America's Cybersecurity Problem (10/23/18)

00:00:26 Jessica Chen: Good evening, and welcome. My name is Jessica Chen, and I'm the director of public programs here at the 9/11 Memorial & Museum. As always, I'd like to extend a special welcome to our museum members, and those tuning in to our live web broadcast at 911memorial.org/live. I'm also very pleased to welcome students from the cybersecurity program at the Urban Assembly School of Emergency Management.

00:00:48 Tonight, we are joined by Avril D. Haines. Avril was the first woman to serve as deputy director of the C.I.A., having been appointed in 2013. She has also served as deputy national security adviser to President Obama, and as legal adviser to the National Security Council. She previously held positions in the State Department, the Senate Committee on Foreign Relations, and The Hague Conference on Private International Law.

00:01:14 She's currently at Columbia University working on Columbia World Projects, in addition to being a lecturer at Columbia Law School. In her role as deputy national security adviser, Avril faced the challenge of responding to the 2016 cyberattack on the Democratic National Committee. We are especially fortunate to have her here tonight to share her thoughts about the state of American cybersecurity and her insights into the rising threat of cyberattacks to our national security. We'd like to thank Avril for taking time out of her busy schedule to share her insights with us.

Without further ado, please join me in welcoming Avril Haines in conversation with executive vice president and deputy director for museum programs Clifford Chanin.

(applause)

00:02:00 Clifford Chanin: Thank you, Jessica. Welcome, everybody. Welcome, Dr. Haines. We always, in our programs, try to connect to current events. But I have to say, the news is very generous in its abundance, and the things that we can talk about. So with your permission, though we will talk about cybersecurity tonight, I also could not miss the opportunity to ask you about some of the things that we've all been reading about in the news, which have just yesterday brought the director of the C.I.A. to Turkey to evaluate the Turkish intelligence, and make her own assessment of the events that resulted, finally acknowledged by all, in the killing of Jamal Khashoggi.

00:02:44 And so, let me ask about what a director of Central Intelligence is seeing and doing over there at this point. What is she assessing? What is she looking at? And one step back from those more detailed questions, how do you assess this situation? What happened? Did it go wrong? Was it planned out this way, as badly as it turned out? And what do you project looking forward as the outcome of this on Saudi Arabia and on U.S.-Saudi relations? Big questions.

00:03:18 Avril Haines: Yeah, no kidding. Well, first of all, it's great to be here. And I really appreciate the invitation, and particularly for this institution, given how much, frankly, 9/11 has had an impact on all of our lives. But I'd say, certainly in my profession, it's a day-to-day issue. And on Saudi Arabia more generally, honestly, it's very hard for a person, I guess, in my position, with my experience-- and I think most of my colleagues would say the same thing-- to believe that... that Mohammed bin Salman didn't order, essentially, the... you know, the capture of Jamal Khashoggi.

00:04:03 And the question of whether or not he was intended to be killed at the consulate or not I think is, you know, still a question. But it also seems very likely that he was, given the additional information that's come out. I mean, the fact that what appears to be a body double having brought there, you know, being dressed up in his clothes, being essentially... you

know, walking around in order to try to promote the story that was being told, all of those seem to suggest a premeditation that would indicate that they did, in fact, intend, you know, potentially to kill him, but, of course, they might have done that also even if they were capturing him and bringing him back to Saudi Arabia.

00:04:43 So, so I... You know, some of the details, I think, are ones that you still want to hear the facts on. But it's just very, very hard to believe that it isn't Mohammed bin Salman doing that. I think one of the implications of that is just how... I think how much he has grown in confidence in his position and in his power in Saudi Arabia. And that, I think, is, you know, not surprising in some respects, but we see a lot of signs of it, but this would be one of them. And I also think there's a sort of a recklessness to this activity and other things that we've seen surrounding that.

00:05:22 Then there's the reaction of the Trump administration, obviously, to the sequence of events. And I think, you know, to the extent that the Trump administration already has not been direct and immediate in their demand for an investigation that goes beyond Saudi Arabia, I think that is a real problem.

00:05:44 And mostly because, first of all, this is unacceptable behavior that we should in no circumstances... and I think there are, you know, on a bipartisan basis, agreement on that view. And moreover, I think it sends a signal to the region and to others in the space that this is somehow something that we're willing to tolerate.

00:06:02 And then, secondly, the fact that, you know, if we have Director Haspel-- who I have tremendous respect for-- and I think she'll go to Turkey, and the kind of things that she would be doing would be meeting with Turkish intelligence, and with Saudi intelligence, presumably, and looking at whatever information they have in fact collected, and, you know, examining it to try to give the best analysis that she can, and that the agency can, and that the intelligence community can, for the president and others to see.

00:06:31 That's a useful thing insofar as it's helpful, I think, for her to be there and for her to actually collect that and provide that analysis and the credibility that goes behind it. And I have no doubt that she'll say what she thinks internally, in other words, to the president and otherwise. But there has to be a response to this kind of activity, and I think that's the test of the administration at this point.

00:06:54 And then the final thing I'd say on this is just that, you know, one of the concerns that I have with the Trump administration's approach to Saudi Arabia more generally has been that there appears to be just, you know, a willingness to overlook a variety of things that Saudi Arabia is doing that is, you know, unacceptable, such as the Khashoggi piece, but also things that have been doing in the context of the war in Yemen and in other areas, in favor of the idea that a relationship with Saudi Arabia is such, of such strategic importance, basically, to our national security that we are willing to put these other things aside.

00:07:32 And I think that's damaging, not only to our credibility and our sort of general policy on these types of issues and the kind of signal it sends across, you know, to other countries about what we're willing to accept and what we're not willing to accept, and creating a significant amount of hypocrisy in the way in which we approach these issues with other countries.

00:07:50 But it's also, I think, a strategic mistake from a long-term perspective. I don't think... I think if you look at where Saudi Arabia is likely to be in the next several decades, essentially, in the region, I don't think they're going to be nearly as influential as they were, for example, ten or 20 years ago, in the Middle East.

And I think, honestly, we should be thinking about that and we should be recognizing how much damage the kind of relationship that the Trump administration currently has with Saudi Arabia is likely to do to our future policy and our future national security interests in that region. Lengthy answer, sorry.

00:08:24 Clifford Chanin: No, I... It's entirely speculative. But Karen Elliott House, who knows Saudi Arabia very well, writes in "The Wall Street Journal" today on the possibility that it may come down to a choice by the king between his relationship with the U.S. and the continuation of his favorite son as the crown prince. That, you know, if the U.S. actually stands up here and says, "This cannot stand," he might be forced into making a choice. Does that ring at all true to you? And if so, do you think he would tip one way or the other in that?

00:09:01 Avril Haines: Yeah, I have to say, I think it's far more likely that... essentially, that the kingdom doubles down on the idea that this is a rogue operation, that they essentially scapegoat this on fairly high-level figures within the kingdom, and that they try to promote that theory, even despite the evidence and the information that will come forward. And I think they'll do everything they can to make moves to try to essentially, you know, indicate investigations or other things, until this, from their perspective, calms down, and then they'll move in that direction.

00:09:38 I think if the Trump administration were to take a particularly hard line, which strikes me as unlikely, and to force that kind of a choice, I mean, I... You know, I'm just... you know, sort of hypothesizing, and I'm not sure it's all that useful, and I am not a particular expert on Saudi Arabia. But it does seem to be unlikely that King Salman would choose, in a sense, the United States relationship over Mohammed bin Salman.

00:10:03 I do think, though, that if there is a significant international reaction-- not just the United States, but a series of countries across the board-- and there's a recognition of the damage that this is doing, it could be possible for Mohammed bin Salman essentially to have to step back from the position that he currently has, and for there to be a kind of a shift that allows some space and time, with the idea that he might eventually come back into power at some later time. That seems to me the kind of thing that I've seen before in a sense, historically. But it's... We'll just have to see how this moves forward.

00:10:38 Clifford Chanin: One last question about this. Turkey, of course, has played a pivotal role in all this, and they have presumably masterfully and quite deliberately dripped out the leaks about what happened, constantly setting the Saudis up to be contradicted in the latest version of the Saudi story of what happened there.

00:10:58 How do you see that triangular relationship between Turkey and Erdogan the president, his rivalry with the Saudis, the complicated relationship back and forth that he has had with the United States? Does this sort of move him higher in some way on the... in the pecking order of American allies or relationships, or is he, perhaps, getting a little out in front of himself, even, under these circumstances?

00:11:27 Avril Haines: I mean, there's historically been tension, obviously, between the Turks and the Saudis. And it's not really surprising that Erdogan has taken this opportunity to stoke the fire a bit and to make it a little bit, you know, kind of poking at the Saudis on this. I don't... it doesn't seem to me that those activities should make him higher in the pecking order of American allies.

00:11:53 On the other hand, I think it's useful to get as much information as we can from the Turks in order to better understand the situation. But I think that's... that's at least how I would approach it.

Clifford Chanin: Fair enough, fair enough. Okay, back to cyber. So a couple of days ago, the director of national intelligence, the FBI, the Department of Homeland Security, the Department of Justice, released a statement. I'm just going to read a couple of quotes from it.

00:12:20 "Foreign interference in U.S. elections is a threat to our democracy. Identifying and preventing this interference is a top priority for the federal government. We are concerned about ongoing campaigns by Russia, China, and other foreign actors, including Iran, to undermine confidence in democratic institutions and influence public sentiment and government policies. These activities also may seek to influence voter perceptions and decision-making in the 2018 and 2020 U.S. elections.

Elements of these campaigns can take many forms, including social media, to amplify divisive issues.

00:12:56 "Currently, we do not have any evidence of a compromise or disruption of infrastructure that would enable adversaries to prevent voting, change vote counts, or disrupt our ability to tally votes in the midterm elections. Some state and local governments have reported attempts to access their networks. Thus far, state and local officials have been able to prevent access or quickly mitigate these attempts."

00:13:18 So, it seems fair to say that this warning is a continuation of the previous warnings and the previous campaign, as identified, by the Russians to not just alter the outcome of elections, but to alter Americans' confidence in their electoral process. How do you assess this particular statement at this point in time? Is this said from a position of confidence that we have things in hand? Or is this, on the other hand, a way of saying, "There's stuff going on here that we need to warn you about and we don't know the full dimension of it"?

00:13:57 Avril Haines: Yeah, I mean, I found it eerily familiar in the sense that it was very similar to our October 7 statement that was just before the 2016 elections. And, you know, it's a sort of a... We know that there are efforts to interfere, right? I think the fact that they list Russia and China and other... You know, including Iran type of thing is probably to largely sort of be consistent with President Trump's perspective on this, that, you know, it's not just Russia that's trying to interfere, even though we know historically that it's true, that not just Russia has tried to interfere in our elections from a kind of a covert influence perspective.

00:14:35 But in any event, you know, so there's interference occurring. Here are some of the things that we've seen, right? You should be on notice that in fact people may be trying to have an impact on your vote, in effect. But our election infrastructure is strong. We don't see anything that tells us that there's something that's going to affect the vote, right? And we're doing everything we can to manage that piece of things.

00:14:59 And I think that's the sort of basic arc of, you know, that statement, of the statement that we did back in October. I think there's value in making those statements in order to try to tell the public, you know, "We have intelligence that indicates that in fact, people are trying to interfere with the election. You should be on notice in that respect." But it is also, you know, and this is sort of part of what happens when you're in government and you're looking at these issues, You also want to reassure the public that that doesn't mean that the integrity of the election has been undermined.

00:15:31 And a part of that is just, you know, generally to reassure the public on that point. But it's also because one of the objectives typically of these interference campaigns is actually to undermine confidence in the election. So you're also trying to combat their objective, in a sense, on this scenario. But it's... but I... I mean, I think it's sort of... It's interesting that this is one part of our response, and this is likely to be a feature for the future.

00:15:57 I think one of the questions is just, so how do you, as a public citizen, actually respond to that, right? What do you do with that information? How do you deal with it? And I think that's the piece that we haven't really successfully figured out, right? We haven't really given you enough tools to say, "Okay, I understand that somebody's trying to interfere, but how can I then evaluate information more effectively?" Or, "What is it that I can do to actually protect both me and others around me from seeing this kind of interference and being affected by it?"

Clifford Chanin: So let's take that as the next question.

Avril Haines: Yeah.

Clifford Chanin: What elements of cyberliteracy do you think individuals can adapt in their own lives so that at least they and those around them could be safer?

00:16:39 Avril Haines: Yeah, I... So there's things that individuals can do, but right now, on this type of an issue, it's actually institutions that need to deal with it. So one of the things that, you know, we've seen a lot of, and that we've learned, obviously, over the last few years, is, one of the critical issues, is that you have, essentially, computers that are able to automate responses that appear as if they're people, right?

00:17:04 And that tends to be one aspect of these types of campaigns. And there are ways in order to tell if it's a computer versus an individual that's behind, you know, essentially a Facebook, you know, intervention or an account, or things like that. And so trying to get organizations to actually identify them and to, you know, attribute and to prevent them from being the things that you are seeing is one area where this can be done.

00:17:31 Another piece is in, actually, you know, doing the kinds of things that you're seeing, now, organizations being pushed to do, which is actually to find out if there are false accounts, other things like that, so that you actually don't have to, you know, figure that out for yourself.

00:17:46 But another thing that I think is really important in this area is, is actually pushing platforms to reveal more information to the public about both the kind of algorithms that they use in terms of the prioritization of information that's pushed to you as an individual consumer of information, but also information about who's paying for ads, essentially, so that you can see that information as it's put out. And essentially whether or not the particular... Like, why it's being pushed to you. Is it because you're in a particular demographic that is of interest to that political institution, or something else?

00:18:23 And those are the types of things that folks like our Knight Institute at Columbia, for example, that has written letters on this point and sort of been making... you know, sort of presenting a platform on these issues, saying, "This is the kind of information that should be made available to the public. This is the kind of information that would help us all absorb this information more effectively and be better at understanding it, and dealing with the kind of interference that we can expect from foreign actors."

00:18:52 Clifford Chanin: The work in 2016 and the warning in 2016, the reporting and now the investigations into 2016 election results all focus on the Russians. This statement itself, as you said, mentions the Russians, but couches it in the context of others.

Avril Haines: Yeah.

Clifford Chanin: In your view, are the Russians the main threat to the electoral process or confidence in it?

Avril Haines: Yes.

(laughter)

Clifford Chanin: Okay.

Avril Haines: (inaudible)

00:19:22 Clifford Chanin: And, and tell us a little about the strategy of this. Why are they trying to do this? It seems self-evident, I grant you, but there's a strategy behind this. This is not really a new realization that goes to the 2016 campaign. They are in, as they have always played, a long game, and they may well have found a vulnerability that we have a hard time fixing.

00:19:45 Avril Haines: Yeah, no, I think that's absolutely accurate. So for decades they've... what we would call in the intelligence community, essentially pursued active measures, as we'll call it. And, in essence, it goes beyond just kind of intelligence collection, but also to promoting disinformation. And in promoting disinformation, it looks like things like conspiracy theories or other ideas and so on that are actually false.

00:20:10 And they tend to do it effectively to promote, you know, candidates that they think are going to be more likely to align with their interest, but they're also doing it to undermine our faith in our democratic processes. That's one of their sort of typical objectives in this context. And they do it, you know, sort of to sow chaos, in a sense, right? To sow disorder and to promote the idea that democracy actually can't manage and resolve the kinds of issues that we're dealing with as a way to sort of undermine democratic influence.

00:20:46 Putin and, you know, the people around him, in a sense, believe that the United States has done the same thing to him and to the Russians. And their view is that the United States was really behind, essentially, you know, what are frequently called the color revolutions, or, you know, a variety of different protests and movements that have happened in the near abroad around Russia and in Russia itself.

00:21:16 And in a way, he has this view that he's just doing to us what he believes we're doing to him. I mean, the fact that we're not doing exactly the same to him and that, in fact, you know, the movements in Ukraine and other things like that actually evolved out of dissension from the population in those particular circumstances is not something that he believes, you know. So saying it won't make a difference to him, in that respect. But that's sort of the perception that he's under. And he sees, I think, Russia as being, in a sense, in a fight against what is U.S. influence and Western influence in his region of the world.

00:21:56 And so, you know, this is an area where I think you're exactly right. In many respects, the strengths that we derive from the internet and from an open society are also what make us particularly vulnerable in these circumstances. And what's particularly interesting about what... the way in which the Russians approach these kind of information campaigns is that they really sort of zero in on areas of division in the country.

00:22:20 And they promote them and they exacerbate them. And it's... you know, it's one of those things where you, you know, you can recognize that the

country is particularly divided. That's not the fault of the Russians, per se. But it is, nevertheless, something that they've taken enormous advantage of in this context. And I think when we were going through it in 2016, one of the key questions was, you know, in learning that they were trying to interfere, that's really not that surprising on some level. Historically, they've done that before.

00:22:50 Then you recognize that through the use of social media and other types of, you know, tools, essentially, that are available to them in today's world, they can be more effective at interfering, right? They can get to a broader audience. They can.... it's a broader scale. They're capable of having more impact, that type of thing. You sort of say, "Okay, well, so there's that type of interference. We'll have to respond to that. We want to try to promote ways for the public to understand it, to be able to respond to it and manage it."

00:23:18 But what else can they do? And that's sort of what's mentioned in the rest of that statement, and what was mentioned in our statement, which is that then you also see them looking at things like register rolls for election, you know, infrastructure, things like that. And in that context, you could imagine that what they could do might be to change, for example, the address on a register roll, right?

00:23:41 So that when you go to vote and somebody looks at your I.D., they say, "Well, that's not the right address, and therefore, you know, you're actually not the right person to do this vote. And, therefore, you can't vote," right? And that could actually affect the vote. And so one of the things we did was work through, you know, so how could they actually change the votes? Is there a way for them to throw the election itself, affect the vote count? And learned that the election infrastructure is so diffuse, frankly, and so complex that it's not something they could easily do.

00:24:15 But at the same time, they could still, in a couple of places, do what I was just describing, and, again, undermine your confidence in whether or not the election that took place was in fact credible, right? Whether or not something had happened that they had been able to affect the outcome

of. And that would, actually, have a very significant impact on our willingness to accept a particular candidate, how we might react to the election, all of those types of things that could really create considerable challenges for democracy.

00:24:44 Clifford Chanin: One of the things I don't think any of us realize is how idiosyncratic our actual vote counting system is. I mean, it is run on a 50-state level. The differences in quality and security and approach vary radically across those states. And so there really is no comprehensive way that the federal government can actually assure anything about voting outcomes, because the votes themselves are the responsibility of the individual states.

00:25:13 And, so, in the 2016 case, there was pushback from some of the states when you made a warning, as the Obama administration, a warning about what was coming, and the need for cybersecurity measures just to protect the vote. And that was not acceptable to all of the secretaries of state or commissioners of elections who you were dealing with.

00:25:36 Avril Haines: Yeah, yeah, it's a really interesting... I mean, on the one hand, you're very happy to hear, right, that the electoral infrastructure is so diffuse that it's very hard for another country to actually interfere in such a way that they could throw the vote one way or the other. But at the same time, exactly as you're describing, you know, you might think to yourself, like, wouldn't states want to encrypt, for example, their register rolls? I mean that's a pretty basic point, right? And that doesn't happen across the vast, vast majority of your states.

00:26:03 The, you know, there's also sort of a very basic kind of cyberhygiene stuff that you would imagine that would be useful for states to do that... it's just challenging. I mean, there are a lot of institutions, and this isn't to say that... that people aren't trying their best, in many respects. But there are a lot of things that you would wish them to do that you know they can do that would make them more secure, that they're not actually doing. And so that was one piece, was just trying to give them information to say, "These are things you could do that would actually make you safer. You can do them if you want."

00:26:36 Another piece of it is sort of bringing in, you know, the federal government to try to assist, right? Both in terms of sharing information, but in also providing resources, training, other things like that that could help. And we encountered significant resistance to this, as you pointed out. And one of the challenges was just the sort of classic federal-state relationship, right? This sort of sense that the federal government was kind of coming in and directing the states on issues that they felt, "This is in our jurisdiction. "Don't, you know, don't come in here. We're managing our process just fine. We don't need you, thanks very much," kind of thing.

00:27:11 And we tried to go to Congress to try to get help from, basically, members of Congress to facilitate, essentially, that kind of relationship and do the best that we could to assist with the states. And it was, it was not easy. It was definitely a complicated piece of things.

00:27:28 Clifford Chanin: I think it's also true, the electoral systems are sort of the poor stepchild of local government, or state government. That the money doesn't go there. The employees are often seasonal. Not necessarily, you know, who you would want to put in trust of this sort of sacred element of our system. And it's, it's really a product of a much more innocent time. And it seems to be wide open to these kinds of, at least attempts at manipulation.

00:27:53 Avril Haines: Yeah, it's really... I mean, if I learned nothing from my time in federal government service, it was that our electoral infrastructure really needs to be upgraded in many respects. But in addition, there's a recent report that was just issued, I think, in September by the National Academy of Sciences on the future of voting. And they look at a variety of different issues associated with the electoral infrastructure.

00:28:16 And one of the things that they indicated that I thought was particularly interesting is just, look, you can't reduce to zero the risk of tampering for really any electoral infrastructure process that you've got in the United States, right? But what you can do is reduce the risk, obviously. And in

addition, if you have a really very good and reliable audit system that tells you whether or not tampering has occurred, it can also drive a better process so that you can actually be relatively tamper-resistant. And you can then have greater confidence in the election that's taken place.

00:28:50 Now, one of the challenges with that is... and one of the processes, by the way, that they suggest, I'll just tell you briefly, that I thought was fascinating, they have a kind of, a risk-limiting audit methodology that they provide, which is an administrative audit that you basically do if you're managing the election, where you kind of take out certain ballots on a statistical basis. You say, "Okay, this sampling," and then you check them to make sure that you've got... you know, that they are accurately recorded and so on. And that gives you a relative... you know, some confidence that there's been no tampering.

00:29:18 However, you have to trust the administrators, right, who are doing it. And you have to have, basically, sort of a tamper-proof chain of custody of the actual paper ballots that are finally, you know, provided at the end of the day, to get to the people who are actually looking at these, you know, sample ballots in order to actually tell whether or not there's been tampering.

So what the study suggests is, you could combine this with something called end-to-end verifiability, where, if I'm an individual voter and I go to the poll and I get a receipt for my vote, and it has, say, a number on it, I could actually use that number to then check after I voted to make sure that my vote was recorded, and recorded accurately.

00:30:01 And all of it would be encrypted, so it would still maintain my privacy about that. But it would give you confidence as an individual, right, that, in fact, the vote has been taken, that my vote was recorded, and that, you know, the election was well-carried.

What's interesting about this is that when you try to convince jurisdictions to do a very, you know, significant audit like this, that really gives you an enormous degree of confidence, there's a lot of nervousness

among people who are running the... you know, the electoral jurisdictions, right? Because it can also rebuild problems in the system.

00:30:33 And that's not... this is not because people just want to, you know, sweep under the rug problems, but rather because they also want to be sure that their system is sufficiently credible, right, that when they do this audit, it doesn't undermine the credibility of their election system, right? There's a whole kind of vicious cycle that you get into.

So we have a lot of work to do on these issues. And I think there are some great ideas that are out there, but we need to start implementing them and, you know, really sort of hold up some pilot programs to demonstrate, "This is the way to do it and this is the way it can be done across the country," in a way that gives us all confidence that we can have an election that we, you know, feel actually represents what it's intended to represent.

00:31:11 Clifford Chanin: Let me go back to something you mentioned before, and it was in my question, as well, and this is the personal role of Putin in all of this. And I believe the early break in this intelligence and in this matter coming to the attention of President Obama in 2016 was reporting in the intelligence community that pointed the finger at Putin himself.

00:31:36 So this was not a rogue operation, to borrow a phrase that's been in the news lately. But this was actually coming from the very pinnacle of the Russian government. What can you tell us about that, and whether you think Putin is still involved in the way that was originally described?

00:31:56 Avril Haines: Yeah, I mean, I... it's absolutely true that the intelligence assessment that I think was released in January 2017 that really sort of tried to collect all of the intelligence that had been collected during this period, I think up through the end of December, essentially, of 2016, identified that Putin, in fact, from... with a high-confidence assessment that Putin had been involved in making the decision to interfere in our election, and specifically for the purposes that had been identified in the intelligence report, which was essentially to denigrate Clinton, to, you

know, undermine faith in the election process, and then to promote Trump over Clinton in that scenario.

And so, absolutely believe that was in fact the case. And I also think he will continue to be involved in those kinds of decisions about interference in our election. And I think he does it through the frame that I mentioned previously.

00:32:56 Clifford Chanin: We come to the response of the administration. And this was a really complicated dilemma-- the partisanship of the election, the uncertainty of what a government statement or intervention would do to heighten partisanship, as opposed to get everybody behind this. But, you know, you have reflected on this, and you were one of the people in the administration who was intimately involved in the entire episode, and managing this, essentially.

00:33:30 But retrospectively, you say, "The picture we have now we didn't have then. Honestly, we could have done better from the policy perspective. In thinking that through, I think we all have a piece of that to live with. I do think, though, even knowing that, I'm not sure our reactions would have been any different." That the dilemma doesn't resolve itself particularly around what the outcome of your decision-making process is.

00:33:53 You still have all of these uncertainties about what you could have done under that. That said, the active... the active response of the administration came after the election—the expulsion of Russians, the closing of certain facilities, certain kinds of sanctions. This is post-election. Take us back to the logic leading up to the election, where you have these warnings, credible intelligence, ultimately, the intelligence community coalesces around this assessment, and yet, aside from presidential statements, there was nothing done. What's the sequence of events that was of concern in terms of stronger action than that?

00:34:34 Avril Haines: Yeah, and I should explain those comments, I think, put them into context for you. So... and maybe I'll just do that in the context of explaining the events. So we received information, obviously, about

the interference in the election, and as I mentioned, you know, the questions are, okay, what exactly does that mean? How confident are you that you can attribute this to the Russian government, and if so, to Putin? And where is it going, right?

00:35:01 Because you sort of have a snapshot in time where you're... prior to the election, and you're trying to understand, so what's the purpose that they're trying to get at and what additional steps are we likely to see? And so at that point, we had clear information that indicated an information campaign, so the kind of things that I mentioned before, like disinformation, active measures, that type of thing. And we knew that they were using electronic media, you know, to do that. We did not know the extent, and that's the piece that I was mentioning about the policies.

00:35:36 So in other words, one of the things that I've learned since I was in the administration that I think is a really, you know, interesting data point that affects how you analyze the interference is as follows. There was a Pew poll that was taken in early 2017, I think, that indicates that roughly two-thirds of American adults receive their news through Facebook.

00:35:58 That's a remarkable number. That is not something that either the analytic community or the policy community, I think, was taking into account in the context of how the information was being sown through social media by the Russians, right? There's that.

In addition, we didn't know the extent to which the Russians were using social media in this context. So those are two pieces of, you know, both sort of an analytic point and just a basic point of information that we didn't have to pull together to really understand the potential impact that the information campaign could have under those circumstances. So... so that's one piece of the problem.

00:36:37 In addition, we saw them scanning, as I mentioned, register rolls at state level, basically. But the register rolls that we saw them scanning were not the active registration rolls. So they were the sort of... you know, the ones from last year, things like that, like, basically ones that had been

prior to the current active ones. And at that point, when you look at that kind of information, you say, "Okay, well, so... so what does that mean? Are they actually just testing to see whether or not they can actually get to registration rolls that are active? And then what would they do with them? And how could they affect the election as a consequence, and, you know, how would that play itself out?"

00:37:15 And as the intelligence community was working through that, the president sort of identified kind of our major objectives, right? Sort of said, "Look, the first thing we have to do is make sure we're trying to protect the integrity of our election. So we need to understand better how we can help defend the electoral infrastructure from any attack, and, you know... and do everything we can."

00:37:36 And so that line of effort goes to getting a national intelligence assessment for essentially the election infrastructure, which was done quite quickly, and then, also doing everything we could to support states in defending their electoral infrastructure, which, again, was, you know, outreach that DHS was doing, and others. And then trying to work with Congress to facilitate that kind of effort with the states. So that's one kind of line of effort.

00:38:03 In addition, we needed to think through, how do we respond to, essentially, this information campaign and the actions that the Russians are taking? How do you, you know, effectively respond to say, "This is unacceptable," and also deter further activity in that respect? And then the final piece, which was really the most concerning at that moment, right, which was, if they are in fact intending to affect votes, right, prevent Americans from voting, or affect what they actually vote, if they do vote, then we need to actually, you know, prevent them from going down that road.

And so then you kind of have a discussion in government where you say to the analysts and the folks who work in these areas, "What's the most effective way we can do that?" In other words, "What can we do today that will deter Russia from going down that path?"

00:38:53 And there was really, frankly, unanimity within the analytic community and from the policymakers that the most effective action you could take at that moment would be a private message from the president to Putin to say, "Don't go any further. Don't do what you're doing now. We know what you're doing. And if you go further, there will be significant consequences." And that was a message that was delivered that's now public, essentially.

00:39:23 You know, that there was a pull-aside at the G20, and the president delivered that in September to Putin. And at the same time, when the president delivers a message like that, that says, "There will be significant consequences in the event that you pursue this," you have to actually figure out what those consequences are, right? Because you can't have the president of the United States bluffing in that scenario. You have to actually understand, okay, so what does that look like?

00:39:48 So we had to provide, essentially, options for what we would do in response to what had already been done. But then, also, we had to think through options for how we respond to, you know, them pursuing the line that we were concerned that they were pursuing to actually affect the vote count. And in that scenario, we delivered the message. We worked through our options. We sort of do our regular process.

00:40:11 We additionally were working on the state and government pieces, and we asked the intelligence community and DHS basically to put together a statement that could be made public so that the American public would have an understanding of what we understood without, obviously, endangering-- we call it, sources and methods, essentially, that had provided us the intelligence. So all those things are sort of moving down a track.

00:40:35 The intelligence community is consistently tracking the behavior, right? Trying to understand better what's happening and whether or not there's movement in the direction of affecting the count. And what they tell us is, they seem to see basically the Russians backing off from the register

rolls piece, right, from affecting the vote count. So at that moment, the analysis we had to do was essentially, okay, we have a number of things that we want to do in response to the information campaign and the active measures that the Russians have been engaging in. We don't see them moving further down this path of actually trying to affect the vote count.

00:41:13 Should we react now, before the election, or should we react after the election? Is there any advantage one way or the other, right? So if we react now, before the election, the question is, you know, what could possibly happen? What are the possible responses from Russia? Well, it's possible if you go down this road, the analysts said, okay, that Putin will actually reverse course and, in fact, move forward, possibly, as he was planning to do originally, to try to affect the vote count.

00:41:48 Does it have an impact on deterrence? In other words, does it make a difference in terms of his behavior on the information campaign, or more generally, if we have a response before the election or after the election, for him doing this again in the future? And the view is, no, it's not going to make a difference. We're basically almost on top of the election at this point.

00:42:07 You know, whether we have a response now or have a response right after the election, the deterrence value that it has for him interfering in future elections is roughly the same, right? So we said, "Okay, it does not appear to be some big advantage to having our reaction right now as opposed to waiting another month or two, essentially, till after the election, to go forward with it."

00:42:30 And so that was sort of the logic, initially, for why it is that we said, "Okay, we'll wait to do our PNG-ing for 35 folks": closing down the dachas, having a variety of cyber-reactions, the joint analysis report, the cybersanctions that we did, and so on. And we did them in December as opposed to prior to the election.

Clifford Chanin: Let me ask one more question, and then we'll take some questions from the audience. Dr. Haines has a plane to catch, so it won't be quite as expansive as we normally are. Two years of hindsight. You know, what is your assessment of the impact of the Russian campaign on the outcome of the election?

00:43:08 Avril Haines: I mean, the intelligence community assessment that was done in January said, "Look, there's really no way for to us tell, right, like, how much impact the information campaign had on Americans' votes." And I still continue to think that's true. In other words, I just don't know how you measure the sort of... the impact that, you know, their sort of false accounts and views that they were propagating in particular social media spaces, et cetera, had on a person's decision as to whether or not to vote for Clinton versus Trump or not to vote at all.

00:43:40 But I do think that, you know, to the extent that the objective was not about affecting the outcome of the election, but rather in dividing us more, in, you know, making us question the democratic process and so on, I think that was successful. I mean, I think it's absolutely remarkable how much success, in effect, they've had as a consequence of the act and measures of the campaign.

00:44:05 And I suspect it was, frankly, far more than they expected at the time. But it is something that we need to deal with as a country moving forward. And I think that's... you know, that's part of the effort that's engaged in. But it's... it's something that all of us can contribute to, in a sense.

00:44:21 Clifford Chanin: General Hayden, who was previously director of the C.I.A. and NSA, as well, and I don't remember the exact quote, but he essentially said, from the point of view of an intelligence professional, this was a very successful operation. Sort of grudging admiration, almost, for what this was. This was a success from the Russian point of view.

Avril Haines: Yeah. I mean, I think they succeeded in creating greater division and sowing the discontent and so on. I think the other thing that

really was probably the most disappointing moment for me was the fact that we were unable to get a bipartisan statement in response to this. And I think that...

Clifford Chanin: Pre-election.

00:44:58 Avril Haines: Pre-election, yeah. And it's one of those things where that was another kind of factor that we were looking at in the context of when to come out with our responses. But it's... One of the challenges, obviously, in making statements about the fact that there's Russian interference from the White House perspective is that you have a president who is the head of one of the political parties, right? And you don't want the statement to be perceived as a political statement, because it essentially reduces its credibility.

00:45:27 And that was one of the reasons why we wanted DNI, the director of national intelligence, and the secretary of the Department of Homeland Security to make the statement, because generally, those are institutions that are perceived as less political. We didn't edit the statement. We didn't... you know, we said, "You should put out what you believe to be the case, and we're not going to put this out from the White House and try to promote it."

00:45:50 But, ultimately, if we had gotten a bipartisan statement to say the Russians are interfering in our election, I think that would have had greater impact. And I think it's just another example of where the divisions in this country have, frankly, made us less successful at approaching our national security and promoting it. And I think that's a pretty depressing thought, frankly.

Clifford Chanin: Indeed. Let's see if we have a question or two. The lady here. Just wait, if you will, for the microphone to come to you. Here it comes.

Audience Member: Have you been assisting in the Mueller investigation at all?

Avril Haines: No, not at all.

Audience Member: Okay, then I have no...

00:46:32 Clifford Chanin: There you go. While we're on this side, gentleman raising his hand right behind you, Dani.

Audience Member: Early on, you spoke about, the biggest part of the equation for cybersecurity is on our side-- what we read, what we do, how we respond. That struck me, from a medical point of view, of doing critical appraisal-- you know, you read an article, you critically appraise the data that you're reading-- I guess... and within the scientific community, the authors' list, who they're getting money from, so you can make a judgment on what they're saying.

00:46:59 I guess the big question is, do you think people can learn critical appraisal? Or are you locked into your mindset? You know, you don't know what you don't know, and you're not about to learn anything new. I mean, how do we get... how do we nationalize critical appraisal on what we're reading?

Clifford Chanin: Small question.

Avril Haines: Yeah, seriously.

(man talking off mic)

00:47:36 Avril Haines: Yeah-- no, no, no, it's totally fair. I'm a physics major, so I have a science background. I am also somebody who tends to be on the more optimistic side of things, so I do believe that we can learn critical appraisal. And I really think that we have to in order to actually be able to deal with the internet. And... but I also believe that we can do a better job of helping people have the tools to do that critical appraisal, for just... exactly as you're describing, right?

00:48:09 I mean, I find when I read articles-- and I don't know if this resonates for all of you in your different fields-- but when I read an article about national security or about national security law, it is utterly clear to me that the authors' perspective and their experiences color what they have to say, right? I mean, you know, in a sense, if it's in my area, and I read it, I could probably tell you, this person grew up in the State Department, or this person was at the Department of Defense, or in the intelligence community, and so on. It's just natural that our experiences and our knowledge and so on, you know, have an impact on what we have to say.

00:48:50 And so understanding who the author is for a particular article or perspective, I think, is critical for us. And it's a useful thing. Now, I'm not suggesting that there be no anonymity allowed. I do think that there has to be some space for that. I mean, after all, the "Federalist Papers" were written anonymously. You know, there is actually value in allowing people to say things without it being attributed to them personally under certain circumstances.

00:49:19 But I do think, you know, at the very least we should be able to tell the difference between whether or not something's automatically generated and whether or not it's a person who's putting it forward. And I also think that if there's paid advertising for political purposes, it needs to be identified. So that's my... yeah.

Clifford Chanin: Fair enough—another question. This gentleman here in the middle. You may be hard to get to for the mic, but give us a moment. We'll pass it along. And I'm going to ask our high school kids if they're going to come up with a question next. So you're going to be next. So hang on.

00:49:55 Audience Member: Thank you. So you just talked a little bit about the success that... at least from the Russian perspective, that they had. And my question is, do you see other nations taking a look at this and thinking, "Maybe this is something we can do, too?" Because other nations certainly have capable threat actors. Or, on the other hand, do you feel like this deterrence is going to take effect, like... I believe John Bolton just made a comment about, you know, cold calculation of cost-benefit, and, you know, there are consequences for them doing this.

00:50:29 Avril Haines: Yeah. So to the first question of just whether or not other nations take a look at this, I think certainly they do. And I think one of the... one of the asymmetries here is that the United States is just particularly vulnerable in the cyber area. I mean, we gain enormous advantages as a consequence of the fact that we use the internet for so many things, for our prosperity, for, you know, our government actions, our military, et cetera.

00:50:56 But we also have a significant percentage of the infrastructure that supports the internet throughout the world, frankly, in the United States. And it is something of great value to us, right, that at relatively low cost, an adversary can attack, and do so in a kind of a nonconventional way. And I think that gets to the second part of your question, which is to say that, so then how do you develop deterrence, and how do you actually promote a policy that makes it more costly for other countries to do attacks on the United States in this kind of way, right?

00:51:37 And in my view, one of the ways that we've historically approached these kinds of issues is through developing normative behavior, right? So we sort of say, "This is acceptable, but this is not acceptable." And we see if we can get a consensus among a wide range of states to agree with us that that's true, right? So we... we're promoting a norm that basically, attacking critical infrastructure in certain ways is unacceptable.

00:52:01 And that was something that we promoted at the G20. There were a number of state leaders that signed on to that, right? Like, you start to

develop kind of momentum for those types of norms. And then what happens is, when another country breaches one of those norms, you're able to say to your partners and allies, "You agreed that this is unacceptable behavior. And, therefore, we should all respond collectively in response to it." And that raises the cost for another country.

00:52:27 And I think, you know, one of the things... We talk about sanctions. You know, is sanctions a response to everything? No, it should not be a response to everything. But it is remarkably effective under certain circumstances, and it's much more effective if you actually don't do it unilaterally, but you have other countries joining with you in doing it.

So that's an example of a place where you could have a response like that. But there are a lot of areas just traditionally where we've done that. The law of the sea is a really good example of this. I mean, we support freedom of navigation around the world. It helps us, you know, in terms of supporting our military, but it also helps our private sector, you know, be able to travel around the world and do trade in a consistent, kind of stable way.

00:53:05 And we developed a very detailed sort of legal framework for what's acceptable, what's not, that sort of thing. And we mobilize it when there's a problem. When somebody violates something, we can work with other countries to push back on that kind of action and promote it. And it means that we don't have to have a destroyer in every international strait around the world in order to promote freedom of navigation. So it's just another way to think about it.

00:53:29 Clifford Chanin: Has anything in this line been codified yet, or is it still developmental and a hope?

Avril Haines: It's... I mean, I think it's... It's still developmental, but there are... Codification in the international realm is not an easy thing to identify. In other words, there are statements that have been made. There's a U.N. government experts group that has done interpretation of existing law that applies in the cyberspace that's a kind of a piece to that.

00:53:57 There's work being done by a variety of companies that are doing something called a tech accord that has now over 68 companies, I think, that are a part of it, that are trying to establish their own norms of behavior and promoting, essentially, state facilitation of those. So there's a lot of things that are out there, a lot of, you know, ideas for how to approach this. But we're still at the very early stages. And, I mean, honestly, it took decades and decades, even hundreds of years, for the law of the sea to develop. I think it's going to take time, but it's critically important that we invest in it.

00:54:28 Clifford Chanin: Last one. Yep. If you'd stand up. Go ahead.

Audience Member: So what are the long-term effects of these hacks? Not only the DNC and the election, but, like, private corporations, like credit companies? Because that affects all people, the Social Security, credit card numbers. How would we protect ourselves in the future? Like, what's the plan in the works to protect average Americans from hacking?

00:55:08 Avril Haines: Gotcha. We could spend an entire hour on that, I am...

(laughter)

Avril Haines: It's a very good question. Why don't I just list a few things that I think are important? And honestly... There's work for everybody to do in this area, and I think further development to be had. I am struck by how often, in cybersecurity discussions, we get to a point where we talk about how much institutions and individuals could be doing to make themselves more secure with the tools they have available to them today, but they don't, right?

00:55:44 So, you know, just actually exercising good cyberhygiene is something that doesn't happen in many institutions, private sector institutions, you know? Just doing the patch that needs to be done, or, you know, doing

dual-key identification, or, you know, things that can protect you more effectively but take a little bit more time or a little bit of hassle, right? Like, those things are really useful and need to get done. So that's one thing.

00:56:10 Another thing is basically, you know, there are some ideas about whether or not we should re-engineer the structure of the internet in order to make it more secure, that that wasn't one of the things that was, you know, sort of a key principle when it was developed. I think, my own experience, it doesn't look to be as if that would be easily feasible, but I'm listening. And there are a lot of ideas out there, and I certainly don't want to dismiss them out of hand.

00:56:32 I think another area is in developing the kind of norms that we were talking about before, in the sense of trying to push back against bad behavior in this space. Another piece of this is that so much of our critical infrastructure is owned by the private sector. I mean, there was a recent report that was done on energy infrastructure, for example, and 90% of it in the United States is owned by the private sector. That means you really need a substantial private-public partnership on these issues so that you can have sharing of information across these spaces.

00:57:04 And that has proved to be incredibly complex and challenging. And even getting legislation that supports that and, you know, harmonizing our standards is something that needs to be done. So you need the sort of policy and legal frameworks that facilitate that kind of action. You need to have the collaboration on an international basis. You need to help other countries be more resilient in responding to attacks when it occurs. So there's just a whole series of things that need to be happening.

00:57:30 There's, also, I think, key questions about whether or not we can promote privacy more successfully in this day and age through a variety of different mechanisms. And if we had more time, I would talk about some of the really interesting ideas that some Columbia professors have been working on in this space that I think would be useful. But I suspect some of you will end up doing some interesting work in this area. So I

look forward to seeing what kind of ideas you can come up with to help us. Thank you.

00:58:02 Clifford Chanin: Indeed. You know, I think two weeks from tonight, in fact, we're going to know something about the security of our electoral system.

Avril Haines: Indeed, yeah.

Clifford Chanin: Coming up.

Avril Haines: Let's hope it's good news.

Clifford Chanin: We certainly do. But this has been wonderful. And I do want to ask everybody to join me in thanking Avril Haines.

Avril Haines: Oh, thank you very much. Thank you. (applause)