THE BROOKINGS INSTITUTION

SAUL/ZILKHA ROOM

NATIONAL SECURITY IMPERATIVE OF ADDRESSING FOREIGN CYBER INTERFERENCE IN U.S. ELECTIONS

Washington, D.C.

Friday, September 8, 2017

PARTICIPANTS:

MICHAEL O'HANLON, Moderator
Senior Fellow and Director of Research, Foreign Policy
The Brookings Institution

JOHN R. ALLEN
Distinguished Fellow and Chair, Security and Strategy
The Brookings Institution

SUSAN HENNESSEY
Fellow, Governance Studies, The Brookings Institution
Managing Editor, Lawfare

ALEX HALDERMAN
Professor of Computer Science & Engineering
Director, Center for Computer Security and Society
University of Michigan

DEAN LOGAN
Registrar-Recorder and County Clerk
Los Angeles County

* * * * *

PROCEEDINGS

MR. O'HANLON: Good morning, everyone, and welcome to Brookings. I'm Mike O'Hanlon with the Foreign Policy program, but we have an ecumenical cross-program team here from not just Brookings, but across the country to discuss the crucial issue of foreign elections -- excuse me, foreign interference in American elections, especially through cyber means, but more generally the national security threat to our democracy that we saw vividly last year and that remains unresolved. We've got a remarkable panel that I'll introduce in just a second, but let me, please, first remind you a little bit of the nature of the issue and where we stand in trying to address it.

On the latter point, just as a little metaphor for where we stand, I'm wearing my lucky shamrock tie today not because it's St. Patrick's Day, but because this seems to be about the extent of our strategy so far on how to deal with this threat, which is hope for the luck of the Irish. (Laughter) I don't think we've gotten a lot beyond that. And today's panel is going to help us figure out how we can do better. I am not the expert, they are. All four of them have extensive experience in the broader issues of cyber at one level or another and also elections, and I'll get to that in just a moment.

I want to remind you very briefly of the stakes and I'm sure most people in this room are well aware that on January 6th a multiagency report of the U.S. intelligence community asserted with high confidence that there had been significant meddling in the 2016 elections. It probably did not change vote tallies, per se, but that, you know, it could have done a lot of other things. And I'm just going to very briefly read from a couple of the key findings of that report.

"We assess with high confidence that Russian military intelligence used the Guccifer 2.0 persona and DCLeaks.com to release U.S. victim data obtained in cyber operations publicly and in exclusive ways to media outlets and relayed material to

WikiLeaks. And also that Russian intelligence obtained and maintained access to elements of multiple U.S. state or local electoral boards."

Since that time, which is now almost it seems a lifetime ago in American politics, we've had a number of other reports, including something Michael Chertoff wrote about this week in the *Wall Street Journal*, big problems in Chicago with hacking into databases of voters there. We've had some *New York Times* stories about how various kinds of voter registrations that were being done electronically seemed to have been hacked into; may or may not have impeded the actual vote tallies. It didn't seem to change any votes, but certainly slowed down voting even on Election Day. So we are perilously close to a situation where even the last elections may have actually be affected in their outcome in some ways, leaving aside all the issues of false news and information operations along those lines. And we're not necessarily any better to being prepared for the next time around.

So today's panel is going to help us figure that out. And again, I'm delighted that all of you are here, as well.

Immediately to my left is my good friend and co-director for our defense team here at Brookings, General John Allen, retired General Allen, who, of course, he's a Marine and Marines love to tell you that they're not big thinkers. But I think we can decisively put that theory to rest at a time when we've got the James Mattises and John Kellys of the world holding together a lot of the Executive Branch. And retired General Allen is working a good deal on artificial intelligence as one of his main research areas, including on the very issue of election security that we're talking about today.

Next to him is my good friend and colleague Susan Hennessey from our Governance Studies program here at Brookings. She's also the managing editor of the runaway hit Lawfare. She is a graduate of Harvard Law School and alum also of the

National Security Agency where she worked on these issues from the inside, but has been one of the most prolific and illuminating writers here at Brookings on these topics and, frankly, one of the most illuminating writers in the entire country. Thrilled to have her part of the panel.

Just to her left is Alex Halderman, who is a professor of computer science and engineering at the University of Michigan, where he also runs a program Computer Security and Society. You might call him a patriotic hacker of sorts in the good sense of the word. He has been involved, and I'm maybe taking some liberties with that term, but his bio emphasizes that he's been involved in testing various American cyber operations of electoral registrations, vote count systems, et cetera, to see how easily they could be hacked and, therefore, to try to figure out how severe problems were. He's done this in regard to D.C., California, and he's been active around the world in helping improve election security from India to a number of other countries, as well. We're just thrilled that he flew in from Michigan to join us today.

And even further away is Dean Logan, who came on the red-eye overnight from Los Angeles, California, where he is the registrar-recorder and also the county clerk for the county of Los Angeles. And, therefore, oversees and is officially responsible for elections in the most diverse and largest county, single jurisdiction, local election system in the country. So he's seen in it all in a part of the country that, again, combines all the different elements of cyber risks and concerns that we see today. He's also the president of the California Association of Clerks and Election Officials and is involved in a number of initiatives out there, as well.

The format for today will that we'll essentially go down the row and then back with two big questions I'm going to pose sequentially to each panelist. And then we'll go to you for the second half of the discussion with your questions and concerns.

And so, John, if I could begin with you. And again, it's going to be essentially the same question for everyone, but I may rephrase it slightly from person to person. If you could just help us understand how you see the nature of the problem today, the threat to American democracy and elections from foreign interference through cyber.

GENERAL ALLEN: Well, Mike, thanks very much. And ladies and gentlemen, it's terrific to have you here with us at Brookings this morning and to share the panel with three magnificent authorities on this subject: Susan, Alex, and Dean. And Mike, to your tie, my name doesn't sound like it, but I am also Irish and I had this moment of panic that I had missed St. Patrick's Day. (Laughter) I guess I did, actually, and wondered whether it was today or not.

And to the Marine four stars who are wandering around Washington I'll add a fourth to that number and that's a fellow by the name of Joe Dunford. He's the current chairman.

Look, my concern is one that's based in many respects upon both our national and -- our national security, but also our domestic security. I stood in front of the National Association of Counties about two months ago at their annual convention and I gave them a brief on what I believe to be a systematic, large-scale strategic influence campaign that for the first time in my life over 40 years wearing the uniform, after having participated in multiple conflicts overseas in Iraq, Afghanistan, against the Islamic State, I looked at that group in the audience and I said, you know, I always felt pretty proud being Marine that I could say that I was part of the first line of defense of the United States of America. And that I had spent most of my life defending the institutions of American democracy. But I then said to them with complete sincerity I now think that you, the leaders of the counties of America, in many respects are the front line of defense of the most profoundly essential institution of American democracy and that’s our voting and protecting our voting system and our voting records and the integrity of the system.

And I think two things have happened now as a direct result of this Russian campaign. And let me just make a quick point about the Russian strategic campaign. Russians have got a lot of help in this. And whether it’s the Chinese entity, which I think is less involved specifically on electoral intrusion, or whether it’s Unit 180 of the North Koreans, who using that entity or another organization called Lazarus might, in fact, be attempting to strike the American electoral system -- election electrical system as a direct result of some of the problems we’re having now today; or the Iranian cyber army or the Syrian electronic army or the digital caliphate of ISIL. These organizations have a lot of capacity to share assets and resources across their capabilities.

My very sincere concern is to prevent a conversation like this from going immediately to the issue about cyber issue. And we’ll have to talk about that because that’s a very important part of it. But one of the most important outcomes of the Russian influence campaign, frankly, ladies and gentlemen, is not just to have the capability of intruding into records and processes, but, frankly, to shake the confidence of the American voter in that most profoundly important aspect of the American democracy, which is our voting, which is what defines us as a great democracy.

And so not just have we seen that here in the United States. I spend a great deal of my time overseas and in particular in Western Europe, and in particular working on issues associated with NATO. And we’ve seen that the same influence campaign, which not only leverages relatively advanced cyber capabilities, but an influence campaign where those cyber capabilities are tucked up inside a broader narrative, which is supported by the intrusion of fake news into social media and the use of social media itself; and organizations of trolls, which ultimately comment on the news that they have seen and then further echo it and further retransmit it. It's a very sophisticated campaign.

And so we see that institutions like the EU and NATO are under direct attack in this regard to shake the confidence of the people in the institutions, to shake the confidence of the people in their own governments, and to shake the confidence of the people in their processes ultimately for the selection of their leadership in these liberal democracies, which is basically all we've got left is this organization of liberal democracies.

So as a guy who's spent a lot of time overseas dealing with what I believe to be threats to America, I now recognize that at the speed of light the very heartland of America is under threat today. And I stood in front of the county leadership with all sincerity and told them that the enemy has moved beyond my reach both in terms of my retirement, but also in terms of our capacity to deal directly with this issue. And now in many respects the first line of the defense of American democracy and the last line of defense of American democracy is in the hands of our states and in our counties.

And so, Mike, that's my concern. And I'll stop there.

MR. O'HANLON: Thank you, John. Extremely well couched and sets us up wonderfully to go next to Alex. Susan, if you don't mind, I'll save you for the Bryce Harper position in the batting order, and ask Alex to now frame for us the problem. And again, after we go down and begin to understand the problem, we're going to come back through the same lineup and ask for solutions. So that's the basic format for this morning as you probably have surmised already. But Alex, over to you.

MR. HALDERMAN: All right. So continuing with the problem, and I have to thank you. That's just such a wonderful way to set things up because I couldn't agree more than we're, unfortunately, living in a world where the states and even the counties and local municipalities running elections are suddenly on the front lines of international conflict.

But I want to focus my remarks on the state of vulnerability in our election system. Because when we ask, well, are we having a crisis of voters not having sufficient confidence in elections, one really important piece of that is, well, how much confidence should we rationally have in the results of our elections? Are our elections able to provide us with high confidence the way they're being conducted today?

And much of my research in cybersecurity over the past 10 years has been looking at the election equipment, the election implementations, the computer voting machinery that powers American elections and elections around the world. And I can tell you based on that experience I don't have a lot of confidence. So let me explain a little bit about some of the vulnerabilities in election equipment.

American elections today are highly computerized. We rely on computers to manager our registration system, often to managing check-in at the polling place, in many states to count the votes, to receive them from voters and count them, and then finally to tabulate them from across the state and report the outcome. All of these different steps rely on different kinds of computer infrastructure.

The infrastructure for voting, maybe that's the piece of infrastructure that people in this room will have had the most direct experience with, consists of two primary styles of voting machines: either optical scan machines where the voter fills out a ballot and then usually puts it through a computer scanner right in the polling place or puts it in a ballot box to be later scanned at a central location; or the other style is what's called DRE or direct recording electronic voting machines, where the voter interacts with some kind of computer or electronic machine that will take their vote and record it in an electronic memory.

Both of these styles of machines, the optical scan machines and the DRE machines, have been in many cases across the country -- now the models in use have been taken into research laboratories by independent security experts or academics, and in virtually every case where such a study has been conducted by a qualified group the findings are that the machines have vulnerabilities that could allow someone to hack in and alter the software that's running on them in ways that would potentially allow an attacker to change votes. These are findings that have been found in state-sponsored studies in California and Ohio, findings that I found myself in my own work.

One story, for instance, 10 years ago, my research group while I was a grad student at Princeton, we got our hands on the most widely used touchscreen voting machine in the United States, the Diebold AccuVote TS. The manufacturer claimed very good high level of security. After a couple of months of reverse engineering this machine in the laboratory, well, we had found that basically there was no effective security in this machine. With just momentary physical access to the memory card that's used to program the ballot before the election, we could insert vote-stealing software that would then reprogram the machine and cause it to forever after behave dishonestly and select whoever we wanted as the winning candidate.

Now, you don't even need physical access to the machines to perform this kind of attack. Because as I mentioned, before every election essentially every voting machine in the country needs to be programmed the design of the ballot. Who are the candidates? What are the races? Study after study has shown ways that by corrupting that ballot design file you can introduce malicious software into the machine, essentially like a computer virus would spread.

Those ballot designs are created on other systems called election management workstations that could be operated by the county or could be operated by an independent contractor. If someone can hack into those machines, which often aren't very well protected, then they can spread malicious software, vote-stealing software, to voting machines over a very wide area, a state, maybe a county, it may be a large portion of the state. In Michigan, for instance, 75 percent of counties use just 2 small independent contractors to do this pre-election programming. Those are just the biggest bull's-eyes I can imagine for sophisticated attackers.

So we have a problem of insecure equipment. We have a problem of registration systems on the Internet that, we know in 2016, DHS says at least 21 state registration systems were probed in an attempt to break into those online databases. We know that at least one vendor of election equipment was targeted by attackers in 2016 in attempt to break into their systems and thereby spread infiltration attempts to their customers, the local municipalities.

So we know that these attacks are no longer just purely hypothetical. They're now things that powerful, sophisticated adversaries are attempting.

Now, whether any of them have succeeded so far we don't -- in changing votes and actually influencing the output of the election infrastructure, we don't have any strong evidence that that has happened yet. But I think it's only a matter of time.

Ten years ago, when I started this, if you had asked me is it possible that foreign governments could hack into American elections and change the result, I would have said, well, maybe that's a theoretical possibility, but it sounds like science fiction. Well, today we're hearing about nation state cyber attacks every day, including attacks against some of the most well-hardened targets. Our election systems are known to be vulnerable and they are being targeted, and it's only a matter of time until an attack succeeds.

MR. O'HANLON: Thank you. Very stark and sobering framing of the problem, but very clear, as well. And appreciate sort of the technical primer. Let me ask one quick follow-up before going to Susan.

In light of what you just said, what’s your best guess as to why apparently Russia didn’t change vote outcomes in 2016? That they just didn’t try or that they might have tried, but not just gotten around to it yet, but next time they probably will?

MR. HALDERMAN: Oh, that’s just such an excellent question and I wish we had all of the information that the intelligence community has available to them. And I’m not sure that they have -- they haven’t given us a lot to go on to answer that particular question.

My best guess, though, would be that there has long been a pretty strong norm against cyber attacks on election systems. I think that’s a norm that our government has maintained. Right? We certainly have the capability to hack into other people’s election systems. So going that extra step and hacking into ours would have been a severe escalation of cyber warfare.

My best guess is that they were afraid of the retaliation that they would receive, especially after it became apparent that the Obama administration was aware of some of the attacks that were happening. I’d love to know what others’ best guesses are.

MR. O'HANLON: Good, thank you. Susan, over to you. And again, the same question, just how would you define the basic problem?

MS. HENNESSEY: So first, I wish I could show the audience all of your faces as Alex was speaking. (Laughter) And sort of your jaws were dropping as were all of ours.

So, look, we shouldn’t kid ourselves here. I think we should be candid and frank about the nature of the problem and how frankly terrifying it is. But there really are two different ways we should be thinking about sort of our electoral system, our election infrastructure.

And one is the broader context in which elections occur. The sort of process of public debate and information and sort of all the things that surround elections that are important parts of how we go and make that sort of critical core democratic choice that General Allen was discussing. And then the second is the actual management and administration of elections. And I do think we have to think about those two things sort of in separate buckets because the threats and solutions and the risks are quite different.

So in terms of the threat to that broader context, things like disinformation campaigns, we know the threat is high. We know it materialized. We know it will happen again. I mean, it will happen again until we candidly address it as a country. There's complex solutions and in some cases they're going to come up against core values, like freedom of speech. And those are going to be difficult questions, but they are ones that we're going to have to address.

The second issue, that bucket of election management and administration that Alex was really speaking to, is the more complex and potentially pernicious threat. I feel relatively confidence, although less so after hearing you speak, that, one, Donald Trump is President of the United States because the appropriate number of Americans in the appropriate jurisdictions actually went and pulled the lever for him. I think that's a really important thing that Americans can have that level of confidence, that whatever we think about the broader context, our fellow citizens went and made a democratic choice and that choice is being lived out at the moment.

The second sort of issue, though, however, is the confidence that we might have. So you don't actually need to target all of the various electoral systems, hack all the right machines that are different in the right counties. That requires quite a bit of sophistication, political sophistication, knowing where to target.

The other issues is -- so it requires political sophistication in knowing where to target. You also have to do it without detection. So you might be able to do something without forensic detection, but you also have to be able to do it without the detection of our intelligence community. And so I do agree that it would be good if the intelligence community could come forward, provide more information. They're in the difficult position of trying to protect sources and methods, so they have challenges of their own. But that's a pretty difficult challenge right now, so I don't know that that risk has materialized.

There is, however, something that's far easier to do, and that's to undermine confidence and to create and to insert real questions about the outcomes of elections. And all you really need to do for that is to penetrate systems such that it raises questions for smart people who say I'm not positive anymore that this election, that this outcome is actually valid. And that is sort of the broader question that we're all going to have to address.

And ultimately, it comes down not just to a question of cybersecurity, but one of messaging. There is a sense in which we can have the conversation about how vulnerable our election systems are, how uncertain we should be about the results in a way that actually achieves the end. Because we're all talking about how insecure it is, all of a sudden Americans are thinking, geez, did we really elect this person? Can we really trust the outcome of our vote? And in some ways we have achieved our adversaries' own goal.

Now, the prevention of that is not just to put our heads in the sand, but we do need to have a really careful conversation that addresses the real vulnerabilities, talks about solutions in a way that, at the same time, is sensitive to not wanting to actually create the bad outcome of undermining that overall confidence. So it's a very delicate dance and I think it's one reason why it's really important to have the conversation right now, far enough out of the next election, so that we can have sort of a non-political, non-partisan conversation about how we're going to address these issues moving forward.

MR. O'HANLON: Thank you. And Dean, to stay with the baseball metaphor, batting cleanup from the land of the Los Angeles Dodgers, who we all in Washington are terrified by, maybe a little bit less so the last couple of weeks.

MR. LOGAN: As you should be. (Laughter)

MR. O'HANLON: But yeah, we are, don't worry. And thank you again for flying across the country to address this important topic with us and we'd love to begin with the same question to you. Just how do you define the problem and its seriousness?

MR. LOGAN: Great. Well, thank you, first, for the opportunity to be here and appreciate the -- it's very humbling to be on a panel with people with this expertise and background in these issues. And I appreciated your introduction. I'll riff off of that a little bit and say that I think key to this discussion, I think the real point here from an election administrator's standpoint is I haven't seen it all. I've seen a lot as an election administrator, but I think that that's a central message to what we're talking about here is none of us have seen it all and there's more to come. And I think that, from a practitioner's standpoint, is kind of the defining issue, is that we are now in a position where we have to anticipate those things that are known, but also prepare ourselves to deal with those things that aren't known.

And I appreciated the way that the discussion was framed by General Allen and always appreciate Alex's doom-and-gloom framework that scares us all and makes me long for my days of being a shoe salesman instead of election administrator. (Laughter) So I appreciate being able to do clean-up because I also really appreciated Susan's perspective about how we message this. And I think I'll try to kind of piece this together from my standpoint.

First to say that the threat is real. I mean, certainly I don't have to reframe that based on what we've all heard today and what we've seen. We wake up every day and hear about new vulnerabilities, new attacks, new information or theories about what happened during the 2016 election and what could happen in the future. This morning we wake up to an article about the vulnerabilities of the German electoral system and their upcoming election, which goes to the broader framework that General Allen talked about. We're also reading today about the massive data breach from Equifax. And all of those things are relevant to the discussion we're talking about.

So as election administrators we have to be aware of that and we have to recognize that and recognize that that is a part of our responsibility now. It's not solely our responsibility, so I was encouraged to hear General Allen say that he was making that presentation before the National Association of County Officials. And hopefully, that same conversation, and I know it is, is happening in forums like the National Conference of State Legislators because this is not something that can be resolved or combatted simply at the local election administrator level or even state election administrator level.

We operate in a decentralized environment that has many advantages to that, but we also operate in an environment where elections in this country, by and large, are under-resourced. Under-resourced in terms of just raw funding, but also under-resourced in terms of training, expertise, and equipment to combat the kind of things we're talking about.

So in one sense, that's daunting. In another sense, it's encouraging.

And I agree, this is the time that we need to be having this conversation. I will say it’s not a new conversation in the election administration field. We’ve been having this conversation for quite some time and there is important work being done in this space, but there’s more that needs to be done.

We need to recognize that this is an influence campaign. And I think one of the dangers historically that we have seen in the elections process is we tend to spend all of our time focused on looking at what happened in the last election and diagnosing that and not looking forward to what could happen in the next election. I’m not saying that they’re mutually exclusive; both have to be done. I mean, we should learn from what happened in 2016 as we prepare for 2018 and 2020, but we can’t get so stuck in the weeds of what happened in 2016 or what was perceived to happen in 2016 that we find ourselves the month, the week, the day before the election in 2018 and unaware of those things that we don’t know that are happening in the current election cycle.

And I guess I would close by saying that the other thing that I think is we have to look at this from a holistic standpoint. Yes, what’s new is this nation state influence, and that’s big, it’s daunting, and we’ve got to pay attention to that. That doesn’t take away from the additional threats and vulnerabilities that were already existent in our election system and that we’re working towards. So we have to look at this holistically and we have to look at the way it’s framed to the electorate.

Because the other crisis we have that I think we have to be very aware of is we have a crisis of participation. When we have the electorate waking up every day hearing reason to believe that they shouldn’t have confidence in the 2016 election or that they shouldn’t have confidence in the ultimate power of their vote, which is the foundation of our democracy, what that leads to is lower voter participation. And in the end, if we put all the resources necessary, which is a big if, in combatting the issues that we’ve talked this morning and create a secure system, a secure system is of no value to our democracy if people aren't participating in the election, if people aren't showing up and voting and making the decisions that are left to the electorate to make in this country and that we value. And we are seeing slippage in that.

And so we need to be sure that we are conveying a message about where voters can get the right information. What are the trusted sources of information? We need to be honest and up front about the environment we're working in as we're working through the threats. And we need to convey a sense that the best offense is participation and that complacency and lack of participation is not going to be an effective defense to this threat.

MR. O'HANLON: That's excellent. And before I start with you and then come down the row asking for what we need to do about the problem, especially what we need to do that we're not yet contemplating or making happen, I want to follow up with one quick additional question that you've all made me think of in listening to your openings.

And that is, you know, understanding the nature of the cyber threat to our elections, there are several categories of concern. There's the concern about sort of false news and propaganda. There's the concern about email theft and release, the WikiLeaks DNC kind of thing. I was well aware of those two before today and I think most people were. Then there's the concern about the interference in the processing and, you know, the event of the election and the voting itself. And that's what some of the *New York Times* and *Wall Street Journal* reporting and Bloomberg and others have been sensitizing us to, that there were some efforts to complicate people's access to their vote. And then there is the Alex scenario of actual votes being changed, if not already, then some day.

So those four categories, sort of propaganda, false news, social media misuse; and then theft of email and sort of disclosures that are embarrassing or harmful; and then slowing down or putting molasses or interfering with access to the vote; and then changing the vote. If those are four categories of threat, which is the most serious so far? And is that going to be the one that's the most serious next time?

Maybe that's too vague of a question, but I hope you can at least help me think it through a little bit because I think I heard from Alex that hypothetically the last category could become a much greater concern even if it wasn't last time. But I want to see if others would rank order these threats, if the question makes any sense to you at all. If I'm just spouting gibberish, feel free to tell me so and we'll go on to the next question.

MR. LOGAN: Well, I think a lot of that depends on where you sit and what your role is in the process, so I think it's hard to prioritize one over the other. I think, and you probably can guess this from my remarks, I think for me as an election administrator the most immediate threat is this crisis of confidence and crisis in participation. Because in my world and in my operation, while we're between elections that's another thing that is often misperceived. The next election for me isn't in 2018. The next election for me is the first week of October. So, I mean, we are constantly in an election mode and we have to continue.

I mean, the health of our democracy depends on continuing to conduct elections and continuing to let that process go forward. And as I said, if people aren't participating, then we're losing in that battle. And arguably, if people aren't participating, the chaos that General Allen has been created and they've successfully derailed our election system without even having to hack it.

GENERAL ALLEN: Or go to war with us.

MR. LOGAN: Right.

MR. HALDERMAN: Yeah, so I think you're right, it depends where you sit. These are all serious threats, though. And I think we can simplify the taxonomy just a little bit into kinds of information warfare and kinds of cyber attacks against election infrastructure.

We've seen attacks in both of those categories in 2016 and I think we're going to see them become only more sophisticated going forward, so we need a strategy for defending against both information warfare and attacks on election infrastructure.

MR. O'HANLON: Good, thank you. Susan, any comment?

MS. HENNESSEY: So I broadly agree, we're going to have to learn how to walk and chew gum at the same time on this. We have immediate threats and we have long-term threats, and ignoring one at the expense of the other is sort of a recipe for disaster.

I think what we need to understand holistically is this is the core of our democracy. This is not some, you know, tangential issue that comes up once every two or four years when we're all thinking about. This is really what it means to be American. This is a central -- you know, the fact that we only just designated it critical infrastructure coming up to the last election as opposed to recognizing it as critical infrastructure, sort of the most critical infrastructure, from the outset really speaks to the need for a pretty strong wake-up call and for the necessary resources and awareness that should follow.

MR. O'HANLON: John, any thought on that question?

GENERAL ALLEN: It's a tough question, very complex. I think from my own experience working counterterrorism issues, much more human behavior has been a result of perception than reality in so many ways. And to Dean's really important point, and the panel has touched this, the enemy wins if the American voter perceives that there is no value ultimately to going to the polls anymore because no matter what I do it isn’t going to make a difference. There’s the potential that my vote has been compromised. There is the potential that the system overall will not register my or the population’s views as members of a democratic society. And so we have to do several things.

At the ground level, because all politics is local and, by coincidence, all voting appears to be local, it doesn’t make any difference when John Allen shows up in front of a conference and briefs county executives or county officials on the problem. What matters is what happens as a direct result of that or what happens as a result of the activities occurring at the county, as well. And I think there’s a twofold dimension to this.

One is that county officials and state officials have to constantly be educating the voter that it is inherent responsibility in a democracy such as ours for Americans to go forward and vote. You know, we are very quick to point out all the things that government should be doing for us in a democracy. But inherent to a democracy functioning is the voter or the members of the population assuming the responsibility for the strength of the democracy, as well. And in a very real way the strength of the democracy of the United States is founded upon our capacity to register our opinions through the voting process.

So first and foremost, I think Dean made an extraordinarily important point and that is we have got to teach the American voter that the enemy wins if we cease to vote. The enemy wins if we have struck an absence or created an absence of confidence or a crisis of confidence in the process.

But then the county and state officials have to do all they can to try to resolve the issues that Alex has talked about, which is to bring us to a system that may be proof from interference. And, of course, we know that there’s virtually no system on the planet that is proof from interference, but there is the capacity, and we know this as time has gone on, there is the capacity to layer mechanisms of defense and systems of defense that can give you a relatively high confidence. But the problem is, because so much of the voting process in the United States is local, the problem is there are very unlevel approaches from county to county and state to state across the country. One of the reasons is because we don't impose federal standards on this process.

So the more we can do at the county level and state level to help our officials at that level to understand the problem, and clearly we have one of the leaders in the country sitting on this panel right now in terms of both understanding it and embracing the solutions, that's not the case in other places. And I've had very intimate conversations on this with other counties where their capacity for cyber defense or cyber protection is very, very limited. And until we're able to provide both education and resources to try to support the integrity, the electoral integrity, the cyber integrity of those systems, then we're going to have difficulty in ensuring that American voters have confidence in their system, as well. That's our challenge right now. It's a two-headed challenge.

MR. O'HANLON: So thank you. And now let me ask, starting with Dean, so what do we need to do that we're not doing? And how much help, by the way, do you need and want from Washington? Recognizing that elections are local and state responsibilities for the most part; recognizing that sometimes it's even hard to have the conversation with Washington about the problem because you get into classification issues, local officials may not have the clearances; recognizing that Washington doesn't seem able to pass budgets to help even when it wants to on some issues. So what do we need to do about these problems specifically and what would you like to see Washington help you with the most?

MR. LOGAN: Well, I think first and foremost it's acknowledging the threat, recognizing the threat, which we've already talked about. And then I think we have to frame it in the context that we've just had here.

I think it is going to require layered solutions and what we need from Washington versus what we need in our local jurisdictions or in our states is going to vary as much as the election jurisdictions do around the country. I think that right now we're at a place where the critical thing is information sharing. We need to be sharing information. We need to be sharing information in a timely manner. We need to be sharing information in a context that can be absorbed and understood by the people that we're talking to, and that means election administrators are one audience for that, but, as I said before, county councils, state legislators, and county information security officers and state information security officers are key components of that. This is not something that, as you say, in most jurisdictions, or as General Allen said, in most jurisdictions this is not something that the election administrators themselves is going to have the capacity or expertise to tackle.

I will say on a positive note I think that train has left the station and I think that's evidenced by, I can tell you as an election administrator, it's evidenced by how frequent the communication on these issues is happening. In the space right now it's evidenced by the fact that we have two members of the U.S. Election Assistance Commission sitting in this room today for this dialogue, who I hear from on a daily or if not weekly basis on these issues. By the way, not just post-2016, but pre-2016 elections and during the election cycle.

It's evidenced by the decision to make the critical infrastructure designation. A lot of questions about what that means and how those resources are going to be distributed and how that ultimately functions. So there's frustration around that because it's new and some information's not coming as timely as we would like it, but I think that there are signs that that's happening. I think it's recognizing the shared responsibility, so I talked about that before.

And I think it gets down to kind of the nuts and bolts, and that's where I go back to my comment about the next election is next week for a lot of jurisdictions. So, yes, we have to figure out what we need from Washington in terms of resources, what we need from our state legislators, but we also need to figure out what do we need for next week. And for next week we need policies, like solid commitments to post-election audits, risk-limiting audits; a commitment to a standard of a tangible paper ballot of record that you can go back and verify the totals. That was an interesting point made in the articles today about the vulnerabilities in the German election was that ultimately they have a paper ballot that they can go back to. But again, a paper ballot's not of value unless you actually do go back to it and check it against something on a regular basis. So, in some cases, we lack good best practices and good, clear policies in that regard, so I think that's an important place to start.

And I say that because the reality is that the systems that we need that will best combat this aren't on the market today. We operate in an election environment with a very limited market, a very proprietary market, which I'll link to the stories about the Equifax vulnerability and the timeliness of when that information was provided. And when you operate with proprietary systems that are commercially based, we as the public officials that run elections don't have control of when we get the information about a potential hack or a vulnerability. We need to address that, so we need to create an environment where when something happens, to steal a line from TSA, when you see something, say something. And so if you see in a particular state or a particular voting system that there's a potential vulnerability or a potential intrusion, we need to create an environment where it's safe to talk about that and it's safe to talk about that and to create a mutual aid process in response to that.

Parallel to that, we need to be working towards a systems infrastructure that doesn't rely on proprietary processes, that is publicly owned, and that is resourced at a level that is appropriate to this kind of threat, and it's not today. Elections are one of the least funded parts of our governance. It's difficult to go and compete with other critical public needs, and so we need to find a way to have a place at the table to have that dialogue, but also we need to be realistic about that. There are a lot of needs that need to be met, so we can't expect that there's just going to be a huge infusion of federal or state money.

And even when there is an infusion of money, we need to be sure that that money is spent effectively. And one of the things in retrospect which have a lot of positive things, the Help America Vote Act. So I certainly don't want to stand here and be on record being critical of that.

But the reality is that the reactive infusion of federal money into the elections process after the *Bush v. Gore* decision created a rush to market of systems that were trying to solve a symptom of the problem, but were not ready to solve the ultimate problem, and we're still today dealing with the ramifications of that.

MR. O'HANLON: Thank you, great. Alex, same question to you, please.

MR. HALDERMAN: All right. Well, if I was doom and gloom in the "what's the problem" question, maybe I can paint a rosier picture of the solution. Because I think of all of the major problems we have in cybersecurity and critical infrastructure, the voting system is probably the easiest to secure. From a technical level the solutions are straightforward.

Dean has already gestured towards some of the most important pieces of that, but essentially what we need is a system that relies on physical fail safes and something that is going to be simple so that local election administrators can be responsible for their own front-line defense. And that's what brings us back to paper and post-election audits.

So President Trump said it very well on Election Day, that there's something nice about old-fashioned paper ballots. You don't have to worry about hacking. Well, that's absolutely true. A vote recorded on a piece of paper can't be retroactively changed by someone hacking into a computer.

And there's been sustained growth in the fraction of the country that votes using paper. It's now up to about 70 percent of voters in 2016. We need to push that number towards 100 percent and upgrade the technology for voting in jurisdictions that are still voting with only computer records of the vote being retained.

And then as Dean said, paper isn't going to do you any good if you don't also look at it. But we can use paper records of votes as a kind of quality control mechanism to make sure that the computer counts are correct. And you do that by basically randomly sampling after the election the paper ballots and making sure that they record what the computers say they would. That's called a post-election audit. And with typical margins of victory, a very, very small, random sample of the votes can give you high confidence that the overall outcome is correct.

So by recording votes on paper, performing post-election audits, we can have a system that using low-tech methods gives people a reasonable basis for high confidence without having to trust any high-tech methods that worked. And it's something that would let the local election officials obtain that high confidence and potentially correct problems with the computer results if discovered without having to rely on the federal government and the intelligence community at all.

Of course, not all the threats are threats of hacking into voting machines and changing votes. So we also need to raise the bar for other kinds of attacks, make it harder to sabotage machines and cause them to fail on Election Day; make it harder to break into registration systems and disrupt things. But these are just normal, everyday cybersecurity problems.

We can apply the kinds of best practices we apply in industry and in government to election systems at the state level to help make those attacks more difficult. So things like training, things like penetration testing, threat analyses, these are widespread common best practices. We just need to make sure that that kind of training, that kind of information is getting to the local levels and election administration.

I'm also more confident I think than Dean is about the odds of getting federal help for the states. I've been working on the issue of election security for the last decade and I have never seen a year like this where people are still having a conversation about the security of elections this long after the last major election. It's usually something people forget about a couple of weeks after voting. And that includes people in Washington, that includes members of Congress.

There's right now even a bipartisan bill sponsored by Senators Graham and Klobuchar that's been proposed as an amendment to the NDAA that would provide money to the states to implement paper ballots, election auditing, and cybersecurity best practices on a voluntary basis, basically empowering the states to take these steps if they choose. And I think that possibility of having federal resources available to the states that currently don't have the resources or don't have the expertise to implement better cyber defenses on the front lines, I think that's wholly appropriate. We don't ask the states to defend against physical attacks by foreign governments. Why should we be asking them to defend their election systems against cyber attacks from nation states? This is an appropriate place for the federal government to offer help.

MR. O'HANLON: Thank you, very good. Susan?

MS. HENNESSEY: Yeah, so I agree with all of that and then I think there's sort of a multipronged approach. And so first is having conversations like this and having them now. We sort of talked about that earlier, but the more distance you have from the prior election and then next election, I think the more constructive the conversation can be.

You know, the second effort is you really do need to develop neutral standards. And these baseline rules will guard against things like believing that there's -- the appearance of politics infecting some of this decision-making. So to the extent we can have best practices for security and also neutral standards for when we have recounts, when we believe the conditions have been met such that a recount is appropriate, that that shouldn't just be when a candidate decides that a recount should occur. But there actually should be a better and more evenhanded administration of, hey, whenever we really do have a question, we want to go back to look at paper ballots or recount the votes.

You know, the third is that there -- I think the Klobuchar-Graham bill is a great first step in terms of offering federal assistance. I do think that needs to be continue to be a state-led effort. Elections are administered by states in the United States for a reason and I do think that there will be persistent hostility, and for good reason, to overly federalizing elections. But that should not inhibit us from offering voluntary federal resources to the states.

That said, as much as I'm heartened by the Graham-Klobuchar NDAA amendment, it's also a little bit sad, right, that these baby steps, these absolutely obvious things that we should be doing, are the best we can do. We should be having a much more sophisticated conversation. We should be seeing far more robust and sophisticated pieces of legislation, funding efforts already. So good baby steps, but we're still nowhere close to where we need to be.

And the final is that we need to reestablish some norms that were broken primarily in the prior election. And that's something that we haven't returned to and I think that we need to. We need to acknowledge that one of the reasons why there were conditions for a lack of confidence in the outcome of the election is because one of the candidates routinely described the American electoral system as rigged. One of the candidates said that they were not prepared to necessarily concede the election if they lost.

At the end of the day, the election, it's an agreement among all of us, just sort of respect to the system. And we want to have a candid, honest conversation about potential concerns, but we also need our politicians to behave responsibly. We need to demand that they behave responsibly whenever they talk about election outcomes. And that's something that was washed away a little bit sort of in the outcome of the election. But it really is something that we're going to need to think about and ask our elected members or aspiring elected members to be more responsible about moving forward.

MR. O'HANLON: Thank you. John Allen?

GENERAL ALLEN: I have very little I could add to this wonderful lay-down here. I'd just simply say that the brief I gave to NACO, the National Association of Counties, had a chunk in it, as well, about critical infrastructure protection. And so while we are going to seek to try to preserve the integrity and the sanctity of the voting system, we are really on the edge, on the cusp of the potential for very vulnerable infrastructure attacks, as well. And it argues for us to think entirely differently about the cyber protection that we are able both to bring to bear ourselves, but also to bring to bear on the networks and systems at the county level.

For example, the WannaCry virus which was out no long ago. When we did the DNA analysis on it there was code in that process that pointed directly back towards a North Korean organization. And, of course, when WannaCry ultimately -- which is a ransomware malware, ultimately registered itself, when it really shut down tens or hundreds of thousands of system, it shut down systems in hospitals, it shut down systems in universities, it shut down police forces, et cetera, et cetera. Every single one of which is a major concern at a critical infrastructure level at counties, as well.

So we have to think about all the really important electoral issues associated with the comments by the panelists this morning. But we also have to recognize that until we are willing to engage in cyber operations against a state that explicitly launches attacks against American critical infrastructure, we're going to have to try to defend ourselves with the best capabilities we can at the lowest level, at the level closest to the public safety realities and the electoral realities within the population.

And I would simply tell you that from my perspective this means that we're going to need to embrace artificial intelligence very importantly in that process. Cognitive end-based, endpoint security is just about the only way we're going to be able to do this because we have artificial intelligence coming at us now. And if we're able to help the counties to understand and ultimately think about the resources that they have available to them, and perhaps think differently about those resources and structure them in different ways not only to protect the electoral system, but also to protect the critical infrastructure with the right kinds of layered defenses. Then we can protect the public, protect the electoral system, and then we can deal with the state and non-state actors as they continue to attack the United States, frankly.

MR. O'HANLON: Thank you very much. So we've got about a half-hour.

And what I'd like to do is take about three questions at a time, so I'll ask panelists to track by memory or by notes the questions, and then decide which of the three you've just heard you want to respond to. So we'll work down the row. This, I think, will be a little more efficient.

And so please, wait for a microphone and identify yourself when you get it. And please, just one question per person if we could so we have time for everybody.

So we'll start up here in the second row. We've got both these hands in the second row, and then I'll take one more. Please, sir, over to you.

MR. HOFFMAN: Thank you. I'm Lance Hoffman, George Washington University Computer Science Department. And I'm very interested in what General Allen said about artificial intelligence. I'd like him to expand on that and the panel a bit, also.

Because I agree with Professor Halderman that the computer parts of these things I think long term can be handled well enough. I'm much more concerned about the information operations part. And that's where I am -- I don't see how -- what the incentives are. Because right now we often have perverse incentives to get security in systems anyways. So what are the incentives going to be at any level to change things?

So my two questions are one on incentives and the other is AI because a lot of people talk about AI, artificial intelligence, but that covers a lot of things. And I'm wondering how that ties in, for example, to identification of who the actors are, attribution, and that sort of thing.

MR. O'HANLON: Sure. We'll go here and then take one more after that.

MS. O'CONNELL: Yes, good morning. June O'Connell, former diplomat. Voter suppression has historically both domestically and overseas been the key to winning elections. You get your people to vote and get the other person's people not to vote. It's a strategy used by our parties and by foreign governments. So it would seem that this time that part of the Russian change was to actually pick a winner. So there were two aspects: picking a winner and destabilizing confidence in the election.

So with that as the suggested premise, what would you suggest be done in Virginia in what is estimated to be a close election? New Jersey's not expected to be too close. So both in terms of picking winners, which seems to backfire, and just good old-fashioned keeping people away.

MR. O'HANLON: I'm not sure it backfired, but I hear your point otherwise. And then we'll take one more question right over here in the third row, please.

MR. ADDISON: I am Doug Addison from FreeFairAndAccountable.org. And I'd like to know from any of you which level of elections -- federal, state, local -- did our intelligence community examine and by which means? For example, statistical forensics, I can't imagine that statistics would in any way compromise sources or means, and that's something that could be published and discussed safely. Thank you.

MR. O'HANLON: John, you want to start with that first question and anything else you want to touch on? And then we'll just work down the row.

GENERAL ALLEN: I can't touch the last one. With respect to AI, I think the value of that as a consideration for protection is very important in the context of the trainable software, which can be trained to the DNA level for hostile or malicious code. It gives you the capacity, as opposed to signature-based defensive systems, gives you the capacity as we have seen with cognitive endpoint security where it wasn't even trained perhaps on WannaCry or Petya or some of the others. But because as the artificial intelligence system analyzed at the code level the incoming file, it didn't recognize the file, but saw the code, recognized it as the code that had existed elsewhere, because it was trained on that code, and stopped it, flagged it with a high level of confidence that it was probably malware. At which point then the operator has the option of letting it in or sending it into the cloud for additional forensic analysis. And with WannaCry that additional forensic analysis pointed very strongly back towards North Korea.

Signature-based systems, of course, leave you extraordinarily vulnerable in between the updates to the systems because of the proliferation of polymorphic threats, hundreds of thousands of systems of malware being produced by itself all day long and zero-day threats, as well. And if the signature-based threats hasn't been trained on the zero-day threat which emerged between the two updates, then the system is vulnerable.

So I think that as we see artificial intelligence generating polymorphic threats and then zero-day threats, it requires I think logically that we want to think in terms of artificial intelligence and cognitive endpoint security systems as the last line of defense in terms of protecting networks associated with elections. From my perspective it's much more than that. It's much more about the critical infrastructure.

And what we saw the Petya virus do to the Ukraine, there are some systems in Ukraine that have still not come up and it's been months. And then there is the theory that it is, in fact, a dry run of that system to be used against us later.

So I think we need to be thinking in those terms about what does cognitive systems, what do artificial intelligence systems give us both in terms of in developing the right kinds of systems, the capacity to red team against enemy threats, constantly changing our own system to detect and to generate the -- if we can generate the red, we can also generate the blue to protect against the two together simultaneously.

I think we've got a lot of capability to do that that we didn't have before under signature-based systems. That's why I like the approach on artificial intelligence and cognitive-based.

MR. O'HANLON: Great, thank you. Susan?

MS. HENNESSEY: So I'll take a high level shot at the final question regarding the intelligence community, what they would have examined. I think it's important to keep in mind the U.S. intelligence community operates primarily outside of the United States. I mean, they have very, very limited ability to operate and provide assistance domestically within the United States, but that's for good reason. So there is the ability to sort of provide limited assistance based on requests for technical assistance. But if you're actually looking at the intelligence community assessment you'll note that that really is about what occurred in foreign spaces and intelligence that might have been derived from foreign signals intelligence, foreign human intelligence, those kinds of sources.

So I think the question to be asking whenever we're talking about, you know, state, local, federal elections, sort of the kinds of statistical analysis that you appear to be contemplating is more what did DHS look at? What did the FBI look at? They haven't produced as granular a report. I think there was a recent *New York Times* story that seemed to indicate that maybe nothing was really looked at at that particular level. So I think it's important to disentangle sort of the intelligence community, their particular sources and methods and concerns, from really the role of domestic law enforcement, which really does have the lead on these kinds of issues within the United States.

MR. HALDERMAN: There's so many interesting things to touch on here. So maybe I can combine a little bit of those two responses and synthesize something here.

So I think we see something about the sophistication of the potential threats here, that if the future best defense for infrastructure is going to involve applying artificial intelligence against artificial intelligence and overseas signal intelligence from the NSA and so forth, it seems like the best strategy for states and local governments, which are never going to be at the same level of sophistication as nation states, is going to be, once again, to go back to these low-tech forms of defense, like having paper and looking at that paper as a quality control. So those are an example of a defense that the states can apply themselves that gives very, very high confidence, but something that needs to be happen routinely and not just when we have some other reason to believe that there has been a problem.

Once you are after an election and are in a situation where some people a problem may have occurred, you're in a very politically volatile situation. So we need to have procedures in place in every state to make sure every election is audited to a high degree of confidence using low-tech measures. That's not happening universally today. Some states are applying audits. Colorado and New Mexico, for instance, have very good auditing regimes for paper, but it's not happening nearly widely enough, and this is something where the states can take steps to help themselves, especially if given additional resources.

MR. O'HANLON: Great, thanks. Dean?

MR. LOGAN: So I think I would just pick up on Alex's comments. I think to the voter suppression question and what can be done at the most immediate elections, I'm not sure I can get directly to your question about Virginia, but I would say that it is -- those first steps are those lower tech solutions and their policy solutions. So some things are as simple, but as profound as be transparent ahead of the election about how you're going to address a close election or controversy over the election, so we're not making that up in the heat of the controversy. Talk about how we're going to approach recounts, how we're going to approach audits, and how people can observe that process so that they are well-informed ahead of time.

The types of suppression techniques that we're seeing today, it's hard to keep up with them. So we have the fake social media accounts, we have the misinformation. I wish I had a full solution to that. What I would say about that is I think we need to -- and this goes back to the investment, is the investment isn't always just in technology. It's not always just in personnel. It needs to also be in things like comprehensive voter outreach and education, so that we can establish the local election authority or the state election authority as the trusted source to find out where am I registered, where should I go to vote.

That translates into policies and new models of voting that we ought to be moving to as quickly as possible in this country. And that is where the best defense against somebody getting into a database and changing your information as a voter is your ability as a voter to go anywhere and vote on Election Day and update your registration; giving you control over your voter registration and your ability to vote, so things like an extended voting period, vote centers, same-day voter registration, those types of activities. But those are policy decisions that have to be made by elected officials who have differing opinions about the impact of those things.

MR. O'HANLON: Okay, we'll go to a second round. I'll just keep working back. So let's see where we are. We'll start with the fourth row here and there are two questions there, and then I'll take one more further back before we come back to the panel.

MR. SAREEN: Hi, my name is Bimal Sareen. I'm a co-founder at CyberForce, a cybersecurity firm focused on critical infrastructure.

Considering General Allen's opening remarks, which seem to indicate a potential multi-coordinated, multistate threat emerging all the way down to the county level where the implementation actually takes place of the election systems, as a practitioner there's a parallel here where the electric power industry ended up mandating, using FERC and NERC, federal standards to implement minimal cybersecurity standards or else they would undergo a million-dollar-a-day fine up to a certain level, based on a certain threshold. Maybe the folks in charge of the elections could consider a similar model?

Because I think leaving it up to chance would be, like I say, why are we dancing around the real threat that there has to be some closer coordination between the federal level as well as down to the county level. And folks aren't funded properly at the county level. They may not have the expertise to even receive the national level agency help that is required and a period of education that we're all talking about.

So there needs to be some sort of a transition planned to have some standards that need to be implemented versus some deadlines. There needs to be some -- we need to probably consider going beyond just voluntary, as we were talking about. This is about our fundamentals tenets of democracy that we're talking about.

I mean, it's not the elegance that we would like to consider. I think it's beyond that. I think it's critical infrastructure, which has a different definition of what we need to deliver at. Just my thoughts, thank you.

MR. O'HANLON: Thank you. And then on the same row. Very good comment.

MR. GUNTER: Hi, Chase Gunter. I'm a reporter with *Federal Computer Week*.

In some of the solutions, like employing more paper-based ballots and tallying, more layered defenses, more secret terminology, what sorts of cost increases would that entail and where would that money come from? And for things like

Twitterbots, Facebook ads, where a lot of people do get their information from, what can be done about that? Is that a policy solution, international agreement? What do you all see about that?

MR. O'HANLON: We'll take one more before we go back to the panel. I'm going to keep working front to back, so the gentleman in the beard here in the fifth row.

MR. GURNEY: Hi, I'm Don Gurney, retired Air Force officer.

You mentioned the Election Assistance Commission, which was almost zeroed out in the current Congress. Could you state how this could help provide a mechanism for providing federal resources to the states and counties, and also best practices information and things like that?

MR. O'HANLON: Okay. Why don't we start with Dean this time and work towards John?

MR. LOGAN: Okay, so I'll go in reverse order because I took the red-eye so I can remember your question. (Laughter) And actually, I really appreciate that question because I was remiss in the earlier question about what can Washington do right now.

First and foremost, I think your point is well taken that it's great that we have the amendment, and I am encouraged by that. What I'm not encouraged by is why, given everything that we've talked about today, why is there even a question about whether the U.S. Election Assistance Commission is funded and why do we not have a full set of commissioners on that board? That needs to happen and that could happen immediately if there's the political will to do it.

And the reality is that agency has established a communications mechanism. They have access to all of the local election administrators in the country, all of the state election administrators, and they have a framework to share best practices. So that exists already. Let's not try to reinvent that. Let's not try and ship that to another federal agency that doesn't have that infrastructure. Let's just support the agency that was created to do that. And then if we do get additional federal funding, we're going to need that agency to help distribute those funds.

And I'll bridge to the other question, if we move away from voluntary standards or put more attachments to standards, again, we're going to need that federal agency, and agency that actually understands and knows elections administration in order to administer that. And that exists, so we have the bridge to do that.

What I would say about the non-voluntary standards, I get that and for the most part agree with that. I think that what we have to recognize is the market and the infrastructure that we run elections on in this country, it doesn't have the capacity to support that right now. So I think that even though standards that are voluntary, I think for the most part there's a significant effort made to meet those standards. It's just a matter of are they resourced to do that and are there systems to support that?

And then to get to the cost issue, I think, again, I think we've been stymied on the cost issue by a very small and, until recently, shrinking market of voting systems, vendors, and election management system vendors that have products that they're investing in keeping alive rather than developing products that are built for the current situation and built for the environment we work in today. So now I'm starting to sound like doom and gloom. (Laughter)

But I think there's an uptick on that. I think there are initiatives going on around the country to change that. We are seeing an expansion of the market that we haven't seen before and we're seeing that expansion in areas where we're getting away from solely proprietary systems and end-to-end systems. So I think there's some hope there.

Certainly we're doing work in L.A. County to move towards an open source-based, publicly owned voting system. We have the capacity for that because we have an electorate that's larger than most electorates of most states in the country, so we're in a little bit of a different situation there. But we're also trying to do that in a way that we can share that information and components of those systems with other jurisdictions moving forward. So there is progress being made on that, but it's a slow process and it's, frankly, driven by resources.

MR. HALDERMAN: All right. I can comment, too, on the resource question. So I point you to a recent study by the Brennan Center. And Larry Norton, one of the authors, is looking at me right now, so I don't want to completely mangle his numbers. But I believe the finding is that the cost to replace all of the paperless equipment in the country with optical scan ballots would be between I think it's 150- and $400 million as a one-time investment nationally. The cost for post-election audits, my own estimate to audit to high confidence every federal race would cost an average of about $20 million a year. We're not talking about very high or significant numbers here to get these low-tech defenses in place.

MR. O'HANLON: Thank you. Susan?

MS. HENNESSEY: So I'll take on two rather briefly, so the first question about implementing mandatory federal standards. So I think as a threshold matter you potentially have sort of constitutional issues that might arise as the federal government starts to actually mandate that states administer elections in particular ways as opposed to sort of using the carrot instead of the stick.

The other thing to keep in mind is the reason why we have designed our system this way in the first place. A lot of people cheered the responses of the various secretaries of state in rebuffing requests from this Voter Fraud Commission that the President has now empaneled for requests for voter information. And a lot of people are really suspicious about either the empirical grounding for that effort in the first place or the reason for wanting that data. So a lot of citizens really were glad to see secretaries of state saying, you know, go jump in the Gulf of Mexico, we're not giving you that data.

The same sort of principles that empower them to say no are the same that empower them to administer their own elections. It's all sort of part of the same fundamental tenets. And so as we start to think about the extent to which we want to federalize elections in the name of security, an important goal, whether or not we might at the same time be eroding other valuable things that come from having that sort of federal -- that federal system in the sense of various states administering their own.

Then sort of on the Twitter/Facebook question, look, I think ultimately we're going to need to see more responsibility, transparency, and accountability from the companies themselves. And so to the extent that that can be done on a voluntary basis, so oftentimes whenever large companies are staring down the barrel of possible regulations, they suddenly have a dramatic change of heart in their willingness to adopt certain things voluntarily. So I think that there is a hope that these companies that have resisted some of those obligations in the past might be willing to do so, especially if Congress starts talking about things like implementing the same requirements that we currently have for other forms of election advertising in terms of reporting where funding came from and being transparent about those numbers.

Hopefully, we will see these large technology companies decide to adopt some different practices in order to give us not just solutions, but also enduring transparency into what people are seeing, why, and who's paying for it.

MR. O'HANLON: Great.

GENERAL ALLEN: And I'll pass.

MR. O'HANLON: Great.

GENERAL ALLEN: That's good.

MR. O'HANLON: Okay, let's go to a third round. So I called on all men last time. I'm anxious to try to change that this time. So I'm going to make sure --

MS. HENNESSEY: We've got a woman here in the row in the middle.

MR. O'HANLON: Okay, yes, we'll start there and then move along. And then my good friend Susannah Goodman from Common Cause, as well. So we'll start there and then come up here and then we'll find one more person further back.

MS. STERN: Okay, thank you. Elisa Stern, I'm a negotiation and conflict resolution consultant.

The panel talked about voting as one of the bedrocks of democracy and yet we don't see that narrative being played out in the same way that we saw women's -- the push for women to vote or more recently for marriage equality. We don't see, you know, marches for people demanding equal access to voting. We don't see the public screaming for more resources for better voting equipment.

To what extent do you think that this public push is needed? And what are your suggestions for ways to galvanize the public beyond to push for these changes that you've been suggesting? Thank you.

SPEAKER: While we walk the microphone up here, I'm going to thank you Susannah for her help in conceptualizing this event and all she does on this issue.

MS. GOODMAN: I just wanted to ask the general about lifting the visibility of this issue in the national security community. The Graham-Klobuchar amendment has not passed and I don't -- you know, it is stymied in sort of procedural issues and jurisdiction issues. And so we may not even have that tiny baby step of federal help.

And it’s very clear that until the Senate and the House understand this as a serious national security concern, that they’re going to be very reticent to power grab from the states. So if you could comment.

GENERAL ALLEN: Sure.

MR. O'HANLON: Then we’ll have Pete Schoettle in about the eighth row. He’s got his hand up there in the blue shirt, please.

MR. SCHOETTLE: Thank you. First, my compliments to the panel and to Mike for setting this up. I’m a retired Brookings, but I’m an active election chief judge in Montgomery County for the last 12 years.

MR. O'HANLON: Good for you.

MR. SCHOETTLE: And I have serious questions about the validity, Alex, of your approach, hacking into machines. I have 11 machines in my precinct. They’re under constant view all day long. So your methodology of taking a machine back to the lab and reverse engineering doesn’t work. Each machine is independent. For somebody to take the machine, turn it upside down, take off the tamper tape, unscrew the lock, take out the memory, modify the memory, put it back in, put it back upright with a dozen poll watchers right in front of the person can’t happen.

Secondly, each machine is independent. None of them are linked electronically. So at the end of the day, I turn in 11 different reports. If you bug one machine, you don’t affect any of the others. Each machine has about 300 votes during the day. So if you hacked one machine, you could change maybe 300 in my precinct.

At the end of the day, we bring paper results and electronic to the Board of Elections. They’re totaled there. The media is there. If the Board of Elections changed the results on the way to the state, the media would have immediately discovered, hey, they're telling the state something different than the media reported when the results were brought in.

So I just don't see the validity of worrying about hacking individual machines because they're all independent. To effect the county you'd have to bug maybe 2,000 machines. That's one county in the state and you have a dozen counties.

MR. O'HANLON: Thank you, Pete.

MR. SHUTLEY: Wait a second, one second. So the vulnerability is bribing somebody in the Board of Elections in the off season and they change the software, but they have to change it for all couple thousand machines for one county. I'm not saying this problem doesn't exist, but this particular vulnerability is not the problem.

MR. O'HANLON: I'm going to let Alex begin with that question.

MR. HALDERMAN: What kind of machines do you use?

MR. SHUTLEY: Well, we just changed. We used to have optical scanner -- now they're optical scanner, they used to reading papers.

MR. O'HANLON: Before you go, I just want to say I'm glad for the question. I bet you're going to have an excellent answer. But I also know that this gets to the dilemma that Susan and others have emphasized, that we don't want to make the problem sound so bad that people feel discouraged from voting. So while it's a serious problem, hopefully it's not a catastrophic problem, at least not yet. So there's this tension in the messaging that we're all trying to convey in this kind of an environment, so I think you help, you know, crystalize that and dramatize it.

Over to you.

MR. HALDERMAN: All right. So let me respond to that because I think perhaps my remarks were not clearer. The problem really is as bad as I was describing, but what you point out is a common misconception from people who are seeing some of the defenses that are in place, but don't really fully understand the capabilities that attackers have to attack the system.

So those machines, before every election, are being programmed with a memory card. You're putting in a memory device into those machines that has the ballot design. That is the threat vector that I was talking about earlier. Right? So if an attacker can compromise the data on that memory card, they can cause the machine to misbehave. And that is something that doesn't require physical access to each machine. It's something that can be done even though the machines aren't connected to each other.

This is a strategy of attack that very famously was carried out to sabotage Iran's nuclear enrichment program by making the centrifuges in their factories spin themselves apart essentially. And those centrifuges were also not networked together or connected to the Internet. So the way that the attackers reported by the New York Times to be the U.S. and Israel attacked the Iranian program was by creating malware that would spread virally from disconnected devices via USB sticks to the systems that were used to program the centrifuges and then into the centrifuges.

MR. SCHOETTLE: Stuxnet.

MR. HALDERMAN: Stuxnet, exactly. This is called jumping an air gap. This is well within the arsenals of sophisticated nation state attackers today. Exactly the same thing applies to voting machines used in the style you talk about and despite all of those defense that you talk about.

MR. O'HANLON: So while we're on this technical issue I think this is something Susan knows well and probably John, as well, so let me go in that order. And then we'll finish up with the final comment of the day on any questions that are outstanding with Dean.

So Susan, over to you.

MS. HENNESSEY: I wouldn't touch a Stuxnet question with a 100-foot pole. And I imagine General Allen will feel the same way. But I will try and address quickly two of the other questions.

GENERAL ALLEN: In fact, I want to leave the room. (Laughter)

MS. HENNESSEY: But I will briefly address the other two questions, the first being sort of why don't we see more calls for this in public? I do think there is a strong community-based tradition among particularly disenfranchised communities to try and empower people to vote and to fight against efforts, sort of community-targeted voter suppression efforts. I agree that it hasn't sort of taken hold at a sufficiently national level and I think that really is because we need to start thinking about this as a moral issue.

It is wrong to try and prevent an American citizen from exercising their franchise. And until we start thinking about that as really a question of right and wrong, about standing up for our fellow citizens even if they don't look like us, even if we don't share -- even if we aren't going to ultimately vote for the same person, but just really viewing that as sort of patriotism, democracy, fundamental pre-political commitments, I don't think that we're going to see the sort of groundswell changes. And I think that's a real shame. I don't know how you change the political calculus there.

On the question of how do we get the political will to get the minimal funding that I think everyone on this stage agrees, you know, as much as I'm always nervous about, oh, are we appropriately messaging? Are we scaring people too much? I am heartened to see that this is headline news and I think that that's the only way that we are going to get Congress to commit the funds that they need to. You know, there was a front page article in the *New York Times* just this week on this issue. I think the more that it endures, the more we talk about it, sending Alex out on his terrifying roadshow to get people to care about this issue and to care about this issue far enough in advance, I mean, that's the only way that ever works to get Congress' attention. So I'm heartened that at least that is changing, but I'm not terribly optimistic.

MR. O'HANLON: John, over to you.

GENERAL ALLEN: Yeah, wonderful question and I think it's really at the heart of much of what concerns me every single day. And while the process of voting seems to be a local issue, it isn't certainly a local issue. It's really a national security issue. It goes to the point of the integrity and the security of our system of government and then goes to the larger issue of the integrity and the security and the safety of the American people.

So I think in many respects it is very much a national security issue. It can't be thought of solely as the purview of the counties, which are trying very hard to make a difference, and the states, et cetera, and with sort of a loose connectivity to the federal government. This is a national security issue.

And when I travel through Europe and I meet with leaders in many of the countries in Europe where every single day their critical infrastructure or their national intelligence entities or their financial systems are under cyber attack, there's no question in their mind about whether this is a national security issue or not.

So I think there are responsibilities that we have. And I just leaned over to Mike a moment ago and as a result of your question, he and I are going to write an op-ed to get out -- talking about this as a very serious national security issue. But we also have to empower the Congress to feel that they have the top cover of the support of the American people in moving out smartly to do some of this.

Now, we saw this recently with the bill that was sent to the President sanctioning the Russians on this issue. That's attempting to land a blow at the perpetrators. We need to land a blow domestically which both fortifies the process, but also fortifies the voter. And we need to be thinking in those terms, as well.

So, as I said to the National Association of Counties, look, the enemy has gone right past me. And the enemy is in the assault on some of the most precious aspects of our democracy today. And we need to empower the Congress to feel as though that's a responsibility of theirs to do all that it can to fortify the voter, but also to fortify the system, but also to think of it in terms that lift it above the level of a county problem or a state problem or a loose amalgamation between federal interests and state and local interests. We have got to address it for what it is, which is a direct assault upon the integrity of the democracy of the United States of America.

And if we're able to depict it that way, we can then call upon the patriotism of our citizens to go out and vote. I don't care who you vote for. I don't care how you vote. What I care about is that you not let the enemy take your sense of the integrity of your voting system away from you. Let's defeat them by fortifying the voter and then let's do all that we can to create a system that is proof from interference ultimately so the voter has confidence in that, as well.

It's a two-headed problem. We have to address both heads at the same time. It's not a local problem. It's a national security problem. And Mike and I will get something out on this. Thank you.

MR. O'HANLON: Thank you, John. Dean?

MR. LOGAN: I think that's a great conclusion. I think that it comes back to our earlier comments about how we frame the discussion. We're talking about something that is foundational to our representative form of government here and there are so many different pieces and so much information that's floating out there for the average voter to comprehend and try to make sense of it is nearly impossible. And so I think framing the very real threat from a national security standpoint the way you just heard is an important piece.

I agree and understand and have been through presentations to understand the threat that Alex has talked about, about the voting systems. But I also appreciate and respect the perspective that the gentleman brought as a person who works at a polling place on that.

And I think that it goes back to your earlier question about why didn't we see that type of activity happen in 2016? I think by and large it's because of the nature of what you described. It's not that it can't happen. It's far more difficult, though, than confusing people, giving them misinformation, and just flat-out deceiving them. That's cheaper, easier, and has more immediate effect. That's the real threat we're dealing with today.

So it's not that we shouldn't address the issue with voting system vulnerabilities, we have to because it's going to come and bite us and we're fortunate that it hasn't, that is before now. But how we frame that and how we address the immediate needs, needs to talk about what actually did happen in 2016.

And ultimately, to round out to the question of why don't we see the concerns about voting the equivalent of, you know, the women's march or other activities like that, in one respect it sadden me that we don't because it is so fundamental to what we do. And it gets back to the fact that that is the ultimate offense. I believe that firmly. The ultimate offense is high turnout and high voter participation.

I think we've lost our way in the elections process. Along the way we stopped making voting about the voter and I think we have to get back to making voting about the voter. We need to make sure that as we're addressing all these system issues, all these security issues, that we're creating a voting experience that conveys the significance and the relevance of the power of the vote. And I think we've lost that and need to get back to that.

And there's a lot of efforts underway to do that, but it's at the end of the list for resources. And I think we need to shift that priority and again make voting about voters.

MR. O'HANLON: Let me thank all of you because there are a lot of people in this room who have asked outstanding questions, but also I know a lot of people who've done a lot of work on this very important question for our democracy. And let me also ask you to join me in thanking the panelists. (Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

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

Carleton J. Anderson, III

(Signature and Seal on File)
Notary Public in and for the Commonwealth of Virginia
Commission No. 351998
Expires: November 30, 2020