Speaker 1:	00:56	[inaudible]. Okay.
Shane Harris:	01:07	I think we're ready to get started here. We'll get everybody come in and take your seats. I appreciate it. Thank you. I'm Shane Harris with the Washington Post and I'm very glad to be moderating. Uh, what is very timely panel. This is a subject that I think we've discussed a few times here at Aspen over the years. Uh, but we're going to try and stay very focused on the future of this very important security topic and what it means for the integrity of our democracy and our election systems. Um, you've got everyone's bios in front of you, so I'm not gonna go through them at length, but I'm going to introduce everyone here, uh, up with me on the stage starting to my immediate right. This is Suzanne Spalding who was the former under secretary of homeland security for national protection and programs directorate. So someone who spent her career in government very much, uh, at the intersection of public and private sector and what the government does to try and protect our critical infrastructure.
Shane Harris:	01:55	Our new name. What's that? Your new name? What's your new name? Cyber, cyber security and infrastructure security agency. There you go. Ali tells you what we do. Government loves acronyms to write a to her right is Tom Burt, who's the corporate vice president for consumer security and trust at Microsoft. Uh, and uh, he's actually going to have the honor of a little bit later revealing if you've had a chance to go out here and vote on the Microsoft, uh, secure elections booth for your favorite fictional president. Tom is going to actually reveal the results of that, um, at the end. Uh, then we have Laura Rosenberger who is a senior fellow and director for the Alliance for securing democracy at the German Marshall Fund of the United States and spent a significant time out of time in government herself with the NSC and working on a lot of big issues as well.
Shane Harris:	02:42	And then of course, Michael Chertoff, who was the former Secretary of homeland security, uh, some wandering, we gotta get fewer secretary now what would you be thinking? So we might get to some of that. This was clearly in your bailiwick. Then. Um, what I want to start with is actually a, a something that special counsel Robert Mueller said back in May, I, he'll be testifying on Wednesday. We suspect a in his only public comments, a following. I think what stands out as the most significant, uh, investigation and probe into Russia's interference in the 2016 election. Uh, he kind of went over in brief, uh, the findings of his report, but there was one place that he emphasized twice. He came back to it. [inaudible] talked

about in the beginning and he talked about it in the end. I'll just read briefly here. You started by saying Russian intelligence officers who were part of the Russian military launched a concerted attack on our political system.

Shane Harris: 03:30 Uh, he then went through to go through talking about the leaking of a stolen DNC emails to wikileaks and the way that, uh, Russia sort of weaponized social media. I liked the idea that Russia was a Facebook customer. That's a really good way of thinking about how they explored that platform. And at the end he went back to this, his, his, his first point and said the central allegation of our indictments, that there were multiple systematic efforts to interfere in our election is an allegation that deserves the attention of every American. This is only public statement and he ends with that, which I think tells you that is what he's trying to get across. So, Mike Chertoff, I want to turn to you with that. Start us off in a big picture here. Three years now since the Russian government began this campaign against the 2016 election, do you think the American people have paid enough attention to this threat?

Michael C: 04:15 Uh, I think there's been a fair amount of attention paid, although it's gotten muddled a little bit because a lot of immediate focus tends to be on, was there collusion? Was there no collusion is somebody gonna get indicted or not indicted. And in a sense that's irrelevant to what we're seeing here. There's no gap. No one serious we can test. And this includes any challenges community that the Russians did in fact, systematically, uh, metal in the election process, both by putting out stolen documents by, I hate to use the word weaponizing, but in a sense weaponizing social media, actually having operatives, you know, agents actually in the u s trying to ferment, uh, social disorders like out of a chapter of the Americans. And I, just to put it in context, this is not new. This has been going on in Europe for at least 15 or 20 years. Um, it's gone on, uh, the, I mean they've hacked into campaigns in the u s in the past. What, what was new in this case was actually releasing things. And just recently there was reporting about a meeting between a top eight to Salvin, usually deputy prime minister of Italy, along with a Russian representing an energy company where they talked about how to covertly finance a shoving his party. So this is a global issue. It's not just a u s issue. And Lord to that,

Shane Harris: 05:37 I can remember covering the leaks of the emails from the DNC and from the Clinton campaign and people involved in the campaign. [inaudible] complaining, you know, furiously to journalists. Why do you keep covering, you know, John

Podesta's risotto recipe and you know, and some more significant things that were in the email and not reminding people that this is actually an information, uh, did operation, this is a propaganda campaign. Reflect on that if you want, cause I know you were sort of somewhere in the front lines there, but talk about like what, what the Russians were trying to do there and what the strategic aim is. Right. Because this wasn't merely about trying to get Donald Trump elected or just turning Hillary Clinton. There are bigger aims that they have here as well.

Laura R: 06:17 Absolutely. And full disclosure, um, that I was Hillary Clinton's foreign policy advisor in 2016 so I lived as change as referenced, uh, there from, uh, a very specific place. Um, you know, watching the weaponization of those hacked hacked materials, which again is secretary Tirdof said, um, is a tactic that we've seen the Russians use in, in Europe, um, over the better part of the past decade. Um, so I, I, two points I'd make on this one is on the strategic piece. I think it's really important for us to bear this in mind, um, because we often tend to focus on this question of, you know, did they change the election result or not? You know, did you know, to Secretary Chertoff's point, it gets conflated at times with the question of collusion. Um, one of the things we know from, from Robert Mueller's report, um, and I would just suggest that if anybody here hasn't read it, please read it.

Laura R: 07:05 Um, I actually think it's sort of an obligation for all of us in a democracy, uh, to understand what's in that, what's in that report. Um, the Russian operations, as far as we know, um, started at least as early as 2014 in the United States. There's actually evidence from some researchers that it started as, as early as 2012 or 2013. Um, and it never stopped after 2016. In fact, the activity on social media actually increased in the aftermath of the election. Um, and, and this is of course, um, as secretary turnoff set a transatlantic problem. Um, so the strategic aims really aren't, you know, we heard yesterday on the, on the panel on Russia about Russia as a declining power. Um, it can't really compete with us, um, you know, on conventional military terms in a way that it would win. But these are spaces, the social media space, the, the cyberspace where Russia believes it has an asymmetric advantage.

Laura R: 07:58 And by the way, other, other authoritarian regimes in particular are using these spaces, um, to the same ends because as democracy is the, the very openness of our information environments, um, is something that, that they can attack and leverage through these tactics. Um, so the goal really at the end

of the day is to weaken us. I mean, it's pretty simple. Um, and it's to divide us as Americans. It's to pit us against each other. We're usually pretty good at doing that on our own and they just throw a little, a little oil on the, on the fire here. Um, but one of the things that worries me is on the question about the, the public awareness piece is actually if you look at public polling in the u s right now on Americans sort of acceptance of whether or not Russia did interfere in the election in 2016.

Laura R: 08:43 What you get actually is an extremely partisan answer. And so about 80% of Democrats will tell you yes, the Russians did. And about 40% of Republicans will tell you yes they did. Um, and so when it comes to building resiliency to actually inoculate against these threats, it's, it's really, um, it's really quite quite problematic. The last point I would just make is on your question over the, the coverage of the hacked emails. Um, and I think that, um, you know, two pieces to this one is a social media and, and the weaponization of social media, we have to bear in mind that it's still part of the broader information ecosystem. And so whether it was the reporting on those weaponized documents that had been released, um, whether it was through inadvertently covering, uh, personas like Louisa Haynes, who was a, uh, purportedly a and African American activist in New York who was very hard on Hillary Clinton and very much a fan of Jill Stein or didn't think people should vote. [inaudible] turns out Louisa Haynes was a Russian troll in St Petersburg. Um, but she was covered in a number of, of news articles, um, in traditional media. Um, so a lot of the broader information environment has been weaponized. And, and I think that for a democracy, we need to have much more sort of thoughtful conversations about what it means to be protecting our democracy, reaffirming trust and reaffirming truth in an information warfare environment, which is basically what we're in.

Shane Harris: 10:02 I'm curious what you all think it was the Russian campaign ultimately successful in sewing this division or were the divisions already there and they were exploited and magnified? And maybe Susie, maybe you want to address, cause I, I struggle with this idea of are we giving the Russians too much credit for, you know, further dividing us where we kind of already there and they just took advantage and nudged us in another [inaudible] in that direction.

Suzanne S: 10:25 So what Putin does is take advantage of weaknesses of our own, making a, he exploits and leans into divisive narratives, uh, and weaknesses that we have created. And, and Laura is exactly right that this is, this did not start on election day and it did not

end, uh, after the election in 2016 the intelligence community in January of 2017 told us this was part of a broad longterm campaign to undermine democracy. This is not just about elections. And that's my big worry is that we're missing the boat. We're missing the boat here. We're, we're, we're, we're so focused on elections, really important. And Lord knows I spent all of 2016 as the under secretary of DHS responsible for cybersecurity and critical infrastructure trying to secure our election infrastructure. Um, very important, but we need to understand this as broader based. And I think in terms of what Putin's objectives are at the end of the day it is to weaken us.

Suzanne S: 11:19 But I think, I actually think it's number one audience for a lot of this is his own population. Uh, I think what Putin like, like all autocratic leaders is his number one goal is to stay in power. And he is terrified of his own population and he doesn't, he doesn't want them to see having lived through the color revolutions, the United States and liberal democracy as something they should long for. So what he wants to portray to them is, is democracy and chaos. The boxer that is corrupt, that is in the tools of the political elite. And so when I got out and in January of 20, knowing that this was part of a broader campaign, I thought, well, I'm going to do a little red teaming here. If I were Putin and I were trying to undermine democracy and uh, and, and confidence in democratic institutions, where would I go next?

Suzanne S: 12:06 What other institution is as dependent as elections are on the public's confidence in the legitimacy of the process to respect the outcome, the justice system. All right. Our courts, our justice system. So I thought, well, I haven't heard anything about that. Maybe for once we can get out ahead of something because I think this is where Putin will go next. But when I started looking, I discovered very quickly that we were not getting out of anything. Putin has in fact, and the Kremlin has in fact been engaged in a coordinated campaign, uh, undermining public trust and confidence in the justice system. And as always, we see it elsewhere before we see it here. The Lisa Case in Germany, which many of you may be familiar with, a young girl of Russian heritage and Germany who claimed she'd been abducted and raped by refugees, by immigrants. Um, very quickly, uh, conceited that she'd made the whole thing up.

Suzanne S: 12:58 She'd spent the night with a friend and was afraid to tell her parents, but Russia media grabbed hold of the original story and ran with it. And, and over a long period of time accused the German authorities of covering this up turned out protesters in the streets. Six months later, we're now in twin falls, Idaho. And

we see the same thing happening. We have seen this. So we put out a report with document the evidence of this, the four narrative frames. But the point is yes, they didn't invent the narrative that judges are politicians who wear robes, but they are really leading into it. And, and they are not the only ones who find fault with the justice system. My friends who are judicial reform advocates are patriots. Their goal is to make us stronger, to cause changes, to make the justice system more perfect, more fair, right, to make us stronger. That is not Putin's goal. And when you tell judges that, when you say [inaudible] [inaudible]

Shane Harris: 13:55 you effectively, you and your colleagues are targets of this campaign, are they surprised to hear that? What do they tell you?

Suzanne S: 14:00 They get it right away. And we have been working for the last year and a half to raise awareness among judges. I'm all over the country speaking to a judicial conferences and training. We've done training for federal judges with the chief justice of the Supreme Court. Uh, introducing the, the subject and, and talking to them about cybersecurity as a means of making sure they don't have the hack and leak of emails and the disruption to the courts that causes a lack of competence, but also understanding disinformation training their communications folks, et Cetera. The judges get it. The lawyers get it. The general public, not so much. Yeah.

Shane Harris: 14:36 Tom, one of the things that you all at Microsoft revealed this week is that it's not just Russia that we kind of have to be concerned about now in terms of what you're seeing and tracking and attacks on political organizations and attempts to interfere. Um, you all come up with a report citing Russia, Iran, North Korea

Tom Burt: 14:52 having launched nearly 800 cyber attacks against political organizations over the past year. The vast majority of them targeting groups based in the u s tell us what you're finding here and, and, and, and what you think is hearkens to, was we're looking forward to the 2020 election and is this really something that other countries have learned from what Russia did and now they want to adopt it to? So let me be clear about the, the information that we, um, uh, when public with a couple of days ago. Um, we have, we've notified almost 10,000 customers that they've been under attack by a nation state activity group just in the past year. And when you stack rank those activity groups by their country of operation and by the volume of notifications that we did, the number one, um, uh, volume are activity

groups operating out of Iran. Number two was group operating out of North Korea and number three were two operating out of, out of Russia.

Tom Burt: 15:48 And I get asked a lot what about China? Yes, we see activity there as well. But in terms of volume, um, of attacks relative to our customer base, we don't see them as active as those activity groups in those other countries. Now that's not politically focused. That's all nation state attacks across all of our customers. And what we saw with Iran for example, is an incredible increase in spike in activity. Once the United States announced it was withdrawing from the nuclear treaty, um, we see a significant increase in activity there with North Korea. We saw a significant increase in activity as the, um, the nuclear discussions were ongoing and, and the targets that these organizations go after were, you know, somewhat predictably, um, people involved in the policy issues there. The other thing we talked about though, where the number of notifications we've done with our account guard service, so that's a service, a free service we launched as part of our defending democracy program, um, just 10 months ago.

Tom Burt: 16:48 And, um, that service enables campaigns, campaign committees, but also NGOs think tanks and academics who are closely associated with the account, with the electoral process to participate. Um, and we've expanded it from the United States to now 26 countries, 10 months. We've got 56,000 accounts that have signed up for the account guard service. We've trained a thousand people globally on how to operate their campaigns in the most secure way. Despite all of that, in 10 months, we've notified 781 different accounts that they've been under attack. Um, most of the, the, the slight majority of those have been, uh, radian based actors and second have been Russian based actors. But what's interesting there is that because we include NGOs think tanks and academics within that zone of, of politically influential organizations, the attacks that are coming from Iranian actors are not necessarily in any way associated with trying to hack our democratic process.

Tom Burt: 17:49 That what we see there are just a subset of the same group we see among the 10,000 largely looking at oil and gas organizations in the Middle East, energy organizations in the Middle East and multinationals that is largely their, their interest. Let's look at the Russian, um, actors, however, who continued to be very active. And there we see a pattern of engagement that looks an awful lot like the same pattern of engagement we saw in 2016 in 2018 in France and European parliamentary elections really with almost every significant

election cycle since 2016 you've seen the initial effort being to infiltrate NGOs, academics and think tanks likely to be influential. And that could be part of preparing for a disinflation campaign. It could be part of just getting into a network where you can then launch a phishing attack that's credible against a campaign to increase the trust so that people will click on a document and now they're infiltrated. So what we would say from the data we've seen so far is that we are seeing the early stages of the same kind of pattern of activity by the same actors that we've seen before and we should expect they're going to continue. I think there's often a public perception that the federal government is sort of not

Shane Harris: 19:09 doing anything to protect this. Like it's coming at us like a freight train. We see intelligence officials going up on the hill and warning the Russians are going to repeat the same things they did. We hear, you know, private sector intelligence essentially saying this. But there is a lot going on. I mean at the DHS level with the state's coordinating with FBI according with the intelligence community. Maybe if for my shirt off and Suzanne Spalding, I know you're not in government, but you know how these things coordinate. So what is happening right now? What is sort of the machinery that's going on to try and get ready for 2020 that we should be paying attention to and that people should, uh, uh, you know, be watching.

Michael C: 19:43 I think it's fair to say they're kind of two agencies that are principally involved in this. One is homeland security through um, Shisha which is our dealing with the election officials in the various states and localities. Cob. They've got an information sharing group where they brought together a large number of people to share information about where the threats are and also talk about best practices. Um, there are efforts and Vaughn, they're volunteering Jewish [inaudible], a lot of the local election authorities. We testing the cyber security of their databases and their machinery. Um, and they are beginning the process of trying to educate people, including partnering with, uh, some, uh, nonprofits and advocacy organizations about what this information is and how you can be a critical, uh, evaluator of that kind of information. The other agg obviously is a FBI, which actually takes the lead investigating different information and counter-intelligence, uh, including obviously efforts to subvert the election process.

Michael C: 20:48 Now, one of the challenges is this, you've got a widely distributed, a number of authorities that actually are operationally responsible. In some cases the state secretary of state. In some cases it gets down to the counter you thirties. So

you're trying to bring everybody up to a certain level with different degrees of funding and different degrees of expertise. And I know Congress has appropriated some money, but not enough frankly. Um, in order to make that push to get secure infrastructure, having placed the capability to deal with, um, uh, attacks. Um, I can tell you the former secretary, Jay Johnson and I are, have just joined the advisory board of a, of a company called us cyber dome. Cha Actually nonprofit a five oh one C four, and they're going to offer two campaigns free our cybersecurity advice so that they can raise the level of security [inaudible]

Shane Harris: 21:46 one of the things that I find interesting about where we are right now with all of the work that the federal government is doing is I think that arguably you could listen to some of the rhetoric coming out of the White House and think that this isn't really that big of a threat. And I want to actually share something that was a really revealing anecdote and a piece by my colleague Dustin Volts of the Wall Street Journal this week who reported that there was a meeting this week in Austin, Texas with state election officials and the senior DHS official charged with defending the government's are, are according to the government's work, uh, was they're talking to state elections officials and he was really defending what DHS is doing exactly what you're describing and saying, look, we've, we're, we've got all this machinery moving. Uh, and then the, uh, the Vermont director of elections spoke up and said, yes, that that was true, but that president Trump quote is playing the biggest role right now in the public perception that nothing is being done here.

Shane Harris: 22:33 Uh, he cited footage of the president meeting with Vladimir Putin and given what he called his sarcastic finger wave, telling him don't metal on the elections and the perception, not only that this isn't really a big deal, but obviously the prison has talked about the Russia hoax sort of implying that, uh, you know, maybe there wasn't even really an intervention. And if there wasn't, certainly didn't have any effect on the Heloc, on the outcome of the election. I mean it seems like the president is a headwind right now to what the government is trying to do and it's certainly not playing the role of educator in chief. If I can jump in on this one. You know, I think one of the challenges we have as as a nation is that once we saw what was happening in 2016 so much of the focus has been on, you know, who was involved, who's to blame, what's the problem?

Shane Harris: 23:16 I think we understand the scope of the problem quite well. And what we really need to do is pivot to solutions, um, and put the

energy that's gone into did it really happen and what was the effect of what was done and change that into, um, as much energy going into how do we find solutions. And I see that happening. I see that we meet with, I knew I was going to knock that over. [inaudible] um, we see it happening with, um, you know, the, the discussions we have with the officials at DHS and elsewhere in government

Tom Burt: 23:46 where there is a lot of focus at the federal level. But that focus also has to be at the state and local level. And one of the things we have to do, I think, and it's part of what we're trying to do, I'm with our defending democracy program is say there are things that in the private sector we can bring to bear in the public sector we can bring to bear, but we should all be focused on what can we do to make things better. So for example, just in terms of people being confident in the vote itself because we've seen reported that as many as I think 21 states were attacked by the Russians in the 2016 cycle, nobody has any evidence that the vote was actually affected. But you want voters to go to the polls knowing that their vote is going to count and have trust in that system.

Tom Burt: 24:28 And that's why we'd done the election guard thing, which is we developed this technology that we're donating for free to the community that actually enables a voter to confirm that their vote got counted and alerts election officials in the media and third party watchdogs all run technology to confirm that the vote got counted and was correct and it's going to be more secure than the vote has ever been before. Um, that's just a solution. We're contributing that as part of our responsibility to, you know, helping to secure our democracy. We work in trying to help secure or a number of people now and it's great that it's not just us, but across the private and public sector working to help campaigns operate in a secure way, secure their communications, secure their collaboration, and we need that same focus on the disinformation campaigns. You know, we're working with a number of people to try to, um, and to try to, uh, finance efforts to do technological solutions to disinformation.

Tom Burt: 25:27 But it's an enormously complex problem that needs a lot of focus. And that's a place where I think increasing coordination between the public and private sector much more than we have even today is going to be necessary where the focus is not on blaming but on solving issues. Let me go on to come to Laura in a second, but I also, I wonder though, I think that that's all correct and this is clearly happening, but at the same time, if you have a whole of government approach, you need the head

of government to be bought into it. I mean, I imagine, imagine if on September 12th, 2001 President Bush had come out and said, yeah, well I'm not really sure this was international terrorism. I mean, you know, yes, this attack happened, but I don't know if we can be so clear about who now who did this. And then you had somehow like a military and homeland security response trying to work without the president being bought into it. I mean, it seems like not only is it rhetorically important, but when you have someone who's also casting doubt on it, like I said, it's that headwind. I mean is are we, is that a key piece that we're missing here for a real whole of government approach?

Laura R: 26:23

Yeah, I'm glad you mentioned the nine 11 parallel here, which as I've looked at the forensics of what happened over the past few years on the Russian attacks, on our democracy, there's actually a lot of similarities to the failures that led up to, um, you know, not detecting the nine 11 attacks in advance. Um, not being able to respond effectively. Um, particularly in terms of information sharing, um, gaps within government, um, authorities, gaps within government who's responsible for things. A lot of these issues fall in the gaps and seams in our bureaucracy. Um, I know sometimes this can sound like, you know, Washington sort of bureaucratic speak, but in the interagency process in Washington, if nobody's responsible for something, if it doesn't have a home, it falls on the floor. You know, it just falls right between the scenes. And I think that's what we have with this problem, number one.

Laura R: 27:15

Number two, you know, secretary tirdof mentioned, you know, for instance, the, the recent, um, reporting on the Russians with uh, attempting to finance Mateo and these party in Italy. Um, there's a wide range of tools that the Russians and others use to attack our democracy. They're used in combination with one another. If we're not seeing the whole threat surface together, we're missing part of the picture. And that's another reason why coordination is so important. And it is one of the reasons that I am concerned by what we continue to hear. Um, out of the, out of the president. Um, you know, we don't yet see the NSC, um, playing an interagency coordination role on this issue set in the way I think is absolutely necessary. We do see good efforts being made. I'd actually like to highlight one that was just announced this morning. Um, uh, the director of National Intelligence, Dan Coats announced the creation of an election threats executive at DNI who will report to him, um, has tasked every part of the intelligence community that works on election security issues to appoint somebody who's the senior lead and is creating a task force within.

Laura R:	28:16	This is the kind of thing that we need at the broader governmental level and not just focused on elections but steps in the right direction. But these coordination gaps are, are really, really problematic and it has to come from the White House. Um, it is the interagency coordinator in our system and we don't, we don't have that. The last two pieces I would just make on the, the concerns about the sort of messaging from the top, um, one is that, um, deterrence matters. Um, and uh, you know, anybody who's studied deterrents knows that it requires capability and credibility. And right now I'm, I don't hear credible, um, messaging coming out that there will be consequences for this kind of activity if it occurs again and it's already occurring again. Um, so we have a, a sort of deterrence problem and as other actors are engaging in these behaviors, we see Iran, Saudi Arabia for instance, engaging in some pretty sophisticated information operations, not aimed at elections but aimed at other parts of our political discourse. Um, so you're, you're getting more and more actors in this space. Um, so deterrence failures there. And then the last Pete is pieces what I mentioned earlier, this resiliency piece and it relates back to what Suzanne was rightly talking about, right? These institutions in our democracy that are based on people's trust. Um, and, and so we really need to ensure that the American people do believe that our election systems are, are, uh, credible. That there is integrity in the outcome of the elections that other institutions, democracy are sound.
Suzanne S:	29:42	And when we have, I'm messaging to the contrary or that leaves questions about that, um, it really, really just makes the attack surface actually that much more vulnerable.
Michael C:	29:51	Let me, let me ask something because, um, I, I'm afraid we take two narrower lens. We talk about this in terms of what goes down online. There was another story I was in today, I think it was Reuters that a Russian oligarch, uh, in London, um, is quite close to one of the candidates for prime minister and the conservative side. And, uh, although he's pitched himself as a dissident, apparently in conversations with the reporter, he's actually bragged about the fact that he's close with, uh, Patricia who's the current national security advisor that he used to work with the Russian Defense Ministry. And he's in there trying to help one of the candidates. There's a whole money laundering issue, um, that's involved here as well. And one thing that we ought to do, not, not just for elections but more generally is have a lot more transparency about beneficial ownership and the movement of money because that is infusing, uh, misbehavior all over the west.

Suzanne S:	30:50	Yeah. So I will use that as an opening to plug my colleagues. I plugged my report beyond the ballot, but my colleague, Heather Conley at CSCS, who's done the Kremlin playbook and just came out with the Kremlin playbook to about the enablers that talks about the ways in which, uh, Russia is achieving effectively state capture, um, but also all kinds of interference in elections. And, and I think to pick up on Laura's point, it's, it really is important I think for us to understand this is not just about choosing a winner, uh, in the, in our elections. Uh, the reason that undermining confidence in our democratic institutions weakens us is that, and what Putin is trying to do was captured very well in the Hashtag that they really pushed in the run up to the midterms Hashtag walk away, right? They are trying to convince a significant segment of our population that democracy is broken, that our institutions are irrevocably broken.
Suzanne S:	31:48	Mike is Right. It's not just online, uh, a r t, which was conveniently shortened from Russia today, uh, state sponsored, uh, television and online media program has a weekly program called America's lawyer. It's hosted by an American trial attorney. And every week they tell you how irrevocably broken and corrupt our justice system is. Here's my worry with undermining the credibility of the courts and the legitimacy of the courts. We are asking our courts right now to save the democracy to save our republic, right? We are asking them to resolve constitutional clash between the Congress and the president. And if the outcome of that court decision, whoever loses, decides that the courts order doesn't need to be complied with. And, and how odd was it to see the attorney general, uh, s seeming to be breathing such a sigh of relief that the president decided to abide by a Supreme Court order on the census? But if, if a decision is made not to comply with an order to hand over tax returns, for example, hypothetically, uh, and a significant segment of the population has been softened with the help of Russian, uh, interference to believe that courts orders can be ignored because they're not credible or legitimate. And then I think we will have a hard time getting, uh, enough Republicans in Congress to stand up. Where are we then? Where is our democracy at that point?
Shane Harris:	33:18	I want to talk briefly before we get some questions about this issue of, of deep fakes. Uh, in the context of disinformation in the kind of, you know, actual fake news that can often spread in social media. Um, this week the DNC actually put out a warning to campaigns and their staff to delete face app, uh, which if you did use it this week, you know, you don't have to raise your hand and confess. Uh, but it was this app that essentially takes your photograph and adds aging and enhancement technology

to it. Just show you what you'll look like in 30 years. It turns out the company is based in St Petersburg, um, which you can connect the dots, but it was enough for the DNC at least to come out and issue a warning to the campaigns. Get this thing off your phones immediately. Don't use it.

Shane Harris: 33:57 When we talk about defects, we think about, you know, someone creating an image of someone saying something you didn't say or even like taking something like doctrine footage of, for instance, Nancy Pelosi to make it look like she was stumbling or ill or had been drinking or something, which then kind of gets amplified. It strikes me that what people are trying to do with that and is not necessarily maybe make people believe a completely different reality, but just create enough doubt and nudge people in a direction of it undermine trust in the media as a purveyor of truth. How much do you all worry about this as being sort of a new innovation that's gonna become a problem? Or are we, are we overreacting to that for that, for the next election cycle? We'd like to take it.

Michael C: 34:34 Well, I will, I mean, um, and I, I'm co-chairing this transient Lana Commission on election integrity with Andrews Rasmussen and we're looking at are there technological solutions to this? So, I mean I think it's an issue because to the extent you get to the point where you have really accurate, completely fabricated or audio and video, uh, it does create a tension between what you see with your own eyes and what reality may be. Um, and I'm particularly concerned that the news media be able to accurately distinguish between what is the defect and what is real. Because the worst thing is to have the media then pick up on it and propagate it. That being said, before we press the panic button, a Photoshop has been around for a long time and that's an easy way to alter photos and the Republican's survived because eventually what's happened is we've gotten in you're to the fact that there may be manipulation of at least a still photographs, but I think the larger issue, um, however this plays out is a systematic erosion of the ability ever to get ground truth. And if I'm Putin, you know, it's not my, my end game is not this candidate versus that you just to make it show difficult for the public to understand or to trust what ground truth is that basically you have no ability to get unity of effort and people just check out. So to me this is a, we need to take it seriously, but I wouldn't panic. Yup. Yeah. Lauren, oh, sorry. Then Suzanne. Yeah,

Laura R: 36:09 I'd broadly echo that. But I would say too is there's other technologies that are coming down off the line that are equally worrying to me. Um, the face that, for example is a, is an

interesting one. There's a lot of disagreement within the security community, the moment about how big of a threat that, that, um, particular app actually is. But it speaks to I think a broader sort of awareness or lack thereof among the public about what is happening with our data, what is happening with our information and what is it being used for. Um, and in an environment where we have technological change happening very quickly and at a moment in time when we have sort of rising authoritarian regimes and cracks in democracies, I think that this introduces, um, certain broad dynamics of the geopolitical level that have impact on our lives. That we haven't fully wrapped our heads around.

Laura R: 36:58

Um, your questions about how will different regimes use data that's in their hands, right. China for instance, um, has been a topic of a lot of conversation because of its legal regime that basically allows its ministry of state security to gain access to, to anything that that is in the hands of a, of a Chinese company. Um, a lot of concerns around that. I don't think that we have yet had the conversations necessary in our public square, in Congress around these issues. The, the hearings and in Congress, um, around social media, um, and, and the online space, uh, tend to leave a lot to be desired in terms of the level of discourse. Um, but I think there are really significant implications to this. You know, the, the growing amount of information online, the growing amount of, um, of information that is governing sort of how we see our daily lives, um, in ways that is, is being, um, you know, with algorithms ordering things for people.

Laura R: 37:54

Um, you know, I just don't think that we, we've really had the conversations necessary to wrap our heads around this. So I think on the, on the examples you used in the deep fakes and uh, misinformation generally and, uh, hate speech out there, right. My sense is that Russia at least is practicing Jujitsu. All right. They are trying to use our strengths against us. The First Amendment right, protection of free speech, robust marketplace of ideas, a robust, even a robust though often dysfunctional online dialogue. Uh, I really believe those are strengths that we have and that Russia is trying to get us to unilaterally

Suzanne S: 38:36

a by restricting that. And I think what we need to do is to, is to reinforce our strength is to fight not on the ground that Russia wants us to fight on, but to lean into our strength, which is transparency, right? If you think about where, where do we have a comparative advantage? The last panel talked about some of our comparative advantages, but one of our greatest

		comparative advantages that the United States has is our ability to operate in a transparent world. Think about that compared to our adversaries, Russia, China, North Korea, Iran, who's best prepared to deal with the transparent world that is coming at us full steam ahead. The shelf life of secrets is vanishingly short. Whoever figures out how to operate in a world with fewer secrets is going to prevail. I call it training to fight in the light. If you train to fight in the dark, you could turn off the light and have the advantage over your adversary. We need to train to fight in the light. We need to use transparency as our first default go to weapon against this
Tom Burt:	39:36	in the interest of time and because Andrew Mitchell and ambassador rice are here and we have to come up, I'm going to take two questions at the same time from the audience and briefly we'll get answers. You right here, male and then uh, anybody on this site. And then you over there.
Speaker 1:	39:48	Okay.
Tom Burt:	39:50	We'll keep our responses brief. And then Tom's gonna tell us who, who our next fictional president is.
Speaker 1:	39:54	[inaudible]
Audience Member:	39:57	thank you very much. I'm Deborah Haynes from Sky News in the UK. Isn't it true that while obviously Russia is a master at disinformation that actually in our democracy is there are plenty of right wing parties that are using these disinformation tools because they see that as a way to, you know, dog whistle politics with pup support create division. We've seen that in the European Parliament elections. Yes, there was evidence there of Russian interference, but there was also a lot of evidence of rightwing parties using those same tools. And you've got a US president that has a quite loose relationship with the truth in order to get support. How do we make truth appealing? Cause often the fight with this information is that the disinformation is actually more sexy. And so, um, you know, t to fight back and to make truth matter, uh, it seems to be the only way to protect our democracy. How do we make that happen?
Suzanne S:	40:46	Okay. And then the question from over here, hi Aaron Waters, we're more DHS communications. Ah, wanted to get back to basics a little bit and talk about the public engagement and an understanding and their role in cybersecurity. How um, can you talk a little bit about that? It seems we've gotten a little bit far from, from those basics and talking about cyber hygiene in the

like, um, and how that, you know, is impacted by it by all of this that we've been talking about today.

Tom Burt: 41:08 Important questions we ask to be brief. So who wants to take the first one? Making truth matter again. Oh, well I was actually gonna go to this day. You can take a second one then in terms of what the public can do. We actually published a really interesting blog on this just a couple of weeks ago where we looked at a vast quantity of data about how people get attacked and whether passwords matter and the prior panel was talking about the importance of moving to biometrics. That's true. Eventually we'll get to places where using biometrics as your authentication is going be widespread, but we're not there yet. What everybody can do today and our analysis shows that it'll eliminate over 99% of all attacks on consumers and enterprises is turn on two factor authentication on every account you have. And people have been preaching that for a long time. But when you survey what both consumers and enterprises actually do, people aren't doing it. So there's a basic cyber

Michael C: 41:58 for hygiene thing you can do that will really protect you and protect your company and protect your organization. Everybody should go do it. Great. Any thoughts on that? Probably the first, ah, you're right. It's uh, you're, we're seeing our indigenous political groups, particularly extreme right wing groups, gleefully adopting the same techniques to kind of propagate your own views. Um, and I think there are two ways to deal with this and neither of them are magic bullets. One is the platforms themselves, social media platforms, but also the mainstream media often operate on the business model that you've got to get eyeballs and that means you've got to lead with something startling. And in fact, there are algorithms that if you under short changing, if you look for particular topic, it will then suggest other topics that are more extreme versions of that. We need to have everybody in the media start to look at that business model and begin to correct for that. And then the second thing is you got to educate people. I mean, at the end of the day, when you get these techniques there, people have to be skeptical. And that means you've got to start educating people about critical thinking in schools, uh, using our civic institutions, even our religious leaders. And it's not a fast, instantaneous solution, but it is something that we need to invest in.

Suzanne S: 43:12 Absolutely. We need to start seeing civics education as a national security imperative. [inaudible] Bingo. Okay. Tom, very quickly give us the results very quickly. The results, the results [inaudible] been funded.

Tom Burt:	43:24	No. Um, it was very interesting as we did the demonstrations that we walk people through the, the, the fictional presidential results, every voter was convinced that the answer was quite obvious. There was only one obvious choice, but in fact there were more than one. I'm finishing second with 28% of the vote was Selina Meyer, and perhaps she'll be a candidate for the ticket. Um, finishing first was a Josiah Bartlett with 39% of the vote. Um, so she's the veep.
Suzanne S:	43:54	All right. Thank you all for your attention. Thanks to our great panel.
Speaker 1:	43:57	Okay.
Suzanne S:	44:01	Please stay in your seat. We are quickly going to change this stage so we have the full amount of time with Andrea Mitchell and Susan Rice. I know it's not something.