise, they can help states and localities deal with the cybersecurity risks that are very serious. But it's not just a problem of government. Like in the digital world, there's a lot of disinformation that's being spread through social media, and so we need digital literacy campaigns so that people themselves learn what they can do to spot

disinformation, how they can help others avoid disinformation. I mean it's a challenge in the digital world. You know, you're surfing the internet, you're looking at a variety of sites, it's hard to know which piece of information comes from which side and how useful or valuable that side is. You know, are they promoting good, fact based information or are they promulgating falsehoods.

And so people need to become more sophisticated just in terms of how they access digital information, how they evaluate it, how to spot fake sites from real sites. So this is something that schools need to do a better job, nonprofit organizations need to help, efficacy organizations, like we all play a role in kind of helping our fellow Americans figure out how to do a better job.

And then the last piece is really the role of the news media, because what has happened in past elections is there has been disinformation circulated, it goes viral on social media, and then traditional news organizations have picked up on it and really amplified that message. And so journalists have to be very careful in what they report on because if they're reporting on fake news, false information, disinformation, or just doctored images or videos, they're giving credence to all of that information even though the information is factually inaccurate.

So journalists I think play a very important role in helping us figure out what is more useful information, what is less useful, what seems to be coming from a legitimate site versus information that comes from a fringe site or a marginal site or a site that's playing in outright falsehoods. So we all are going to have to work to address this problem. So government plays a role, the average person plays a role, and journalists play a very important role here as well.

DEWS: So what can we learn from some of the examples of successful campaigns to combat foreign election interference? Say, in the case of Sweden or in France?

WEST: What other countries are doing is just being very vigilant and making sure that when fake sites come up that they quickly address them, they go to the social media platforms, provide evidence that this is a fake site, and get the platform to take down those accounts. It could be a news platform, it could be a social media account, or various other things. So they have been much more aggressive than we have been in that regard.

There are nonprofit groups in many countries that are now monitoring social media sites to see which ones seem legitimate, which ones are not legitimate. They're helping to keep false information from going viral, which can happen very quickly in a digital world.

So there are a lot of constructive lessons that we can learn from the experiences of other countries. And the piece by Margaret Taylor did a great job of looking at some of the European countries and how they have been trying to combat fake online information.

DEWS: I want to finish with a quote, again from the piece that you co-authored with Raj Gambhir, and it has to do with the cost of election security. And that's another argument that some opponents of a federal role in election security have made is that, oh, it costs too much. So I'm going to quote, "Having secure elections is essential to democracy. Democracy is too important to be risked for a relatively small amount of money." How much money are we talking here?

WEST: The House bill that already has been passed but not voted on by the Senate asked for the federal government to provide the 50 states with $600 million to upgrade their equipment and safeguard the election infrastructure.

Now, in a country as rich as the United States, that's not a lot of money when the

whole integrity of the election process is on the line and the substance of our democracy is on the line. Like those things are so important that spending that amount of money is an expensive investment in our future. Because if we don't get it right in 2020, it's like we're going to risk a very dismal future.

And so spending the money now to protect against cybersecurity risks is something we absolutely have to do.

DEWS: Well, Darrell, I want to thank you for taking the time today to walk through some of these issues.

WEST: Thank you very much, Fred.

DEWS: Darrell West is the Vice President and Director of Governance Studies at the Brookings Institution. You can learn more about this topic on our website by searching for the Cybersecurity and Election Interference series.

The Brookings Cafeteria Podcast is the product of an amazing team of colleagues, starting with audio engineer and producer Gaston Reboredo and producer Chris McKenna. Bill Finan, Director of the Brookings Institution Press, does the book interviews, and Lisette Baylor and Eric Abalahin provide design and web support. Our intern this summer is Betsy Broaddus. Finally, my thanks to Camilo Ramirez and Emily Horne for their guidance and support.

The Brookings Cafeteria is brought to you by the Brookings Podcast Network, which also produces Dollar and Sense, the Current, and our events podcasts.

Email your questions and comments to me at BCP@Brookings.edu. If you have a question for a scholar, include an audio file and I will 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.

Until next time, I'm Fred Dews.