[Music]

Unidentified male: You are listening to a podcast from the Stanford Center for International Security and Cooperation.

Suzanne Spaulding: Thank you very much. It's such a treat to be here despite the weather. I will confess that when Amy and I first spoke some months ago and she suggested that, you know, I think about whether I might like to come out for a week as a visiting fellow, I was picturing that beautiful April day when I was here with President Obama. I don't know how many of you were able to participate in that event, but that was the weather that I was picturing. But I was also thinking about that day as I made the decision to carve out a week and come here because I remembered the reason that the President came to Stanford. It was, as you will recall, really an unusual, if not unprecedented move for a President of the United States to come to the West Coast to this University and to meet particularly with a tech company, right, in the private sector, to make the trek out here to meet with the tech industry out here, innovation. It was because he recognized the important role that this university particularly and others in the region, but Stanford in particular plays in advancing important policy imperatives, particularly in cyber security, both in terms of intellectual scholarship, but also in training the technical and policy and translators that we need to go forward.

But it was also again that meeting with the private sector here. It was a recognition of how badly we need in Washington and in government the innovation and the different kind of thinking that the private sector brings. We have never needed both of those, both the intellectual scholarship on policy and the innovation that the private sector can contribute than we do now. We have never needed it more than we do now with the threat that I wanted to spend a little bit of time talking about today.

So I thought what I would do is to start by talking a bit about what we did at the Department of Homeland Security in the run up to the election and our role in the election security in that year of 2016. Then I will talk to you a little bit about what I have been doing since noon n Jnauary 20, 2016 and what the project that I am engaged in now. So sort of started with looking at adversary threats to fundamental Democratic institutions writ large and now doing a deep dive on adversary threats to public confidence in the American judicial system. So that is kind of what I want to walk through a bit today.

So going back to the spring of 2016 when we really started focusing on the security of the election coming up. I had crated when I went to DHS in 2011 shortly after I arrived, I created an Office of Cyber and Infrastructure Analysis. As Amy said, I was in the incredibly fortunate position of leading and organization that had both physical and cyber security in its bailiwick, responsibility, mission set, which I think for any of you who may be coming tomorrow to hear me talk more specifically about risk management and cyber security, you will hear this is a constant theme of mine. I think it's really important to take this holistic approach to protecting critical infrastructure

from cyber and physical and not put ourselves in a cyber and technology stovepipe when we are talking about cyber security.

But the name is horrible, National Protection Programs Director. I started from day one trying to get the name changed to something that would tell you what we do. I believe the House has passed and I believe the Senate at the end of last week passed the legislation to change the name to Cyber Screening Infrastructure Security Agency. So that's good news.

But we started out and had this Office of Cyber and Infrastructure Analysis, which has this holistic look at consequences, particularly, look at what should be worried about. What's the whole gamut of election infrastructure. We will try to get our arms around that and figure out how. This is the risk management approach that we would advise to the private sector and to my colleagues across government, right. Start by assessing your risk and really emphasize consequences. So they came back to me with a nice paper talking about starting with voter registration databases through the formulation of the ballot in states, the secretaries of state's offices, and the elector's offices, and the loading of those ballots into voting machines, and the security around the voting machines, and then the tabulation process, and the transfer of those tabulated votes, and then the announcement, all the way through to broadcast media announcement of early vote returns of them.

So as we looked at that, we thought about where should be really focus, how do we prioritize our efforts here. The assessment was that it would be really very difficult to change the outcome of a national election by changing vote totals in election voting election machines. Not because it's very hard to—you have an election voting machine in front of you to hack into that or to tamper with it, but because the states have for many years developed a number of protocols and security arrangements to keep malicious actors from getting physical access to those voting machines. They also use a wide variety of kinds of voting machines. They use a variety of vendors so the machine are all a little different. So if you had access to one, it doesn't mean that you udnrestand how to get into all of them. It also that sort of biodiversity as I refer to it makes it hard to propagate. I mean first of all, the states have clear protocols that these machines are not connected to the internet. But even if they were, it makes it harder to propagate malicious elements throughout all of the voting machines, etc. So our conclusion was to make a difference on a national scale would be very difficult, extremely difficult.

However, it was clear that the voter registration databases were not so secure. As we went into the summer through the spring and into the summer, we began to see, in fact, malicious activity at, that appeared to be targeting voter registration databases. Why were we concerned about that? We were concerned about the ability to cause disruption on election day, right. So if you could get in and mess with the integrity of that data in any number of ways, you could remove a bunch of names. You could change voting, polling places for individuals. You could mess with the spellings of their names. You

could do all kinds of things so that when people showed up on election day, things did not go smoothly. We have already seen what can happen when lines get really long on election day and the type of issues that can bring.

So we were very concerned that they could do something that would reduce pubic confidence in the credibility, the legitimacy, the outcome of the election. We reached out to the states, the secretaries of states are the ones who run the elections in each of the states, to let them know of our concerns, to let them know that we were seeing adversary activity, that in some states and that we wanted to make sure they knew what resources we could bring to bear to assist them and try to work with them to make sure that we were doing everything we could to make sure those elections were secure.

The states, not surprisingly, pushed back. They have always been nervous about a federal takeover of elections. This is one of the things that is most sacred to them. States run elections. That was critically important to them. They did not really, they were not particularly interested in having the federal government come in. We did, ultimately, after a lot of meetings and conversations and discussion to get most of the states to agree to accept the services we were offering for free, particularly the remote scanning of their public facing internet system so that we could tell them if we were seeing things and what we were seeing and give them early warning.

But one of the things that we realized early on is this really is, this election infrastructure meets our definition of critical infrastructure, which is assets, systems, or networks, whether physical or virtual, the disruption of which could have a debilitating impact on economic security, national security, or public health and safety. Our assessment was that if you really could disrupt election infrastructure, you could have a significant impact, a debilitating impact on our national security. It was clear that a foreign adversary could come in and mess with that fundamental pillar of our democracy.

So then we started what many of you may have read about in the press, but turned out to be a very contentious conversation with the states around whether election infrastructure was critical infrastructure and what that meant. At the end of the day, really, I will say over the objections of many of the states. We did make, the Secretary did make a public statement that this is critical infrastructure. Election infrastructure is critical infrastructure meets the definition. The practical implication of that was simply that we could then clearly prioritize it within DHS in terms of the attention that we could give it. It provides the basis for an institutionalized framework structures, sector coordinating councils for the private sector vendors and all the private sector folks involved in election including the broadcast media, etc., and the government coordinating council. That could include state government and federal government entities to really come to work and developing a strategy and a plan for protecting elections going forward. There are some special legal protections for critical infrastructure, particularly for information you share with the government about your vulnerabilities. We can't share it with anyone else. We have to protect it. It's not discoverable, etc. Those were

available. Then finally, sanctions that can be imposed on attempts to tamper with critical infrastructure. So that was really our focus. We set up a war room on election day and we were in touch with the states. We were tracking carefully how things went on election day. We had talked with the broadcast folks and assured that they had secure ways and redundant ways of getting the tabulations, etc.

So we get through election day without any major incidents. We sort of paused to catch our breath. Over those succeeding months, lots of discussions about the Russians tried to meddle in our elections. Now what do we do about it, right. As we have those conversations, you know, growing across the government recognition that this was not just about elections.

[A/V issues]

The DNI came out with their assessment and made it very clear in this public unclassified document, so I am going to read a couple of quotes since you can't read them. "Russian efforts to influence the 2016 U.S. presidential election represents the most recent expression of Moscow's longstanding desire to undermine the U.S. led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations. We assess Russian President Vladimir Putin ordered and influenced campaign in 2016 aimed at the U.S. presidential election. Russia's goals were to undermine public faith in the U.S. democratic process." So that was a very straightforward, clear intelligence assessment as of January 6, 2017.

So when I got up on January 20, 2017, and I had an opportunity to be home and watch the cable news all day, which was a big mistake, and watch what was going on on the Hill and the conversations that were taking place, I became increasingly frustrated. A, that the focus was all on the elections, most of it looking backwards, right, which we had to understand what happened. That's a really important activity that is being undertaken. But those who were thinking ahead were thinking about the midterms in 2018 and the next election of 2020. I was really discouraged that there wasn't a greater recognition that this was not just about elections. This was about—this was the elections were one aspect of this long-term campaign to undermine a democracy and to weaken us, right, to weaken our allegiances, to sow discord and dissensions and chaos in the system. I think most importantly to undermine the appeal of democracy primarily for his own population.

One of the things that I have learned over the years that I have been looking at our foreign adversaries and cyber security, it's not just cyber security, everything they do, bottom line, what is the most important thing to them? Regime preservation. For everyone, whether it's Russian, China, North Korea, Iran, at the end of the day, that is their most important agenda is staying in power. For Putin that means, and he watched, right. He was there for the fall of the Wall and the dissolution of the Soviet Union, which he thinks was the most horrible thing to happen in the history of Russia. Most of

you who know the history of Russia, that's a pretty dramatic statement. They've had some horrors. He watched what happened to Suddam Hussein. He watched through the Arab Spring. He saw what happened Qaddafi. So he, aspect was to show that democracy isn't this shining city on a hill that is wonderfully operating system that is efficient and all of the things that folks think of when they think about democracy and that we have been trying to promote around the world. But that instead it is a flawed system, that it's corrupt, that it's messy, that produces crazy results, and that can't be trusted.

So that, if you recognize or think that that is a key objective of Vladimir Putin and the Russian government, then I start to think okay so what would I do? If I were Putin and I wanted to undermine democracy, I wouldn't stop with elections, right. I would go after the fundamental institutions of democracy. I would go after the courts, the Congress, the President, the media and undermine public confidence in those institutions.

So I started talking with John Hamre at the Center for Strategic and International Studies. He was immediately on board. A colleague there, Heather Conley had and her team had researched and published *The Kremlin Playbook*, which I would recommend to all of you, which is a detailed look at what Russia has done in Eastern and Central Europe. Their emphasis is really on the way Russia has used economic influence and sort of traditional corruption to achieve in a number of instances state captions of these Easter and Central European countries, but it has also included information operations and setting up of fake affinity groups and working with and finding other affinity groups, so a whole kind of influence operation.

So we pulled together a round table, a bipartisan round table of national security and Russia and media experts to talk about, because my other frustration aside from the fact that it was all focused on elections was that people were not talking about what we needed to do to counter it. Every, all of the focus was on these invistgations that were going to take place and the sense was that we let the investigation play out. When they are done, they will come to us with recommendations and then we will begin to move forward assuming that we have gotten buy in from the people in the federal government that this is really a problem and needs to get addressed. My sense was there here right now, they are continuing to do the things that they were doing, and we need to be thinking about and developing strategies, taking action right now to counter these activities.

So we had a round table in June. We had a great discussion. Summarized that discussion. Had a second-round table several months later and produced a report, which is now on the CSI website on countering adversary threats to fundamental democratic institutions. So I will walk through just sort of the highlights of that report.

So it starts by summarizing the information in *The Kremlin Playbook.* It talks about the ways in which technology is now being used, obviously, to advance the kinds of operations and achieve a directness right into your inbox and on

your Facebook feeds and social media interactions and a scale that really it has not been achieved in the things that we had looked at in Eastern and Central Europe. I am sure you have seen some of these statistics yourself, but the Facebook testimony in front of the Hill, particularly in their answers to the questions for the record, 126 million people saw three posts that were from 470 Russian accounts and pages that are affiliated with the Russian internet research agency, which of course is what was Mueller's indictment laid bare. It was the work of this entity within Russia and the internet research agency. So their ability to get their narratives out and again for Russia, it was not so much a positive narrative. This is a distinction I think between Russian and China. China is doing influence operations as well, but for China it's primarily promoting their system. For Putin, it is really about tearing down ours. It's really a scorched earth. That's what you see reflected in the social media. Of course, what we saw and continue to see is interventions on both sides of an issue like, the issues around racial injustice.

So what we know the Russians do is they lean into, they don't create these divisions. They lean into existing divisions. They lean into our own vulnerability. They add fuel to the flames. They exacerbate those. So we saw interventions that were pushing people on both sides of the Black Lives Matter issues, for example, issues around racial injustice. We see them very active in the issues around immigration and refugees. I will come back to both of those when I talk about the deep dive into the judicial system, because if you can imagine they are particularly relevant in those areas.

So but the most important conclusion of this bipartisan group that came around the table over the course of 2017 was that we need a national strategy and we need to be acting now. We need the federal government to lead a process that will develop a strategy to counter adversary threats. We say adversary threats and not just Russian threats because we understand that Russia is not the only one engaged in this. So the yare right now the clear and present danger. There are others that are engaged in influence operations and even more will take note of what Russia has achieved and follow suit.

We need a national strategy now which we don't have and at least as of a week ago there had been no interagency policy committees, which is how you start the interagency process to bring a team together for an ITC at the assistant secretary level to begin to talk about what is the problem, what is the challenge, and how are we going to address it, and tee up recommendations that would go up the chain to a deputy's committee and principle's committee meeting. None of that has happened in over here. So this group thought it was very important to go on record and say we really need to be doing this. That national strategy needs to have at least three key elements. We need to look at how do we prevent this from happening, how do we deter this from happening, and how do we reduce the effectiveness of the information operation. So in that is in the deterrence, obviously, there are the sanctions. Congress tried by passing legislation that provided authority for the imposition of additional sanctions, which of course hasn't really been exercised yet.

We were also mindful that as we look at additional kinds of financial leverage that we can impose, there is a sort of cautionary note that you don't want to turn the financial sector into a battle space. Really, we saw in 2011, 2012, there were DDOS attacks on the banks from, attributed to Iran, and believed to be in retaliation for the role the banks played in implementing sanctions imposed by the government on Iran. So this is not an idle concern. Having said that, we need to be able to use the significant financial leverage that we have as a country to deter bad behavior. We need to look at the range of options that we have including pointing out the weaknesses, for example, in Putin's regime. There is a lot of concern about escalatory activities, but again I think you can't allow yourself to be paralyzed by concerns about escalation. You need to be mindful.

Prevention is going to be largely, frankly, a task for the technology companies, perhaps with assistance from the government, particularly funding research. It's going to be efforts to help the state and local government protect their systems, again, with I think financial resources grants, etc., in addition to the kind of technical help that we have been offering and continue to offer. We are getting the secretaries of state cleared. When I say we, I mean my former we, the Department of Homeland Security. Then reducing the effectiveness, I think, is actually one of the places where we really need, again, we are really going to need the innovation and the creative thinking of people like those assembled around this table and in the Hoover Institute and Annie's group, the SESAC because it's very difficult, but I will say that civil society has taken hold of this issue and a lot of work is being done.

That brings us to the last part, which is a recognition that we may not get a national strategy organized by the federal government, just given the politics of this, speaking candidly. So we end with a call for action for a whole of nation approach, to do what we can do now. There, we list, again a number of things. Critically important is education, education of and I will again speak to the judicial project. We are educating judges, court personnel, educating the media, educating the press, educating congress, educating the bar, the lawyers about the nature of the threat that we face, that this is happening. So the people are more aware.

Then we need to provide the tools and the technology so that the people who want to be assured that the information they are getting is not being fed to them by a foreign adversary who is intent is to weaken this country, that we give them a way to do that, that we give them the tools. This is again where some of the social media companies are trying to step up and do a better job first preventing this by stopping by being able to better identify and stop the bots that automatically spreads so much of this, by providing greater transparency. There is legislation in on the Hill that Mark Warner and Amy Klobuchar have put in to require the kind of transparency for ads in social media that we have for political ads on television and on the radio and traditional media. So to provide a kind of transparency that could help those,

again, who want to be helped to be able to determine whether they are accessing legitimate information.

So we put out this report in February. Last fall as we were sort of writing this up, I had another talk with John Hamre. I said I think there are a number of areas where we could do deep dives. I didn't get any farther than the first one on my list, which was the judiciary. He said, "That's it. We've got to do that. No one else is looking at this. We really need to do that." So I will tell you a bit about my concerns with respect to why I think we need to be urgently focusing on the judiciary.

So what we saw in the run up to the election was both cyber enabled information operations and the internet research agency kind of making things up or spreading narratives, right. So we saw doxing, what we call doxing, those of you who do cyber security know what that is. But it's a theft of emails and the weaponization of that information, so leaking those emails in ways that they hope will be damaging. So we need to think about cyber security aspect of this and an information operations aspect of this.

As I thought about what could you do if you wanted to undermine the judiciary, I thought about all of the ways in which you could use cyber intrusions to accomplish that. So go back to the doxing. I don't think Judge Kozinski on the Ninth Circuit is the only judge in the country who looks at pornography. Other embarrassing kinds of emails that you could hack in and get and release. If you wanted to lean into existing narratives, skepticism, right, which is what we know they do, there is a large school of thought out there that judges are just politicians who wear robes. So how could you lean into that narrative? Well, the first thing I thought was I would hack into an elected judge's emails. There are bound to be political. There is going to be all kinds of stuff in there about campaign promises and fundraising, etc. Most Americans don't make distinctions between state elected judges and federal judges appointed for life. So you could do that.

You go back to the things we worry about in cyber security, data confidentiality, data access and data integrity. Think about how those would play out. So data confidentiality, courts have all kinds of sensitive information about people who, domestic abuse situations. They have financial information. They have case management information. So think of that when I tell the judges, just think about all of the ways in which if someone got access to that data and made it public, that could be a real problem.

Data access, we have had DDOS attacks on the courts where the courts have had to sort shut down for a while. The public can't access things that they need to access in the courts, the judicial opinions, etc. That, if you had repeated DDOS attacks, think about what that would do in terms of public confidence in the judiciary.

Then the one that worries me the most, which is the one I think generally speaking is the next crest for cyber security and that is data integrity and reliability. Think about it if someone got in and—and this is again what we worried about in the run up to the election, right. How could you undermine public confidence by corrupting the integrity of that voter registration database? Well, suppose your corrupted the integrity of, for example, release records. Who is supposed to be released from prison, who is not. If you corrupted the integrity of decisions and you could hack in and get an early draft of a decision and publicize that and show that the judge changed their mind so that you undermine this notion that somehow these opinions are handed down from on high and create some doubt in the public's mind about how judges arrive at their opinions. I actually think a little more realism there, a realistic attitude about how judges arrive at their decision, right, would not necessarily be bad, but we are not ready for it, right. So judges need to be ready if that is going to happen. But if you mess with the integrity of the decision, so you have different copies of the decision up to now. Nobody knows which is the official decision of the courts.

So a number of ways in which we talked yesterday about you might use cyber, for example, to attack the physical security of the courts or of the jails. If you had this kind of successful cyber intrusion activity, again repeated in the courts all across the country at the state level and the federal level, how you could begin to undermine public confidence in the courts.

Beyond the cyber enabled, what we are seeing already is the ways in which information operations are being used to undermine public confidence in the courts and respect for the courts and a sense of the legitimacy of the outcomes of the judicial system and the justice system.

So back to 2016, early 2016, some of you might remember what came to be known as the Lisa case. This was in Berlin. Ambassador McFaul could probably tell this story much better than I can. But in Berlin, there was a young 13-year old, Russian heritage girl, who claimed that she had been abducted by immigrants and raped. The authorities ran that to ground and pretty quickly found that that was not an accurate story. That in fact, she had been staying with a friend and this was simply not true. But by then, it had been picked up and amplified and fed into the anti-immigrant fervor. There was a huge pressure on the prosecutor and prosecutors are part of who we are going to be working with as we go forward here because they are right in the line of fire. Huge pressure on the prosecutor to bring these supposed abductors to justice. One of the slides that I would have showed you shows quotes from the Russian foreign minister, Lavrov. I will see if I can fast forward to it. But basically, they, again, fed fanned the flames and accused the German authorities of basically engaged in a cover up and that the prosecutor was engaged in a cover up and this was another example of sort of the corrupt justice system. So that's Berlin.

Fast forward later in 2016 and we are now in Twin Falls, Idaho. Twin Falls, Idaho, for reasons that still aren't entirely clear to me became like one of the

ground zeros for battles over refuges, particularly Syrian refugees. They had been having lots of discussions around the town. There had been a group that had been set up to sort of fight against bringing Syrian refugees into Twin Falls, Idaho. Suddenly, there is an allegation that a young girl was raped at knifepoint by two young Syrian refugees. Once again, the authorities investigated, and they found there were no Syrian refugees involved. There was no knife. It's not clear there was a rape. Something bad happened in the basement of this building, the laundry room of this building with two young boys and a young girl, but it was, again, the stories had been wildly exaggerated to feed into the narrative that you let Syrian refugees come into your town and your children will all be assaulted. Again, the prosecutor was under tremendous pressure fed by social media to prosecute two Syrian refugees for a rape at knifepoint. The judge that ultimately heard the case because of the state court systems and the way juveniles, these were juveniles, are treated could not talk publicly about their sentence, but it did leak out that they did not receive any jail time. At which point again the social media erupted. The judge's picture is posted online by a site called Bare Naked Islam, which is a Russian affiliated social media account with a picture of the judge and a big red arrow, corrupt judge. They later posted his home address.

So again, you begin to see then that moving forward to 2017, as we began to understand more and more about how the Russians had gone about social media influence operations, I remember reading one of the first places where they started organizing in person rallies, you remember that they didn't settle with just simply trying to influence your thinking, but they actually tried to turn people out. In some cases they successfully did for physical rallies. One of the first places they did that was Twin Falls, Idaho. I remember thinking at the time that's really odd, Twin Falls, Idaho. But they knew enough to know that this was, again, a place where there was a fissure that could be exploited and a place where they could add fuel to the flames. They went right after the judicial system.

Again, fast forward to 2017, in the fall of 2017, you may recall that we did see three additional facilities, diplomatic facilities of Russians, a consulate in San Francisco and I can't remember what the other two were. It was these three additional diplomatic facilities in addition to the two that we have ceased in December under the Obama administration. Putin was I think in China at the time and had a press conference. He was quite excited about this. He said, "This is a violation of our property rights and I am going to ask my envoy in the United States to sue in the U.S. courts." His next sentences was "And then we will see how effective this much lauded American justice system is." So I do believe that they have, that this is part of their strategy, that they have our justicial system as a pillar of democracy in their sights. It is clearly implicated in the issues around racial justice. It is clearly implicated in the issues around refugees and immigrants. You think about the courts that are dealing with the various suits around the travel ban, for example. So for tactical reasons around Mueller's investigation and where that might go in the courts at some point, as well as for the broader strategic goal of undermining

our confidence in democracy and the institutions, I think we need to be—and it's one area where we find we might be able to get out ahead of something before we have a huge disaster and we are trying to make up for that.

So we are training federal judges on cyber security and their responsibility as defenders of democracy to step up and do what they cane personally in terms of cyber hygiene, as well as driving their systems to improve their network architecture in the courts all across the country at the federal level and the state level. So my bumper sticker for them is "Defend democracy. Change your password." So I hope that we will, I mean there have been efforts for years to get the court system to improve their cyber security. Judges have, frankly, been one of the biggest stumbling blocks. They don't want to do things differently. So we are trying to do that.

We are working on efforts to educate the groups that I talked about about this threat and what information operations we are seeing. Some of you who have been following the Russian influence operations may be familiar with something called Hamilton 68. Hamilton 58 is a project of the Alliance for Democracy. They have been tracking 600 Russian affiliated social media accounts. They have a running series of bar graphs that show you what are the trending topics, right, what are the things that they are seeing, the Russians trying to push and promote. So I went over to talk to them a couple of weeks ago to talk to them about my concerns that we may be missing data about attacks that are undermining public confidence in the judicial system and asked if they would go back and look at their data through that lens. The following week, their report came out, the security dispatch. Here is what it said. "Russian linked accounts continue their assaults on the U.S. justice system by seeding Twitter with a steady diet of content meant to undermine faith in the rule of law. Since the launch of the dashboard, content focused on undermining law enforcement and the justice department has increased steadily suggesting an attempt not only to divide Americans, but to erode faith in our system of government." That was because they went back and looked at their data through this lens. They recognized that of course they have been telling people that Comey, dump Comey and the negative narrative about Comey and about Mueller and the investigation had been on their graphs and being charted. They didn't, they never sort of put it all together as this may be a concerted effort to undermine the particular pillar of our democracy, confidence in our justice system and our judicial system.

So I am meeting in a week or so with the folks in the intelligence community to ask them to do the same. I have talked with reporter who are looking at this. I think, again, I think it may be hiding in plain sight. I think there may be more of this going on, but we are just getting started on this project. We are, as I said to Amy yesterday, it's hard to get the sort of government mission-oriented person out of me. I am having a hard time transitioning to having the luxury of a more scholarly approach. So when we set up this project, the first thing I did was reached out to the courts. We had a dinner with the head of the federal judicial center because of the training for judges and we had the head of the Judicial Conference Committee on Technology and Innovation

and the counselor to the Supreme Court Chief Justice. We said you know, we wanted to start looking at this. They said, "Oh my god, you are right. We are on board. Let's start training." They want to invite 25 of the most influential judges from across the country. They are going to come in and we are going to have these conversations. So I talked to the National Center of State Courts. They are off and running. They are going to do a comic book and graphic novel. So folks are moving out on this. So we are moving forward on parallel tracks. We are, as I wanted to do when I got on in January. We are moving now to counter these activities because we know they are going on right now even as we continue to do the research and analysis to understand the nature and scope.

But at the end of the day, what our report suggests and what we understand as we do this deep dive is that all of the things that we talked about and prevent and deter and reduce the effectiveness by, you know, through the social media, technologies, etc., at the end of the day, what we really need to do to strengthen, revive, respect for and confidence in and a sense of the importance of democracy is that we need to reinstill that narrative. So if you are probably familiar with the work of _____ [00:47:02] am I pronouncing his name correctly? Who has written about the survey results that show, for example, three quarters of the young people don't think it's important to live in a democracy. They haven't lived, they didn't live through world wars. They didn't see the ravages really of fascism and communism, totalitarianism. They don't understand. Folks say they have become complacent, but in any event, they don't fully appreciate why. They see democracy is messy. Democracy doesn't always produce the kinds of results you wish it would. So you know, they have concerns about it's not something that they necessary would hold up. We also have trained our young people very well to be nonjudgmental. So I participated in an activity with the American Bar Association and Justice Kennedy years ago when my kids were in high school where they tried to get young people to talk about they were in a foreign country that was totalitarian, how would they talk to them about democracy and women's rights and things like that. All these young people who were, who am I to judge. Why should I tell them my system is better than their system?

So we have a real job on our hands. Our institutions need to live up to the respect that we need to have in them. We need to make sure they deserve that respect, but we also need to strengthen that narrative. We need to be teaching civics in our classes. We need to create a public that is more discerning about the information that it takes in, etc. Very typical. I am sure you saw the MIT report that just came out about how fast false information grows. It brings to mind, of course, Jonathan Swift quote about lies being so swift and truth lagging far behind and the quote that is attributed, I think wrongly, to Mark Twain about lies are halfway around the world before truth can get its shoes on. But the MIT report is an empirical study and it's overwhelming how much more appealing, how much more broadly it is retweeted, and how much more quickly it permeates our information sources, false information. So we have a huge challenge on our hands. But I will say again one of the

things that is in the report is a list of all of the activities under way by civil society and work at our academic institutions. One of the recommendations that we make in the report is that we need to do research to understand what resonates, why people are so susceptible, what are the kinds of and how can we use that knowledge to both promote a more constructive, positive narrative and to defeat those negative scorched earth narrative. Civil society, there is a lot of people working this issue. There is a lot being done and I am hopeful every day the government will catch up. I will stop there. I talked longer than I meant to.

[Applause]

[End of audio]