BROOKINGS INSTITUTION WEBINAR

ELECTION INTEGRITY AND SECURITY IN THE ERA OF COVID-19

Washington, D.C.
Friday, July 17, 2020

Opening Remarks:

FIONA HILL, Moderator
Senior Fellow, Center on the United States and Europe
The Brookings Institution

Keynote Remarks:

CHRISTOPHER C. KREBS
Director, Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

Panel 1: Safeguarding Election Security:

FIONA HILL, Moderator
Senior Fellow, Center on the United States and Europe
The Brookings Institution

DAVID BECKER
Executive Director and Founder
Center for Election Innovation and Research

MARK HARVEY
Senior Vice President, Enterprise Resilience
Federal Reserve Bank of New York

SUSAN HENNESSEY
Senior Fellow, Governance Studies, The Brookings Institution
Executive Editor, Lawfare

Panel 2: Adapting to New Disinformation Tactics:

CHRIS MESEROLE, Moderator
Fellow and Deputy Director, Artificial Intelligence and Emerging Technology Initiative
The Brookings Institution

DAVID AGRANOVICH
Global Threat Disruption Lead, Facebook
Former Director for Intelligence, National Security Council

ALINA POLYAKOVA
President and Chief Executive Officer
Center for European Policy Analysis

LAURA ROSENBERGER
Senior Fellow and Director, Alliance for Securing Democracy
The German Marshall Fund of the United States

* * * * *

P R O C E E D I N G S

MS. HILL: Hello everybody, welcome to the Brookings event on election integrity and security in the era of COVID-19. I'm Fiona Hill, a senior fellow at the Brookings Institution. And I'm delighted today to have several colleagues join me for an in depth discussion of this topic. We're going to do a two-part event today, starting with the panel that you see before you, which are going to focus on safeguarding election security to the integrity of the electoral systems and process.

And then we have a second panel that will begin at 3:15 p.m. on the problems of tackling disinformation, and the implications for the election campaign that we're in the midst of for the election in 2020.

We're delighted to be able to start off today with keynote remarks from someone who's on the front line of this, a great colleague of mine, Chris Krebs, who is the director for cybersecurity and infrastructure security at the Department of Homeland Security. He has a whole agency that he directs that is completely devoted to the subject of today's panel.

And we're really grateful, as Chris is coming right from the frontlines of dealing with these issues that he's got some time to spend with us today. Chris is going to give us an overview of what the government is trying to do to tackle this issue head on.

And then we're going to go into a discussion with Mark Harvey, another colleague who, most recently was also in the National Security Council along with me as the senior director for Resilience. So, the person who was in charge of coordinating all of the initiatives that Chris and other colleagues were engaged in that are directly related to election security and integrity.

Mark, after leaving the National Security Council, spent the last several months as a resident fellow at the Harvard Institute of Politics, where he was also trying to work to create a sort of public outreach on these issues so that people would understand what's involved and the various issues of election interference and action firms that we've all been concerned about since the 2016 elections and the 2018 midterms.

Mark, will also be joined by David Becker. David Becker is the executive director and founder of the Center for Election Innovation and Research. So, a non-governmental organization that is especially devoted to this precise issue we're dealing with today. And David spent many years at the

Pew Research Foundation, looking at polling and public opinion and attitudes towards voting in elections.

And then last but not least, Brookings colleague, Susan Hennessy from Lawfare, who was deeply steeped in all of the legal aspects of dealing with elections and voting and who many of you in the audience will know from her work at Lawfare on various issues related to governance and legal affairs.

So, without any further ado, I'll turn over to Chris. And thank you again, Chris, for joining us today. And then we'll go straight into the panel discussion. And I've also received many questions from audience members in advance. And we will go straight into answering some of these questions. And I want to thank everyone, for being so diligent in sending in questions ahead of time. Chris, over to you. And thank you so much, everyone for joining us today.

MR. KREBS: Fiona, thank you. It's great to see you again. Thanks to Brookings for having me on. Election security is an issue that I've spent an incredible amount of time on for the last three and a half years my tenure here at the Department of Homeland Security, and particularly as the leader of the cyber and infrastructure security agency,

Youngest agency in the federal government about coming on two years old, established by law in November 2018. We are the nation's risk advisor, just the simplest way to put our role. The things we do are in support of state and local governments, the private sector and other federal partners. We don't have a compulsory mission, we are engaged in public private partnerships on a daily basis.

Elections have been one of our top priorities since 2016. At one of the issues that, or the way I -- the ways I described what happened in 2016, and why it's so top of mind as I describe it, or liken it to 1957. A Sputnik moment almost for us. In ’57 when the Soviets put Sputnik into low Earth orbit, it was a pretty chilling moment, I think for the United States based on the reading I've done at least.

And it wasn't as much that it was the fact that the Soviets beat us to space, beat us to putting a satellite in space, but they clearly demonstrated a capability that could overcome the defenses that we've built, or in the natural or the geographic defenses that we have in the Atlantic, in the Pacific and polar ice caps to defend us against an assault by a foreign adversary.

That missile, that ICBM effectively that put Sputnik into space, demonstrated an ability to reach out and touch us. 2016 I think was a similar sort of wake up call for the United States and in the

American people.

Previously, cybersecurity had been an issue that you heard about in terms of tax on banks, of theft of intellectual property, of hacking Sony because you didn't like a video. This was truly an affront to the American people because it demonstrated the potentiality to undermine democracy at large. That's why we take it as seriously as we do here at CISA and with our partners in the federal government.

So, what I want to talk about today are where we've been over the last several years, where I think we need to go in the next couple months, and close out with a few thoughts on what you as the, as an American voter in particular can do.

So, first and foremost, when I think about the work we've done over the last three and a half years, we've developed what didn't exist before. And really more than anything, that is a vibrant election security community of practice. There have always been experts in election security. David Becker on the panel here is going to be one of those folks that'll talk to you about elections.

But previously, they had been excelling effectively in pockets. But what we've been able to create, through some of our partnership mechanisms here at CISA, is a true community of practice, government coordinating council, sector coordinating councils, bringing all levels of government, state and local partners and the private sector together to work on these thorny issues. To understand threats, to isolate and identify trends to develop best practices and investment guidance.

That has led to another key achievement. And that's the establishment of an ISEC, an Information Sharing and Analysis Center. These are the sorts of information sharing mechanisms that every other sector has had, or has, like the financial services ISEC, the multistate ISEC.

But prior to 2017, no such ISEC existed for the election infrastructure community. So, we established that ISEC with the help of our partners at the multistate ISCE in upstate New York. We have all 50 states and thousands of local jurisdictions that participate in this partnership where we can share information, again trend information out there, emerging threats and risks and share quickly and effectively with our partners.

The second piece is we've absolutely improved the cybersecurity and resilience posture of American elections. I've said it before. And I'll say it again, the 2020 election will be the most secure election in modern history. Why is that? Well, in part it's because as through this vibrant election security

community of practice, we've been able to truly raise the awareness of cybersecurity threats with our partners. They get it, they they've gotten it for a while, but they get it and they're taking action.

Just a great example is the patch rates, the patch cycles, the time to patch for critical vulnerabilities has been cut in half over the last year and a half across the state and local election community. That is a critical step towards improving the hygiene of the networks that we're going to rely on here.

The other aspect is we have more sensors, in fact, we have sensors on, intrusion detection sensors, on every single state election network, all 50 states. And in fact, in the state of Florida, all 67 counties have these intrusion detection systems. They're called Albert Sensors. So, compared to every other critical infrastructure sector, or subsector, we have bet -- the best comprehensive visibility across the election infrastructure sector than any other sector. So, if there's a tremor out there in the forest we'll feel it, and we can act on it. So, feeling that that is an absolute metric of success.

Another metric of success or progress over the last several years is in the 2016 election. About 80 to 82% of votes were cast with an associated paper record. Why is it paper record important? Because it leads to auditability. Auditability is a key element of being able to determine the integrity of a vote, to roll it back, make sure you got the right results, and more than anything proving through an audit, a post-election audit process that the votes are cast, are counted as cast.

Where are we for 19 -- 2020? Well, we were on track for about 92% of states. They've retired a number of the systems that don't have paper ballots associated with it. But in part because of what we're seeing with COVID I think and an expansion of absentee ballots, we'll probably see an increase. We may be over 92% because of an increase in absentee ballots. And again, that ability to audit, to conduct post-election audits, is critical to again establishing the integrity of the election.

The last thing I'll mention on what we've done over the last several years, is we've truly developed a unified United States government effort in support of our partners in the state and local vovernment. Now, this isn't just a system mission. We absolutely have coordinated support from the intelligence community, I work day in day out with the National Security Agency and the team that General Nakasone and Neuberger built up, but others in the intelligence community are supporting as well.

They're on the lookout every day for threats against our election infrastructure. We're also seeing very active participation engagement from the FBI. I think you probably heard Director Ray two weeks ago, mentioned that they kick off a counterintelligence, a Chinese-related counterintelligence investigation every 10 hours. Many of those are about integrity and political interference.

The third piece is the Department of Defense, absolute great partners with Cyber Command. again the other side of General Nakasone's shop. Working with them in some of their defend-forward engagements. Where they go out there and they work in the sphere of influence of Russia, Ukraine, Northern Macedonia, Montenegro, and they get on networks and they see activity of foreign actors.

And what we're able to do with that information is not just take the cybersecurity aspects, the indicators of compromise, but we can look and see what the playbook is, what are the targets of concern in Ukraine and elsewhere that we can bring back. So, if they're targeting voter registration databases, if we're targeting -- if they're targeting election ag-reporting, those are the sorts of tips that we can provide our state and local partners here where they can funnel or vector their investment.

So, again, the top three things I think we've really done over the last several years. develop that community of practice, we've increased the cybersecurity hygiene posture, and we have a unified USG effort behind this mission.

So, where do we need to go with the next several months? We're about 100 and some odd days out from November 3rd. Early voting starts in under 70 days. So, we're absolutely in the pipeline towards a very significant election. So, what are the three things we need to do?

Well, first and foremost, change is in the air. Change is absolutely in the air. And I mean that literally, COVID. COVID is changing pretty much how every election across this great country will take place in November. So, it's critical that voters understand and the election officials can share the information on what's happening in these elections and how the changes is going to happen. And I'll come back to that in just a minute.

Also, I have to say that compared to where things were in 2016, we're not seeing that level of coordinated, determined cyber activity from adversaries. We absolutely have better visibility across the networks. And we're just not seeing that same level of activity that we saw in 2016. I'm

paranoid by nature. So, I start red teaming and threat modeling and say, hey what do we think the bad guys can do?

Last summer, we kicked off an initiative with our state and local partners that was primarily informed by the increase of ransomware attacking state and local networks. So, what we said is, hey wouldn't it be a pretty bad day if a voter registration database, which is highly networked, highly centralized, was attacked by an incentivized actor, like a ransomware actor in advance in the months ahead of the 2020 election?

So, we worked, kicked off this initiative with our state and local partners to again increase the posture, improve the cyber hygiene of these databases and make sure that they are not the less -- the next on that list of ransomware targets.

But we do anticipate that in this, if they were going to do something in the next couple months, and I'm not just talking about up to and through and to November 3rd, but in that period after the election. Absolutely ripe for a destructive or disruptive attack by capable adversary. So, we have to be ready. And that's why we put so much emphasis again on paper backups and auditability out in the system.

But the last thing talking about is educating voters. Let me take it back to COVID. Like I mentioned, COVID has changed the way that everyone pretty much across this country is going to vote. Whether it's a consolidation of voting centers, a number of the volunteers that typically support elections, deciding to stay home because they may be in an at-risk cohort or population. There's absolutely going to be changes. Folks are expanding early voting, expanding absentee voting, they are going to be changes. So, it's critical that our state and local partners get the information out there in the hands. But also private sector, social media platforms take a, play a role in educating and informing voters.

So, from day one, or at least, you know, mid-February, we've been working closely through our Government Coordinating Council, with our state local partners, and with the CDC and the HHS to get good guidance out there to election officials on how they can disinfect and sanitize and implement good social distancing and other rules like a go mask on Election Day in in person voting. But understanding that they're going to use other types of voting too, including absentee. So, what are the good security protocols they can put in place.

It's critical to understand that any kind of voting has risks. The issue is identifying the appropriate security controls and processes you can play -- put in place to manage that risk. But again, to the extent that we can expand rapidly, any sort of paper ballot backup, that is going to lead to post-election audit success.

So, I think I'll wrap it up here. But I want to leave you with a few parting thoughts. First, our top priority in our election security effort is to ensure that American voters decide American elections. There's no greater priority for us.

And to do that and to ensure that we've taken unprecedented steps across the U.S. government, all levels of the U.S. government, whether it's DHS, CISA, whether it's the intelligence community, the Department of Defense, law enforcement, in support of our state and local partners, to make sure that we achieve that top line goal of American voters deciding American elections.

We've also taken incredible steps out there in the state and local community to include that cybersecurity posture, to make it that much harder for the bad guys to achieve their successes. And don't, you know, we're not fooling ourselves, there are bad guys that want to do bad things. Russia wants to destabilize. China wants a more compliant state. And Iran probably wants a little bit of both. So, we're going to be prepared. We've got the defenses up, and we're ready for it.

But I tell you what, the American voter has a role to play here. What we're looking for is a prepared voter. Please make sure you have a plan. Educate, understand how things may have changed in your state and in your jurisdiction. If you have a normal polling place, you're ready for ready to go to, make sure that it's still that location or you may go to another place.

We also want participating voters. We're going to need hundreds of thousands of election volunteers, election official volunteers to help support the election in November. So, please, if you're interested, if you got the ability to do so, we -- I encourage you, volunteer to be an election official. And I'm sure David Becker's got a couple thoughts on that as well.

And the last thing is we need patient voters. This is a time of change. Processes are going to change. It may not be the case that we have all the information to determine the voter on November 3rd. So, we're going to need patient voters to understand that because of the changes, it may take a little bit more time. So, again, we want a prepared, participating and patient voter. Those are the

keys to success for 2020 in a secure and safe election.

So, with that, back over to you, Fiona, thanks again for the opportunity to speak to the group today.

MS. HILL: This is fantastic, Chris, thank you so much. And I think the three P's that are very important to bear in mind. And we've all been talking in preparation for this event that the election this year is more of a process than an event in terms of, you know, expecting quick returns on the voting results. And I think that all of our panelists will speak to that.

Because you raised a couple of questions, Chris, I'm going to actually just ask if you could elaborate a little all because we've had so many questions coming in on a couple of the issues that you just talked about. We've had a lot of people coming in wanting to volunteer actually and asking, what can they do as citizens? And I think you've partly answered that. And hopefully David, who is, you know, the head of an NGO, can actually give some people some concrete ideas on this.

We've had people worrying exactly about the consolidation of polling places. So, a retired, unless Madeleine Haberman, for example, asked us about what are we going to do if polling places are reduced to two instead of 20? Now, this is obviously clearly somebody who's thinking exactly in your terms about planning and preparing.

Others, a spokesperson for the Democrats Abroad in Belgium, obviously kind of thinking, you know, about the vote that gets cast in other places. Gerald Loftus, saying that, you know, if most election monitors tend to be senior citizens, is there an effort underway to actively recruit and train younger volunteers?

Getting exactly to your point about participation, and this is often a big difficulty of retirees often have more time on their hands. I mean, I suppose we could argue there's an awful lot of people with unfortunately more time on their hands now than they had anticipated because of COVID-19. Lots of students and others who may not be able to return in person to the universities. Maybe there's other things that, you know, we can think of in ways that people get involved. And I'm sure that David, in particular, has thought about this.

And then we've had a couple of people actually worrying in the questions about the mail in voting and the paper ballots. And is this something that we haven't thought about in whereas the

adversaries could interfere with this, interfere with the mailing process in some way. I suppose, hijacking of mail trucks could be one obvious thing, but, you know, that might be less likely. But, you know, what could be new targets here that we might not have thought about for security breaches.

You know, clear there's a lot of concern here about, you know, the risks of volatile schemes, questions asking here about whether there might be some risk of again of the mail being compromised in some way. And that there's, you know, security breaches that we might not have thought about. And also about the general mail in voting, you know, will there be, you know, enough capacity to handle that?

So, I'll just throw that to you. And then I'll get back to the rest of the panel because, you know, a lot of people are worried about mail in ballots being printed by foreign adversaries and sent in, you know, for example. And I mean you've touched on this, Chris, but what would you say to people?

MR. KREBS: I'm watching David Becker squirming in the off back -- in the green room studio.

MS. HILL: Well, I will definitely be bringing in David, Mark and Susan.

MR. KREBS: Yeah, so --

MS. HILL: I just wanted to put this to you, because you touched upon them in your overview and --

MR. KREBS: Yeah.

MS. HILL: And give you a chance to say what the government is doing and then we can see what everybody else is doing on this.

MR. KREBS: Yeah. So, you know, first things first, election officials are natural risk managers. I've never seen a group that’s adaptable. I mean, think about what they have to deal with over time. You look at Hurricane Michael a couple years ago down in Florida, wiped out a county, pretty much in the Panhandle of Florida, a month or two before an election. They were able to stand up alternative polling locations.

They're just natural for us risk managers. And I think they’ve, over the last several months with the primaries, have done a pretty good job of anticipating some issues. You know, to the consolidation of vote centers or polling locations, you see what transpired in Kentucky where they used a

big arena.

And that that's another issue I didn't touch on but, you know, we should expect that not all of the, you know, the classic historical polling locations to be used. You know, there may be schools that are out of service, fire departments that we need, you know, emergency technician, or EMTs to be, you know, make sure that they're safe and secure.

One of the great ways to do this, or to identify new space, is sports arenas. You've seen, I think down in Atlanta, with the, whatever they call it now, where the Hawks play. You know, these are big open spaces, you can have socially distance places. And I think what happened in Kentucky where they used a venue like that, and they actually had pretty good success. I think there were some challenges there at the end of the voting day that the courts intervened and allowed the, allowed voters to continue through.

But it also shows a couple complexities on the mail in side of, I think the math was there was 2200 potential ballot configurations at that location. When you came in you -- they would have to gin up or spit it out a ballot. And that, I think, that shows that the complexity of a foreign adversary in particular, you know, first off getting special cardstock or paper from a very small number of vendors that know their customers very well. And if it shows up as, you know, the order coming from St. Petersburg and paying in rubles that might not, you know, clear the smell test.

So, and then understanding the different configurations, the ballots, printing them out the right way, getting the right signatures, which get checked on the back end. And that's one of those methods of validating or ensuring that voters --

So, again, I talked about it earlier, every kind of voting has some risk associated with it. It's critical to identify those security controls and implement them in a way to mitigate that risk. And that's in part why, you know, when I look at New Jersey and they're moving away from their direct recording equipment, technology, those that you touch the screen and it goes to the removable media, no paper ballot associated with it. You know, if they expand other kinds of voting that have paper records associated with it, you know, that's potential for a net positive risk reduction measure. Again, getting to that auditability piece.

MS. HILL: That's great, Chris. I know everyone else is eager to get into this. I'm going

to just turn quickly to Mark, and then, you know, to David and Susan. Because Mark, you've worked all different dimensions of this. Not only did you work at this at the federal level and in the executive branch, but you've also worked at the state and local government level in your career. And you're now off to something else that we can't disclose yet. Although we can see that you're in a very unusual location. You know, to start tackling on some of the front ends of some things Chris has been talking about.

So, Mark, probably you could just give us a quick observation. Then I'm going to ask David to come in on some of these very specific, you know, questions about what organizations like David are trying to do with the public at large and with voter monitors on voters. So, Mark, if you could just add a few more things.

You know, you've been actually trying to teach how you do this to students at the Institute of Politics at Harvard as well, you know, who might be indeed be, you know, future Mark Harvey's and Chris Krebs, as well as future voters. So, Mark, perhaps you could add some of your perspectives to this.

MR. HARVEY: Absolutely. And thank you so much for having me. Thanks to Brookings for having us today. It's a tremendous panel. And Chris said some incredible words. And frankly, from having been there at some of the start of it and seeing some of those early meetings between the federal government, state and local governments, one of the biggest things that Chris has done has been to develop a trusted relationship with them.

And this will not happen without it. It was very hesitant at the start. And they've worked very hard over the last three years to gain a lot of trust around the states and localities. So, please do not discount that, because it is the currency upon which this entire system of systems works.

And the system of systems is the most important part to consider here. When I got asked, when I got to Harvard, hey can I make sure, or what can I do to make sure that my vote is counted and that the vote is, you know, has integrity? My answer was, don't just think about the vote, think about what has to happen in order to hold and certify an election. Because that's includes registering voters, getting candidates eligible for the ballot, generating those ballots, getting them to polling locations, recording the votes, tabulating those votes, reporting them back to a more central source at the state level, certifying those votes, and then communicating that certification to the appropriate place where those office holders will enter into their new public service position.

That's a lot. That is a number of different systems together. The second part is that it becomes, again, a system of systems when you realize all of the resources that are necessary to do all of that. We've had a lot of focus on cybersecurity after 2016. But let's recognize all of the resources necessary along the way there. You've got people, you've got data, you've got your physical infrastructure, your facilities, your transportation, your physical plant necessary to make those happen. And then you've got your information technology and communications.

So, that layer of resources all has to be working together. Because we can have wonderful cybersecurity controls and the best sensors in place, but as we saw with Twitter a couple days ago, once you have an insider that is willing to corrupt the entire process, now you've lost trust, and you've lost faith in that.

So, we've got to think about all of those resources together, how they get utilized in executing an election. And then the best word that Chris just used was controls. What are the controls that we have in place on top of those processes to make sure at every step along the way, that we add an ability here to provide for a level of integrity, to think through confidentiality, availability, integrity, just like we do with any other cyber system that's out there.

And those are things that are going to have to happen before the vote in terms of the legal controls that are in place on who gets to register or how they get to register, how somebody qualifies for an election, how ballots are generated, how an election is administered. And then afterwards, on the certification process, and really the audit process.

And let's also recognize that we created a lot of these problems for ourselves. Because after 2000 we started to incorporate more technology into this. We made these more complex processes. And then as that evolved, all of a sudden that revealed new vulnerabilities.

So, when you think about pulling those four categories of resources together, people, the data, the physical infrastructure and the information technology, the gaps between those and how they are used, configuring them, create vulnerabilities in the system, flaws that can be exploited to cause harm within there.

We have to think through with COVID, the fact that we are rapidly changing every single one of those four categories. We're going to use a different set of people to administer our elections, with

a new group of volunteers. In many cases, we are using new sets of data or trying to capture new sets of data. That happened in Iowa during the first primary where they said we don't just want one final result we want three results that all get compared and creates auditability. Well, now that's tripling the amount of data that you're collecting and processing.

We're using new or different physical infrastructure. The minute that we take out of the existing polling place and go into an arena, a sports facility, a civic center, anything that's different from what we've -- been done before, we're now introducing vulnerability into the system.

And we are also using new information technology. Many, many states have bought new sets of voting equipment with the funds that were made available after 2016. They're just being configured and used for the first time in the primaries in 2020. And this will be the first general election where those things are used and used at volume. And yet we're also asking people to change how we utilize how they vote. Go much more absentee, mail in than walking in. So, changes in the utilization rate of all of those, again, introduced vulnerability.

All of that said, gets to that key point of requiring patience. And I think probably the best thing that could be done for November is tell everybody take a week off. Tell the entire media, don't report a single result, don't report ballots cast. Take the week from November 3rd to November 10th and air 1776 and Mr. Smith Goes to Washington and Hamilton and have a great week of civic pride. And say at the end of this we will announce who's won.

Because that will give us time to count ballots from every capability, every way that they've been cast. It will give us time to do risk limiting audits. And it will identify if and where there are potential concerns that will need to be adjudicated appropriately. And not put the undue pressure of quick reactions, social media, who's ahead, who's behind for a process that is not unfolding, but is actually being counted. So, there's a lot wrapped up in making this system of systems work appropriately and actually work appropriately when there's a lot of motion within each bit of it right now.

MS. HILL: Thanks very much, Mark. An actionable item, a week off for everybody. Anyway, David, your organization is also new in the terms of it was something that you saw a necessity for after 2016 and in terms of setting up really active outreach for voters and electoral systems. And I know that you have lots of issues to go over here and ideas to raise. So, I mean, I think they're all very

eager to hear from you about, you know, what you see is most important in this space based on what Chris and Mark have said.

MR. BECKER: Yeah thanks, Fiona. And thanks for having me on the panel. I completely agree with everything Director Krebs has said. He's -- I think one thing that has been very clear over these last several years, is even in these highly partisan divisive times, if you talk to election officials across the political spectrum, across the country, they'll say, they'll tell you how well CISA has been working with them to secure their systems. And that's a tremendous victory. And it's one of the reasons we're as secure as we will be in 2020.

I mean, I've been doing elections for a long time, over 20 years, since my time in the Justice Department and voting section, with both the Clinton and Bush Administrations and then working with Pew. And then since 2016, founding my new organization Center for Election Innovation and Research.

And it's very clear that since 2016, there are two potential targets here that we need to be concerned about. One is the actual election infrastructure. And as Mark accurately pointed out, we've been relying upon technology more and more. In some ways, that's very good technology can do some things very, very well. It can count votes much more accurately, much more quickly. You can provide for access for people who have challenges, etc.

But that technology does become a target and it has been a target. We know for instance, the voter registration databases in a couple of states were targeted and other, many other attempts were made to infiltrate systems unsuccessfully in 2016 and after that. But perhaps the bigger targets for our adversaries has been the minds of the American voter. And to diminish confidence that we all have that our system of democracy is working, and that the election results actually reflect the voice of the people.

And we have to be very considerate of both those targets. Election officials have a very, very difficult job because they have to secure our systems. And they've done a much better job of that. I mean, we've, as Director Krebs has mentioned, we've now got paper auditable ballots in many more places. Georgia now has auditable paper ballots, South Carolina has auditable paper ballots, Philadelphia, large counties in North Carolina, these places did not have auditable paper ballots in 2016.

And they do now.

And we will have risk limiting, statistically robust audits of those ballots statewide in states like Georgia, like Michigan, like Virginia, we didn't have that in 2016. That is a remarkable improvement.

So, we've done a better job of securing the actual infrastructure since 2016. That's absolutely true. It doesn't mean we've crossed the finish line we're going to need to continue to improve. But we're, we are more secure in 2020 than we've ever been.

I think one of the challenges we face is that voters are not necessarily absorbing that message. They're not really absorbing the facts of our security and integrity of the system. Election officials, again, Director Krebs is exactly right. No election is without risk. And so election officials, what they do is they try to balance risk and integrity with access, because it's very important that all eligible voters who can vote have access to a system so they can express their voice.

And, you know, we can build a house with no doors and no windows, but it wouldn't have much use. So, we are trying very hard to build a system that every eligible voter and only eligible voters can participate in and that we can be sure that counts are right. And I think in large part, we've done a good job of that.

I think there are three things we're going to really need to look for going into this November. One, we're absolutely going to need to look for expanded mail voting, we're seeing that in every single state. I anticipate there -- every state we'll see a record for mail ballots cast. That is a good thing for those voters whom mail voting serves best. Mail voting is a very effective option, but for many voters who might need some assistance, it might not be the best one for them.

And one thing we have to remember in a presidential election, it is the election which the largest number of infrequent voters show up to vote. These are many people who have never voted before, or vote once every four years. Primaries, we see much more of the frequent type of voter voting, voters were much more familiar with the system who have filled out ballots very often. So, they're much less likely to make errors. And mail voting is a form of voting that could be prone to errors that the voter isn't aware of that could cause their ballot to be rejected or their vote not to be counted. So, we should look for expanded mail voting.

But my second point is, that's not going to save us in and of itself. It's going to be really

important to divert some of the stresses to the system to mail voting. But we should expect a lot of in person voting. In Georgia, for instance, where they sent mail ballot applications to every single voter and advance to the primary. And they had, they blew away every record for mail voting, 1.1 million people voted by mail in Georgia in their June primary, which is about half of the total votes counts -- cast actually. About 800,000 people still showed up to vote on election day to vote in person at their polling places.

So, we're going to need to have ample opportunities to vote in person. And they're going to need to be different than we've experienced in the past due to COVID. They're going to be larger to accommodate social distancing, for instance. There may be precinct consolidations. That in itself isn't a bad thing, it may be a good thing. It may be that there are more places that people can vote than just one single place. There may be what we call vote centers, where you can vote in multiple different places, and we'll need to figure out how to accommodate that.

But we'll need to figure out how to make that work. And probably the single limiting factor for that will be as Director Krebs mentioned coworkers. Getting enough people to volunteer to serve at the polls, to serve at their democracy. It is such an important job, I can't recommend more to all of you who are watching this, if you have the time please volunteer to be a poll worker, get trained. We're going to need millions of poll workers in November. And every election official I talk to has a real challenge recruiting ample coworkers, and they see cancellations on election day.

And the last thing is voter education. Director Krebs is entirely right. Change is in the air. Everyone is going to experience a different voting experience than the what they've seen in the past. They're going to see different options for voting. They may see different deadlines. They're going to see different locations in their polling places. Those are all going to need to be expressed to voters, explained to voters over time. We're going to need resources for election officials to do that, that voter education is going to be absolutely crucial.

And I think even as we get closer and closer to Election Day, we'll also see court decisions that may change things on a very rapid pace. So, that aspect of voter education, creating an informed electorate is going to be important, so that voters can plan as Director Krebs mentioned, that plan is going to be essential.

We now in the age of COVID, have to make a plan just to go to the grocery store. That's

something we didn't have to do before. Similarly, we're going to have to do that when we vote. And the key to that is learning about your options early, requesting things like a mail ballot, if that's right for you early. Filling out and returning that mail ballot early or going and voting early in person, if that's best. The fewer people who show up in the afternoon on election day, the better it's going to be for everyone, the voter, the election official, everyone.

So, I -- that's what we're seeing overall and I'm fairly optimistic that message getting through to election officials from what I'm what I'm seeing and talking about.

MS. HILL: I'll just ask you a quick question though, David, and it's a practical one because I mean some of the questions in have reflected on this. You know, in terms of preparation and planning, first of all how do people find out about being election monitors? And when do they need to apply? I mean because, you know, here we are, you know, already, as you said, just about 100 days or so out here. So, should they be doing that now?

MR. BECKER: So, we often joke, I mean, the answer to any question in election is it varies by state. But in general, most, in most places you can apply now. The best single place to go is the National Association of Secretaries of State has created a website called CanIVote.org. And that directs you directly to your state's official site. Particularly in this age of disinformation, it's really important to go to official sources for information. And I really recommend you go to someplace like CanIVvote.org, there's a button there that you can click to volunteer to be a poll worker. It will usually take you to your appropriate site.

But, if you know which county you live in, for instance, you can go directly to your county election site and usually volunteer directly there. Be persistent. Election officials are very busy, depending upon what their election schedule is. There are many primaries coming up in August. But definitely try to volunteer and that's the best way to do it. And plan as early as possible because that means they can get you trained earlier.

MS. HILL: That's great. Thanks. So, that was a bit of practical advice, are very useful as we do these things. Susan, you also, along with lots of other Brookings colleagues, have got one of activity going on, on related to voting. And I know you have a research project that's underway to address some of the concerns that have been raised here.

But you've been working very closely on some of the legal aspects of this. And I wonder if you might, you know, share with everybody sort of things that, you know, you've shared with us, most of us in preparation for this event. And then of course, any comments you have on, you know, what's being said here. Because obviously, there's a lot of complexity to the legal issues surrounding that. But there are many ways that you and other colleagues have devised for how we can tackle this. I think you're so on mute there, Susan. Sorry. Yeah.

MS. HENNESSEY: I'll unmute myself. No, look the -- if I could put it varies by state on a bumper sticker for the next, you know, six months, I think that's a good motto. You know, look there's a lot of confusion and misunderstanding about the laws surrounding elections, in particular federal elections.

And really the way to understand it is there's a way to understand sort of what happens in advance of an election. And then there's a way to understand the laws that govern what happens after an election to the extent that any questions are raised.

And so whenever we think about sort of the federalism issues, the relationship between the federal government and the states, there's a misunderstanding in both directions simultaneously. So, we have a lot of assertions of, you know, fear about the federal government getting involved and changing an election, or sort of authoritarianism concerns, things like that.

But I think fail to understand that states -- that elections are fundamentally and constitutionally under state control. But the, you know, the Constitution says that states get to have, get to determine the time, place and manner of an election. And essentially, elections occur all the way from the time you cast your votes through certification with very limited compulsory federal involvement.

Really, it's the state's relying on some degree of federal support. And so I think that's one thing that there's a lot of sort of misunderstanding of the degree of federal control.

At the same time, there's a second part to that federal elections clause. And that's that Congress can actually change anything related to the time, place and manner, except for where you choose your senator. And so one thing, you know, I completely share sort of the, you know, lauding the efforts of CISA and Chris Krebs' team and sort of the generally increased cybersecurity posture that we've seen over the past three years.

That said, you know, there's a few places in which I think we have to be candid that there really are, have been missed opportunities. And so we are going to need to plan to go into this election with sort of a clear eyed resilience based model planning for some kind of failure to occur. And deciding what we do at that point.

And so I think there are really two places. So, one is that Congress has not managed to pass comprehensive bipartisan election security legislation. We've had some sort of bills that provided some additional funding here and there at the margins. And this is really sort of a baffling thing because there is large bipartisan agreement on the core issues. This is one of the areas in which Republicans and Democrats really, really do agree on the big stuff. And somehow we have not managed to get over the little stuff. And I do think that that leaves us sort of more vulnerable.

The other thing I think we should note is that we're having a conversation right now that is fundamentally about deterrence by denial. Whenever you're talking about nation state behavior, and ultimately we are mostly focused on the nation state threat here, ordinarily we're talking about tools of deterrence that are not pure, hard security, sort of how do we secure our systems against attacks. We're sort of, we're thinking about the tools of traditional diplomacy, of foreign policy, coercive diplomacy, right.

Sending a message, an incredible message to other countries that don't even try it. One, it's not going to work because we've secured our systems. But two, you're going to face real consequences if you do. And I don't think that that has successfully occurred over the past three years. So, it does leave us in this moment, 100 days before an election having a conversation that really is a conversation about deterrence by denial. How do we secure our systems from attacks?

I sort of share the view that the idea that a foreign country is going to be able to come in and change the outcome of an election and we're not going to know it, you know, there that's a relatively low risk.

That said, I do think we need to be really focused on the possibility of a foreign adversary or a very sophisticated nonstate adversary, doing something that inserts some degree of uncertainty, right. So, creating some sort of situation in which a reasonable, good faith expert can only say I have 90% confidence in the outcome.

And what happens is if an adversary can insert even 10% uncertainty or 5%, election

lawyers will do the rest, right. We have a naturally adversarial system that is designed to take that uncertainty and amplify it. And so I really do think that this is a moment in which we need to start thinking about what are the legal mechanisms, what would occur, how would we go about settling open questions in the event that an adversary did sort of insert this degree of uncertainty?

And ultimately, that's a state law question. And it's 50 states with radically different laws. People who remember sort of the 2000 hanging chads sort of I think debacle we can all fairly term it as. You know, should not be anxious to sort of repeat that, but understanding the part of the education system that needs to occur at this point. Certainly educating voters that you need to be more patient. Mail in ballots take a long time. You know, resetting the way that the media communicates with the public on these issues.

But also getting them to understand that look, the rules in Florida operate this way, the rules in Ohio operate this way. And that is part of reinforcing institutional credibility, and messaging to the public that we do have a system that is sophisticated and robust enough to tackle these questions head on. We don't, if there is some kind of concern, we don't just need to hide them. We do have these mechanisms by which to settle these issues and to really start thinking about how the variation, what the variation looks like across states.

A little bit just to plan for the idea that something will happen or something is likely to happen, and how are we going to get to a place from there in which the American public has confidence in, you know, the sort of the core of democracy, right. The idea that we did in fact conduct a free and fair election.

MS. HILL: Great, Susan, because actually we're getting, so, I've got my glasses on, because all these questions always come in very small print, so I can barely read them. But we're getting a lot of real time questions. Because obviously people are very engaged. I have all the advanced questions, then we're getting some others coming in, as well, as all of you are speaking.

And I think that this point that, you know, you're making that everybody else has made of the complexity of our system, it's not a whole system. It's not a kind of a one size fits all. But a lot of the questions and concerns that people have about foreign adversaries messing with the system, it'd be difficult to mess with 50 systems simultaneously.

I mean, Chris, I mean, I think he had to go and don't worry, we did thank him for his contributions before he had to leave there. You know, said if you got in an order from paper from some Petersburg, we'd have to make sure it's from St. Petersburg, Russia and not St. Petersburg, Florida Of course, because that would be a legitimate order. You know, for paper.

You know, you would know that there's something, you know, was afoot. But there's a lot of people asking questions here about, you know, worrying that even our allies might try to use election interference for countervailing benefits, you know, to kind of try to, you know, also, you know, see some sort of benefits from electoral outcomes.

You know, is it possible to mess with voting machines and the programs that compile those? Is it possible to, you know, mess with the mailing in systems? Is the mail in system on the postal service, the best way to withstand a cyberattack, or an attack from a foreign adversary? Does this complexity helps us to, in fact, avoid some of the problems that people are most concerned about?

So, Susan, this seems to be in something you're seeing there, somebody suggests that yes, this complexity actually could be advantageous in the same time that actually makes the tabulation of the vote and the whole process more convoluted?

MS. HENNESSEY: That's the arguments -- this is, I think, a true tension at the heart of this and an argument the federal government was making sort of in advance and during 2016. Saying, don't worry, we know that each -- that any one individual system might not be fully secure. But there are thousands of systems, right.

And the reality is, is that if any one individual in the United States knew the precise county and the number of votes you would need to change in order to change the outcome of the presidential election, that person would be making many, many millions of dollars as a political consultant, right?

There is an entire industry in the United States that works 24 hours a day, seven days a week, every single day of the year, whether it's an election year or not, trying to answer these questions.

So, the idea that there's a foreign adversary that is able to sort of take this pinpoint interference and actually change outcomes in some kind of predictable way. You know, I do think that complexity decreases that possibility. That said, I don't think we should be patting ourselves on the back

of saying, don't worry, we're insecure in 10,000 different ways, right. That only helps sort of to the extent that you really are concerned about the big question of, you know, can somebody else change the outcome of an election.

When we're thinking about this issue of introducing uncertainty, you know any amount of additional complexity that is added into the system, especially novel features, things that people are not accustomed to, that does become an opportunity to, you know, to raise real questions, you know, potentially to amplify questions, sort of. I know the next panel is a really great panel sort of related to disinformation.

And, you know, so I think that there are legitimate, you know, legitimate questions to ask. That said, I do think that it's sort of incumbent upon experts to be really, really clear with the American public that there is no evidence in 2016 that any vote was changed. That the Senate Intelligence Committee released a comprehensive report that really, really shared a lot of information about what happened. It should give people a lot of confidence and sort of thinking about how can we translate I think that really high degree of reliability that we got following 2016, although notably not until 2018. And how can we create a system in which the government is informing the public conversation in a way that is transparent, that has institutional credibility, you know, so the public can have confidence.

MS. HILL: Yeah. Susan, I mean, that's a great point. And you made a point in a personal discussion that all we had just a little bit ahead of the panel, that, you know, part of the issue that we get so fixated on this, is that it's turnout. You know, if we all listened to what Director Krebs, what Chris said, about, you know, everybody getting out there and voting, you know, we want more people to go out and vote, and not just be monitors of voting. There would be, you know, much less room for these kinds of errors having a larger knock on effect. Because it's where you have a low term out, particularly in certain precincts, where it increases some of the opportunities, and anyways to have all of these various outcomes we're worried about.

Perhaps, you might want to say a little bit more about that, Susan, because I --

MS. HENNESSEY: I do think we need to acknowledge that our sort of, you know, that the crisis or a potential crisis of security is playing out against the backdrop of a crisis of participation. This is most salient whenever we're talking about the sort of disinformation operations, influence

operations, things that are, you know, it's hard to sort of get hard forensic evidence about the actual sort of impact on things like that.

That stuff that can create real questions that you actually aren't able to answer when the margins of victory here are in the hundreds of thousands or even the tens of thousands sort of spread across your various counties. Whenever you have a country that sort of hovers around 30% participation rate among eligible voters, you're always going to have margins that kind of look like that.

And so if we were instead a country that had much higher voter participation margins, that would mute the impact. It doesn't solve the problem, you know, new problems do exist. That said, it does mute the impact of sort of this new, you know, disinformation propaganda questions that arise. And I do think that, you know, each issue needs to be sort of confronted in its own bucket. That said, it's a comprehensive effort here to secure elections and to secure the confidence of elections in the minds of the American public.

And that's one thing that if people are wondering what they can do, and how they can do their part, making sure that people vote and that lots of people vote, I do think would get us to a much healthier sort of security posture much faster.

MS. HILL: Yeah, I mean, it's very true that we really do need to impress some people in all different ways. And obviously, David, this is one of the things that you're doing with your organization as well. I mean, just what a privilege it is to be able to vote. You know, we're thinking back at the Civil Rights Movement. We're also thinking about 100 years last year with the amendment that gave women the right to vote.

And it hasn't always been something that we've had. I mean, they're even in, you know, other countries or even sometimes in this context, you know, you hear people talking about only certain people should really be able to vote. So, this is the fundamental act of agency that we all have as citizens in the United States. Its everybody should really get out there and vote and do their part.

Now, David, we're getting some questions in here from the audience, which actually I think will be something that you'll be pleased to hear, as an NGO, about donors. So, if people, you know, who have the means and who want to, you know, play a more active role are really concerned about the integrity of the vote or getting people out to vote, what can be done now for a donor thinking about how

can they help out to improve election security for 2020? What can funders fund in the kinds of things that organizations like you and others are doing and I know our Brookings colleagues are doing lots of research and diverse things as well?

And if audits is one of these, you know, is there anywhere that there can be public private partnerships on helping ensure audits, for example? You know, are there funds available for this, you know, kind of activity? So, a lot of people are asking here, what can they do not just showing up to vote, not just trying to monitor, but if they've actually got some funds to spend on here, in this kind of public private context, what could they do?

MR. BECKER: So, first, the bad news, we're very close to an election, we're less than four months away from the November election. And many -- the technology is pretty much locked in place. One of the things I would recommend is, it's not useful now to file lawsuits or argue for a change in election technology. In fact, that kind of chaos, that kind of change could have a really detrimental impact on voters and on election jurisdictions.

There are some, so that's just bad news to start, and that's very quick. The good news is there's still some opportunities, audits is one of them. Georgia just held a pilot on a risk limiting audit that they're -- that's going to lead the way to a statewide audit. And in November, there are some primaries coming up where there are other pilot opportunities.

And again, more good news is many states are already moving in that direction. They are trying to do better and better and more audits. And we're going to see more audits than we've ever seen before by an exponential factor in November. That's all very, very good news.

You know, I think the biggest thing that funders can do right now, and it goes to Susan's last point, which was such an excellent point. The goal of many adversaries right now is to diminish citizens of a democracy, their confidence in our elections in our democracy. And one of the ways, one of the things they'd like to see from that, one of the tangible things is for people to opt out of democracy, to stop participating, to stop voting.

And in fact, in the United States, we already start from a perspective where turnout of over 60% is very rare and turnout of over 50% only occurs once every four years. All other elections have below 50% of eligible turnout in the United States. And that's been going on for quite some time.

And in fact, if you look at turnout outside of presidential elections, mostly turnout has been declining over time. There have been some blips in the radar, 2018 being one of them. But that's a challenge. And it's absolutely true that we fight back against our adversaries when we participate, when we engage.

But it's also very true tactically as well. Every single vote is a data point. Every single interaction with election offices is a data point. If someone has interfered with voter registration databases, every time you check your voter registration status, there's an opportunity to catch that problem.

Every time, if someone was to intercept the mail ballots and try to vote them, every time that real voter goes to vote would be an opportunity to catch that person. There's so many checks and balances in the system it's virtually impossible. I'd never say impossible, it's virtually impossible to change the outcome of an election in a way that would be undetected.

But there are ways in which an adversary can interfere in our elections in a way that would be detected, and are in fact intended to be detected and cause chaos. In fact, if you look at the Illinois voter registration database intrusion in 2016, that's exactly what that looked like. They were the Russian GRU was sitting inside the Illinois voter registration database for about two weeks undetected, accessing data at very, very low rates, so they wouldn't be detected for about two weeks.

And they weren't being noticed. And right before the presidential conventions were to start, they started accessing information at thousands times more greater effort at that point. So, in such a way that the Illinois state election officials said there was no way we couldn't detect it, it sucked up all our bandwidth right away. We shut it down right away.

And, you know, I think it's a reasonable inference that they were trying to be detected at that point. They wanted it to be known that they were inside the Illinois voter registration database. And obviously Illinois also, not really a swing state in the presidential election, it's -- it was just a database that they could get into.

So, again, voting is really the key. So, how do funders and others encourage more voting? That's going to be a real key. We just released a report last month, my organization, about the decline in voter registration as a result of the pandemic, because people aren't going to motor vehicles

agencies anymore. Third party groups can't set up tables or really do door to door and try to register voters. That's going to be an ongoing challenge.

So, thinking about ways that funders can help reach potential new voters and to educate voters with official information is going to be really key. I founded a separate nonprofit called the Electronic Registration Information Center, ERIC, which 30 states now belong to which helps them reach out to eligible but unregistered citizens and encourage them to register to vote. And about 20 to 25 million of those individuals will be contacted by the states themselves. States like Texas and Georgia and Michigan and Kentucky and Florida. All doing that in about September of 2020.

Those kinds of efforts can really be encouraged and anything that can get more official information to voters and get them to engage that's probably the best use of resources at this point.

MS. HILL: That's a really great point. I mean, are there restrictions on some of this. I mean as were speaking there, I was thinking about, you know, when people go to supermarkets, you know, often there are, you know, obviously people collecting for various things. But there may be restrictions on private sector voter registration. Is that the case? I mean it has to be in an official setting?

MR. BECKER: So, there's a lot of opportunities to do voter registration. I think the practical limitation is probably more restricted than the legal ones right now, given the pandemic and the need for social distancing. But there are significant restrictions that can occur, again, varies by state, on public-private partnerships.

And some states have the ability to partner with philanthropies to assist them with some of the efforts, especially with regard to voter education. Other states have pretty strict laws with regard to using outside funds for that.

And I know, in talking with a lot of states, they're trying to figure out ways to navigate that system so that they can manage it. There are a lot of highly responsible funders out there representing a wide view, a wide variance of political views, who are trying to assist in this regard and trying to connect those in the right way and make it legal, is something I know I and many others are working on.

MS. HILL: Yeah, I mean, that's important is having this bipartisan. I mean, as a fundamental rights of citizenship not because it's kind of politicized in any particular way. And I think that's a very good point that you've made.

I'm going to go back to Mark, because Mark, I mean, all of the other questions that we've had a really related to the space that you were working in as resilience when you were a senior director of the National Security Council.

We've had questions about, you know, just the risks -- the physical infrastructure you were talking about that might have them knock on effects, not just to the people and the data. You know, so one question coming in as, you know, if you were thinking like a terrorist bent on disrupting the voting process, which frankly, our adversaries are often thinking in exactly the same way, this is at the state actor rather than a nonstate actor.

Would you consider like, you know, mounting disruption to power grid, which the network requires to function? I mean, obviously, that's where paper ballots and other things might come in. But as the, you know, worries about this kind of, you know, the grid system's very vulnerable. And we've seen, you know, the grid blackouts. You know, obviously, you know, in the, in November, you know, when, if you kind of have polling in a, you know, particularly there's all kinds of things that one in a might think about.

You know, it's very interesting watching what just happened in Russia, because Russia is one of the adversaries we worry about. Where a lot of people may have noticed that Putin has just put himself, you know, back in the picture of having these amendments voted on that would allow him to run for two more presidential terms.

And they actually opened the voting up beyond, you know, because they were worried exactly at all the points that we've been talking about. Worried about low turnout. Then the legitimacy of the voting would be in question. They were worried about in a COVID environment about getting as many different kinds of people voting as possible over a huge and very varied landscape.

And Russia is the largest territorial landmass in country terms in the world. And so they actually made this a long going ongoing process over several days. It's been remarked upon a lot in a Russian domestic context about how much effort they actually went to, because they needed to have a legitimate vote and a large enough turnout so that Putin could say that he had the general public's backing for these constitutional amendments.

Now, clearly we just want to have more people out there and participating. You know, so

it's this question about pulling out the process, what would happen if it was a major disruption? You know, we talked about before Chris had mentioned hurricanes and, you know, imagine weather events, you know, we could imagine large storms, snow storms, not just the terrorist disruptions, but Mother Nature getting in on the act.

I mean, Mark, what are the things that we're, you know, should be worried about in this, and what can we do to address them -- or have we already done to address them when you were there and working on these issues?

MR. HARVEY: Yes, I know, a lot of what's already been done to address them happened right now. There's been a dramatic increase in early voting that has taken hold across the country over the last two decades. To the point that while we're all talking about Election Day being four months away now, the election starts off pretty much two months from today. In person early voting will start in the middle of September. I think the earliest will probably be about September 18th or so, running the math in my head here.

And it's instructive to think about what has transpired in the country in the last 45 days. And think about that, what can transpire in the 45 days in between September 18th and November 3rd.

The end goal of our adversaries is not to elect a particular candidate. They might have won they prefer, they might not. The end goal of places like Russia and China is recognizing the core way our system functions and removing that. They want to remove from the government, the consent of the government.

It's the exact same reason that they target other elements of our critical infrastructure. Because if they can take out a power grid, if they can take out a gas line, it shows that the government is not capable of protecting the American people from those sorts of things. It removes our trust in government to be able to do that.

We've done a very good job of removing trust in governments since Watergate. And it's at relatively historic lows. And frankly, I think the performance within the pandemic over the last four months as removed even more. And that is a massive vulnerability that we have.

No matter what type of technology is used for voting, no matter what happens on Election Day. But we need to recognize that it's a 45 day window that we've got right now. And people are going

to be voting based on different information.

I had a boss that always used to love to give the story of how four days before the election in 1992, Ross Perot went on national TV and accused the Bush White House of sabotaging his daughter's wedding. Now, it didn't tell you a whole lot about George H.W. Bush, but it told you a whole lot about Ross Perot and his mental state at the time, and his through process at the time. And that might have changed people's minds.

When you think back to 45 days ago, and you look at where approval of President, federal government, any one of our major institutions was then versus where it is right now, given those 45 days' worth of developments and think about doing that at the very start of flu season. You have a very fluid ground on which we are going to hold this election.

And whatever the results, however it comes out, we have to recognize that the consent of the governed is what is at the core of any argument here. And that's going to happen from the political and process arguments that will also happen from the legal arguments. Especially if we get into cases where we have very narrow margins.

We have a system that is built for blowouts. And it is built to be able to say we've got a 10,000 or 20,000 vote margin in any individual race. When it gets down to narrow ones like we saw in Florida, and I think that was 527 votes at the end of the day, you can have problems. But it's doable.

For all the 527 votes in Florida talk that we have from 2000, nobody recognizes, or we haven't really talked a lot about that it was 380 some odd vote difference in New Mexico. They had the process, they went through, it wasn't the heart of the legal battle. It's doable.

So, how particular judges rule on some of those changes and those dynamic changes that may have to be made throughout that election period of 45 days, is going to set the foundation for what challenges post-election might actually happen once the election lawyers all come in and, you know, at least there's reporting the other day the GOP is looking at about $20 million worth of legal fees in this.

I don't know if Democrats are looking at this side. But we're going to have a lot of that going on. Because that's how things actually happen. I'm sitting a couple of miles away from ground zero in New York right now, there was a primary election on September 11, 2001. That they suspended, that they rescheduled, that goes through a legal process that a judge is going to have to sign off on at

some point.

Every election hours get extended for weather, for transportation challenges, for infrastructure disruptions. There are ways to do that. And as Chris said at the top, you know, election officials are natural risk managers, because they deal with that every time. David mentioned being at DOJ. The DOJ has had within their civil rights capabilities, offices set up for every single election since 1964 to look at civil rights challenges, that actually pop up.

So, there are ways to lay the foundation and to provide real time changes in how an election is administered in that 45 day window. The question is, what level of controls do we have on that? How is that administered? Can we do that in a fair way when every state is different as we have on the bumper sticker? And what is that going to lay the foundation for in the post-election time?

I recognize that we've got typically about three weeks of time to certify those election results and that's also in our current environment, the amount of time that's a lag between a mass gathering event and a spike in cases. So, what's going to happen in that intervening three weeks that will put tremendous public pressure on our election officials and our legal system to interpret the rules in a way that will fit to ensure that the governed have consented to the choices that are made?

MS. HILL: Well, thank you Mark. We'll be coming up into the next panel, so I'll just turn back to David and Susan to see if they want to add anything more on that. I mean, I'll just give you an indication of some of the questions that have been coming out. There have been so many of them that unfortunately, I haven't been able to touch on, but I think one way or another, we've already answered some of these and what I'm going to do afterwards is, as I mentioned, is I'm going to share all the questions that have come in with all of you. And I know there'll be more events at Brookings and David, you will be doing events as well. And hopefully, we'll be able to sort to publicize to everybody all of these events so that over the course of time all of these questions will no doubt get addressed in a one way or another.

Alex, Mark coming from CNN, for example, is worrying that cozy bear (phonetic) campaign on a tax on the COVID vaccine research has just been reported. And some of these other GIU tax over Twitter that we -- a tax that we talked about before seem to run an inside role, could be indicating some of the things we'll likely see in the November elections. The kind of just getting people generally to

be worried about hacking and damage that can be done.

We've had a lot of questions about, we're obviously only as strong as our weakest link. What's our weakest link? And I think some of the weakest link is actually voter turnout in our just, as you're saying, where the margins get very small and get very tight and depending then on which precinct has the best systems for ensuring the audits, all the any kind of legal challenges where those margins are very tight. But David and Susan, is there anything that you'd like to leave everybody with before we move over to the next panel on the specific issues of disinformation?

MS. HENNESSEY: Yes, I'll just give a very brief and extremely policy wonk free (phonetic) and that's that all of the issues that we're talking about here rest on top of systemic issues that aren't solved in hundred day periods. So, one of the challenges of election security is that elections are run every single month, every single day of the year. Every single month of the year throughout the country because there are hundreds and thousands of times. Getting the public's attention and mustering the kind of political will that is going to be necessary to make the long-term, sort of systemic changes, right. Things like changing sort of states' relationships with vendors. Mandating -- actually having mandatory federal cyber security standards. All of these that are really critical to this core question of consent of governed, democratic legitimacy, electoral legitimacy.

And so, to the extent that you're sitting here right now and thinking, I'm really, really concerned about this as we're look at the next election. Also, think about how to translate that into advocating for the kinds of policy changes that might not necessarily help your perceived candidate in November, but are going to address the long-term questions. Now's the time to start picking up the phone and calling your senator. Getting yourself educated on the very unsexy, uncool, but sort of bread and butter reforms that I think are going to be necessary because otherwise, every four years, we're going to be back here having the same sort of conversation about how can we make things a little bit better, like the margins.

MR. AGRANOVICH: Yeah, that's a great point. And I'd just add very briefly, we have to remember our adversaries are targeting our confidence in democracy and they win whenever, from whatever our political perspective is, we lose confidence in our elections. We feel like our vote or our voice matters less for some reason and that arguments about those are coming from across the political

spectrum. There are folks on the right and the left who are making arguments about why we shouldn't trust the outcome of elections. And I think it's really important, from the perspective of all of us as citizens to be aware of the confirmation bias that we're all susceptible to.

Then the media silos that we all reside in, we're getting information that tells us that we're right. And it feels good to be right, but when those messages are telling us that we shouldn't trust the other party's election official, or we shouldn't trust the other party's voters because they are trying to undermine democracy. That message is actually serving an anti-democratic purpose literally (phonetic). And it is not about Democratic party versus Republican party, it's about autocracy versus democracy and we should be very skeptical about messages that tell us that we shouldn't trust our democratic institutions in our circumstances.

Susan's exactly right. There's still a lot of work to do and it's going to go well beyond the 2020 election. We are not perfect. We are not across the finish line yet. But on the other hand, we need to have confidence in our democracy and our election system and be looking for, hopefully, on November 4th, where we're all going to be, is we're all going to be saying, "That was great. What a great success. What a great success by Republican and Democratic election officials to run an election that was successful." That would be a lot better than being angry.

MS. HILL: That's perfect. David you've given the perfect segue doing my job for the next session. Thank you so much for doing that because part of the issue that we're dealing with here is our own polarization, our own propensity for spreading around misinformation and disinformation is becoming a national security threat and is also undermining our own confidence in our systems. And this also causes what the next panel is going to talk about.

I want to thank all three of you and Director Chris Krebs for coming in today and I just for laying this out in a very clear way. Clearly, communications and transparency and fact-based information is very important for everybody who is involved in this process. There's a lot as you've laid out for everybody's listening to this to do and showing the way. The things that they can do. I just commend all of you on the great work that you're doing and David, ascribing organizations like yours are out there now and I hope that we also continue the partnership with Brookings and all of our colleagues as well as we get there to the elections. And the artwork that Mark's going to be in the future.

And I just want to handover to Chris Meserole, another Brookings colleague, is going to moderate the next session. Chris is a deputy director here at Brookings who is in charge all of our artificial intelligence on emerging technology work. So, all the places where it's become very complex and very complicated, and Chris is in charge of helping us all figure this out and to coordinate all of the efforts of different Brookings colleagues. So, Chris over to you and sorry to have run in a little into your time, but I think that we've had a framing for the next session. And I'm going to listen eagerly to what happens next. Thanks a lot, Chris.

MR. MESEROLE: Well, thank you, Fiona, for the great introduction and for hosting such a wonderful and insightful panel on election security. I can't imagine a better, more informative discussion carried out by such incredible colleagues. And I'd echo, for our viewers at home, I'd echo their call that you all become as informed and active in ensuring our elections go as smoothly as possible.

As Fiona mentioned, we're now going to build on a conversation that our prior colleagues had by focusing, not just on the security of the ballot box and American electoral infrastructure, but also by focusing on the information environment at large. Particularly, with respect to disinformation and influence operations. So, we're going to be looking, as Chris Krebs put it, not just our infrastructure, but our American mines and how we need to secure those.

As part of that conversation, we're thrilled to be joined this afternoon by three amazing colleagues. The first of them is Laura Rosenberger, who is a senior fellow at the German Marshal Fund and Director of the Alliance for Securing Democracy and previously served in a variety of roles in the State Department and National Security Council. She is, by far, one of the sharpest minds I know of in the disinformation and influence operation space and we are delighted to have her joining us this afternoon.

Second, we also have David Agranovich joining us. David is a global threat detection lead at Facebook where he works on disinformation and related threats. And previously served as Director for Intelligence on the National Security Council. And again, we're delighted to have him with us today to share some of his expertise and experience.

And last, but not least, we have Alina Polyakova, who is currently the president and CEO of the Center for European Policy Analysis, or CEPA. But previously, was a wonderful fellow colleague

here at Brookings where she's a scholar in our foreign policy program and led our global work on disinformation. So, welcome back home, Alina. It is a pleasure to have you with us again.

Without further ado, I think we can just kind of go ahead and dive in. And I want to start with some level setting on what exactly -- why disinformation is so important; what got us to this point. And Alina, since you were one of the first analysts to start flagging Russian disinformation, even as far back as 2014, 2015, I was wondering if you could just talk a little bit about what alerted you to the role of Russian disinformation campaigns originally. And then what happened in 2016, 2018 that kind of led us to the point where we're at now.

MS. POLYAKOVA: Well, thanks so much, Chris and it's wonderful to be, at least in this Russian panel and to see all of you, and to see some former familiar faces, former colleagues from Brookings as well.

So, just to get directly to your question, well, for me, you asked about why I cared, I suppose when no one else did, back in 2014, obviously, most Americans only woke up to the problem of disinformation broadly in the context of our el3ections in 2016 with a now, very well-known Russian activities, social media and elsewhere, which are again, in the news just this week. And I hope we get to talk about the recent reported cyber-attack that the Russian GRU unit, APT29, the exact same unit that was involved in the hack and dump operation in 2016 was involved in. So, they're still added, so to say.

I think it'd be interesting to talk about the reason for that, but taking the clock a little bit six years, know what was happening in 2016, some of you may remember, of course, the revolution in Ukraine. And at that time, I was living in Europe and I had spent a lot of time working on Ukraine for research purposes and I started to notice a sort of skewed narrative emerge in English language media and what was happening in Ukraine on the ground. And I was on the ground, so I knew what was the reality. One was being reported something very different and what was really kind of seeping into even the top U.S. language media and the time were really misinformed narrative around this idea of what was happening in Ukraine was not democratic revolution, but it was some sort of fascist coup. And that, of course, was something that was very familiar to me. It was the typical Kremlin media narrative and I was really surprised to see it being reproduced in some forms in English language and also, German language media at the time. And that's when I first got the sense that Russian propaganda, which is what

we called it back then, was a bigger issue than I had thought.

At the time, I thought it was really just an issue having to do with Ukraine. Soviet-mind states like Ukraine, like Georgia, like Estonia, Lithuania, Latvia have been the targets of Russian propaganda or disinformation for a very long time. And we're pretty familiar with and knew how to deal with it to a certain extent. What was new was that these narratives were now appearing and seeping into the Main Street English language media. And that's when I thought this is a real problem to think about it.

But then, quickly, I realized that in D.C., this really was not anywhere on the radar of policymakers because I think we tend to think that what happens somewhere over there in Eastern Europe is going to stay somewhere over there in East Europe. So, by the time 2016 rolled around, those of us who had spent time looking at what the Russians had been doing in the Ukraine, I can say that I wasn't surprised. I was absolutely surprised by the brazen nature of the influence operations that the Russians carried out in 2016, but not by the tactics.

The tactics were very similar to what we had seen the Russians basically test in Ukraine previously and all of that really came to the United States in 2016 and then other European countries after that. And basically, around every single event that the Russian government sees as important to itself, every single election now has an influence operation component behind it.

And, of course, now, in 2010, that's really the reality that we're living in. I think it's hard to imagine an election today in which we don't have to be concern3ed about foreign influence ops.

MR. MESEROLE: I was wondering if you could talk a little bit more about that. And (inaudible), you mentioned the Russian hack earlier, but what are the -- obviously, this is a threat that's evolved over time. What are you seeing now as kind of the main trends that you're most concerned with, particularly, with Russian disinformation, but even more broadly?

MS. POLYAKOVA: I think my biggest concern now, as someone who has worked on Russian for a long time is actually not Russia. And what I mean by that is, of course, now, the toolkit, the broader influence toolkit that spans beyond the information environment has been out there for a long time and because there hasn't been a focused strategic response to counter and deter these kinds of operations. Other states have already been using this toolkit in various ways. And I'm sure David will talk about that from the perspective that some of the work that Facebook has been made to take down, some

of these state sponsored influence ops, but even beyond that, my concern is that we haven't even dealt with the Russia problem and now we have obviously, the China problem and I know Laura will want to talk about that. And Iran and North Korea and basically, any actor, non-state actor as well that has some sort of stake, or has a profit driving incentive to be involved in an event that has a lot of eyeballs on it. Elections tend to be these high attention events, which is why there's such incredible opportunities for state actors of political agendas, or even for non-state actors to have profit or economic agendas.

So, my biggest concern is that we've seen a profound evolution of the tactics because as we have identified and exposed how these operations work, especially in social media, the adversaries have adapted. And what we've seen at least from the Russian activities in some countries in Africa and also in Eastern Europe, is that they're getting much better obfuscating their origins. So, in 2016, in a way, it was an easier place to attribute and identify these campaigns because as most people recall, they were being run straight out of St. Petersburg at the time. The so-called troll factor, the IRA was based there. They gave a very powerful data point to be able to attribute that this was a foreign influence ops, when you can easily trace back some of these accounts and Twitters or Facebook where they were originating. And now, we know what the Russians have been testing in other parts of the world has been, that are blending in with domestic voices, franchising out some of these operations to local actors. And this kind of information warfare by proxy is much more difficult for us to identify and expose.

And I think that's just one of the vectors to be honest with you. I think the other one that I would not be surprised, but it is very difficult to know if it's happening, is, of course, infiltration of community groups, whether it be on Facebook, Instagram, and other social media and the fact that we don't have much insight to what's happening on non-American platforms. Of course, TipTok comes top of mind and we don't have any insight into what's happening in TipTok where the disinformation is from because they're not subject to the same kinds of transparency, values, and principles that I think are very much embedded in western companies, the kinds of pressure western companies also face to be more committed to those values and principles.

So, I think the space has become much more complex. There's a lot more ways to obfuscate, to get around detection, which makes it much more difficul to identify. And it's just a much busier environment and we never fully doubt with the original bad actor and now we heave dozens of bad

actors to deal with.

MR. MESEROLE: Thanks Alina. I think you raised about a dozen points that I want to come back to through the course of this conversation. But the two I want to pick up just immediately are, you referenced China a few times and you also mentioned this kind of information asymmetric word, counted space. And I know, Laura, you've been doing a tremendous amount of writing on both those topics. And so, I was wondering if you could just kind of give, in your sense, of what's happening. What are you seeing with China, in particular? Why is it important within this -- most Americans, certainly, I think -- many of our viewers probably think of this disinformation and influence operations as a Russian issue. But clearly, it's broader than that now, so I'd be curious for your thoughts on that.

MS. ROSENBERGER: Yeah, thanks Chris and thanks Alina for picking up some of those right there for me. So, the way I think about China and frankly, Russian, in terms of what they're doing with disinformation and information manipulation more broadly -- and I'm going to use that term primarily as that's my (inaudible) because I think it gets at the broader subset, or the broader set of what we often, you know, when we was disinformation which is a subset of information manipulation.

Now, to me, information manipulation is today a tool that Beijing and Moscow and authoritarian regimes, in particular, see as a means of influencing state power. They see it as a legitimate tool of power and one that, as you know, is an, and as Alina noted, is asymmetrically advantageous to them. An authoritarian regime's control and manipulation of information is sort of baked into the cake of what they do, right. These regimes are afraid of information if it's freely in the hands of people. They see it as something that is for government to control and they see it as something that they can recognize to their own advantage. And Moscow -- Alina outlined, has really advanced the tactics to do that on a broad scale in a way that weakens and undermines democracy. And, of course, while their most recent social media kind of operations have a particular script and scale, there's the long history to Russian views that we had to tackle (phonetic) back to the Cold War.

What we've seen with China has been a little bit different. So, if we were having this conversation a year ago, I would have told you that China's tactics when it comes to information manipulation looks pretty different from Russia's. That China's goal was largely aimed at promoting a positive image of the People's Republic of China and Chinese Communist Party. That creating and

amplifying positive narratives about China and suppressing unwanted narratives as well as suppressing of people and organizations they didn't want to have a voice. That those were the main tactics that we saw China using. And that most of their information manipulation really had to do with things that were about China, which is pretty distinct from what we see from Russia with information manipulation.

It's not trying to sell itself to the world. China, as an objectively rising power is, and so the information pieces are a big part of that strategy. Interestingly, what we've seen over the past year really starting at about last August with the height of the Hong Kong process last summer accelerating during COVID has been a turn a far more aggressive direction by PRC states and state affiliated actors in the information space. So, a couple of the pieces that I think are indicative of them.

The first is that we've seen a lot of what people have called the wolf warrior tactics. These Chinese official spokespeople from the Prime Ministry as well as from their state media outlets, really aggressively engaging in almost troll-like behavior on Twitter, much like we see Russian officials often doing. Like, the kind of stuff that goes viral and gets lots of clicks and gets you big followings. We've seen a whole lot of that in a very negative, negative direction.

A lot of that again has been around COVID, but we've seen that also begin to happen around the protests about George Floyd and police brutality and racism in the U.S. But we've also see, I think, the development and greater use of actual disinformation of what deliberately false information, particularly around COVID-19.

And I'm going to say this was largely about a couple of things. One, is deflecting blame from the Chinese Communist Party of its own failings in response to the virus initially. But the second was really to assert confusion and doubt about the origin of the virus. When we saw multiple conflicting narratives being spread by PRC state officials, state media, as well as amplified (inaudible) covert networks, it looks very similar to what we saw the Russians do after the MH-17 shoot down and the poisoning of Sergei Skripal. Now, did they say, let's look at that playbook and let's sort of recreate it ourselves? No, but there were a whole lot of similarities there and it was really the first time that we saw official Chinese actors engaging in this kind of, let's show confusion, doubt and chaos tactics. The other thing I think is notable about the Chinese doing to sort of hand back outs to this (inaudible) is a lot of their content is really in the discrediting democracy, which sounds pretty similar, in fact, to what we see from

Russia, right. And so, around the George Floyd protests, a lot of what we've seen has been really interesting commentary like, look at this chaos in the U.S. Democracy is a mess. Well, of course, the truth of the matter is protests are a sign of a democracy that is working through the process of addressing its own challenges, right. And it's sort of a misunderstanding that on the part of the Chinese officials, on sort of the significance of protests in the democracy. But that's been the narrative they tried to push.

Similarly, we've actually seen just earlier this week, one of the Chinese Foreign Minister spoke with (inaudible) tweeted, isn't it crazy -- I can't remember her exact wording, but basically, like, "Gee, the U.S. has two 70-year olds that are running for President. This is a failing of democracy. Democracy sucks." That was the basic tagline of her tweet, right. This is a wholly new kind of tactic from Chinese officials. It's not about China. It's about discrediting the U.S. It's about discrediting democracy and it's using that weaponized information platform to do so.

The last thing I would back to your question on the asymmetries here is that I think it's really important and I know today, we'll probably talk about keep the other half, so much time. We're starting to have a limited scope conversation, but I think it's really important, in particular, to understand from what China's doing, that I believe its use of the information manipulation is not just about that topic itself. It's about advancing and creating a separate -- a different information model distinct from what democracies have. It's free and open flows. The information model that Beijing is trying to advance is one that has sovereignty at the center, that believes that states should be able to inspect data is of strengthening systems, that believes that it should be able to censor content. And they're trying to export those things around the world. And they do that in terms of infrastructure and they also do that in terms of governance of information.

So, the information manipulation tactics are part of this bottom strategy and I think that it's important if you think about what do about the challenges to think about them in an (inaudible) way.

MR. AGRANOVICH: Thanks Laura, that's incredibly helpful and I think one -- I want to come back to that point about information and democracy versus authoritarian regimes like we see in China. I do want to just quickly follow-up on a point that Alina made about kind of platform governance on foreign owned social media platforms, like TikTok, which has obviously been in the news a lot lately. Is that something also that you see as kind of part of China's effort, or do you think that that's kind of a

private company? In the U.S., we would kind of separate out the private sector from the government. Do you see that -- how do you see that relationship within the Chinese context?

MS. ROSENBERGER: Yeah, it's a great question. I think that the Chinese export of its envisionist platforms is going to be an increasingly big part of the conversation that we're seeing here and when I talk about that infrastructure aspect, that's absolutely the kind of thing I'm getting at.

When it comes to TikTok, TikTok's doing its best to attempt to argue that it is wholly independent from the Chinese government. We can have a long conversation about what state capitalism means in China. The laws governing access to data as well as the fact that all organizations over a certain size have to have not only a government cell, but a party cell within their companies. We can go down the list of the ways in which independent company, private company means a very different thing in the China context.

On TikTok, there's been a lot of hyperventilating lately and I think that some of the commentary has missed the point, which is I think a couple of things. One is, as Alina said, we don't really have a transparent sense of what's happening. And then TikTok did release a transparency report for whatever that is worth, but without an ability to have greater insight in a lot of different ways, we really don't have an understanding of what's happening there. The data collection pieces, I think had gotten misunderstood a little bit. I don't -- Facebook and Google are massive surveillance collection systems for data and I have concerns about that too. But there is a distinction there between the way in which there was a private company that don't have the ability to imprison and in some cases, physically or otherwise abuse their citizens. And in China, that is the reality, and so there's a really big distinction there, I think, number one.

Number two, is that I remember from having conversations with people that (inaudible) a couple of years ago, who were like, what's the problem? It's just a video sharing thing. It's just fine. There's no politics on there. It doesn't matter in the political sense. And I pull all these platforms especially when they go to particular sides, take on new applications, take on new uses and we've absolutely seen that being the case with TikTok. There's no reason it would have been the exception to the rule.

And so, I do have deep concerns with the way in which TikTok's platform is purely

algorithmically driven, right. And it is a total black box to us what's being surfaced, what's being promoted, what's not even appearing on the platform, right. It's not even a question of takedowns in the way we think about it in a Facebook sense. Algorithmic suppression we know is something that China has used internally, but it uses on platforms like WeChat and WayBook, so we would have to receive it the same thing here.

Now, the quandary for me, as I've written about is, doing things like banning platforms, or denying access to certain kinds of things. Also, fuels not only undemocratic in certain instances, but at the end of the day it creates the sort of information reality that our adversaries might want in terms of basically, creating two separate information universes. One of which is for the cause platform and one of which is not. That maybe where we're heading and we may need to have really deep discussions about how manage that, but I think that needs to be a very strategic broad conversation, not about individual whack-a-mole (phonetic) platforms, but frankly, how we use democracies are going to build an information model that promotes the kind of information society that we want to live in and that affirms to democracy (phonetic) and that needs to be done holistically, not just in deciding on individual ban.

Now, again, when there are true national security implications, as we've seen with a couple of particular other Chinese companies and things like that, then I think that that, yes, we can definitely take action on those things. But, in general, I worry that across the slate of these issues, we tend to take action on individual pieces of the puzzle, rather than thinking about the solution to the puzzle from the big picture perspective.

MR. MESEROLE: That's great. I want to come back to you later. I know you just wrote a paper as well, kind of the idea of a democratic model for our information, to be consistent, I want to definitely pick up on that thread in a bit.

First, though, I want to turn it over to David. And we've heard a lot about some of the trends that Laura and Alina have been noticing in the disinformation space. Particularly, with respect to Russia and China, but also even in terms of tactics, right. It's harder to attribute disinformation campaigns now. It's harder to identify them in some ways. What are the trends that you all are seeing, that what Laura and Alina reference that resonate with you and what you're seeing in Facebook? And if you can talk about that and what the trends are that you're seeing right now, that would be great?

MR. AGRANOVICH: Definitely, and thanks, Chris, for the opportunity to join this conversation. It's a really, really timely time to talk through all of this stuff. Just maybe to level set, my team focuses on both the coordination of our investigations and disruptions of these types of operations on Facebook, as well as thinking through some of the scenario planning around what new tactics do we anticipate seeing as these operations evolve and adapt to the enforcement that's being taken against them on different platforms.

So, a really timely question and I appreciate it and I think Alina and Laura touched on some of the tactics that we are starting to see out in the wild on Facebook and across these operations.

So, the first thing I wanted to call out is, this conversation, even when I was still in government back in 2016, 2017 period, focused really heavily on foreign interference because that was the 2016 elections had just happened and public attention was focused on the Internet Research Agency and to a lesser extent, I'd argue potentially even more impactful, GRU activities targeting the DNC and the (inaudible). But as we've conducted our enforcement actions over the last several years at Facebook, about half of the operations we see using these types of deceptive tactics are domestic in nature. So, they originate within the country where they're targeting and they're operated by individuals who are in that country who understand the language, understand the culture. And so, what that has done is it's created an interesting challenge.

Our policies on the Facebook side are foreign, domestic, agnostic. All right, so, we enforce on both pretty much equally if they're using the same domestic tactics, but the conversation around how we should approach this issue legally, or legislatively reading from a national security perspective, is oftentimes bracketed into that foreign conversation. So, there's a bit more to talk through on the domestic front.

We're seeing that trend increase as time goes on. We've announced, I think it was last week, four takedowns from around the world. One of which was in the United States. All four of those operations had strong domestic tests and were primarily domestic operations. The second trend we've been seeing, as Alina noted, the operational security of these networks has improved considerably. Some of that, I'm sure, is just because as we and other platforms and other entities in government take more aggressive actions to expose these operations. They learn from the ways we're discovering them.

There's an interesting parallel to this though, which is as these operations have become more effective at hiding, it also seems to complicate their ability to reach its broader audience because they're spending a lot of time hiding from us, which means it's hard to be loud and reach a bigger group of people. A corollary to that is the fact that in addition to becoming better at hiding their activity on any specific platform, they've distributed activity across multiple platforms and increasingly to off-platform websites.

So, in many cases, 2016, 2017 is relatively straightforward to takedown a network of accounts on Facebook and in doing so, the content that they posted goes away, the pages that they run go away. But now, these operations leverage websites that they've registered with a domain register and so, even if you remove the Facebook or social media side of the operation, some part of it persists in the wild. And I think both Alina and Laura mentioned this, but we also see an increased reliance on authentic communities and proxies to enable these types of operations. The most -- the best example of this was the effort by the -- what we assessed to be the IRA to use a network based in Ghana to target the United States. Both to hide the IRA's role in the operation, but also, just to give them one more step to try and obscure what was really happening there.

And then the last piece I wanted to touch on from a trends perspective, we saw this happen in the 2018 mid-term elections and I think Mark, Mark Harvey on the last panel noted that one of the goals of many of these operations is to undermine public confidence in the election itself; to undermine the public confidence in democratic systems and institutions. And we saw an operation in 2018 where the goal was to get people to believe that our political system, political discourse online and the media was wholly controlled by undermined Russian actors. There's a bunch of really interesting case studies that were written on that front.

We call this perception acting internally and what the challenge that it presents to us, both as a platform into our partners and industry and in government, is to counter claims of widespread interference you have to be transparent, which is one of the reason why we publicize all of our takedowns, but you also have to have built the partnerships and the connector tissue between simple society experts like Alina and Laura. Teams like ours, so that when there are extraordinary claims like what we saw in November 2018, that the Russians had undermined all of our public communications, that

we can push back on that and help clarify that the evidence that we have what's actually happening.

So, I'll pause there. Those are some of the main trends that we've been seeing in the wild of influence (phonetic) operations.

Mr. MESEROLE: Thanks David. That was great. I know, Alina, you've got a quick two (inaudible) that you wanted to raise.

MS. POLYAKOVA: Yeah, and I just wanted to put an opinion of what David just said about one of the evolution vectors of these kinds of operations and that is that this kind of ecosystem approach, the cross platform, cross online entity coordination that we're seeing and I think this also highlights the issue that Laura raised that on the other side being on the platform side, or even on the broader internet environment side, we're not seeing the same kind of coordinated response. So, while the actors, the malicious actors, or whatever you want to call State actors, non-State actors, carrying out information influence ops are increasingly spreading in this wide net where you see activities and content reverberating across whether there be websites, YouTube, Instagram, median and even some of these other more subversive -- certain parts of the internet, like, Reddit, or Gab, right, would not see that kind of coordination to respond to those attacks. And to the extent to which that's not really possible, or something that we should discuss, but I think one way that comes out is in the kinds of policies you've seen of the various platforms launched when it comes to content controls where we see a lot of differences in how platforms are responding to misleading and false information. Especially, we've seen this around public health misinformation. So, some content that is prohibited on like, Twitter, is not prohibited on Facebook, or somewhere else. And I think that allows those kinds of loopholes allow for these continued kinds of operations to be carried out even if we're responding in all these other ways.

MR. MERSEROLE: Thanks, Alina. I think that's kind of a natural segue to where I want to steer that conversation next a little bit, which is not just what's going on, but what to do about it, right. I think one of the natural starting points -- I do want to get to the policy side of this question, but -- and the government side, but David, I think you raised the issue of this being a cross platform issue --

MR. AGRANOVICH: Yeah.

MR. MESEROLE: -- so, I'd be curious to hear more about your thoughts on what Facebook is doing and what the sectors as a whole needs to do to address this. And then, obviously,

anything that Facebook internally is doing and kind of addressing the issue of disinformation on their platform and trying to remediate and secure information environment, if you could speak to that a bit, that'd be great.

MR. AGRANOVICH: Yeah, of course. So, I think the -- I think there's four main ways that we've tried to address the trends that I had mentioned at the top. And the first is kind of to Alina's point on content base enforcement being challenging. We've deliberately scoped our policies to focus on a specific set of deceptive behaviors. So, the goal there is to say, look, it doesn't matter who you are. Even if we can't necessarily attribute you to a specific individual or a group, if you're engaged in this core set of deceptive behaviors, then there's enough there for us to take an enforcement action.

That addresses two of the challenges, right. It addresses the foreign-domestic problem because it's agnostic to the location of the actor, and it addresses the challenge around attribution becoming harder because it doesn't mean we have to say that this is the IRA, or this is Iran, or rather, if it's a network what is misleading about aspects of their activity, then we can take some sort of an action.

The second piece is frankly, to the cross platform nature of many of these operations, building partnerships and information sharing throughout the industry is an important pillar of the work to counter these types of operations. And so, there've been a couple of examples. Perhaps the best one is some of our enforcement across Iranian operations where we might find an operation, or one of our partners in industry finds an operation, shares information about that network with us, or we'll share with them and then you'll see another takedown come that platform a week later, or a day later, sometimes at the exact same time.

That type of virtuous cycle of information sharing, whether it's within industry, or with partners in government and civil society can help us kind of get our arms around what's becoming increasingly a multi-platform, multi-societal sector threat. And then, the last piece I wanted to hit on was kind of a deterrence and resilience approach. One of the benefits surrounds government, right, our tools to deal with these types of operations were legislative change, or kind of the traditional levers of State power. You can indict some people, sanction some people, but ultimately, we were responding to a battle space we didn't control.

One of the benefits that we have at a platform like Facebook, is because the challenges occurring

on our platform, we can change aspects of the platform to make the operations less effective. So, we think about this as, if we see an operation that's leveraging an aspect of the platform to hide themselves more effectively, or to reach people more effectively, to think through ways we can change the products to introduce friction. So, our admin location transparency. So, when your page gets over a certain size, the location of your admins becomes public.

Yeah, it has a bunch of other benefits outside of the influence operation space. One of the benefits in this space is, it forces you to either become revealed that you're actually located in country A and not country B, or to take a bunch of steps the type of infrastructure you would need in order to consistently hide from us, where you're actually located, which means, its own right, raise other signals of badness.

And then the second part of that approach of deterrence and resilience is working both on the platform to build more resilience with users, right, to show people more information about what they're interacting with and working with partners to help build resilience in broader society.

The last example that I wanted to note was kind of a -- make it illustrate really well, where we've come from 2017 until now. We, being the broader community that work on these campaigns. Alina, I think at the outset mentioned secondary infection, this operation that the British government just mentioned was potentially linked to some of the trade leaks starting the election. In May, I think it was of 2019, our investigative teams were the first folks in the space to uncover secondary infection and publicly discuss the fact that it existed.

And when we did that, what was interesting was, it was a completely different operation than the things we had seen in 2016 and 2017. In the 2016, 2017 period, the goal was like this broad audience to create personas, designs to directly interact with users. And then, May 2019 period, you had an operation that was far more sophisticated in its operational security; was far more disseminated across multiple platforms; and whose goal seem to be much more about this amplification of targeted leak information, or forged documents, or doctored tweets, or what have you depending on the time we're looking at.

The secondary disclosures that we made were specific to activity on Facebook and some stuff that happened on some other platforms. Where things really became an effective response was

when we had shared information with some of our partners at Graphika, a social media research firm based in New York that does excellent work on a variety of different threat actors. Because when we were able to take what we had shared with them and turn it into an investigation that now spanned over a year that's resulted in several different rounds of disclosures on their part. I think I've identified over 300 websites and platforms that the secondary infection operators were active on. And then, we're able to pull the curtain back on this activity across the entire ecosystem. So, I think that that combination of public disclosures, deep investigations on platforms to uncover what otherwise, not be visible publicly and then partnerships with researchers in civil society to pull all of these threads together from multiple platforms. That gets us to a place where we can really get our arms around some of these complex operations.

MR. MESEROLE: Thanks, David. Laura, I want to turn to you. I think David just described a bit about what Facebook is doing on its platform, and what some of the interesting information sharing that's happening within the private sector. And if you have thoughts on, or response to what David said, it would be great to hear those. But also, I'd be curious for your thoughts on the limitations on kind of self-regulation, or co-regulation, and what needs to happen from a policy perspective to get better focus (phonetic) on this issue.

MS. ROSENBERGER: Yeah, thanks, Chris and thanks, David. So, I think a couple of the pieces that David put on the table are important from a government perspective as well. And a few of the different pieces he laid out there, information sharing, came up whether that's sharing across platforms, whether that's sharing with researchers, but also I think the piece of sharing information with government, especially when it comes to foreign actors is really important.

government entities have unique visibility into the activity of some of our adversaries in cyberspace and the ability to share certain kinds of signatures and information with platforms to be able to look into that information and what may be happening on their platforms can be really important in terms of providing leads and starting to know where to look. I think one of the things that strikes me in this space is that my own view is that I actually don't think outside of limited areas. We want government routing around on social media to monitor what's happening.

There are spaces where that is appropriate, but largely within the U.S. domestically and

particularly, when it comes to really sensitive things like political issues, that is not a space where I think it's appropriate or good for democracy to have government monitoring. But at the end of the day, that's going to require government and the platforms weighing together different kinds of information about what platforms are happening on their systems and what government is seeing happening from foreign actors.

Now, that's going to get at your domestic piece and I grant that, but on the foreign side, I think this is really, really important and we've made progress on that front. It was one of the biggest challenges and completes (phonetic) after 2016. There's been substantial progress on that front. It's like the, unfortunately, in my view, a lot of that sharing remains very at a clock and it's through various informal channels. And I have concerns about the sustainability of that and I have concerns, frankly, about some of the protections that I think need to be written into information sharing mechanisms, protections for privacy, protections for speech, protections for classified information, right. And so, I think that seeing a more formalized and robust wave of sharing information between the government and the private sector also has to be a part of this.

On the question of self-regulation, or co-regulation, I think the regulatory conversation has gotten really (inaudible). And unhelpfully by political conversations about whether platforms are biased in one political direction, whether platforms are silencing, or censoring certain kind of people, or -- and then there's the broad question about 230 and what's happening with that, or breaking up Facebook. And my own view is, all of these are red herrings for the real conversation that we need to be having, right.

Those are not the kind of regulation that I think the vast majority of us in this space are actually talking about. And so, we're having arguments about these kinds of regulatory framework that are not what anybody who's actually an expert on these issues is recommending. What I do think we need to be doing, starts actually with -- if we talk about the guts of the system, right. I think we need to actually start up talking about data as the first point here. And if we look frankly at how, again, the differences between the democratic model and the authoritarian model, a lot of it comes down to data, and who gets access to it, and what happens with it. And how we think about that. And in democracies, certainly, the U.S., we had a very hands-off approach to data. The EU, obviously, led in this space with GDPR, Magnum GDPR is not perfect. It's providing a roadmap, but for certain states that are seeking to

take some action here. But the connotations that need to be happening go way beyond just data protection as it played out in GDPR. We need to be having substantial conversations about that, privacy data, security data governments, right. The ruling out of the EU this week on a privacy show is really significant in a space where the U.S. has not actually been in Egypt (phonetic) substantially.

I know that sounds like it's a different conversation from a topic -- from regulating the platforms around disinformation, but actually, the data feedback views that feed variety, that feed into the ad (inaudible) system, it promotes so much of this content. Data's actually a really big piece of engine system for surfacing disinformation and other kinds of manipulative activity. And so I think that when it comes to regulation, it's less necessarily about the platforms themselves, and regulating their activity, but it's more about thinking again, back to this earlier candidate (phonetic), what is a democratic internet look like, and how do build it and what are the pieces of that. And the data piece for me is absolutely front and center. It's one right now, frankly, where we could be doing so much more with Europe. And we could be really, really working together as democracies in a substantial way and we have been absent. And so, I think that that needs to be sort of top of ticket in terms of what we do there.

The last thing I'll say is, I could -- we could have a long conversation on the policy front, but the one thing I do not think should be up for regulation is, content. I do not believe that with narrower exceptions, right, like terrorism and other kinds of violent extremism, or threats to harm, I do not believe that in a democracy, government has a place in regulating content. And the good news here is when we look at disinformation and the majority of the challenge that we see actually doesn't relate to the content itself. It's the behavior that accompanies the malicious actor spreading it, right. And so, there's lot of content neutral ways of addressing the broader information, manipulation challenge that we see.

Now, under 230 and existing law, platforms do have a right to regulate content and to moderate it. And that is their right, but I do not believe that that is something that we should have democracies beginning to regulate.

MR. MESEROLE: Thanks, Laura. That ties in pretty well with one of the questions that came up, that came in about what kind of -- are there any models elsewhere particularly in Europe for the kinds of data governance that you're talking about, or responses by democracies more generally to this issue.

So, Alina, I'm going to turn it over to you. Are there a kind of policy frameworks that are in line a bit with what Laura described that you're familiar with that would be useful for countering disinformation?

MS. POLYAKOVA: Well, I think Laura's point is just so important because we're talking about disinformation. We started this conversation talking about information influence, is the preferred term here. But once you actually start to think about what do we do about it, we cannot get away from having a much broader discussion on the digital regulatory agenda. And I think the problem with looking at specific ase studies, so what, for example, has Germany been doing, or France been doing? It's been pretty uneven. I would say I don't think anyone has come up with the golden goose when it comes to regulatory environment and what actually works. And I think the big issue has been that the focus has been on "illegal content" and expanding the definition of that beyond, or Laura said, which is things that we all can agree should not be appearing in the public domain, like child pornography, extreme violence, terrorism, things of that nature. But most disinformation doesn't fit into that narrow category, but what we've seen from a lot of European countries, is a desire to push on that specific agenda. To expand the definition of so-called illegal content exactly because the free speech laws that govern most European countries are a much less expansive version of free speech than what the First Amendment allows in the United States.

And so, what I see happening and Laura's point about working together, with democracies so critical here, is, of course, that the digital environment, the internet is not bound by national borders. So, national regulatory frameworks cannot actually address what we're actually talking about. But the problem with where we are today is that we have these kind of hodgepodge regulations and laws coming from all over Europe. Then, we have the European Commission, at the EU level trying to come up with some sort of regulatory agenda that will be unveiled by the end of this year supposedly. And then, we have the United States. So, we have calls here and there for, I think, quite misguided regulatory suggestions like, antitrust is going to be the panacea. It won't be, or do away with 230 is going to be the panacea that saves us. It won't be. None of these silver bullets work because there's isn't a silver bullet. But the problem is that what I see now is this huge riff emerging between Europe, especially where the Commission is going, the European Commission and regulation and where the United States

or might go, depending on what happens in November, I think. But we're not coming together and having some dialogue where we can come to some middle ground or set of understand about what does a digital agenda that is rooted first and foremost in democratic principles actually look like. And there's lot of ideas out there. They've been out there for years.

Laura's written about this, I've written about this, many of you have written about this, but it's just not, we're not getting there and I think that is what we really need to be looking toward, is how do we actually bring to the table the private, the civil society space, governments to have inputs in coming out with a set of regulatory agendas. And there are some efforts in this space that I think will have some (inaudible) results, like the Paris call effort, but, of course, the United States is not a part of that. So, that's a big outlier there. But there isn't one that includes all of the stakeholders and all the governments I mentioned. So, there's some way of punting the question a bit, but I don't want to point to a single example because there really isn't one country getting it right. There's some countries that are getting some things right, but we haven't seen really a comprehensive approach to this.

MR. MESEROLE: Thanks, Alina. I think we've got a little bit of time left, but -- and I want to raise one of the questions and it's in line, I think, with this broader question about democracy and norms around influence operations. One of the things that we've seen this week, learned this week, was that the U.S. has kind of heard the Trump Administration has authorized potential hack-and-leak operations, which are pretty commonly used within disinformation campaigns. It's certainly been used against the U.S. and I would be curious for your thoughts and comments on whether that's something that -- there's one issue of defending the U.S. against these attacks. There's another issue of us offensively using them and I'd be curious of any of your thoughts on whether or not that's in line with what a democracy should be doing.

Alina, I'll go to you first.

MS. POLYAKOVA: Just very quickly. First of all, I'll just say that maybe it's a very controversial (inaudible). I do think we need to be on the offensive when it comes to countering and building resilience against information influence operations. But it doesn't mean that we -- being on the offensive means we do what they do to us and we just do it to them.

And I think that's what's happening here. It's a relatively narrow view, what it means to

get on the offensive. We could do lots of different things. One, we were just talking about is building coherent front and actually seeing a democratic digital domain as a value, not as something that we have to defend, but as something that is a universally desired by most people in the world to have free and open discourse in the online space. And we need to see that as an asset, not something that we're constantly having to kind of defend as like, oh, this is the way to do it and the way that China's doing it. It's not the way to do it.

So, I actually think the -- this often happens with this Administration. Perhaps the intuition is not the incorrect one that we need to get ahead of this game; that we need to get out of this kind of whack-a-mole approach when we are just reacting to every single influence ops that gets thrown at us. But the follow through, I think, is not the right one here.

MR. MESEROLE: Laura, I want to turn to you now. I know you've written really eloquently and really well about what should or shouldn't be in bounds for democracies to do in this kind of environment and so, I'd be curious for your thoughts on that too.

MS. ROSENBERGER: Yeah, all this (inaudible) to a point that Alina made there at the end. And my view is, in general, across as you said of disinformation and some of the questions more broadly about cyber tactics that we have this tendency in these conversation to talk about what it is we're trying to counter, instead of talking about what it is we're trying to achieve, right. And what we're trying to achieve is simply the defeat of a different model, which again, in my view, all these tactics are part of a different information model and a far turning one that our adversaries and competitors are trying to advance.

We have to have something affirmative to offer, right. If we're constantly on the defensive, we are not necessarily either coming up with something to offer, but also, as we mentioned earlier, these are asymmetric tactics and so definitionally, when we are responding in a symmetric way, we are responding in a way that is to our disadvantage and so, what we need to do is develop an affirmative agenda for what we actually want to achieve. And how do we go about doing that. And build from that. And that means a couple of things.

One, we absolutely need to put down a plan (phonetic) of principles front and center in what we do. Not just because it's the right thing from a moral perspective. It is, but not just because of it.

Because in this context between democratic model and authoritarian model, living our values is strategic. We can't win if we don't live our values. So, that's one big piece of it for me.

The other piece of it for me is again, given the asymmetries and the tactics themselves, we're never going to win in a hack-and-leak faceoff, right. In the race to the bottom of who's going to go further and who's going play dirtier, it's definitely not us, right. We're going to lose. We also, the way here, particularly, if we're talking about China, also, even with other -- we are probably the most exposed in terms of a vulnerability of our digital and internet infrastructure. And so, if we start to open this can of worms, we are the ones who are most likely to lose here. So, I have deep concerns if that report from the adversaries (phonetic) is true about the authorization of hack-and-leak campaigns. I think it is exactly the wrong kind of thing for us to be doing.

Now, to Alina's point, that doesn't mean that nothing offensive is on the table. I do think that maybe in this space, we need to get away from the terminology of offense and defense because it's not always clear what's what. But I do think that we do need to be not only affirmative, but very assertive and in one of the papers I recently wrote, my colleague actually came up with a concept, Lindsay Gorman, we co-authored a paper together, and she used a parallel that we talk about in the maritime space of freedom of navigation operation that we use around contested territory. She talked about freedom of information operations where we use truthful information and openness in an offensive way to pierce the closed information bale that our authoritarian competitors are constructing for themselves.

And to use information again, harnessing it with the democratic principles in mind, but in that way. Not as it's recognized because if we recognize information, we lose, democracies lose. But we do need to find a way to harness that information in a way that's consistent with democracy.

MR. MERESOLE: Thank, Laura. I'm cognizant that we're almost out of time, so I want to just have one kind of last lightning round and go around each of you and if there's one takeaway for our audience that's concerned about disinformation in the lead up to the next election, what would you say to our audience about either things they're concerned about, or things that we should be proactively doing? Alina, I'll start with you.

MS. POLYAKOVA: Thanks, Chris. So, just to clarify is the questions in terms of -- who's the we in the question? I just wonder is it like, we, as individuals, or we as governments?

MR. MESEROLE: Well, let's just -- we haven't talked about it as much. I always talk more in the last panel about it, so let's do we, as individuals. If you do want to do governments, feel free to do so, but let's focus on individuals, so if you'd rather go there.

MS. POLYAKOVA: Yeah, this may sound a bit cliché, but I do think that having a critical eye to information is part of citizens' responsibility. I don't think we can really, should I (phonetic), given we live in a digital world where we're all revolve with information at all times. And it may seem that we're asking people to do too much and I certainly think that there is a role that governments and the private sector have to play to not put all the burden on the individual to do the hard leg work of figuring out what is a legitimate story, what is not, when they're being delivered a lot of this content via algorithms that they have no control over. But I do think that, when you're on social media, or in the case of some members of my family, getting email chains, which we never talk about, but email chains are a huge way that some share misleading content. Especially, perhaps, some of my parents' generation. Now, when you receive that content, look at the source before you share it. You don't immediately just share something because of a headline. Don't immediately assume that it is true because it's online and I do think that a lot of people don't take that time -- kind of take a deep breath before they click, or before they click share, before they click like. Even if it's coming from your cousin or someone you know, that in itself doesn't mean it's accurate. And just taking a moment to think about, that's just how it sounds kind of sensationalist and tabloidy to me. A lot of this kind of click bait stuff does. Does this conform with things I've heard in the past from major outlets, but I think the big issue here that it's just a very different conversation. It's not really part of us in the scope of this discussion, is the fact that very much increasingly, we're living in very different realities in our country. And that very much, I think, overlaps with the kind of political polarization, the economic and equalities we're seeing, the kind of racial inequalities we're seeking, that people living in one type of community have a completely different interpretation of events than people living in another type of community. And so, we tend to not see, or not want to believe things that don't conform to our world view. So, I think we could all use a little bit of openness, I think, to understanding others' points of view, even if they may sound really ridiculous to us sometimes and to have a little bit of patience and I'm sorry to say, it sounds a little hippie, but a little bit of kindness for other people instead of judging them immediately for having -- maybe holding ideas that we,

one, know not to be true, or to strongly disagree with. And I think if we just start there, we might go a long way.

MR. MESEROLE: Happiness (phonetic) is always encouraged. Thank you, Alina. David, I'm going to turn to you and then we'll close with Laura.

MR. AGRANOVICH: Sure. Yeah, I think Alina's points are really salient. If there's anything I could add to that, it would be to remember that this problem is a whole of society problem. That it isn't to say that we don't have a responsibility at Facebook, we do. I have a huge responsibility to fix the mistakes of the past and to find these operations and remove them, but we have to be thinking about how to build resilience in every part of our society. That means, tech companies doing their jobs and keeping things safe on their platforms. That means governments sharing information when they need to and using the levers of a state to protect their people. It means civil society continuing to hold us all accountable.

The other thing I would just maybe emphasize is the importance of being careful about speculation around disinformation influence operations around elections. I think there's a proclivity to jump to the assumption that the person that you're disagreeing with on Twitter is a bot, or the candidate that you didn't like won because of a troll operation. Something that stuck with me ever since before I joined Facebook is a really brilliant influence operations researcher named Alicia Wonlis (phonetic) at Carnegie now, who read a piece about how disinformation is a fun house mirror held up to society. And it stuck with me because one of the challenges here is that to solve the influence operations problem as best as one can, you have to actually go after the underlying fractures within a society that are exploited by these campaigns, right. The IRA does not create from whole (inaudible) divisions that they attempt to exploit.

So, the solution here is one in which we do, to Alina's point, need to think about how we can, as individuals, as a society, as a community, work to mend some of the divides that make us vulnerable to these campaigns.

And then maybe the last piece is just that as Alina mentioned, constant vigilance is incredibly important here. That we're asking that you're constantly asking questions about where the information you're seeing is coming from. Seeking out more information before coming to a conclusion.

So, that's all I'd add and I really appreciate the opportunity to talk about this stuff with you.

MR. MESEROLE: Thanks so much, David. Laura over to you.

MS. ROSENBERGER: I'll always think of Alina as a hippie, so I'm glad to have it validated now. I'll be really brief. I think the most important thing that people can do -- I agree with everything that Alina and David laid out, but to me the most important thing that people can do is participate in the democratic process. The goal of these operations is so often to make us doubt the integrity of the process, to weaken our faith in the democracy, to weaken our faith in institutions. And the best retort to that is to double down all those institutions and to participate in whatever way that means for you as an individual, but I think that that's absolutely essential because if we allow democracy to be discredited; if we allow our faith to be shaken, then our adversaries win. That doesn't mean democracy doesn't have problems and that we don't need to address all these challenges, but if we don't participate, then we've already lost the battle.

MR. MESEROLE: I think that's about as good a point to end on as I could imagine, so thank you very much Laura. Thank you to David and Alina as well for joining us. And thank you to our audience for taking part today. It's been a real pleasure to have this conversation. Thank you.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020