Center for Strategic and International Studies

TRANSCRIPT
CSIS Event

"Hacking Democracy: A Super Tuesday Kickoff with the Cyberspace Solarium Commission"

RECORDING DATE
Tuesday, March 13, 2020

SPEAKERS

Suzanne Spaulding,
CSC Commissioner; Senior Adviser, Homeland Security, International Security Program, CSIS

Patrick Murphy,
CSC Commissioner; Former Undersecretary of the Army; Former U.S. Congressman (D-PA)

Angus King,
CSC Co-Chair; U.S. Senator (I-ME)

Christopher Krebs,
Director of the Cybersecurity and Infrastructure Security Agency,
U.S. Department of Homeland Security

Nina Jankowicz,
Disinformation Fellow, Science and Technology Innovation Program, Wilson Center

Debora Plunkett,
Senior Fellow, Defending Digital Democracy Project, Belfer Center;
Former Director, Information Assurance Directorate, National Security Agency

MODERATOR

Beverly Kirk,
Fellow and Director of Outreach, International Security Program;
Director, Smart Women, Smart Power Initiative, CSIS

Transcript by superiortranscripts.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

SUZANNE SPAULDING: Good morning. Welcome to CSIS. I'm Suzanne Spaulding. I am senior adviser for homeland security here at CSIS and director of the Defending Democratic Institutions Project. And I also have the honor of serving on the Cyberspace Solarium Commission. And so this morning we thought it would be appropriate on Super Tuesday to have a conversation – public conversation – about our recommendations related to election security.

The commission's report will be rolling out in its entirety on March 11th, so next week. But we're giving you an early preview of our election recommendations. And we really wanted to focus and highlight those, for obvious reasons. So I hope that all of you who are here nice and early this morning took the opportunity beforehand to vote if you a re eligible in a Super Tuesday state, and if not that you will do so later today. We will reinforce that message of getting out and voting all morning long, several times.

We're going to start with a few opening remarks from one of our co-chairs of the Cyberspace Solarium Commission, Senator Angus King, who served with Representative Mike Gallagher as the – as the leaders of this effort over the last several months to pull together this report. Senator King was the – is in his second term in the United States Senate. He was the first independent to be elected United States senator from Maine. He serves on the Senate Armed Services Committee, the Intelligence Committee, the Energy and Natural Resources Committee, and the Rules and Administration Committees. He also was two terms as governor of Maine. And he won his reelection there by the largest margin in Maine's history. He served as an outstanding leader of the Cyberspace Solarium Commission.

I just want to say that this gathering of these commissioners, that we met just about every week for two hours on Monday afternoons, which meant that our members, including Senator King, had to get back to Washington every Monday in time for that meeting. Most importantly, it was the most nonpartisan group that I have met with in a very long time. And that tone was set at the top by our bipartisan, bicameral leadership and really outstanding group that was appointed to this commission. So I'm very proud to have been a member. And I'm very grateful to Senator King for his leadership. And we're going to have a few opening remarks that he will make now to give you a sense of the context for these recommendations.

Then we're going to have a panel that will include the honorable Patrick Murphy and will be moderated by Beverly Kirk. And Beverly will introduce the panelists on panel one, but I will now give you a sense of Beverly Kirk's background. Beverly is my colleague here at CSIS, where she is a fellow and a director of outreach as well as the director of the Smart Women, Smart Power Initiative, which includes a regular podcast that Bev has with powerful women from all over the world, really.

And Bev comes to this quite naturally because before coming to CSIS she was a journalist and worked for national news organizations, including NBC, NPR, and PBS. She also founded a media consulting company. She is a member of the adjunct faculty at American University and has a master's in diplomacy and international commerce. So we're really pleased to have Bev moderating the first panel. And then we will move to our second panel, which I will be moderating, and we'll introduce those panelists at that time.

Senator King. (Applause.)

SEN. ANGUS KING: I think what I'm going to do this morning is give you a little bit of background on the Solarium. How did it get that odd name? What does that mean? And then a big picture view of what we've done and worked on over the past year. And then we'll move on to talk about elections and election security.

The Solarium was based upon the original Solarium which was in 1953. When Dwight Eisenhower was elected president, he realized that he had to deal with the Soviet Union – an expansionist, aggressive Soviet Union. Europe was still somewhat it disarray after World War II. And I think it was he and John Foster Dulles met in the solarium of the White House – that's the origin of the name, in the sunroom– and decided that the way they would develop the policy to confront the Soviet Union was to set up three taskforces of very smart people. Kennan was on one of the taskforces, that gives you an idea of how – the high power that this was. And put them – set them to work in secret to develop their own approach to the strategy for the Soviet Union.

And then in July of 1953 they had what I call a national spelling bee, which was a competition between these three groups to propose a policy for dealing with the Soviet Union. Eisenhower was the judge. Eisenhower sat and listened all day and reached conclusions, and they ended up with a kind of hybrid strategy of containment-plus, which ended up being the U.S. strategy toward the Soviet Union for sort of – not sort of – for more than 40 years.

So that's the origin of this idea of a Solarium Commission, and the commission had 14 members – four members of Congress, four members from the executive, and six members from the private sector, including Suzanne and Patrick. We met every day – I think we ended up with 28 or 29 different – 28 or 29 meetings over the course of the last nine months, very intense work, very intense staff work, and have developed a report which will be released next week.

Now let me give you just a bit of background on the big picture. I don't have to spend much time with you about the threat. We know about the cyber threat. It's intellectual property theft, it's ransomware, it's election

meddling, it's garden-variety theft of money. It's chaos. It's – the ability to undermine our society is just rich in terms of the cyber vulnerability.

We are the most wired society on earth; therefore we're the most vulnerable society on earth, and the status quo is not good. The status quo – one of our members represents a utility – three million hits a day – malicious hits a day on their systems.

I've met with small banks in Maine who get a hundred thousand hits a day. This is a small, local bank in the state of Maine – ransomware for communities across the country. We've had towns in Maine that have suffered ransomware attacks, communities all over the country, businesses, and of course, you all know about the large attacks, and then the 2016 elections.

So the problem is, under the current status quo, whatever we're doing isn't working. Do you see what I mean? We're getting attacked continuously, so whatever the policy is, isn't working, and therefore, we need a new and a different policy. And the Solarium Commission's work can really be defined by four words. The four word are define, develop, defend, and deter – define, develop, defend, and deter.

Define. Define the structure whereby we're going to confront this challenge. One of the problems is that the United States government is not well organized to deal with a problem of this magnitude. We've got diverse authorities, no one is really in charge, there's no real structure to how we confront the cyber threat.

We've got individual agencies and institutions that are doing good work, but there's a lack of overall coordination, and there's a lack of emphasis in certain areas. So define – define the structure whereby we're going to confront this.

Develop. Develop allies and norms for an international approach to this problem. We need to be thinking about how do we work with the rest of the world to establish cyber rules of the road that will create a situation where, if there are violations of those cyber rules of the road, there's an international response; that it's not just unilateral, it's not the U.S. versus another country – Iran, or Russia, or North Korea – but it's an international response, and that will make it infinitely more effective. So define the structure, develop the relationships, and the norms, and the allies.

Defend. Be stronger in terms of our ability to stop these kinds of attacks. Resilience, planning for continuity of the economy, continuity of government. Make it so that the attacks aren't very effective in terms of everything from personal cyber hygiene – which by the way, about 85 or 90 percent of the attacks could be stopped with two simple steps: two-factor authentication and don't click on phishing emails. These personal

– those kinds of things have to be part of our resilience, and we have to be a lot more aggressive about those – the things that we can do as individuals and institutions. So we have to defend. We have to be more resilient. We have to make attacks less effective, and therefore a waste of time.

Now, we're never going to get to the point where people aren't going to try to attack us; for one reason: because it's cheap. I once did a back-of-the-envelope calculation during an Armed Services Committee that Putin could hire 8,000 hackers for the price of one jet fighter. That's a low-cost way to sow chaos amongst your enemies in terms of the overall cost of national defense or, in the case of Russia in this case, national aggression.

So we need to be – we need to understand that whatever defense we do is incredibly important, but it's not going to be enough. And that leads to the last of my terms. Remember: define, develop, defend – deter. And one of the problems that we've had is we haven't had a clear doctrine of deterrence. We have a clear doctrine of deterrence in nuclear weapons. It's served us well for 70 years. There hasn't been a use of nuclear weapons since World War II because of, in many ways, the theory of deterrence, which is if you strike, you're going to be struck back in a devastating way.

It's a little more complicated and subtle in the cyber field, and it's not an exact analogy. But one of the problems is that in cyberattacks below the threshold of catastrophe, below the threshold of deaths and, you know, closing down the entire electric grid and that kind of thing, there's been virtually no deterrence. Or if there has been, it's been slow, it's been ineffective and unpredictable.

If someone attacks us in a – attacks our elections, for example, they should know that they're going to suffer some costs. They're going to have consequences. So one of our major discussions in our Solarium Commission was how to define deterrence below the threshold of the use of force, because right now there isn't any. And it's not effective to say we will strike back at a time and place of our choosing. And, of course, it all gets very complicated about attribution, knowing who to strike back at, and that's getting more and more difficult. But those – that's the sort of big picture of what we're doing.

And I want to go back to the very beginning. This is a very serious threat. Our electric grid, our financial system – all of you know how vulnerable we are. And then you put on top of that the development of the Internet of Things, where we've all got this device sitting in our bedroom. Imagine having a little person sitting in a corner of your bedroom who writes down everything you say and every sound you make and reports it to somebody. I mean, we've got that. It's Alexa. And then – but we're headed toward a time when our refrigerator is going to listen to us, our microwaves, our cars. Everything we do is going to be woven together,

and therefore subject to hacking, to disruption and to spreading chaos within our society.

In effect, what's happening is – I call it geopolitical jujitsu, where we're being – our strengths are being used against us. Remember, we learned about jujitsu is when you use your opponent's strength against them. They lunge at you and they're stronger, but you grab them and pull them aside and throw them down. That's what's happening. They're using our First Amendment, our free society, our open society, against us. And we've got to learn how to respond in a reasonable and effective way without compromising the values that make us who we are.

So that's the sort of broad picture of what the Solarium is all about. And now we're going to have our panel come and talk about elections, which is a very timely topic. It couldn't be more timely today.

So Suzanne, do you want to come on up, and Patrick? (Applause.)

MS. SPAULDING: Thank you, Senator, for providing the context for our conversation. And I realize that I neglected one of my tasks. Normally we have Dr. John Hamre here to kick these events off, and he always gives the public-service announcement that I will now give, which is, if an alarm goes off or anything happens, we very calmly go through this door and there will be folks here to help direct us. We'll go out of the back of the building and our meeting place is over at the National Geographic museum. And Dr. Hamre always seems to know what's – what is the latest exhibit there, and I don't know, but whatever it is I'm sure we'll enjoy it. But hopefully it won't happen this morning. We'll be fine.

The other thing I wanted to give you a heads up is that you see that you've got cards – index cards – and that's how we're going to do questions today. So as you're listening and you've got questions that come up, write them down. They'll be collected and we'll ask them from up here. Right? Thanks.

Beverly, over to you.

BEVERLY KIRK: Thank you so much, Suzanne. I appreciate it and your kind introduction.

You've already heard the introduction of Suzanne and for Senator King, so let me introduce Commissioner Patrick Murphy. He was America's first Iraq War veteran elected to Congress and he later served as acting secretary and the 32nd undersecretary of the Army. He is currently the distinguished chair of innovation at West Point and a senior fellow at the Association of the U.S. Army. Welcome to you all.

MS. KIRK: I'm super excited to talk about this topic. And because today is election day, the first question that I want to ask is about paper ballots. Why is it so hard to switch to paper ballots? I know a lot of states have already

done that, and I'm curious what your thoughts are about states needing to adopt this system. Suzanne?

MS. SPAULDING: Sure. A couple things.

One is, of course, the federal government can't mandate that states switch to paper ballots. We can – they could attach that as a requirement for funding, for example, but we take very seriously the fact that state and local governments are responsible for administering elections in this country, and that's a bedrock principle. So that's one challenge.

There are investments that have been made, right, in modern voting technology. This was supposed to be a big step forward years ago, and lots of funding provided by Congress for folks to bring technology to bear to make voting more accessible, which is certainly a value and something we think is really important, and to be able to produce results more quickly. We, of course, had problems in a(n) election not too long ago with paper ballots, with hanging chads, and so that led to also the adoption of this technology. So some of it is cost, is making that change.

SEN. KING: And inertia.

MS. SPAULDING: Yep, and some of it is inertia.

SEN. KING: But don't miss the irony, though, of a high-powered federal commission on cybersecurity recommending paper. I mean, I just sort of love that – (laughter) – concept. But Suzanne's right. I think there are eight states that have full electronic systems. They have invested a lot of money. One of our recommendations is more money through the Election Assistance Commission to states on a matching basis to help them get to a system. And it doesn't have to necessarily be all paper ballots, but there has to be a paper trail, an auditable trail. That's the key.

MS. KIRK: And for those who don't know the role of the EAC, talk about how the commission imagines what it – what is needs to – what needs to happen with it, in addition to having more money?

SEN. KING: Well, one of the – one of the problems with the EAC is that it's totally gridlocked. It's two Democrats, two Republicans, and it just doesn't – it's not really functional. They have proven reasonably effective at giving out federal money over the past several years, $350 million, to states. That's OK. What we're recommending is that a fifth member be added only for cyber-related issues; that a fifth member be a technical person that understands cyber. We think it's a lost cause to try to rebalance the commission totally, but for this case we're recommending that you have a special member who can react on these kinds of cyber-related issues to try to break the deadlock. Otherwise, we're stuck.

PATRICK MURPHY: If I can just jump in, Bev, I think it's important to know, you know, we talked about – and I appreciate Senator King, or Mr. Chairman, his comments about President Eisenhower at the Solarium. President Eisenhower once said, the future of this republic is in the hands of the American voter.

So back in 2000 I was a young captain teaching at West Point right before 9/11 and before I deployed to combat twice. But in 2000 there was 2 million American voters that did not have their votes counted. And what did the Congress do? They had Republican Bob Ney from Ohio, it was called HAVA, Help America Vote Act of 2000. And it passed – it established the EAC, you know, and as the senator mentioned, and as commissioner Spaulding and I have diligently worked with this week, after week, after weeks. It is broken. There are folks that aren't appointed. It is – and, here again, this is supposed to empower American democracy. You have the FEC, on the other hand, that is the referee of that democracy during campaigns. But the EAC, as the senator mentioned, needs robust governance. It doesn't have a general counsel right now. It doesn't have commissioners appointed right now. And that is an indictment on our government and this administration.

MS. KIRK: Let me follow up on that. This inertia, what's it going to take to get things moving, to make change happen, to get the overseer working the way it's supposed to work? We can talk about it being broken and identify that as the problem, but how do we fix it?

SEN. KING: Well, I hope it doesn't take a catastrophe. Often that's what it takes. And hopefully that isn't what it's going to take, that there are enough people that understand the limitations right now. I think our idea of adding the fifth member for certain issues is a creative way to try to deal with at least part of the issue. But overall, there needs to be a broader consensus that elections aren't games. They have serious consequences.

MS. SPAULDING: And I think the EAC does have that good relationship with the states, and the state and local election officials. They have proven in the past to be a sound administrator of grant funding, for example. And so it's one of the reasons that as we looked across where would be the right place to really kind of put some emphasis on strengthening, the EAC, you know, seemed to be a place that we ought to strengthen. And so I think on a bipartisan basis, hopefully, we'll – you know, people will understand the importance of this.

I do think that election security is one of those areas that the public gets, in many ways. Cybersecurity is a big term that covers a lot of things and confuses a lot of people. And I think often their eyes glaze over. They don't know whether you're talking about – you know, that they get a new credit card every few months because their bank has suffered a breach, or you're talking about the electric grid going out for months. But when you

talk specifically about the sanctity of our elections, I think the American public gets it. And that means hopefully members of Congress will.

MS. KIRK: And if I could follow up on election security, particularly at the state level because the commission had something to say about that and I want you guys to talk about it. But you got 50 state and literally 50 different ways of running elections.

SEN. KING: It's way more than that. (Laughter.)

MS. KIRK: It's way more than that?

SEN. KING: A lot of counties have their own – it's hundreds.

MS. KIRK: That's true. So how do you – how do – again, how do you fix that? Because states are going to be reluctant to have some uniform way of doing things if they've done things their way for, you know, literally hundreds of years. How do you fix that? Because that seems to be part of the problem. Everybody does everything differently, right down to have different kinds of election systems. The way you vote, as we just talked about, is different in each state.

SEN. KING: Well, the states are very resistant to the idea of any federal involvement. When Jeh Johnson in 2016 wanted to declare the election system critical infrastructure there was huge resistance, and anger, and no, you can't do this. You're trying to federally take over elections. The states have to get over that. I mean, they just need to understand that this is of national consequence, and it's not simply local. One of the things that disappointed me was that in one of the election security bills, which unfortunately died in the Rules Committee, there was a – originally, there was a provision for red teaming of the states to test their systems. And the states stoutly said that – we can't – you know, you can't do that. Well, when somebody tells you they don't want to be tested, to me that indicates a lack of confidence in your level of security.

So I think this is a real test for the states, this upcoming election. If we have another disaster – and by the way –

MS. KIRK: We already had one.

SEN. KING: It doesn't need to be the state – oh, yeah, we already had one.

MS. KIRK: We already had one.

SEN. KING: But that was without the help of the Russians, right? They did that to themselves, apparently. But it's – an outside interest could screw up this election by delving into about 10 counties. They don't have to do every state. I mean, all of us in this room could – you know, Dade County, and Broward County, and a few in Wisconsin and Michigan. I mean, this is –

you don't need to destroy the entire federal election system to sow chaos in a presidential election. You can do it very selectively. So I think a lot of the responsibility does come back to the states. I do think they're doing a – I think they're much stronger than they were four years ago. It remains to be seen whether it's strong enough.

MR. MURPHY: But I think the senator's point is important, because it is a partnership. And the federal government does have a say in it. The Constitution clearly lays out in Article 1, Section 4, that Congress has a role; the 12th Amendment, which established the Electoral College. And when you have the former CIA director, Michael Hayden, say that in his whole career, in his experience, decades as a general officer in the Air Force and the CIA, and said the most successful covert-influence operation in recorded history was the 2016 election with Russian interference.

And again, I started by talking about 2000, where we had 2 million votes not counted, and Bob Ney, who started the Help America Vote Act, which established the EAC, the Electric Assistance Commission. And now we have 2016. And again, there is a tension. And again, we're here trying to encourage people to vote. We're Super Tuesday.

And, you know, Joe Nye – you know, I'm a big fan– he has a book called Sharp Power. You know, he talks about in America, it's critical that information can be trusted. And we understand there's outside players that are attacking our democracy. And again, you know, I'm a guy that, you know, like many of us in this generation of veterans, that go overseas to help establish democracies, like Baghdad where I was, and yet at home it's getting chipped away by foreign actors.

And so I think what is – and I think Commissioner Spaulding laid it out perfectly – we have this great bipartisan commission led by Senator Angus King and Congressman Mike Gallagher, an independent and a Republican, and we have 75 recommendations that will be announced next Tuesday.

But we have a bias toward action. There's not – this is a commission that made 75 recommendations. It's not some report that's going to be in the Library of Congress that no one's going to look at again. This is going to hopefully be bipartisan. There's going to be some legislative actions. There are going to be some executive actions.

And the state – and if I could just really quick – when you look at – as Senator King just mentioned, it's not all 50 states. You know, when you look at where they're going to try and tip this election – and, you know, in my opinion, when you look at the stats, you know, five states are really in play when you talk about swing states.

In my – this is not part of the commission—this is Patrick Murphy giving you my political analysis, because I used to work at NBC like you did,

Bev, but it's going to come down to Michigan and Wisconsin and Pennsylvania and Florida and Ohio. And when you look at those states – you look at my state of – my commonwealth of Pennsylvania, the EAC, to Suzanne's point, has done a great job. They've pushed out, there's been about $14 million investment in Pennsylvania; 13.5 million (dollars) came from the EAC and about 500,000 (dollars) came from the Pennsylvania state legislature.

The problem is – and we have – we're one of the ones that we have a paper ballot, auditable. The problem is in 2019 – you know, these machines are only used twice a year. So in 2019, in the off-year election, before we have a wave, because people always vote – a lot of people vote mostly just presidential years – in Northampton County, so one of those suburban counties of Philadelphia, one of those battleground counties, 26,000 votes unaccounted for and a machine that's auditable, that had paper ballots – 26,000 votes.

So, you know, we have to do a lot more work. We just can't just pay attention to this every four years. We have to get after it. And I think that's what the commission – that action toward bias is critically important. That's what I'm excited about.

MS. KIRK: And losing 26,000 votes is something that creates a lack of trust in the system, and that's something that is on us, not to mention the foreign actors who want to create a lack of trust in the system. And since the foreign actors have come up a couple of times this morning, foreign nationals are actually banned from contributing to U.S. political campaigns, but they can buy all those nice Facebook ads that you see.

SEN. KING: Well, that's a gap. The law that controls contributions of foreigners was passed in 1971, and it talks about print and TV and radio, but it doesn't talk about the internet. So one of the clear recommendations is to update that law so that it applies to any platform that disseminates information.

And I think it's important – I served on the Intelligence Committee through the whole Russia thing, and we're still completing our work, but just – it appears that Russia started out in 2016 with an intention just to show – just to sow discord; to undermine the system, to undermine Hillary Clinton if she won, to just sow distrust in our – in our democracy. Later on, they formed a preference for Donald Trump, but in other words, they don't have to necessarily come down on the side of one side or another of a candidate to screw up our system because our system is based on trust.

We forget that, that it's all based upon trust. You go in and vote and you see the results that night and you say, yeah, that's who won. And when you undermine that, it really strikes at the core of the whole idea of democracy, of – you know, the first line of the Constitution is "we the people," and it strikes at the heart of that if we don't believe that we the

people are the ones who are expressing ourselves. And that's why this is so – is such a – vitally important.

And I don't want to miss the opportunity to mention an example of what I think is a – is an important initiative. Marco Rubio has a bill called the DETER Act. And basically, it puts into law that if a foreign entity is caught meddling in our elections they will be sanctioned, and it mentions the type of sanctions, and it makes it automatic. It's not presidentially discretion and it's not two years later. And I think that kind of – that's the kind of thing I was talking about. If somebody in the Politburo or in the supreme leader's office in Iran is deciding shall we do this in the American election, I want them to think – I want them to have a calculus that says, well, OK, but if we get caught we're really going to get whacked in some way, shape, or form. In other words, I want to – I want to deter their – because the best cyberattack is the one that never happens. And so I think – that's why I think deterrence is so important.

Sorry to talk so long. I'm a senator; I can't help it. (Laughter.)

MS. SPAULDING: And the point that you made, Senator, and Patrick as well, about the fundamental need for trust, this is a process in which, you know, the public has to have faith and confidence in the legitimacy of the process to respect the outcome. And it's fundamentally important in that way.

The project that I'm leading here at CSIS looks at the justice system in the same way. The justice system is another one where the public has to have faith and confidence in the legitimacy of that process –

SEN. KING: Yeah, the court has no army.

MS. SPAULDING: – right, exactly – to respect the outcome. And again, there's an area in the justice system where we see adversaries, and particularly, Russia as part of its long-term campaign to undermine public confidence in democracy, undermining public trust and confidence in the independence and impartiality of our justice system, amplifying domestic voices.

But the trust issue is the main reason, really, that we are such strong advocates for paper ballots. That is really – it's the – it's the primary way in which you're going to be able to, after the fact, go back and assure the public about, you know, what happened in that election in terms of the votes being cast and counted. And it doesn't even take actual hacking into any systems. Mere allegations that you have, you know, interfered or disrupted in some way our election process can undermine that trust.

SEN. KING: Well, one of the – one of the options is hacking into the reporting system so that the results that are reported on TV at 9:30 turn out to be completely wrong and you get different results at midnight or at 2 a.m. That's another undermining of trust. And so there are all kinds of – not to mention, we haven't even talked about the voter rolls, registration lists.

You could – you could monkey with those and have thousands of people that show up and say, well, you're not on the – you're not on the list or it's a different middle name or something. And so they're – you can make yourself pretty damn nervous just by thinking about the options for making trouble, and that's why we got to attend to it.

MS. SPAULDING: And this is exactly what state and local election officials do. This is – this is their bread and butter. They do contingency planning, you know, forever. What if there's a storm? Today, on Super Tuesday, we had a tornado in Nashville, right? They've done contingency planning. What do we do if the polling places – normal polling places can't open, right?

SEN. KING: And local officials know people. There's a wonderful story from Maine in the '30s when Alf Landon ran against Roosevelt, and there's this little Republican town on the coast. And they announced the vote that night, and the clerk said, "100 for Landon, two for Roosevelt." And somebody in the back of the room said, "the son of a bitch voted twice." (Laughter.) They know.

MS. KIRK: Well, I don't want to get too far into the conversation without inviting the audience to submit their questions. You have the cards on the seats, so if you have questions, if you've written them down – if you haven't written them down, write them down, and our team in the back will come through and collect the cards and bring the questions up so we can ask them.

If I could go back to deterrence for a half second and pull that thread a little bit, should we be thinking of what's going on in terms of the foreign actors as a different kind of warfare and plan accordingly? Because that – maybe it's just me, but if you're going to deter, there has to be a consequence, as you said in your remarks, Senator King. But should we be thinking about this in the warfare term, in terms of responding to this different type of information war?

SEN. KING: Well, it depends on what you mean. I mean, if you mean respond, it has to be kinetic as if in a war, no, I don't think you need to view it in that way. But I do think there has to be some response.

And it is an attack. It's an attack. Those guys that hacked the DNC servers in 2016 did it from afar, but they could have – they could have parachuted four or five people in in the middle of the night and broken in and, you know –

MS. KIRK: But at what point does it need to become a kinetic response? Does it take taking out the electrical grid?

SEN. KING: Well, that –

MS. KIRK: Does it take having, on November – what's Election Day – November 3rd and we've been hacked to the point that we don't know who was elected president?

SEN. KING: I think there needs – this is a case where you want policymakers to have ambiguity. I want the other side to be nervous, so you can't make categorical statements – if this, then that – but it should be, if this, then something. And right now, we don't have that. That, to me, is the most serious weakness in the present system. But I wouldn't want to say, you know, if they do four states it's a missile, and if they do five states it's a bomber – no. I don't even – strike that. (Laughs.) I don't even want to be heard to –

MR. MURPHY: Well, make no mistake –

MS. KIRK: Jump in here.

MR. MURPHY: – make no mistake, I mean, they're attacking America at its core, and not just our democracy with elections, but also our economy because we have the number one military in the world and the number one economy in the world. And when you have one in four American companies that have been attacked via cyber by nation-states – not people in their basement – by nation-states, one in four American companies –

SEN. KING: Wow.

MR. MURPHY: – and then when you have a democracy that – again, it is – couldn't be more public that has been attacked by nation-states, like in the 2016 elections, and are now, again – you know, again we have intelligence officials that have gone on record that they are again interfering in 2020 – we cannot be asleep at the wheel anymore. We need to come together as Americans to put the country first. It's not partisan, it's not anti- or pro-Trump, it's not anti- or pro-Democrat party. It is – this is what our country is all about.

You know, I think one of my favorite quotes – Abraham Lincoln once said, the ballot is more – is stronger than the bullet. Elections belong to the people. And that's what they are trying to steal and take away from us.

SEN. KING: And I think one of the points I mentioned – I'm not promoting Marco particularly, but it – (laughter) –

MR. MURPHY: It would be a great ticket, though, when we talk about 2020, but –

SEN. KING: On the Intelligence Committee, he's one of the ones who has – who has repeatedly said, look, Putin is not a Republican. The next time, the tables could be turned. Putin is an opportunist and, you know, the Supreme Leader is an opportunist. They are not trying to help one party over the

other because they like the ideology of the other party; they're just trying to harm us. And so all of the – politicians on all sides need to realize that this is a threat – well, all citizens need to recognize this is a threat, and it's not a partisan threat. You know, it worked in the favor of the president in 2016, but this time it could be different if the Russians decided that it serves their interest to push somebody else.

So that's what – that's a recognition, we can't be confused by a short-term advantage because, in the long-term, this is really dangerous for the entire country. And they're going to keep at it because why not.

MS. SPAULDING: And understanding the objective of the adversary is really important here. The report talks about our strategic approach, is one of a layered deterrence and rests on two key elements, both imposing costs – which we've talked a bit about – but also reducing benefits, as Senator King said in his opening remarks, that we want to mitigate the consequences so that they are less successful in achieving their objective as part of changing their cost-benefit analysis in making decisions about their activities.

So if the objective – if one of the key objectives here is to undermine public faith and confidence in democracy and democratic institutions, one of the recommendations in the report for countering election interference is to promote more robust civic education and engagement, that would include media literacy. But not just digital media literacy, but an appreciation for, an understanding about what our democratic institutions are designed to do, right? How our democracy is supposed to work. How we as individuals can hold those institutions accountable. Why democracy is important and why it's worth fighting for. Because I am convinced that a key objective, certainly of the Kremlin, is to get Americans to give up, to despair, to look at that chaos and division and just think it's too hard. I'm not going to vote. I'm going to be engaged, right? And that is incredibly damaging to our democracy, and I think they know that. And the way we fight back is to stay engaged and to vote.

SEN. KING: Suzanne touched on a very important point. We've been talking a lot about things like hacking and databases and voter lists, and that kind of thing. But disinformation we really haven't touched upon, and that's a huge part of this. And the more I thought about it and talked to people in Eastern Europe who've been subject to it for years, we need to be more discerning consumers of information. We need to be less credulous about what we read. My rule is, if I get an email and the heading says, you're not going to believe this, I probably shouldn't. (Laughter.)

But I think that's very important, because we're awfully prone to believe the latest rumor that comes across and to run with it. And I can tell you, as a person that runs for public office, it's terrifying, because if somebody makes a ridiculous charge about you online you can never really catch up with it. You can never – it's not like you can put up your own ad and answer it and – you know, because it's always scattered around and keeps

coming up. I'm still getting emails about a vote I took on an amendment, you know, five or six years ago that wasn't accurate, but it just keeps feeding itself. So we need to be – I think part of it is civic education, which is one of the recommendations of the commission.

MS. KIRK: Well, we're beginning to get questions in from the audience. And I want to go to one that asks about recommendations on how to help campaigns secure themselves, because the commission has recommendations about that.

MS. SPAULDING: Great. Yes. So the campaigns are often overlooked in these conversations about election security, right? The public focuses a lot on the security of those voting machines, and we try to get folks to think more broadly about what election infrastructure is, starting with voter registration process and all the way through, as Senator King said, reporting on the results at night. But it's also about the campaigns. And Patrick talked about one of the most impactful hacks in 2016, was the hack of the DNC, and the hack and leak of those emails. And John Podesta –

SEN. KING: And John Podesta clicked on a phishing email.

MS. SPAULDING: Well, he asked –

SEN. KING: He asked advice and he was given bad advice.

MS. SPAULDING: Yeah. So campaigns are a really important aspect of our election security and vulnerability. And they have very little resources that they want to devote to cybersecurity, just to be honest, right? They're all – they're all scrambling for dollars every single day. Well, not all of them. We got a few who aren't scrambling for dollars. (Laughter.) But most campaigns are.

SEN. KING: Don't knock it if you haven't tried it.

MS. SPAULDING: Yeah. Most campaigns are. And so it's very hard to get them to focus on spending some of those hard-raised dollars on cybersecurity. The Federal Election Commission has come out with guidance, very specific guidance, on – that says that if you're offering it in an appropriate and completely nonpartisan, bipartisan way, that companies can provide for, free or discounted, their cybersecurity services to campaigns. And that will not count as a campaign donation from a corporation. And that's the key, because otherwise that would be prohibited. And so there is this FEC guidance. We're going to talk about it some more on the second panel. But it so, but so far, it's ad hoc.

SEN. KING: But I've heard in the last 24 hours that two presidential campaigns were approached, and they said two-factor authentication is just too cumbersome and so we're not going to do it. I mean –

MS. SPAULDING: So there is an education process that needs to go on here. But at least for those campaigns that are willing, there is an opportunity now. And the Defending Digital Campaigns group that got this FEC ruling is up and running, and we have the chair of the board on panel two to talk to us about how that's going. But the recommendation from the commission is that this not be on an ad hoc basis, but that we look at institutionalizing what is now FEC guidance.

SEN. KING: Yeah.

MS. KIRK: And a question here: Is there no path to having the Fed develop a national voting infrastructure that is perhaps opt-in by the states, but make it so compelling that states couldn't resist?

MR. MURPHY: Well, I think it's a carrot and a stick. So that – we're trying to really, from the commission side, take it from the carrot approach and partnering with the states. And that's why you're seeing, like in my home state of Pennsylvania, as I mentioned earlier, about $13.5 million this cycle being invested in Pennsylvania and then matching it with 500,000. That, I think, is the real way forward when you talk about the EAC and what the federal government could do and how we're going to partner.

But there is – as my colleagues have mentioned, there is this tension of – you know, that goes back to our founding of our Constitution, of federalism. You know, you want a limited federal government, and that's why you need to have states' rights and that's why you have to have this partnership. And they do have an allergic reaction every time we try and put standards out. But I think it's critically important that we do it in a way that's more of a carrot and less of a stick.

SEN. KING: But Patrick mentioned early on, a lot of people assume that it's solely a state responsibility; the Constitution assigns it to the states, period, end of sentence. That's certainly the states' position. If you actually look at the constitutional provisions –

MR. MURPHY: Article I, Section 4.

SEN. KING: – Article I, Section 4, it says the states shall set up election process, except the Congress may itself make its own rules. The only thing that Congress can't do is something about the location of choosing senators. Or I mean, it's – but it's a – it's a coequal responsibility. Congress does have the power, if they choose to exercise it. They haven't, historically. But if we continue to have serious breakdowns, I think you're going to see more federal activity. The states are – you know, they're – they have it in their hands to deal with it.

MS. KIRK: And to follow on that question, do you think post-election audits should be required? Do you think this is one way to increase trust in elections?

SEN. KING: If it's close, 1 percent. Many states have that rule, there's an automatic recount if it's within half a percent or 1 percent.

MS. KIRK: A question –

SEN. KING: I won by a percent and a half, so I'm good. (Laughter.)

MS. KIRK: So what –

MR. MURPHY: I won by .6 percent, 1,500 votes – (laughter) – so I'd be – (inaudible). But – (laughter) –

MS. SPAULDING: So then what you would want to require is the ability to have a post-election audit –

SEN. KING: Absolutely.

MS. SPAULDING: – and a – you know, particularly a risk-limiting audit.

MR. MURPHY: And to Commissioner Spaulding's earlier point, that's why it's really important to have auditable paper trails, to give – also to give people confidence. So just like if I go to, you know, an ATM machine outside, you know, I always ask for the paper receipt just because, one, I want to see what's in there. I know you can just get on the screen, but I want to make sure that it's accurate, what I just took out.

MS. KIRK: Well, I think we have time for one more question because the senator's staff has told me you have – you have to leave shortly. This is a question from Voice of America: What level of Russian meddling in election campaigns of this year do you see now? Are they meddling at all? If yes, is it different from 2016 and 2018?

MR. MURPHY: I used to serve on the Intelligence Committee but, Senator, you're still on it, so I'll let you – I'll defer to your judgment.

SEN. KING: Yeah, and I'm thinking about not answering because what I know is classified. So I'm not going to answer.

MS. SPAULDING: Well, I can address it from an unclassified perspective. Again, if you look at the propaganda – the open Russian propaganda outlets, RT and Sputnik, it's – you know, they are not being particularly subtle. Again, I think we're seeing – we're certainly seeing on those channels, a lot of that messaging that we saw in 2016 that the system is rigged, right? And again, picking up on, you know, domestic voices and narratives that are already out there, but pushing very hard and in a very sort of emotion-laden way that, you know, the system is out to make sure that Bernie Sanders, you know, doesn't get a fair shake, that the mavericks – that the least centrist candidates that are out there, which is where they tend to put their emphasis, because that's the best way to sow division and to stir up

strong emotions, and that they are – that the whole system is rigged against them, once again.

And again, the idea is to undermine public faith and confidence in the legitimacy of the process, and I believe to get a lot of voters to stay home, because they think the system is rigged. So we certainly are seeing that in a very open way.

SEN. KING: Let me also say that we learned yesterday that among the RSVPs for our announcement of our Solarium report next week is one of the Russian entities. So they're going to be there.

MS. KIRK: And one quick final question before you have to go. I know that this was a bipartisan commission. Has there been any response from the administration to the findings? Have you shared the findings yet?

SEN. KING: Well, the administration has been engaged. I mean, we've had four members of the administration, from FBI, DHS, Department of Defense and Director of National Intelligence, on the commission right along. And I have to say that yesterday all of the federal agencies – Department of State, Justice, Defense, DHS, ODNI, FBI, NSA, CISA – issued a really good statement on today's election, a joint statement, very strong in talking about they'd better not do it because there's going to be a response.

This is, I think – I was very impressed by the clarity and strength of this statement that was issued yesterday. So certainly, they've been participating. They won't be signing the report because of legal limitations about what a federal agency can do and all that kind of thing. But they've been very active participants and very positive participants in the process.

MS. SPAULDING: And it's one of the unique aspects. I've been involved with a number of commissions over the years, and I've never been on one that had executive-branch folks sitting on the commission. Usually what you do is you work in secret and then you reveal your report. It is, for the first time, given to the executive branch. They parcel it out to the various departments and agencies that might be effective. They take months to review the recommendations and come back with their thoughts on how it might be implemented, at which point usually the administration is over and that's the end of it.

SEN. KING: This commission is the way Congress ought to work but doesn't. I mean, it was one of the best experiences I've had in eight years as being a member of the Senate of people who actually sat around a table, talked about hard issues, agreed, disagreed, compromised, worked things out, did a lot of very substantive work. And I think it's been a pretty extraordinary experience.

MS. KIRK: And Senator, you get the last word, because your staff is giving me the hook. (Laughs.)

SEN. KING: I apologize for having to leave. Through some oversight – I'm not in charge of the Senate schedule, so I have to get back. There are overlapping hearings this morning.

But I just – I want to thank my two members of the commission who really made huge contributions. And I just – I hope that all of you will take a look at the report, which will come out next Wednesday, the 11th. And as Patrick said, we're oriented toward action. We want to be sure that we've made recommendations that we think are doable. A lot of them involve Congress; a number of them involve the executive branch.

But this is an urgent problem. We talked about elections today, but as you all know, it's a much broader problem than simply elections. But as President Kennedy said, this is a problem created by people, and therefore people ought to be able to solve it.

MS. KIRK: Thank you all.

SEN. KING: Thank you.

MS. KIRK: Thank you for joining us. (Applause.)

MS. SPAULDING: All right, we're going to switch panels.

SEN. KING: I've been known to walk out with these after meetings, so. (Laughter.)

(Break.)

MS. SPAULDING: (Off mic) – and Chris Krebs, the director of the Cybersecurity and Infrastructure Security Agency. But we'll go ahead and get started. We've got some terrific panelists here to continue our conversation.

Deb Plunkett, who, as I indicated earlier, is the head of the board of the Defending Digital Campaigns Initiative, which was launched in response to and actually was the, you know, group initially that got the guidance from the FEC, and is now out helping campaigns to improve their cybersecurity. And in full disclosure, I also have the honor of being on the board of DDC. Deb was, prior to that, the head of the Information Assurance Directorate at the National Security Agency for a number of years.

We have Nina Jankowicz. Nina is at the Woodrow Wilson Center for Scholars, and a real expert on disinformation and information operations, and has a book coming out. Nina, what's the name of your book?

NINA JANKOWICZ: How to Lose the Information War.

MS. SPAULDING: Excellent. Great. As if we need instruction. (Laughter.) And Patrick Murphy, who of course has already been introduced.

So, Deb, let's start with your – you know, give us a sense of how things are going with the campaigns, what you're seeing, what – as we're out there reaching out to campaigns, what kind of response you've gotten from the vendors.

Hello, Chris. Welcome.

CHRISTOPHER KREBS: Good morning.

MS. SPAULDING: And what sort of response you've gotten from the cybersecurity providers.

DEBORA PLUNKETT: Sure. So thanks, Suzanne, and thanks for the opportunity.

So maybe just a tiny bit of how we got to where we are, and then jump right into where we are. So in the fall of 2018, sort of as a follow-on to an activity that started with the Belfer Center in Harvard, defending digital democracy, where we developed playbooks and training, conducted training, both at the state level and also with campaigns, just to help them understand security at a basic level and the things they needed to be thinking about. But it became clear to us in that project that we needed to do more. And the "do more" was necessarily then to move outside of the Belfer Center and to establish Defending Digital Campaigns, which was established in the fall of 2018.

But the premise for this, you know, concept to work was that we needed the Federal Election Commission to approve our premise, which was to provide free or low-cost, reduced cost, cybersecurity services to candidates and campaigns. And so, Robby Mook, who is – who was Hillary Clinton's campaign manager, and Matt Rose, who was Mitt Romney's campaign manager, and I, established Defending Digital Campaigns. And through a whole lot of work, just missionary work, really, of some really great attorneys on both sides of the aisle, we were able to get the Federal Election Commission to agree to this concept that we actually could provide free or low-cost, reduced cost services, and that it would not bump up against campaign finance rules.

So we started in earnest. We got the opinion in May of last year, and in earnest started Defending Digital Campaigns. And, you know, my happiness is that two things are happening. One, as I fully expected, companies want to do this. Because who doesn't want their vote to count, regardless of party? And this is a nonpartisan activity 100 percent. But at the end of the day, I want a vote and I want my vote to count. And I don't – I don't want anyone else messing with it. And that means then, we need to make sure that candidates and campaigns have what they need in order

to protect their communications and themselves so that they can go about the business of convincing us that they are worthy of being elected.

So we have companies who are working very well with us. We have over 20 now who have signed up to provide, again, free or reduced-cost services. We also have – we have – as of yesterday, we are helping – we are at about 40 candidates or campaigns that we are working with. But our target is Presidential candidates. And, you know, we have some rules about who will help, because we can't help everyone. But the rules are light touch. So presidential candidates who are polling at 5 percent or greater, or who will qualify for the general election, and then congressional candidates, representatives who have receipts for $50,000 or more and senatorial candidates at 100,000 (dollars) or more.

So we are making moves. And I see the CEO of our company is here, and I think I saw another board member in the back, back there. So Michael Kaiser and Ron Gula. And so we are moving along.

MS. SPAULDING: Great. Thanks, Deb.

Chris, welcome.

MR. KREBS: Good morning.

MS. SPAULDING: I introduced you while you were out of the room.

MR. KREBS: Oh, thank you. Apologies for being late. It's been a long day already. Woken up in the middle of the night with the Nashville tornadoes, and talking to some of the election officials in Tennessee. And then had to get up with a late-breaking briefing over to a bunch of energy CEOs on the COVID-19 situation. So juggling several different issues at the moment.

MS. SPAULDING: You don't get to just focus on election today? Yeah.

MR. KREBS: No. No, no, no. Not so lucky, yes.

MS. SPAULDING: So how's it going so far on Super Tuesday?

MR. KREBS: Well, like I mentioned, you know, we got a little curveball from Mother Nature down in Tennessee. I think folks were expecting some extreme weather, but certainly not to the extent of a couple tornadoes going through downtown Nashville. A really unfortunate situation, but just showing the resilience of the voting process, and the fact that election officials are natural crisis managers, they were able to snap in place immediately some of the contingency plans, and get out information to the voters in Tennessee on what to do, where to go vote, and ensure they comply with the ten hours of open polls in Tennessee.

And so this kind of proves a few things. One is, yes, plans are in place. Everybody's prepared. The second is, trusted sources of information. Just listen to the local election official, whether it's a tornado, a hurricane, whether it's COVID-19, whether there's any sort of outbreak. This is how we're going to counter disinformation, not just now but in 2020. And that's part of the National Association of Secretaries of State and State Election Directors Campaign for Trusted Info 2020. Go to your trusted sources of information. And that's – for the – for the vast majority of the situations, that's going to be your election officials.

MS. SPAULDING: Yeah. So it does seem like it's a situation, as you said, both the COVID-19, where we're seeing lots of disinformation generally speaking, but also this kind of natural disaster that causes disruption. Those are both ripe for mischief in terms of misinformation, disinformation out there. Are we seeing that today?

MR. KREBS: I'm not sure the extent to which we're actually seeing it just yet. I think it is one of those scenarios that we've been working through over the last nine months or so. It was a really interesting thing last year, last summer, as we were sitting back and looking at the increase in ransomware attacks on state and local jurisdictions. I think this happened probably right around the Texas 23 jurisdiction's lockup. And sat back with the team and said: OK, we got this thing we're really concerned about it, the 2020 elections. And then we're seeing this increase in ransomware. How do the two intersect?

And so, doing a little threat modeling, which is sometimes a little unusual, particularly for the federal government, rather than looking back and saying: What happened last time, how can we be prepared for the next thing we may not be prepared for just yet? So we pulled these two things together and said: ransomware, elections, what's highly networked, what's highly centralized that would have a dramatic impact on elections? Ah, voter registration databases. So we put a lot of attention on the voter registration databases which is, you know, in part in the commission report some of the infrastructure systems and put focus planning across all 50 states – monitoring, hygiene.

Funny thing about hygiene, what is that we've been preaching for years, and years, and years on the cyber side? It's good cyber hygiene. What's going to help contain and mitigate the COVID situation? Good hygiene. (Laughter.) It's funny. There's some themes here. But again –

MS. SPAULDING: We stole it from them first.

MR. KREBS: I think that's probably right. But you know, I do hope, though, through all of this COVID situation that we finally kill the handshake and we can just do some elbow bumps or some foot shakes. (Laughter.) It just makes life easier.

But, again, looking at where the risk really is across the system – and there's a lot of attention placed on the actual voting machines and the things you interact with on a daily basis – but the things that are more exposed, again networked and centralized, are those voter registration databases. They are, due to their configurations, actually probably a little bit more – not a little bit, a lot more defensible than those edge points or the endpoints. So putting a lot of effort there.

And you know, I think I would close this out by saying, at no point across any election ever I think in probably the history of this country have we been more prepared. You know, you were in a situation where, I think, a little bit, you know, the intelligence community found it and then kind of dumped it in your lap and said, what are you going to do about it. We've had four years to prepare here. And I don't think there's a single issue I've ever been involved with across the federal government where all aspects of the government, from the intelligence community, Department of Defense, law enforcement, my team, the Election Assistance Commission – which is just a critical part – the Federal Election Commission, everybody's working with common unity of purpose and mission.

And the same goes for the state and local election officials. Four years ago, I think they would have – you know, again, when you first engaged them, they said, what are you, crazy? Russia? No. Everybody gets it now. This is the new landscape or the new frontline in geopolitical conflict. And I think we are in a dramatically better position just because the time we've had to prepare.

MS. SPAULDING: Yeah. And I think it's an important message to convey, and we mentioned on the previous panel the joint statement that was put out yesterday – really strong statement, both kind of warning about potential consequences from interference but also reassuring the public about how much has been done, how far we've come, and at the end of the day reminding people the most important thing they can do is to go and vote.

MR. KREBS: That's right.

MS. SPAULDING: I do think that we have made tremendous progress on the election infrastructure piece and a number of, you know, entities that have been established, including the – in response to the designation, et cetera. I think the much bigger challenge is the misinformation/disinformation piece. And, Nina, I want to bring you into the conversation on that. One of the things that we did not fully appreciate, I will say, in 2016 was the degree to which we should have been paying more attention to what was happening elsewhere, particularly in Ukraine, which you know so well. And so – for lessons learned and what we should anticipate, so tell me what you've been seeing in the interim. And of course, we know, you know, when people say Russia will be back, when they would say that after 2016 – Russia will be back in 2018, Russia will be back in 2020 –

we know they never left. And as Christopher Wray says, director of FBI, this is a 365-day-a-year threat. But having said that, what are – what are you seeing elsewhere in the world that we ought to be anticipating and prepared for here?

MS. JANKOWICZ: Yeah, thanks Suzanne and thank you so much for having me. I think the work that the Solarium is doing is really important, especially on that bipartisan, bicameral basis, sending a message to the American public that this is not a partisan problem but a democratic one. And I think that's awareness that everyone could stand to build up in their communities.

In terms of what we're seeing in Eastern Europe, certainly the threat has not gone away. We have continued to see takedowns by the social media platforms who, I have to say, should be congratulated on the work that they have begun to do, but they've only just begun to do it. You know, Mark Zuckerberg is saying they're taking down a million fake accounts per day, but that gives you an idea of the scale of the problem. It's huge.

And not all of that is coming from foreign actors, and I think that's the new curve and it's kind of hard to get our brains around. We are seeing – and you mentioned this in the first panel – a lot more information laundering. Rather than fake pages, fake groups, fake accounts, we are seeing narratives coming from bad actors – not limited to the Russian Federation but including Russia, Iran, China, and also domestic bad actors – being laundered through the mainstream media and trusted sources in order to kind of take root in society and give them more credence. And that's really scary because in the United States what do you when an authentic American is sharing opinions that they really believe in? It's much harder to play whack-a-troll then, right? And that was never going to work in the first place.

So that sort of thing has been going on in Ukraine for the past several years. But when I was there during the presidential election – their presidential election that brought to power Volodymyr Zelensky last year, I was seeing a lot of activity in groups. And this in part is because of the stipulations and barriers that the social media companies have put in place. So rather than all this activity happening out in the open, it's happening in private and closed groups. It's also happening in encrypted messengers, which haven't really taken on the steam that they have in Eastern Europe and Latin America here in the United States – and thank God for that right now – (laughs) – because that's really hard to track those conversations and see what's being shared on the other side.

So that, I think, is the vector through which this information is being shared, organized and amplified. And, in fact, I think, you know, a lot of the platforms are pivoting to privacy now. We saw Facebook place a Super Bowl ad about groups, right. That makes me extremely nervous, because that's where bad actors are organizing right now. So I think that's what we have to watch out for and be aware of as we're going into 2020.

You're seeing more of that information in your feeds, that's coming from those trusted friends and family sources. But you have to really look at the provenance of that information and say to yourself, OK, what is the original source for this? Where else is it being reported? Is this image something that's being repurposed, or can we trust this image as being original content and not misattributed, et cetera, et cetera? Those are skills, unfortunately, that not everyone has.

MS. SPAULDING: Yeah, yeah. So which, you know, goes to the importance of building a resilient public, right, that the tools that we have at our disposal are limited to prevent this from – people from seeing misinformation, disinformation. Information operations are limited and are getting more limited, as you point out, as it moves to encrypted – end-to-end encrypted applications.

And so, you know, resilience is a big piece of our report, right, Patrick, understanding that, you know, while you do everything you can to prevent and to defend, but at the end of the day, you have to make sure that you can mitigate the consequences.

And Chris, I know that DHS, that CISA is looking at how do we improve public resilience.

MR. KREBS: Right.

MS. SPAULDING: Tell us about some of the things that you're looking at and doing. The commission has some recommendations along those lines that we talked a little bit about – more robust civic education, including digital literacy. But what's DHS specifically doing?

MR. KREBS: So on the election-security front, we have three primary lines of effort. First is focusing on the election-infrastructure piece, owned and operated by the election officials. We've already talked about that. The second is working with campaigns and providing defensive briefings and offering them services similar to what the Defending Digital Democracy or the campaign's piece is doing.

The third, though, is that voter-resilience piece. We're looking at this a couple of different ways, but one way – a good way, I think, at least, to frame the problem is looking at it, particularly when you talk about the federal government's roles and engagement here, is a supply-and-demand problem.

We look on the demand side, and we engage the American public and provide them educational tools and resources to become more discerning consumers of traditional media and new media, social media. And then we have the FBI, law enforcement, the intelligence community, on the supply side, specifically disrupting supply of dis- and misinformation.

So when it comes to that demand side, again, what we're trying to do is provide more information in the resources and tools for the American public to be, again, more discerning consumers so that demand goes down. How are we doing that? A couple of ways.

One is, last summer we released our war-on-pineapple campaign. You may have seen that. Hopefully you did. But it was an – the concept was to take the decomposition of social-media influence campaigns into five – the five constituent pieces of identifying the issues, mobilizing the accounts, amplifying content, taking it into the mainstream, which is from Twitter or Facebook or whatever, into the media, where you get the traditional media spinning the issue up. And then lastly is you take things into the real world, and that means protests, counter-protests. We've seen the Russians. They did this in 2016.

But the idea of pineapple was to pick an issue that's not, on its face, subversive or divisive and you could actually get some engagement. There's actually some psychological pieces behind this. But it's really, do you like pineapple on your pizza or not. And there is a –

MS. SPAULDING: But not just do you like it. Should it be on pizza?

MR. KREBS: I mean, if you want to really go down –

MS. SPAULDING: Should it even be allowed?

MR. KREBS: – to the base. And it's like cilantro almost. It's like, there's no middle ground here. It's very binary. But the uptake was awesome, and it actually moved through – we identified the issues. We mobilized the accounts. We actually got the National Association of Secretaries of State to take one side and the state election directors to take the other one. And it really took off.

The only thing we didn't get was the protests, counter-protests. I was really hoping to get on the Today Show or something like that and be out in, you know, Rockefeller Plaza and have pizzas and signs and all that. We didn't get there –maybe next time. But it was an educational moment, and it proved to us that there are ways to educate and get information out.

So as we move forward into 2020, again, I want to point back to the National Association of Secretaries of State #TrustedInfo2020 campaign. There are things that the individual voter can do to ensure that they're prepared for election day and that, when those texts come in that say Republicans vote on Tuesday and Democrats vote on Wednesday, whatever it is, that you're ready, because you know what the rules are. You know what your plan is for voting. You know what the requirements are for registration, that you've registered. You know if there are any

voter-identification requirements. You've got it ready to go. You know what the hours are. You have your voting plan.

But it doesn't stop there. You know that the election results that come in that Tuesday night are early and they're unofficial, and there are others that have the mail-in and the absentee ballots that will take weeks to tally up. And so this may take some time. We've got to get over that instant-gratification piece of elections. I know that's really hard. And when I talk to friends in the media, they actually wish that would happen too. But they have their own pressures and demands. But there is still so much that we could do to push back, depress demand, and ultimately disrupt the supply side of this as well.

MS. SPAULDING: Yeah, great.

Deb, we talked about the statement that came out yesterday. And Senator King, you know, read the list of entities that had been – you know, that signed on to this statement for the public, and included NSA. Were you surprised to see that, based on your prior role at NSA? And, you know, can you talk to us a little bit about what you see as the role of NSA in election security?

MS. PLUNKETT: Sure. So, first of all, I do not speak for NSA, just for the record.

No, I was not surprised. I was pleased to see that. Election security and protecting our democracy is a whole-of-government problem. And if ever we should not be championing all of the resources of our power, national power, against a problem, it's now.

So NSA has these two missions, signals intelligence, foreign intelligence, where I spent the first two thirds of my career there, which is understanding capabilities and intentions of foreign actors. And that helps to influence – first of all, helps inform policymakers and decision-makers and helps influence national decisions. That information is shared with partners, with policymakers, and is used, again, to make the right decisions based on the plans of those foreign actors.

But the other half of NSA, where I spent the last third of my career, is on that information-assurance or cybersecurity side. And the beauty of the NSA mission is that when you can combine the threat that you've gathered from the intelligence side with the expertise on understanding cryptographic systems, security systems, products and services, then you have a powerful, then, very powerful, combination that you can use to help inform U.S. decision-making. And I believe that's what's happening. And to me, that's exactly what should be happening.

MR. MURPHY: And I want – let me just highlight, I think what Deb just said is very important when she talks about the whole of government. It's actually, as well, the whole of nation. And it's just public-private partnership.

When you hear Chris Krebs talk about the supply chain, yes, it's the voting rolls. It's the registration to vote. It is to make sure that, you know, when you're looking at campaigns and what they're doing and voting that resiliency, it's the ads. It's also when you talk about the public-private partnerships, it's companies, private companies, that are helping out and now able to provide because of the great work here at CSIS allowing those assistance without it being a campaign contribution. That was critically important to make sure that we're all building the resiliency needed to build that trust. And I think that's what's incredibly important, especially when we know that we're in an invisible war, especially when we know our democracy is attacked.

I mean, if you look at Suzanne Spaulding's report here at CSIS over a year ago – I cite it often – about inside the Kremlin's attack on American democracy, time and again it's not just about our voting. It's not just about our elections. It's about our justice system, putting out disinformation, saying, oh, it's really insiders with these insider judges. It's who you know and not what you know.

That's what's critically important, that we push back as Americans and understand that, yes, there is a partisan tenor in America and one side watches one channel and the other side watches the other channel. But we need to come together and make sure we push out that false information and call it for what it is.

MS. SPAULDING: Thank you, Patrick.

Chris, one of the recommendations in our report is to – we talked about this on the first panel – is to really strengthen EAC, the Election Assistance Commission, in a number of ways, both to adequately resource it, but also to try to help clear the logjam, at least on important cybersecurity activities and measures going forward, to have a fifth commissioner that would be specifically for cybersecurity – an expert at cybersecurity – who would be there to weigh in on cybersecurity issues.

We talked a bit about EAC's constructive relationship over the years with the state and local election officials. Talk to us about your relationship with EAC because you've talked a lot about what DHS is doing working with state and local election officials. How do you work with EAC, and how will strengthening EAC help you in that mission?

And I should note that elsewhere in the report – without giving anything away before March 11 – but it will not be a surprise that we have a number of recommendations aimed at generally strengthening the cybersecurity and infrastructure security agencies, as I said.

MR. KREBS: So kind of building on Patrick's point of this whole of government and whole of nation, as well as Deb's point – so General Nakasone and Anne

Neuberger are amazing partners for us right now, and this is something I think that has really blossomed and developed over the last several years – is this ability to work together with the NSA in common unity of purpose.

You've heard me say it before – that I think in some respects '16 and the Russian interference in the election was a galvanizing moment and wake-up call, really, across the federal inter-agencies. I know some of the battles you had to fight internal, and we seem to have gotten across to the other side of the river, and we're all pointing down the same path. But again, the Election Assistance Commission was not always one of those involved in the conversation, so we've put a lot of effort and time in developing these relationships with the EAC.

And the EAC is really – they are the election experts, and it's bigger than security. It's the administration. It's working with the vendors on equipment and other processes. They have this whole scope of issues that are much, much broader than cybersecurity.

So the relationship that we are trying to strike with EAC is much like any other sector where we provide the cybersecurity expertise, the cybersecurity services, the information-sharing mechanisms, the training, the exercises specific to cybersecurity that then supplements their efforts and provides a more well-rounded support to state and local election officials.

It continues to be something where we look at what their resources and capabilities – and ability to reach out an engage and, you know, the stronger we both are, the stronger our elections ultimately are going to be across the country.

MS. SPAULDING: One of the things that EAC has traditionally been good at is administering this grant funding.

MR. KREBS: Yes.

MS. SPAULDING: And so one of the things that the commission looked at is, you know, can we use that to provide incentives for states to continue to improve their systems. And I guess we're down to now eight states that still have paper ballots.

MR. KREBS: So it's only two states that are solely direct recording equipment – the paperless systems in New Jersey and Louisiana. Louisiana is in an RFP process that will get them there soon, but not before the 2020. And then you've got New Jersey that has other challenges from a financial perspective. They're going to need some help.

But there are a handful of states that are still some mix –

MS. SPAULDING: Have some jurisdictions that are still not using paper ballots, yeah.

MR. KREBS: Yeah. But, you know – sorry to interrupt, but that is one piece that I think everybody needs to understand is that, you know, in 2016, I think it was about 82 percent of the voters had a paper record associated with their vote. In 2020 it will be about 90 to 92 percent will have a paper record, and that includes all the historical or traditional swing states.

So you know, this is – there has been positive progress. Are we where we need to be just yet? No, but progress is taking place.

MS. SPAULDING: Yeah, I think that's such an important message to get across, particularly today when we're urging people to make sure they get out and vote. I told you I was going to say that a lot of times this morning.

But one of the things we looked at is both how do we get, you know, funds out to states to make sure that they have the wherewithal to make the improvements in the security of their systems as well as, you know, the voting machines themselves, and optical scanners, et cetera. But how do we avoid the moral hazard, right, Patrick? We talked about, you know, as you just pointed out, a lot of states have made investments in improving their systems, and so how do you make sure that states that haven't, you know, are incentivized, but not rewarded for having sort of dragged their feet, if you will?

And Patrick, do you want to talk a little bit more about that?

MR. MURPHY: Yeah, listen, I think it's – and again, it's a partnership. I mean, we spoke about the authorities given by the Constitution in Article I, Section 4, where the federal government clearly has the authority to play a role. But it's a carrot and a stick. And our commission report, without giving too much away, it's more of a carrot approach. For Chris' department, really putting the proper investments in CISA, but also in the EAC. And again, the EAC, which was established after the 2000 election, where 2 million votes were not accounted for or not recognized. And then there's other proponents when talk about budgets. And budgets, frankly, are moral documents, and we are making these investments.

And what we need to do with the EAC, you know, we look at it like, OK, 350 million, roughly, over the last several years of investments, to states. Again, 14 million to my home state of Pennsylvania. The Brennan Center, though, says that this is a hundred-billion-dollar investment that is needed. So again, we've invested less than 10 percent of what they're calling for.

And to Nina's point earlier, I would say, on the disinformation side, I mean, that's that – that is absolutely true what Facebook, what Mark Zuckerberg, taking down a million bad actors every day. Well, who takes those bad actors down? Yes, it's Facebook, but a lot of times, it's private

citizens reporting when they know that there's something. And that's why we all have a role to play to make sure that we are addressing this moral hazard that you talked about.

MS. SPAULDING: So the recommendation in the report is that – is that there be a percentage, that states have to have some skin in the game as well, and so they have to match some percentage –

MR. MURPHY: Yeah, like in Pennsylvania, as I said, you know, it's about 13.5 million from EAC and about half a million from Pennsylvania.

MR. KREBS: So one key element of all of this, particularly the funding piece is that, I've talked to secretaries of state and election directors and they say, look, we don't care if it's just a little bit of money or a lot of bit of money; doesn't matter. It just needs to be a dependable flow of money so that they can work with their state legislatures to get the budget right. But when you have an unexpected infusion of, you know, $425 million or $380 million, you can't budget against that.

And then give them the time to invest it smartly. There's one case in Minnesota with the 380 million from a couple years ago where the secretary of state was going to invest $200,000 because he was getting a lot of political pressure to spend his – the grant money, but he stepped back and said this is not a good use of taxpayers' dollar. I'm going to wait on this. I'm not going to go buy that thing. I'm going to wait and make sure I've got a smarter investment down the road. So things take a little bit of time. But we've got to have dependability and consistency in the system.

MS. SPAULDING: Yeah, and I – and I think we make that point in the report.

And speaking of the, you know, investments in the system and the public-private partnership, a key partner here is the vendor – election infrastructure vendors. And their changes take years, often, to be seen. Talk to us a little bit about what kind of – how that relationship is going; how responsive are the vendors in terms of, you know, understanding the problem here and addressing it; and then what is the prospect.

MR. KREBS: So initially, after '16, we prioritized working with the secretaries of state. They own the infrastructure, generally speaking, and so we wanted to get our arms around that problem set first.

And then we looked at the vendors and brought them into the community and conversation as well. So we set up one coordinating mechanism for government officials and then a private-sector coordinating mechanism with – that brought the vendors in. And then –

MS. SPAULDING: Which is pretty typical for the way we look at critical infrastructure sectors.

MR. KREBS: Yep.

MS. SPAULDING: There's a government coordinating council and a sector coordinating council.

MR. KREBS: And so as we brought the vendors in, to me it was actually something that made a lot of sense from a Pareto principle perspective. You can get your arms around a dozen or so players and affect 90 percent of the ecosystem. So for us it made a lot of sense from, you know, an economic rational-actor perspective.

But there was still a lot of work we had to overcome. This was not the broader IT industry that had been working with various parts of the government over the last decade plus so they had – they knew what to expect. We had to build trust. And that's really – whether it's the election officials, the campaigns, or the vendors, it's all about establishing trust, providing them resources, providing them assistance, information, bringing them into the fold, and then working through some of the problems.

We are seeing this trust manifest in a couple different areas of progress. And I think one of those areas, as you look, you actually see the vendors now starting to gravitate towards things like DEFCON and the Voting Village. A couple years ago that was unheard of. Now it is just one of those things. Voting Villages and DEFCON, they're not going away. They are only going to be more popular. Get in there, work with that community – the security research community – and help facilitate.

This is – you know, last week at RSA I had a – I was main stage and had a keynote, and the theme was cybersecurity has a posse. It's a build on a meme of Andre the Giant has a posse, Grace Hopper has a posse, all this other stuff. But the idea is, if we all work together, we're going to be able to address this issue. If we try to go it alone, we're toast; we will never overcome this. So if we can all work together, that's where we're going to get to the outcomes we need.

MS. SPAULDING: So what's your greatest frustration? What is – whether with respect to working with the vendors or just sort of generally speaking, where are you – where are you feeling like you're sort of banging your head on –

MR. KREBS: So I'm more of a kind of a go, go, go type. I really want to get stuff done on a much faster timeline. But with this, again, you have to build trust, and building trust takes time.

But this is true in broader cybersecurity, too. We've been talking about do the basics in cyber hygiene now for a decade. And you know, I remember some of the early commission meetings and saying, look, we've got to continue to build awareness, and some of the responses were, who the

heck doesn't understand cybersecurity is a threat. Well, people may realize it at the CISO level, but when you get into the board and the CEO, you're still overcoming some of these challenges of why it's truly a business risk, how you overcome that. And the formula we've got is, awareness leads to investment, which builds capability. So you've got to hit the right level of seniority and leadership that can make those investments happen.

MS. SPAULDING: Yeah. And my sense, too, Chris, since I've gotten out, I've had more time to talk with boards and CEOs about cybersecurity. And again, that it's less that they don't realize there is a risk out there than that they feel overwhelmed by it and they don't know what the path forward is. So often, giving them a path forward, even just the first few steps, and talking to them in terms of risk management that they do every day and the consequences to business, rather than the IT vulnerabilities that make their eyes glaze over. And I think this is where we are getting to with election security as well, that the – that the notion of having a(n) auditable paper trail is a good path forward. Certainly for now, when we – when we have still a lot of work to do to close down technical vulnerabilities in voting infrastructure, is to – is to at least give people a path forward. And then I think that helps folks take that next step and make those investments.

MR. KREBS: But ultimately, whether it's election security or cybersecurity in general, it's simply an engineering problem, Nina's area, that's the hardest space. That is going to be the – if we ever figure the engineering problem out, when we've got to put all this effort on the human element. And that's where I think we are all going to continue to look for answers in the future.

MS. SPAULDING: So, Nina, I would put the same question to you: What's your greatest frustration as you look at how we in the United States are approaching this issue that you have studied so carefully?

MS. JANKOWICZ: Yeah, my greatest frustration is that there are people like Chris all around the federal government working really, really hard on these issues and it's being undermined by a lack of recognition of the threat at the very highest levels of government. And this is something that was really driven home for me as I was doing research for my book and saw that in countries that have recognized this threat for as long as it's existed for them – so that might be decades, it might be, you know, in – let me take Estonia as an example. Of course they've recognized the Russian threat for forever, right? But when they were cyberattacked in 2007 and had all sorts of manipulations and interference in their political system, it took that recognition from the highest levels to change government. And it took a decade to really get to citizens and these citizens-based issues. They couldn't just say, OK, Russian speakers, you know, come and we'll give you Estonian lessons. They really had to do outreach, and it took a decade for that to happen.

But the governments that do have that recognition at the very highest levels are the ones that are starting to win. Nobody's won yet, but the ones that have the worst-case scenario either not recognized the threat or are engaging in the very same tactics that foreign actors are using themselves to interfere in their democracies, those are the folks that are on the back foot. And unfortunately, right now we are on the back foot. It really pains me to see disinformation being spread by elected officials, and they are throughout the government on both sides of the political spectrum I must say. And that's the sort of work that the Wilson Center has been trying to do over the past couple of months, training elected officials not only here in the United States but in other countries around the world that, again, this is a – not a partisan issue but a democratic – small-D democratic one.

MS. SPAULDING: Yeah. And I think some of that will be helped as we broaden our focus, as you mentioned earlier, beyond the very visible and broad-based efforts by the Kremlin to recognize that other countries are also engaged in information operations, and may very well become more involved in trying to interfere in elections for a variety of reasons. And that may help take some of the partisanship out of what should be a nonpartisan approach.

Deb, Senator King talked in the first panel about some of the campaigns not taking seriously, at least seriously enough in his view, the risk here, the threat here. What's your sense of what may be going on there and – you know, I'm going to give you an opportunity to talk about your frustrations as you're out there, working with Michael and the team to bring cybersecurity to the campaigns.

MS. PLUNKETT: Right. If you think about the nature of a campaign, for the most part they are – first of all, it's transient. There are people coming into and out of the spaces, bringing their devices with them, generally. They don't have security in mind. That's not their purpose. That's not why they're there. The campaigns generally aren't funded for security. It's not that – I really don't believe it's not that they don't care. Some of it is they don't understand, they've not been exposed. Now, with recent events they're all a lot more attuned to the possibilities. But generally speaking, they are – you know, ever dollar is spent for a vote. That's the purpose, right?

And so that's not really a frustration. It's just an acknowledgement for me that we have to do all that we can. That's why DDC was born. We have to do all we can to try to help them become secure, so that they can get on with getting their votes. I will tell you, the thing that – the fact that we know – we are generally not talking about intractable problems. We know how to secure communications. We have solutions. We have practices. And they are not complicated.

And so frustration for me is, we know the answers. Like, we know – if we were – if we were talking about really, really tough problems – and I'm sure there are some. But for the most part, the ones that we're talking about with campaigns, they are not. We just need to apply the security solutions and practices that we know will work. And if we can just get them to do that, life would be good.

MR. MURPHY: Right. I think – I think to Deb's point, I mean, it's simple. I mean, 85 to 90 percent of what we solve will be from two things: two-factor identification and, you know, don't phish – you know, don't take the bait. And so if we do that, that would solve a lot of the problems here.

MS. PLUNKETT: That would.

MR. MURPHY: But part of that is building that resiliency, and that confidence, and that acknowledgement that it is an issue, and that, you know, there is this invisible war going on out there.

MS. SPAULDING: And, Deb, I do think – I've said it a number of times – I think the lessons that we learn in working with campaigns, particularly congressional campaigns, should be hugely beneficial as we think about better ways to help small- and medium-sized businesses that often face the same sorts of challenges. They don't have a system. The person who set up the network for the congressional campaign is the son of the candidate, or the daughter of the candidate.

MS. PLUNKETT: Right. Eight-, seventeen years old, or something.

MS. SPAULDING: Yeah. And so they present some unique challenges. And if we can figure that out through this process, that should help Chris in his effort to work with small- and medium-sized businesses, and vice versa. Yeah.

So I think we've got questions from the audience. Yeah, great. So, yeah, so an interest in hearing more about what DHS is doing. We put a lot of focus on the technical aspects of hacking our voter infrastructure, but this question is about what is – what more is DHS doing to help prevent voters from being hacked by misinformation action, campaigns? I think, again, you talked about the trusted sources of information on the basic things – what day to vote, what time to vote, where to vote, that kind of thing. The tougher issue is this broader attack to influence people in ways that would be perfectly appropriate, perhaps, for a domestic public dialogue and discussion, but where you've got foreign interference that is really pushing a key narrative, for example.

MR. KREBS: Yeah, as I mentioned earlier, this is not an engineering problem. This is not a technical problem. This is a human problem. So we've got to continue the public awareness, the public education piece. We worked through what are the options. We could do a Schoolhouse Rock type thing for countering misinformation and disinformation. Those are the

sorts of efforts that I think are going to be more successful. But, again, it's all going to – at the end, at least for the 2020 election, it is going to hinge on where you can go to get information that is trustworthy, and who are those individuals or officials. And so Trusted Info 2020 is one of the primary thrusts for the 2020 campaign. You can go to your local election official to get the information specific to your election.

MS. SPAULDING: Do you worry that in some locations, some states, some jurisdiction, where they are perhaps doing – engaging in efforts to scrub voter rolls and other things that are seen as perhaps being about depressing voter turnout or reducing the number of people who are – who are able to come and vote for political reasons, that we run the risk that even though state and local election officials will not always be viewed at trusted voices, I think one of the challenges that we've seen is that it's increasingly difficult to find trusted voices in communities.

MR. KREBS: Yeah. Obviously getting out of the election security space here. But I think, you know, whatever steps elected officials take – election officials, specifically, take – it's critically important to be transparent, upfront on why you're doing whatever you're doing, and then maintain that line of communications with the public. And being responsive, addressing concerns, it just – it doesn't take much, as, I think, Nina has mentioned, you know, both sides will grab an issue and spin it the way they want it. And that's really going to be a challenge as we continue to move through – move up to November.

MS. SPAULDING: So we've talked a little bit about coronavirus being a vector for mischievous misinformation, disinformation. Is there – does the government have a message for the public on how they should think about going to vote in the midst of a spreading virus?

MR. KREBS: So I think – you know, obviously the primary focus of the federal government right now is on containment and mitigation of the coronavirus in general. As it plays out over the course of the next several months, you know, ideally this does not take off dramatically and can be contained. But we have to have contingency plans in the event. So working through those key messages right now, again in the runup to November. But this goes back to that trusted information. Look to your local election official. They'll tell you about the status of individual facilities, individual election precincts. But this goes back, again, just like cyber hygiene, basic hygiene, with things you can do to protect yourself, but also as you go out amongst the public.

MS. SPAULDING: Yeah. So a question about how civics is a national security imperative, and how it can specifically be used to counter cyberthreats. How – you know, we have made a recommendation about improving cyber education here. But talk about how it can specifically be used to help folks take on responsibility for the cyber hygiene that you talked about and the –

MR. MURPHY: Well, I would just say very quick, to Nina's point, we see in Estonia and other countries, you know, if I could just – it's a broader – it's really broader, kind of like it's your civic duty. So unfortunately, you know, our democracy is based on the majority that vote. But if the majority – it's only the majority that show up. And so understanding and putting out that information but letting them know that if you stay home you are surrendering. That is not protest. That is not –that is un-American to quit on your country. And so that broader theme of why it's important, and that there's players that do want you to sit at home. And then narrow it down tactically on why it's important with the proper hygiene, proper resiliency, et cetera. I think that's critically important.

And, correct me, Nina, if I'm wrong, but that's what we see in nations like Estonia, that have been able to show their people why there's bad actors and why they need to do the proper things to let their voices be heard.

MS. JANKOWICZ: Yeah, I think there's often a misconception that this is either just about, you know, cyber hygiene or it's just about teaching people the five things you need to look for to spot a fake news article. But it's actually a lot more holistic than that, and I always tell the story about the reason I'm up here today is because when I was a nerdy high school student I was in a debate club that taught me all this stuff about civics. I was in Model Congress, we also had a thing in my AP Government class that was called Operation Civic Duty where we had to go watch jury selection which, unless you are on a jury, even then it's not very interesting, but good understanding of how things work.

We had to go volunteer for a political campaign of our choice, but usually not a large campaign; we were all volunteering for, like, local races, and that really, I think, influenced the students that I was in school with – and me – about how government works. And I wish we would have more of that at a much more grassroots level because a lot of the mis- and disinformation that is getting shared around, especially now that we're back in primary season – I'm really having a lot of echoes of 2016 – is about the process itself and how votes are allocated.

You know, you were talking before about undermining different candidates for getting the nomination – I mean, that sort of thing. There's a process for this. It's all in the open, it's transparent. There's no secret cabals who are deciding things, and I think the more people are acquainted with that process very intimately will see that it's actually not as, you know, James Bond-esque – (laughs) – as they think it to be. And that's where civics comes in. So civics, digital media literacy, and the cyber hygiene, they are three sides of an important triangle that will lead to a safer and more resilient democratic discourse.

MS. SPAULDING: Yeah. Yeah, I think understanding how those processes are supposed to work, and I think in the election context that there is a process. If there

are allegations made about having interfered or altered or disrupted an election, that there is a process in place, and for trusted voices to get up and say, look, there is a process for assessing this, and this is how it's going to play out, so helping the public understand how these institutions work and how they are held accountable. But also, as you said, understanding the role they play, right, in holding institutions accountable because I do believe that a big part of the information operation against our democracy is to say the system is irrevocably broken, right? It's not just that there are problems with the justice system or, you know, that there is divisiveness in our population. It is to say it is irrevocably – and there is nothing you can do about it, right? And that's the most pernicious messaging. So this notion of helping people understand how to be engaged becomes critically important in that public resilience piece.

But it's also, Chris, important in the specific cyber context, which is the question from the audience. We always talked about it being a shared responsibility, right?

MR. KREBS: Yeah, so I love this question of why civics matters in national security because why and how does democracy work. It works through participation. What is the overarching objective of the Russians in the '16 case or whoever else? It's to undermine confidence in the process, and it's not just here, but it's also in their immediate, near abroad, sphere of influence – look, democracy is broken. It's chaotic, it's doesn't work. You know, you need to come into the fold, and we'll take care of you. That's really what we're pushing back against here, and only through actual participation – and it's not just the 2018 midterms or the 2020 election; it's overall undermining of just the democratic process.

And I would actually step back and look bigger than just elections. I would look at ransomware. Look at ransomware. It's hitting state and local jurisdictions, and public institutions on a daily basis – big, big hits. It is undermining confidence in the ability of public services being delivered on a daily basis. What else is more pernicious and slower death by a thousand cuts than ransomware?

So we've been talking a lot about the big, big – you know, the big four: China, Russia, Iran, North Korea, but at the same time, we've got this emerging cybercriminal base that is actually probably doing more harm to undermine our confidence in public institutions, and we've got to do a lot more to push back against that specifically.

MS. PLUNKETT: Suzanne, just – I'd like to make a quick comment –

MS. SPAULDING: Yes.

MS. PLUNKETT: – just that we have to keep remembering that our children are watching, and one day they will be us, and it won't be very long. And what an opportunity we would have now if we would start helping them to

understand what it means to be responsible citizens, helping them to better understand cybersecurity and the nexus between it, and bad things that might happen. They are experts on the very networks that we worry about. We have to make sure that we are instilling in those institutions – academic institutions, you know, families – the importance of using this. They are watching. I know they're – I hear from – they're watching us. We've got to do a better job.

MR. MURPHY: At that point – I mean, I have two kids. Maggie Murphy is 13. My son Jack is 10. And Jack and I were watching the debate last week, and he turned to me and he said, oh, Mike Bloomberg, I know who he is. And I said, how do you know about Mayor Bloomberg? And he said – he goes, his commercials come on while I'm playing Fortnight. I mean, they are watching.

MS. PLUNKETT: They're watching.

MS. SPAULDING: Well, and I think if we had still a sense of civic responsibility, right, that that should help as well. I used to always talk about how, you know, people allowing their connected devices, whether it's their printers or their routers or their cameras, to be used, for example, as part of a bot to attack others, well, there's no consequence to that individual, right. And so there's a tendency to sort of say, you know, it's not bothering me.

But if somebody was tunneling under your house, was down there, not bothering you at all but digging tunnels to all your neighbors and robbing them, right, you would not think that was OK. And so that's the kind of civic engagement and responsibility that I think also can help us instill in folks. We do have to make it less burdensome for that end user and cybersecurity generally. But I don't know that we'll ever fully take away the responsibility, and even just as responsibility of being an informed consumer, so that as consumers, we demand that products are more secure. That's a kind of civic responsibility that also needs to be part of that civic education.

MS. JANKOWICZ: Can I jump in with one quick point, too, that came up for me as you were talking, Suzanne, and that's for any of our friends in the media who might be here today or who are watching online, it's also incumbent on you to be very precise in your language. I am so tired of seeing headlines about the hacking of the election when nothing that's being talked about is actually hacking. It's something to do with disinformation or something like that.

So when you say hacking, mean hacking. When you say disinformation, make sure you're meaning disinformation, information that is shared with malign intent, and not misinformation, which is without that malign intent, or mal-information, which is like the hack and leak that happened to the DNC. Get to know these terms. There are people who are happy to

help you. It's important that voters understand what's going on. And right now we're being a bit sloppy about it.

MS. SPAULDING: Yeah, yeah. That's exactly right. And it leads to – unfortunately it leads to a diminished credibility of the voices that are trying to, you know, kind of educate the public in their – yeah. So it's a really important point.

And I do think – my sense is that journalists have gotten much more responsible in the way that they write generally – Chris, I'd be interested in your – what you're seeing on this – in the way they write about election security and vulnerabilities, so as, again, not to play into – not to overstate the vulnerability within the system and not to play into efforts to get the public to think you know, the system is broken anyway, and therefore I might as well not vote because I can't even be sure my vote's going to be counted or counted properly.

MR. KREBS: So this is one of those things, going back to that whole-of-nation, that shared-responsibility piece. Rather than just wagging fingers, we're actually bringing media partners in and running through tabletop exercises and scenarios and positioning some issues in front of us and say what would you be looking for in this case, what kind of information? What should we be thinking about?

And I think it has gotten to an increased maturity and sophistication in the level of reporting. I'm – that's one of the things I'm actually fairly hopeful about as we go into '20 is that there is better reporting than there was in '16 because we've worked through the issues. But still, it is – you know, it doesn't take much for there to be a feeding frenzy.

And so, for us, it's about being very proactive and transparent in our reporting even if we don't have a lot to say. So back during the Iowa caucus, I went on the record quickly and pretty affirmatively saying, I'm sorry, no, we actually did not test that app. And why did I do it? Because there was one news report that had been spun into three or four other news reports that we had tested the app. And that was misinformation and it was propagating, and I needed to nip that in the bud. And the correction in the original article was not going to do the job of stymieing further transmission, so to speak, of that information.

So those are the sorts of things that we have to be quick about, and that's really, really hard.

MS. SPAULDING: It is hard. It's particularly hard when you don't want to repeat false information. You don't want to give more life to disinformation particularly. And so then you sort of are watching to see, is this getting traction or not; once it gets traction, we'll jump on it; at which point, you know it can often be too late. I do think it's a – it's a real challenge.

Chris, I want to ask you one last question about DHS's role. Are there authorities that you wish CISA had when it comes to the information environment, when it comes to – whether it's talking to the platforms, you know, getting things taken down or getting things labeled/marked properly? Are you – are you comfortable with your working relationship with the platforms? And are there authorities, whether vis-à-vis the social media or other contexts, which you think it would be useful to have more of?

MR. KREBS: I think in terms of the information/influence operations space we're still in the early days and we're still trying to figure out what the relevant authorities are. I think we've got what we need right now to be effective.

I think there is a mix of cyber vulnerability information sharing that we need to continue working on. We've talked about the ability to, when we detect vulnerable systems out there on the internet, particularly in hard infrastructure or voting machines, that we need to be able to engage the owner-operators, and that's really difficult when they're sitting under the umbrella of an internet service provider. So we're working with the Congress on a couple bills there.

But kind of circling all back to the beginning, one thing that I think everybody, I'd like really like to keep in mind was, look, in '16 they claimed to have hacked the elections. They didn't actually change any votes. They were not in a position to change votes. When we think about '16, we also have to get back to the strategic objectives of what they're trying to accomplish, and that's undermining confidence in the process. To hack election machines across the country at scale and in an undetectable manner is really, really, really hard. OK, maybe that's not their strategic objective, though. If it is just to destabilize the process, maybe they want to pop up in one spot and say, look, we're here, we're also in a bunch of other places; come find us.

We've got to be prepared. We've got to be ready for this. We have to understand what their game is and how they're going to go about it and not accept the garbage they're going to push at us. This is part of that suppressing demand of making a more discerning public and also working with the media. This is going to – this is going to be the hardest thing that I will ever do in my career right now in the next couple months, and it's going to take a whole-of-nation effort to push back against it.

MS. SPAULDING: So I think that's a good place to leave it because I think the final message there, implicit in what you're saying, is that people need to – need to be resilient. They need to get out there and vote, and not be dissuaded by the efforts to depress turnout, or to get you to shrug your shoulders about the idea of truth, or to get you to give up on democracy, right?

MR. MURPHY: Let's give a round of applause for Suzanne for keeping – (applause).

MS. SPAULDING: Thank you to our great panel. Patrick, glad you stayed. And thank all of you for coming this morning and for your interest and all that you do. Thank you. (Applause.)

(END)