

THE ASPEN INSTITUTE

ASPEN SECURITY FORUM 2016

CONGRESS AND THE WAR ON TERROR

Doerr-Hosier Center  
Aspen, Colorado

Saturday, July 30, 2016

LIST OF PARTICIPANTS

ADAM SCHIFF  
Ranking Member, House Permanent Select Committee on  
Intelligence  
US Representative (D-CA)

GREG MILLER  
National Security Correspondent, *The Washington Post*

\* \* \* \* \*

CONGRESS AND THE WAR ON TERROR

(1:15 p.m.)

MS. STERN: Okay. Okay, I think we're going to begin now. Good afternoon to all of you. I know I hear from so many of you what a great time you are having and I want to thank Clark Ervin. I'm also having a great time, but I especially want to thank his family. His family is here right now. I know they have been putting up with a lot in order for us to have this great conference.

My name is Jessica Stern. I'm a research professor at Boston University. I'm also a member of the Aspen Institute Homeland Security Group. I'm delighted to introduce our next session, Congress and the War on Terror.

The panel is somewhat smaller than it was meant to be. I hope that means we're going to learn -- it may mean we're going to learn even more. How do various leaders on Capitol Hill view the war on terrorism? How do they grade the outgoing administration? With no progress on a revised authorizing resolution, how do they grade themselves? I know this is something Adam Schiff is interested in. And what policies should the next administration pursue?

Moderating the conversation is Greg Miller, who has a storied career. He covers intelligence and national security for the *Washington Post*. He was awarded a Pulitzer in 2014 and was also a finalist for a Pulitzer in 2013. He is also co-author of the book *The Interrogators*. We're really looking forward to hearing from both of you. Thank you.

(Applause)

MR. MILLER: Thank you, Jessica. As you -- this is Congress and the War on Terror and this is Congress here with me today. Mike Rogers -- Congressman Mike Rogers was supposed to attend. He sent his regrets. He had an urgent family matter that came up. So we wish him well.

But I'm delighted to be -- to share the stage with this fellow here. We all know him as the dedicated, fair minded senior Democrat on the House Intelligence Committee. Russian intelligence service I think just knows him as schiffa@mail.house.gov.

(Laughter)

MR. MILLER: He is a ranking member in the House Intelligence Committee. He is on leave from the Appropriations Committee. He is a Democrat representing the 28th district of California, and was first elected to Congress in the year 2000. Prior to his election, Congressman Schiff was an assistant -- he was prosecutor and a state senator.

I just thought we would start by diving into the topic of the week. We've had Director Clapper, Director Brennan argue that it's too early to pin the blame for the hack of the DNC on Russian intelligence. Based on what you've seen, do you have any doubt that this was carried out by Russian intelligence?

MR. SCHIFF: Well, I'm under some of the same limitations that prior speakers were, although probably not quite as many limitations. And, you know, I will say this: clearly Russia has the means. There are a narrow category of state actors and non-state actors that have the technological means. It certainly has a history of interfering in the political affairs mostly in Europe. But potentially we have seen some disclosure of US e-mails or conversations, as we saw with Victoria Nuland some time ago.

But clearly there's a motive here. And when it comes to attribution, there are really two questions and it's hard to tell from I think what the director said the other day which of those two questions he is referring to: Is it too early to say who is responsible because we don't yet have enough evidence to say who is responsible or do we have the evidence, but nonetheless it's too early to have reached the policy conclusion about making a public attribution?

My own feeling and Senator Feinstein -- and I wrote to the President just a couple of days ago -- is: when we do, when the administration does have the requisite confidence in the evidence of attribution, they should make public attribution.

I think -- and I know we've lot of discussion about whether this is a game changer or not a game changer. Certainly, the theft of information is not new. Great many nations engage in foreign intelligence gathering. The fact that our political parties and organizations are the targets of foreign interest is also not new and not surprising.

But if you have a state actor who is deliberately dumping stolen e-mails with an intent to interfere with the political process, that does make this new, at least at the level we're talking about here, a presidential race right before a major party convention.

And I think one of the ways to deter that conduct in the future is by naming and shaming the responsible party. I also think there's a second very important reason to make attribution here, and that is if there is a foreign power who is trying to influence our election, the American people ought to know about that. It ought to be information they have in making their decision.

Now, I realize that puts the administration in a very difficult position, not unlike probably the position that Director Comey was in and the attorney general was in in the investigation of the private server. But nonetheless, I think there's intense public interest and beyond that a public need to know if indeed we can make attribution who is responsible for trying to potentially alter the course of our elections.

I also think that it points out a number of imperatives for the Congress, and chief among them are ensuring the integrity of the election itself. We have had legislation pending for years to require that when we use electronic voting machines that there be a paper

trail. I think that -- I hope that now will fly through Congress because that I think is only the most fundamental common sense.

The other point I would make on this is one of the cyber worries that I have had -- and this is something that Admiral Rogers often emphasizes -- is it's one thing to steal information, it's another to dump information, it's still another to doctor information. And for the war fighter one of the ideas that terrifies me is the concept that a foreign adversary could hack into our system and could alter data. You could imagine the havoc it would wreak if someone was able to alter the GPS coordinates of a target and the consequences of something like that for the war fighter.

Well, if you can hack into the Democratic Party and alter the contents of what you steal and then dump it, how is the public going to know whether it's accurate or not? How is the person who may have been the author of the e-mail, which in itself may have been an embarrassing e-mail, able to say, "This part is accurate and I'm ashamed of, this part is not accurate"? That's a very tough case to make credibly.

So the opportunities for mischief are profound and it is I think for that reason quite breathtaking when you consider the possibilities that this hack unleashes. So for me I do think it's not something to be blase about. I think it is a very serious active interference.

And I think the administration when it reaches the point of confidence in the evidence, ought to make public attribution. It ought to consider potentially further steps. The administration has in the past indicted Chinese hackers. We have used provisions like the Magnitsky law, if we want to escalate even further. But I do think -- and this is true of Ukraine, it's true of Syria, it's true of cyber -- if Russia is responsible, the only language I think that Putin understands is the language of strength and I think we do have to push back with force.

MR. MILLER: Speaking of opportunities for

mischievous -- I'm going to ask you a Trump question now.

MR. SCHIFF: And I should clarify: when I say with force, I'm not speaking literally of force here.

MR. MILLER: You came to Aspen late in the week because you were speaking at the Democratic Convention this week. I don't know if any of you caught the Congressman's remarks there, but I'll read just a short portion: "Trump offers only bluster, tirade, swindle and threat. With malice toward all and charity for none, Trump would separate us from the world and divide us here at home. In Trump's world NATO is a relic, Putin an ally, Tiananmen an example and torture our instrument. This is not leadership, this is calamity." So having established your impartiality, I want to ask --

(Laughter)

MR. MILLER: -- another question that came up this week. Director Clapper indicated that both candidates would soon be getting their initial classified briefings from the intelligence community. Do you think that's appropriate in this case?

MR. SCHIFF: I do think it's appropriate. I don't think you can provide a briefing to one candidate and not brief the other. I do think that the briefing ought to be very top line and should not involve anything that could be potentially revealing of sources and methods. And I have every confidence that that is what the intention would be.

I have to say, I was asked this question during the Convention. I was on a panel that *Politico* put together, and I was asked, "Well, does that apply even in the case of Donald Trump and even in the case of Russia? And I began with my usual flippant kind of response, which is: "The question with Donald Trump is not so much whether he should be briefed, but whether it would do any good." But then I had to think more seriously about whether he should be briefed on Russia, having advocated, from my point of view, that Russia hack into his opponent's e-mails.

And I perhaps answered that question too quickly by saying that I thought he should be briefed on Russia, again, at a very top line. "This is what we believe about attribution, this is the level of confidence we have in that belief whether it's Russia or some other party."

But the more I thought about it, the more I've questioned that conclusion. I am very concerned about not only what Mr. Trump has said about Russia, but about the fact that he is openly entertaining the repeal of sanctions on Russia, potentially recognizing Russia's invasion and annexation of Crimea as now a fait accompli, the disparaging comments he has made about NATO and -- as well as some of the people advising the campaign and their ties to Russia have given me profound concerns. And I ask myself, "Would anyone with that background be given a briefing on Russia by the IC?" And I think the answer is no.

Now, these are exceptional circumstances obviously, so I do think they would have to be very thoughtful about just what kind of a briefing on Russia that they would be able to give Mr. Trump.

MR. MILLER: And our conversation with the CIA director last evening, Brennan was --

MR. SCHIFF: And I know my colleague, Mr. Rogers, is not here to give the contrary opinion, so let me just say I'm sure he agrees with me.

(Laughter)

MR. MILLER: You were promising an impression, but we won't hold you to that. Brennan gave very animated remarks last night about the encryption issue. You are a Congressman from California. You are from Southern California, which -- you know, the Silicon Valley companies are not in your district, but as a California Congressman I think you are acutely aware of their concerns. And as a former US prosecutor, I know that you see the law enforcement side of this issue. Do you see a way forward that bridges what looks like an incredible

divide right now?

MR. SCHIFF: That's a great question. And of all of the issues that we've had at the intersection of security and privacy, I think this is the most challenging. We wrestled the telephone metadata program to the ground. We I think arrived at a very sensible and bipartisan solution in Congress to that issue of how we ought to handle the prior program we had, where the government was gathering domestic call data, and arrived at a very sensible conclusion. And that, you know, was I have to say for a very dysfunctional, off and bitterly divided Congress a great achievement to wrestle with something of that significance and come up with something that made sense.

Similarly, we have enacted cyber information sharing legislation. That was I think an easier task, but nonetheless not easy. This is a whole order of magnitude more difficult. The consequences are much more far reaching. I think the consequences in some respects are only dimly perceived by both government and industry at this point in terms of where we're heading.

Encryption offers tremendous benefits in terms of billions of people around the globe being able to communicate with confidence that their communications are not being overheard by their authoritarian governments in Iran, in Russia, in China, increasingly in places like Turkey. I think that is tremendously important. It's also one of the best defenses we have.

But the cost to law enforcement and the IC are very real also and I don't subscribe to the view that there's no real consequence. I know there's at least one study that says that the going dark problem is overstated because in an internet of things you can talk to your TV, your refrigerators has an IP address. Well, that maybe fine, but most people committing acts of terror or plotting them aren't talking to their TV and the fact you may know when you've run out of mayonnaise isn't all that helpful in a terrorism investigation.

So I don't think there's an adequate substitute

for content. As a former prosecutor the idea that in the near future -- and I asked a group of Stanford students recently how many of them had a landline, and you can imagine not a single hand went up. We're moving to platforms where increasingly voice communications will all be encrypted, which means you can get a wiretap when you make the requisite showing that nothing else will work, but all you'll be getting is gibberish. That's a very different world than the one I grew up in as a prosecutor and the consequences to the intelligence community of not being able to intercept communications, understand them are also quite profound.

So what's the answer here? You know, the tech position at the moment is: it's all encryption or no encryption; you either have unbreakable encryption or you so compromise it it's accessible to everyone.

One thing I think we need to do -- and I met with Tim Cook about this recently to talk about it and I've tried to have conversations with a lot of folks in industry and the government outside of the heat of litigation. And one of the -- I think the downsides of the litigation between Apple and the bureau has been the parties get polarized in their corners and don't want to talk to each other about what might be possible.

But it seems to me that the problems which have been lumped together of data in transit and data at rest are not the same problem. They don't affect the community equally and they don't I think have necessarily the same technological answer.

Data at rest is predominantly a problem for law enforcement, even though we see it can impact the IC in cases like San Bernardino where we get a device that we can't get into. But predominantly that affects law enforcement. The data in motion predominantly affects the IC. And, well, I can certainly understand that if you build a means for people at a distance remotely to be able to intercept communications and decrypt them, that's a door that others can go through and not just the US government would process.

But it seems to me the issue of a data at rest in a device maybe amenable to other solutions that don't have the same risk or that have a risk that can be more effectively mitigated. If it's possible, for example, for Apple or some other phone maker to have a hardwired solution that they would require possession of the phone to be able to open, then the dangers that someone at a distance can hack into the phone are greatly diminished.

So is there a way technologically to design a phone where the maker of that phone through a hard technology, not a software solution, can open the phone; it may be a combination of hardware and software that is not easily replicated. And from my point of view, it's not something that would have to endure for the ages. If China or Russia found a way to replicate the technology to get into a device, that technology can be changed every 16, 18 months just as the phone operating systems are updated.

So that's one question I have: Is there a different technological answer? Are there fewer risks? Can they be better mitigated? It's one of the reasons why last fall I asked the National Academy of Sciences along with Chairman Nunes to undertake an objective scientific analysis of the issue of encryption and what the technological solutions may be, what the risks are, to what degree can we mitigate the risks so we may have other options than this binary choice of either a perfect security or no security at all.

MR. MILLER: I want to get to the topic of our discussion as it was advertised of oversight, Congressional oversight, the core of your job as the ranking Democrat in the House Intelligence Committee. And I want to start by asking you -- and we're looking at the waning of the Obama administration, the final months of an administration that will be closely scrutinized by history for many reasons probably, but I think one of them is likely to be its approach to fighting terrorism.

It wasn't that long ago that it looked like this administration and its approach had a lot of momentum. Al-Qaeda was badly damaged, the drone campaign had

inflicted a heavy toll and it looked like there was a diminishing threat.

Now, with, as I say, just months to go in the term for this White House we're looking at attack after attack after attack in Europe, in the United States, in Turkey, in Iraq and elsewhere. What grade -- how do you explain this? Is the -- was there anything that could have been done differently by this administration and what grade would you assign it in the area of counterterrorism?

MR. SCHIFF: Well, it's a great question obviously and I think one as complex and difficult as the one that was posed to the director about what's the end game in Syria. Because the question I think involves both: How -- what is your ability to shape events around the world and how have you effectively or not effectively taken steps to shape events around the world?

But the other part of the question is: How effective have you been in dealing with events that are beyond your control, those that you can't shape? And I would put the Arab Spring in the category of events that we neither shaped nor have appropriate control over how to respond to. And so in terms of grading the administration, first of all I would look at the question even more broadly than how this administration has done.

I like to ask the question: If this was the day after 9/11 and we could tell that today some, what, 15 years later the world would look as it does today, how would we grade ourselves? Have we employed the right strategy since 9/11? Are we facing greater risk or less risk? And I think viewed from that prism, you probably wouldn't choose the path we went down. This would not look like success.

Yes, we have severely mitigated the threat from core Al-Qaeda by wiping out a lot of its top leadership. We've put Al-Qaeda under tremendous stress and strain around the world. But we have seen the emergence of an even more virulent organization in ISIS: a much more diffused threat, one that doesn't necessarily aspire to the great big attack against the great Satan, but is

essentially outsourcing terrorism to people who can drive a truck, grab a hatchet, grab a knife, grab a gun.

So how do we assess all that? We're still very much at war in Afghanistan. We've been pulled back to some degree in Iraq. We're now on the ground in places like Syria. And it's obviously a very mixed record. Within the events that the administration could either shape or influence, I think they have done a pretty good job.

Now, I remember Leon Panetta getting the question -- and I view part of this at least through the intel perspective -- "Was it an intel failure that we didn't see the Arab Spring coming?" And he answered the question classic California fashion by using a California metaphor, which is he said, "You know, we could see the fault lines. We could see pressure building up along the plates. But in terms of predicting when the earthquake would strike, no, we couldn't predict exactly when or what the magnitude of the earthquake would be."

I think that was a very good way to express both the limits and the possibilities in terms of intelligence gathering. I don't think the Arabs saw the Arab Spring coming and I don't expect that our IC or this administration can have that kind of prophesy and capability either.

Have they responded to the Arab Spring in the optimal way? You know, I think that they have done a pretty darn good job. You can look at places like Egypt -- and I know there's been a lot of criticism certainly from some of our Arab partners that the administration threw Mubarak under the bus. But Egypt was a clear conflict between our pragmatic security priorities and our highest ideals.

We have I think quite legitimately been the subject of criticism over many decades for trading our security for other people's liberty, for making this obscene deal with these authoritarian rulers that as long as they were a partner with us on security, we wouldn't care what they did to their own population.

This was driven home to me more than a decade ago with the meeting I had with Mubarak when I brought up his imprisonment of Saad Ibrahim, who was a secular opponent of the regime who had very little base in Egypt, posed no threat to the regime, but nonetheless was being imprisoned I think in an effort by Egypt to say and make it so: it's either me or the Brotherhood.

It's the same strategy that Bashar al-Assad has used: it's either me or the terrorists. It's why Assad brought most of his fire and attention on the moderate opposition for the early years of this war and even to this day rather than ISIS.

And so I think it was a very difficult dilemma for the administration. I think they handled that about as they should, not abandoning our values and doing their best to both mitigate the national security concerns and impacts while also speaking to the aspirations of millions and millions of people around the world and the ideals of the country.

Syria of course is the most difficult question in terms of grading the administration, and here it just doesn't admit of an easy answer because none of us can say -- as much as you hear people talking without a certainty and confidence -- how would it have been if only we had more strongly supported the moderate opposition from the early days, if only we had followed through on the red line with chemical weapons.

You know, if we had followed through on the red line of chemical weapons -- and I think maybe the more legitimate criticism was drawing the red line than the failure to enforce it. But had we gone and bombed Syria, I am confident that the civil war would have still gone on, but Syria might be awash in chemical weapons at the same time. And I don't think you can definitively say that the result would have been different or better.

So I give the administration pretty high grades in dealing with a world where the level of instability that we haven't seen in at least a generation.

MR. MILLER: So you give the administration high grades. Now, I want to ask you what grades you would give yourself. What grades you would give your committee and its counterpart in the Senate? And I want to set this up by just noting that I think it's fair to say that in your time as the ranking Democrat you get credits -- the committee gets credit for the continued bipartisan work that happens. But a lot of what your committee has done and the bipartisan work that it has done has been overshadowed by the much more partisan work of other committees.

Last year we saw the Senate Intelligence Committee issue a report on the CIA in which the Republicans were essentially on the sideline through the investigation and the drafting of that report. And this year, obviously, we saw the report of the Benghazi Committee.

And let me just read a few stats here. In 2015, the House Intelligence Committee spent \$3.7 million. Since its creation in May 2014, the Select Committee on Benghazi has spent around \$6.9 million. The House Intelligence Committee has a staff of, give or take, 30 people and I think the Benghazi Committee approached that at its peak.

Of course you're overseeing 16 agencies, tens of billions of dollars in spending and this is a committee that's looking at a specific event. What does that tell us about oversight? What is going on here? Is there something wrong?

MR. SCHIFF: Yes, there's a lot wrong. Let me start on the question maybe by giving Congress a grade, giving the Benghazi Committee a grade and then giving the Intel Committee a grade.

The biggest failure of Congress I think in the last several years -- and I know there are a lot of candidates for that accolade -- but I would say would be the failure for Congress to live up to its responsibility of declaring war or not declaring war, which is one of the

reasons why I've been so vocal on the subject of passing an authorization to use force against ISIS.

I think we have set a terrible precedent by letting this war go on without any real debate over it, without any real vote over it. And it's been an issue I think of some mutual interest in terms of the political apathy, and that is: most members of Congress don't want to have to vote on the war. It's a vote that can only come back to haunt you, which we saw with the Iraq vote. So there's little political incentive for people to push this issue in the Congress.

There's also little political incentive on the part of the White House to really devote a lot of its capital to this issue. For one thing the White House doesn't want to be hamstrung by a too narrowly drafted authorization, and on the other hand, they don't want to pass on to the next administration an overly broad authorization.

And I think the President takes the view, not without reason, that this is Congress' institutional responsibility: "I can't care more about the Congress' role than the Congress does. So I will send a draft" -- and they did. "I will urge the Congress to take it up" -- and he has. "But if the Congress doesn't have the guts to do it, then it's their own institutional prerogative that is at stake." And that's absolutely true.

So I give us a complete failing grade in terms of our willingness to act as a check on executive war making authority. Future Presidents are going to look at this and they may still have the same authorizations if we do nothing about it, and they are going to say, "President Obama did it. He said he had a legal and constitutional basis, so I can do it." And I think that is a terrible precedent.

I am, you know, very encouraged I think by the prospect that we may have a vice president named Tim Kaine, because my strongest ally, as I said, on this issue has been Senator Kaine. I also don't think this is an impossible task. There are red lines for both parties,

but I think there's a way to draft it where you avoid red lines of both parties.

In terms of the Benghazi Committee, I would also give that a failing grade. I have to confess I was very skeptical at the beginning of the Benghazi Committee's formation and didn't think that we ought to have anything to do with it in the Democratic Party because it looked like it would just be a political tool.

But I was persuaded to at least test the representations that were being made by the majority about why they formed the committee. And I was skeptical because I had been already a part of an investigation of Benghazi that was conducted on a bipartisan basis by the House Intelligence Committee, conducted by a committee chaired by my colleague who wasn't able to join us today, Mike Rogers.

It debunked after a lengthy work a lot of the conspiracy theories over gun running, stand down orders and the like and it just didn't seem to me after our own investigation -- by the way, Mike Rogers took a lot of arrows in his back for doing an objective job on the Benghazi investigation -- but just didn't seem to me that we would likely uncover anything that the other eight investigations hadn't that altered our core understanding.

Certainly, you can always add new insights and if you spend time on task, you're going to fill in some of the facts and the intricacies of what took place. But after two years, in fact we didn't alter any of the core conclusions of the other eight investigations.

And I think the damage that we did is really twofold: one, I think we raised the expectations of the families who were affected by this, that there was some horrendous cover up, some great scandal that we were going to uncover, that they were going to be given some profound new insight about what happened to their loved ones. And I think it was unfair to give those families that expectation when that was very unlikely to be the case.

I also think we established another terrible

precedent of establishing a select investigative committee to target one of the likely nominees of the other party, because I can guarantee you in the future people will cite this within the private caucus meetings of both parties, saying, "Maybe we should do a Benghazi on them. They did it to us. Or maybe we should do another Benghazi because it did drive down Hillary's numbers." And those are conversations that I don't want to see the Congress ever having.

In terms of our committee, the Intelligence Committee -- I guess I want to end on this because I think it's a more positive story. Mike Rogers, my predecessor chairman and Ruppertsberger brought back to the committee a very bipartisan ethic. It was a very productive committee under their leadership. And Devin Nunes and I have adopted exactly the same modus operandi.

So I think the Intel Committee is the least partisan committee on the Hill. You would hope it would be given the subject matter. That hasn't always been the case. And it's certainly not the case that we agree on everything. We will probably have some debate over security clearances that becomes politicized in the wake of the FBI investigation and now in the wake of Donald Trump's remarks. But we will get past that and I'm confident we won't lose sight in the everyday important business of the committee -- and that is oversight.

And the only last point I'll make on that -- and, you know, I think the passage of our annual authorization bills, the passage of the Information Sharing Bill, the passage of the telephone metadata reforms, all of those things came out of our committee in I think in pretty good fashion.

The only thing I will say -- and for this reason we really need your help in this room -- is unlike any other committee we don't have the advantage of a lot of outside validators of the arguments that we hear. I have great confidence and great admiration for the professionals in the IC -- they are fantastic. And there's nothing I like more than going to places around the world and meeting some of the incredibly courageous

people that work for our IC -- they are amazing.

But I do think that as good as they are, as good as any government institution is, it can be made better. It has to be made better with vigorous oversight, with questioning of authority. And that's very hard for us to do -- not because of the culture, not because of we're somehow captured by the IC, but because we don't have the outside parties who can test the arguments that are being made to us.

We are a small committee. We can't even utilize for much of our work our own personal staff. The notes we take have to stay in the room and we are term limited. There's enormous learning curve by definition when you get on the committee because you're not supposed to know much about it before you get there.

And so if I'm on the Transportation Committee and the administration comes in and they tell me high-speed rail is in great shape, well, I've got a lot of people outside the building who can come and say that was a bunch of nonsense. But if someone in the IC comes in and tells me something, it's hard for me to know whether it's accurate or not. It's hard for me to know at times the right question to ask. Because you can imagine if there's a problem and you don't want to volunteer it and the questioners don't know to ask the right question, it's not going to come out.

Now, I think we've had a very good relationship with those that have come to the committee and presented the committee. I think they have been forthcoming, ensuring their successes and failures. So I'm very self-interested, obviously, but certainly compared with Benghazi and the rest of the Congress, on the AUMF I would give our committee pretty good marks.

MR. MILLER: Okay. We've I think got maybe 10 minutes left, if that, and so I want to try to get through a number of questions. Please voice these as concisely as possible so that we can hear a number of questions because we are running short on time. All the way in the very back, blue blazer.

MR. BIDWELL: Thank you, Congressmen. Chris Bidwell, Airports Council International - North America. And I want to pivot to aviation security for just one second, if we could. Earlier this year Secretary Johnson stated that and testified that the threat to aviation is real, and I'm just curious why given that -- and I've seen no evidence to dispute that assertion -- why is Congress seemingly content with diverting one-third of the 9/11 passenger security fee, which amounts to \$1.25 billion this year, this fiscal year, to non-aviation security functions?

MR. SCHIFF: Well, thank you for the question. And I don't know whether our administrator is still here, but I think he has really done a superb job with a very difficult challenge. I concur with the assessment, frankly, that aviation is still very vulnerable. I am deeply concerned about aviation security and I'll tell you why.

First of all, the kind of attacks that concern me the most are the ones that have the potential of really dramatically changing the way we live. And the attacks that we have had in San Bernardino and Orlando and elsewhere have been awful and obviously every effort has to be made to stop them, prevent them, to mitigate the damage that terrorists can do or homegrown radicals.

But they are not likely to change the way we live as Americans. But another kind of devastating aviation attack in the United States does have the potential of dramatically changing how we live, the laws that we might pass in Congress, the amount of intrusion we may be willing to allow to our privacy.

So those kinds of attacks really do concern me. And my feeling is you direct the resources to the vulnerabilities not that are necessarily the most likely to occur if they have a lesser impact, but those that would have the most dramatic change on the way we live. And I put aviation security in that category.

I would also put in that category danger to our

financial institutions. You can imagine the panic that would be created if someone were able to cast doubt on whether what people had in their savings account was really in their savings account, whether what they owned in terms of their investments was really in fact owned by them. So I have great concerns about our financial infrastructure. I view that very much as critical infrastructure.

Why would we divert funds in light of the -- in my view, heightened significance of aviation security? I don't know and I think that's a very good question. I would certainly favor a much greater investment in our TSA and our aviation security and move quite in the opposite direction than in a diversion of resources. So I appreciate the question.

MR. MILLER: Who else do we have? Here in the front.

SPEAKER: Thank you. [Charlie Gellac].

MR. MILLER: There's a microphone coming.

SPEAKER: Thank you very much, Congressman. I really appreciated your remarks about encryption. That's a fresh look at it. But let me play devil's advocate on the e-mail issue. Weren't Bernie Sanders' supporters entitled to that information, putting aside how it came to light? And secondly, as the devil's advocate, if it is wrong to try to influence voting in another country, was President Obama wrong when he came out against the Brexit vote and warned about impact on trade and so forth prior to that vote?

MR. SCHIFF: Well, I think you can certainly answer the question. I'll start with Brexit first, whether it was a good decision strategically for the president to come out publically. And I know there have been a lot of questions about whether that had a counter -- I don't know if it's counterintuitive -- it may have been a quite intuitive impact on British voters to say, "Thank you, but we're not really interested in what others think. This is a decision for Britons to make."

But it's a quite a different story to publicly express an opinion and privately, surreptitiously hack in and try to influence an election by disclosing private e-mails. So I wouldn't put those in the same category at all.

SPEAKER: Would we ever do it?

MR. SCHIFF: Well, the question would we ever do it. You know, there certainly have been many documented instances in the past where the IC has attempted to influence political processes elsewhere. I can't go into any kind of a covert action question here obviously. But let me address your second question, which was: Did the Bernie Sanders supporters have a right to know and interest in knowing what were in those private e-mails?

When this story broke, I had two concerns. Wearing my Democratic hat, I was concerned that the DNC, which has an obligation to be ruthlessly neutral, objective in a primary, wasn't. And I found that deeply disturbing. As a Jew, I found it deeply disturbing that someone at the DNC was suggesting using someone's faith or lack of faith or different faith as a way of campaigning against them. That I found deeply offensive.

And so, is it positive that that was exposed? Well, it will be positive in terms of corrective action at the DNC. But the other concern I had, frankly, which for me was even a bigger concern, and that is: Do we have a foreign adversary who is trying to affect the outcome of our elections? Because that has to me a very worrying national security element to it that we've talked about. And so I have to say for me that concern has been the paramount one and for all the reasons I mentioned earlier.

MR. MILLER: Coming up on no time left, I want to try to sneak in two quick questions and two quick answers. Over here, this gentleman, and Kim Dozier in the center of the room.

SPEAKER: Yeah, I just had a question. I spend a lot of time in England and Ireland actually and they use

extensively CCTV. And I can't understand why in places like New York City, we're talking about airports, why we don't use more CCTV with facial recognition software? And that seems to me something that will greatly aid intelligence.

MR. SCHIFF: Okay.

MS. DOZIER: And the two quick questions: Has anyone articulated a timeline to you for the defeat of ISIS? I've heard a year-and-a-half, et cetera from foreign officials. And a reverse question: Do you see a rising number of terrorist attacks both in Europe and this country to come?

MR. SCHIFF: On the CCTV question, I am probably not in the best position to answer that. I think we are seeing a proliferation of CCTV and I know certainly in the Boston Marathon bombing that was a very important tool in -- now, some of those may have been private cameras of some of the merchants there in ascertaining who is responsible, how many parties were involved.

I wouldn't be at all surprised to see that technology used much more in a much more widespread fashion. You know, I will also say that I think that the privacy debate is going to turn in a whole new direction. The fact, for example, that when you're driving down Canal Road and you're going too fast, there's a speed cam that will photograph you in your car with your license plate. That database may be a private database or may be in a local police agency.

MR. MILLER: You make it sound like this actually happened to you.

(Laughter)

MR. SCHIFF: I've just been told this by friends.

(Laughter)

MR. SCHIFF: You know, the fact that that

database contains your image, your location, your vehicle, your time and date, where you're going, what direction you're headed, that has far more information than the telephone metadata database ever had. And we haven't even begun to have discussions about that kind of thing, which maybe in government hands as well as private hands.

In terms of ISIS, do we have a timeline for the defeat of ISIS, do you expect more attacks from ISIS. I assume what you mean by timeline is for the military defeat on the battlefield. And I have never heard a timeline. The only times I've heard from time to time are the taking back of Mosul, which have invariably proved to be too optimistic and wrong.

So I don't think we have a -- we probably have an idea of how long we think it should take, but none that have been I think offered to Congress. And I think the agencies would be very loathe to try to venture that kind of an estimate.

You know, I will say a couple of points on ISIS -- as I was listening to the discussion about this yesterday. We are making a lot of military progress, and that's very palpable and observable and measurable. We haven't made much progress in combating the ideology, in combating their use of social media. We're making improvements by moving from us trying to be the messenger about what Islam is, which our government was never going to be in a position to do, to empowering others that are better positioned to deliver those messages.

But the one area that concerns me most I guess that we've had the least progress, which I don't think we had enough discussion of, and that is the political progress or lack of that in Iraq. The political progress in Syria is even more complicated, more far behind. But the military pace is moving far faster than the Abadi government's incorporation of Sunnis into security and into the political establishment, and that's a great risk that we defeat ISIS on the battlefield and it pops up in its third iteration.

And on the point of do we expect more attacks, I

would have to say regrettably, tragically we do both in Europe and the United States. And the final point I'll make on the United States is I think we have to look at every venue and every method we can use to attack the problem of terrorism in the United States. And we have tried stove piping this problem. We've resisted talking about this problem in a more holistic way.

Some of this problem is obviously keeping foreign fighters out and we've been obviously greatly benefited by our oceans and we ought to have some humility towards our critique of our European partners, who don't have the benefit of those oceans.

But part of this is also combating the message to home grown radicals. Part of this is mental healthcare, because a lot of the people who are inspired by this message are in serious mental health crisis.

Part of this is access to instrumentalities that allow terrorist when radicalized to kill us in a more efficient fashion. And that means keeping them off planes. It means keeping them away from assault weapons. And I think we need to break down some of the walls that have prevented us from a more comprehensive solution to this I think long-term problem. Thank you.

MR. MILLER: Thank you, Congressman, and thanks all of you.

(Applause)

\* \* \* \* \*