

National Security Agency

INSA/AFCEA Intelligence Community Panel

Speakers:

**John Brennan,
Director, Central Intelligence Agency;
Letitia Long,
Director, National Geospatial-Intelligence Agency;
Admiral Mike Rogers,
Director, U.S. Cyber Command and National Security Agency;
David Shedd,
Acting Director, Defense Intelligence Agency**

**Moderator: Kimberly Dozier,
Contributor to The Daily Beast, CNN**

Location: Omni Shoreham Hotel, 2500 Calvert Street NW, Washington, D.C.

Time: 1:00 p.m. EDT

Date: Thursday, September 18, 2014

*Transcript by
Federal News Service
Washington, D.C.*

MR. : OK. Ladies and gentlemen, this is plenary session II, and we have an outstanding panel of directors from the CIA, the NSA, the NGA and the DIA. And the panel is going to discuss what the nation should expect from its intelligence community. The person moderating this panel – I want to do a brief introduction in this – she is going to introduce the panelists. But our moderator is Kim Dozier; I think many of you know her, but Kim is a reporter.

She is currently the Bradley Chair, teaching at the Army War College, and a contributing writer to the Daily Beast. She was formerly with AP; before that, she was with CBS. And many of you probably know that during an assignment in Iraq, Kim was wounded in an IED attack – life-threatening injuries – and she does have an amazing book, if you ever want to take a look at it, called “Breathing the Fire.” And the proceeds of that book go to Wounded Warriors.

So without further ado, please welcome our directors’ panel. (Applause.)

KIM DOZIER: Well, thank you very much, Chuck. Thanks to all of you for being here; great turnout, as the directors were saying before we came out here. It’s just us having a chat with 2,000 of our closest friends. (Laughter.)

MR. : (Inaudible.)

MS. DOZIER: So, today we have DIA’s acting Director, David Shedd, NSA’s new director, Admiral Mike Rogers, Tish Long, director of NGA – two weeks from retirement, and her voice shows it – (laughter) – retiring from – I think, about to retire from 40 – how many years of service?

TISH LONG: Thirty-six.

MS. DOZIER: Thirty-six years of service.

MS. LONG: Don’t – four years make a difference. (Laughter.)

MS. DOZIER: Gotcha. And CIA Director John Brennan.

So thank you all for being here. And let me start with – as this is a panel about what the U.S. public should expect from its intelligence community – just a lightning round of what is at the top of your inbox.

Director Brennan, you can start. (Laughter.)

DIRECTOR JOHN BRENNAN: Thank you. Well, first of all, Kim, and everyone here, it’s great to be back interacting with INSA and AFCEA. As a former chairman of INSA I recognize just how important that partnership is between the public and private sector, and also, just how important it is to have open for a like this to address our national security issues.

Our inboxes are overflowing. I have been now in the national security business for 34 years, and there has never been a time that I have experienced when we've had the number and complexity of national security challenges that are facing us. And so it seems as though in that inbox are all the things that consume us on a daily basis, whether it would be the situation in Iraq-Syria, Ukraine, terrorism, cyber – issues related to East Asia in terms of our relationships with our various partners over there and how we are learning to deal with sort of the new environment of world challenges at a time of unprecedented technological change, and at the same time, a lot of my inboxes, and I know, the inboxes of others here, are consumed with a lot of issues related to the intelligence mission itself.

And we at CIA hosted a conference a couple of months ago at Georgetown about not just the importance of having discussions like this, but also making sure that we're able to strike that right balance in ensuring that agencies like CIA, NSA, NGA, DIA and others are able to carry out their responsibilities to keep this country safe, while at the same time dealing with the obvious, unprecedented scrutiny and even skepticism about the role of intelligence today.

So our inboxes are very eclectic in terms of the types of things that we're dealing with: Congressional inquiries, different types of reviews. And so the challenge is a multidimensional one. It's not just a substantive challenge. It's organizational issues; it's dealing with all the things we have to deal with in a budgetary environment that's constrained.

And so I have found that in my last 18 months here at CIA, the diversity of the responsibilities that we have – that run across the substantive administrative legal policy and other issues is something that certainly keeps my adrenaline running.

MS. DOZIER: I can see why you didn't want to go first. So, Tish.

MS. LONG: Let's see. Long list. What did John not cover? I mean, I think he pretty much covered the waterfront there. I mean, you cannot just take a particular hotspot or a particular crisis, because of course, our mission is to watch the world, and our mission is to protect the American public, to protect our nation, working with our allies and to do it within a legal framework.

And so – I mean, John outlined, you know, many of the hotspots at the same time – technology is rapidly changing. At the same time, we are taking care of our people. We are recruiting, training and working to retain the best that we can to keep them challenged, to keep morale up when we have the American public questioning, when we have furloughs and government shutdowns and the myriad of other issues out there. So it is eclectic. It is ever-increasing, it is always overflowing; it's also always an honor and a privilege to do what it is we do.

MS. DOZIER: Thank you. Sir.

DIRECTOR MIKE ROGERS: Well, I think we've all come to the conclusion we've got to get bigger inboxes – (laughter) – given the complexity and the breadth of the challenges we're dealing with – as you've already heard highlighted – if you – the specific question – so what's at the top? You know, the argument I make with our organization is, I believe, ultimately, our top number one priority is to generate insights that ensure the defense of the nation and those of our key allies is our number one priority.

MS. DOZIER: OK.

DAVID SHEDD: My inbox is everything they said, with – a twist to it is, I walk in every day to the Defense Intelligence Agency under the motto, "In Defense of the Nation," in that what I see increasingly – and in my four years of service at DIA is a world in where the blurring of the lines between state and nonstate actor threats is on the rise. And that inbox, today looks even different from four years ago in where that overlay of where technology and the changes in that world fold into the ability of our adversaries to actually do us harm in new and creative ways that sometimes blend with the nonstate actor in terms of those capabilities, and at time, are far more in the Westphalian border states that we know – contained within those borders.

And so, as I look at the intelligence, whether at the collection end of it or the analysis and what's produced, I see a world in that inbox that's increasingly complex. You've already heard – clearly, we all need a bigger inbox, but we need a different inbox that looks at these threats from creative ways where the public-private sector partnership needs to continue to be strengthened as we face adversaries in defense of our nation.

MS. DOZIER: Now, I remember a National Intelligence Council report a few years back. It was looking at the next 30 years, and one of the things it talked about was, expect a proliferation of nonstate actor threats. Far more asymmetric threats – warfare, competition over resources – the kind of things that you all weren't originally – your agencies weren't originally designed to do.

So that brings me to two things in the headlines – ISIS or ISIL and Ukraine. One of them possibly – you could call it a more traditional thing we perhaps should have seen coming, and ISIL that, you know, arguably you all are watching. Did you give enough strategic or tactical warning of either event, in your opinion?

DIR. BRENNAN: Well, I certainly think that the intelligence community did a very good job on both of those issues as far as trying to ensure that the policymakers were informed about the evolving facts on the ground. When you look at a place like Ukraine – and what the policymakers wanted to know is, what types of military capabilities were being brought to bear along the borders, whatever else? What are the options that Putin – others have in terms of trying to pursue their agendas? But in some respects, Ukraine is like a chess game, and there are so many variables at play that it depends on what move someone makes. And I'm sure that Putin himself is trying to calculate exactly what his next moves would be. And the intelligence community was never expected to be this crystal ball that's going to

foretell the future, what we need to do is to make sure that the policymakers understand what are the costs and benefits to the various actors at play. What are the main driving forces and how can the scenarios – worst case, best case – evolve and what are those indicators that it's going down a certain path.

Same thing is true when we think of ISIL. We had been looking at, for many months, how the former al-Qaida in Iraq, which then combined forces with elements inside of Syria, were growing in capability in Anbar, Fallujah, these areas, and how they were expanding their reach. It's so difficult to assess the ability of forces, Iraqi security forces or others, to withstand a determined and concerted effort on the part of these elements that were born out of this area and over a dozen years old, this group dates from. And with all the Sunni tribal elements and the Sunni community who were very disappointed as well as disenfranchised by what they believe were eight years of a non-inclusive government in Baghdad.

There was a combination of forces that developed that really allowed ISIL to, like a water leak, just move forward and not meeting resistance. So I think looking back over the last several months on both of those issues, I think we teed up the right issues to policymakers, but having been a policymaker before I came to CIA, you know, both on the intelligence policy side, these are very, very complex, difficult issues, and you're never going to get perfect insight into those developments that are going to allow you to foresee the future.

MS. LONG: I would agree with John. We did give very good strategic warning. We understood, in the case of Ukraine, the Russians' capabilities, the movement of forces, working very well in an integrated fashion, I might add, to really give the policymaker as complete a picture as possible.

MS. DOZIER: So to interrupt you, you knew in time to redistribute your resources to focus on those areas to give them the geospatial intelligence.

MS. LONG: Absolutely. But what all those indicators don't give you is intent, and that is the most difficult thing to do. So again, as John said, we do our best to lay out the options, lay out the possibilities, what might occur, what could occur, capability being a big piece. But unambiguous warning would equal clairvoyance which is not something we are.

MS. DOZIER: Well, I will have to come at this with a question from – you know, that would normally just be asked by someone public. But you're spies. I thought that's what you do. (Laughter.) I thought – I thought that you'd have the person in the room with Putin having the conversation as he was getting a massage or something – (laughter) – who would know this is what he was going to do next or that – or is somebody listening to the right cell phone? (Laughter.)

MR. : Mike?

DIR. ROGERS: Mike, there you go. I'm going to sidestep that one – (laughter) – to go back to your original question. I thought we did a good job in the Ukraine in particular. I thought that was one where

we were able to provide policymakers and operational commanders a timely sense that the warning cycle was compressing here and the Russians have put themselves in a position to execute a potential sequence of actions that we subsequently saw unfold.

If I'm honest with myself, I wish the transition of ISIL from an insurgency to an organization that was now also focused on holding ground territory. The mechanisms of governance – I'll only speak for me – it's an area we talked about, but in hindsight, I wish we had been a little – I'll only speak for me and for NSA – I wish we'd been a little stronger about.

MS. DOZIER: Understanding that evolving intent of the leadership of ISIL. And can I just ask briefly, why do you all call it ISIL vs. ISIS?

DIR. ROGERS: Because the "L" means Levant –

MR. SHEDD: (Inaudible.)

DIR. ROGERS: – reflective of the broader agenda of the organization. This is not the "S" ISIS, the idea of –

MS. DOZIER: It's not just Syria.

DIR. ROGERS: – a greater Syria. This is – you know, if you pay attention to them, what you hear them saying, their internal dialogue and their very public dialogue, they are about something broader than the idea of a larger Syria.

MR. SHEDD: Kim, I was simply going to say DOD spends an inordinate amount of time and effort on the pursuit of indications and warning, and I believe that in both instances that you have referred to, we as an intelligence community and we individually as agencies provided that warning all the way to the combatant commander but also the combatant commands and the relationship in particular with the Defense Intelligence Agency has a relationship in where – in the case of the Ukraine, General Breedlove, the supreme commander of European Command, and our analytic capabilities forward were on the job every bit as much as DIA and the all-source analysis of, again, the indications of warning post-2008 in Georgia, and Vladimir Putin's objectives. And we remain on that.

On ISIL, I go back to the summer of 2013 – July 21st to be precise – at Aspen, the security forum – I talked about al-Nusra and the extremist end of Syria not staying contained within its borders. That strategic both warning and intent, whether you get to the tactical point of the breakup in June with Zawahiri and al-Qaida and ISIL going its own way, as John has described, with its antecedents AQI, al-Qaida in Iraq, is a tactical question as opposed to a much larger question about them going outside their borders and attempting to establish what they call a caliphate. And that's why the "L" is the much more accurate description and the acronym than the "S" because it is, in fact, about Lebanon, Jordan and beyond.

MS. DOZIER: So a senior intelligence official – who is not here right now, but that's all I'll say – mentioned that what they felt they didn't – that you all didn't see ahead of time was how quickly Iraqi forces would dissolve in the face of this confrontation. And you look back at the drawdown of U.S. forces and also U.S. intelligence officers who I understand had to pack up really fast with no time to hand over some of their equipment and on both the special operations and intelligence side no time to continue some of the training they wanted to do.

OK, that said and done, do you think not having a shrunken presence contributed to not knowing what was going on within the Iraqi forces? And looking ahead to Afghanistan, will that inform your recommendations with the drawdown there?

DIR. BRENNAN: First of all, if you have presence on the ground, if you're operating on a daily basis with whether the – your counterparts or others – it provides much greater capability in terms of trying to drive them a certain way. On the issue of the Iraqi forces, one of the most difficult things to do is to determine the will to fight, and it gets to this issue almost of intent. You can look at what their capabilities are, you can look at where they're positioned, but in the face of what is truly unspeakable barbarism, which is a – basically ISIL is a murderous, barbaric, psychopathic gang, criminal gang, and what they were doing in terms of the slaughter of individuals and having the Iraqi security forces at these outposts, I think they were just totally overwhelmed and I think there was a cascading effect there too, which is something very, very difficult to calculate and assess.

But not having a presence there and being able to – you have indirect capabilities in terms of intelligence, whether it be from overhead or whether it be from your sources, but unless you're actually there, you're second, third-hand information that makes that assessment difficult.

MS. LONG: It's really tough to add to that, especially from a geospatial intelligence standpoint. You're not going to get to, again, intent or will, and that's really what it came down to in this case. And, you know, I think for any of us to put ourselves in the ISF shoes for, you know, what they were faced with and what they are still faced with –

MS. DOZIER: What the Iraqi security forces are –

MS. LONG: The Iraqi security forces are extremely brave in the adversary that they are fighting right now.

MS. DOZIER: So do you think at this point – just to ask a present-day question – have you all been able to improve the intelligence picture such that you can get them actionable intelligence but also protect the U.S. advisors on the ground from things like insider attacks, which means you've got to know not just about the threat, but the people that you're fighting alongside?

MR. SHEDD: That's a work in progress.

DIR. ROGERS: Right.

MR. SHEDD: Obviously, there's a significant DOD component to it, including from DIA, one that wakes me up at night in terms of the insider threat, because of the dynamics that you have, which are not only presented by the Islamic State in their presence in Iraq, but also the Iranian presence, the confluence of what would be adversaries in terms of what we have to face there. And as a result, and with many years of experience, we are – we are expending a huge amount of effort to, obviously, protect our own, in an environment that is extraordinarily dangerous.

MS. DOZIER: Which means –

ADM. ROGERS: – and I'd only add, clearly it's a focus for all of us. To go back to your previous question, I think it also points out to us, as senior intelligence professionals, that part of our job is to ensure that policymakers and operational commanders understand what the limitations are. So, for me, at least, I'm constantly reminding people Iraq of 2014 is not Iraq of 2010 and your expectations in terms of what intelligence can generate, in terms of the level of insight, the timeliness of the insight, needs to be (gauged ?) to reflect the environment we're in now, and not necessarily the environment we've been used to, you know, for a long time.

MS. DOZIER: Which means you're telling the policymakers that they're going to have to accept a higher level of risk, because they don't (so ?) much.

ADM. ROGERS: Or uncertainty. Our ability to generate the levels of insight.

MR. SHEDD: And that would certainly be true in Afghanistan. Depending on the size of the presence and the force protection that enables – it's a huge enabler in terms of what you're able to do – it's directly correlated to that presence.

MS. DOZIER: So let's step back and – from Arab Spring to ISIS, the threat has changed, the way conflict seems to develop has changed; it is less like Ukraine and more like what we're seeing in Iraq and Syria. How has that changed your intelligence mission?

DIR. BRENNAN: Well, a lot of the developments of the Arab Spring were internally generated, and we were talking just previously – when you have a Tunisian fruit merchant who self-immolates and that is the spark that sets ablaze not just a Tunisian forest, but a forest throughout the Arab world, how do you, you know, have the intelligence that allows you to identify that spark? What I think what we need to do as intelligence professionals is to look at those phenomena right now that are changing the landscape, how populist movements, how nonstate actors, how others are really influencing the shape of the future of this region and how the economic and political and other drivers really are changing the course of history in this part of the world. And it – you know, social media has just exploded and we as intelligence professionals need to continue to exploit the environment to find out where is it that we're going to find the insights, those nuggets that are going to give us a sense of some phenomena that may

be developing now, slowly, but it's going to result in something of strategic significance. And that's where we want to make sure our analysts (or ?) professionals are attuned to the different sources that are out there that are going to give us that type of insight.

MS. LONG: And so I think that speaks to our agility and our ability to update our capabilities. It also speaks to our partnership; our international partnerships, our partnerships with private industry, like John mentioned, social media – crowdsourcing: The ability to gather information from many different places, many different sources and make sense of it, integrate it, conflate it on the fly to understand what's real, what's not, what's important. So I really think it speaks a lot to agility.

ADM. ROGERS: I'd also add, from my perspective – sorry, David – I often hear this phrased in some ways as it's an either/or proposition, and my view is the intelligence professionals, we have to be capable of generating insights against monolithic, very traditional nation-states, while at the same time we're generating the kind of insights for the social underpinnings of change in less established, less monolithic nation-states to groups and individuals. I often hear people tell me, well the future is all about, you know, groups. My attitude is don't assume that the future is a linear projection of the present, first, number two: The task before us as intelligence professionals, to be able to cover the breadth of challenges that the nation and its key allies faces, and we can't optimize ourselves for one scenario.

MR. SHEDD: And just building off of what all three have said, the great example of the inbox where you opened, Kim, was – is Libya today. Do you treat it as a nonstate actor? Do you treat it as a nation-state? And my argument is our analysts have to see both sides of it because as it appears to be breaking up and the traditional foundations of governance are more than fraying there, you have a tribal break-up that is a set of nonstate actors, and so your whole dynamic of how you look at the problem set changes with it from a very traditional analytic standpoint and even your collection standpoint, as Mike said.

MS. DOZIER: OK. So I have a comparison question. You know, when Osama bin Laden was killed – 2011 – the debate in media circles was, well, is counterterrorism over? Do we now see the intelligence community shift to, you know, the Asian pivot, what's happening with Russia? Yet now, we have al-Qaida and ISIL vying for followers, influence. Is the U.S. at war with an ideology? Is that where it's going?

DIR. BRENNAN: The use of violence for political, ideological objectives has been used for millennia. And as we talk about more and more these transnational, subnational actors becoming engaged, as we see al-Qaida or ISIL or others, we have to, I think, as an international community, come to terms with how we're going to deal with these ideologies and movements that are exploiting the weaknesses of various countries because of economic problems or political disenfranchisement and authoritarian regimes or whatever. And so we're not at war with an ideology. What we have to do is try to combine our capabilities in the U.S. government, working with our international partners, to make sure that these developments and these movements that are really designed to undermine peace and stability and using violence – we cannot kill our way out of this. We have to find a way to address some of these factors and conditions that are abetting and allowing these movements to grow.

MS. LONG: It is not new and I do believe it is all about our partnerships and coming together as an international consortium to figure out how we counteract –

MS. DOZIER: Well not new, and yet, I have never heard an assessment that there are 20 to 30,000 extremist fighters focused in the near-term on U.S. targets in the region and in the far-term U.S. and Western targets, you know, at home. That's – that sounds to me like it's a change. It sounds to me like it's a, you know, a multiplication of the threat by magnitude. No?

MR. SHEDD: Well, when we talk of the 20 to 30,000 as it pertains to ISIL, as we've seen their efforts in – that led up to Mosul and then Mosul, the freeing of the prisoners and others that have joined the ranks, very difficult to measure the size and capability of the truly committed versus the numbers that we extrapolate from conditions on the ground as we see them. To then translate that into a: And then, therefore, the homeland is threatened by 30,000, I think is a mistake. Are there elements therein that would wish to do us harm? Absolutely, and will plan to do so. But the capabilities that we have built up over many, many years and predominately after 9/11, I believe are in place to certainly counter that threat to a major degree.

MS. DOZIER: So at this point, what is the top militant threat to the United States? Is it still al-Qaida in the Arabian Peninsula vice (ph) ISIS – ISIL?

DIR. BRENNAN: When you say threat to the United States, are you talking about U.S. interests, national interests?

MS. DOZIER: Right.

DIR. BRENNAN: When I think about the region – Iraq, Syria, Jordan, the Gulf area, whatever – this phenomenon of ISIL right now is very, very destabilizing, very, very much a threat to vital U.S. national security interests in the region, which includes the stability of our close allies and partners. So from that perspective, this is something that has to be cauterized immediately and destroyed as quickly as possible, but when we look at other groups – you mentioned al-Qaida on the Arabian Peninsula – we – they have a track record of trying to – whether it be down aircraft or carry out attacks here in the United States. So this is one of the parts of the eclectic inbox that we have.

There are these strategic developments that really pose serious threats to our national security interests in many parts of the world, but then there's also the wolf that is trying to get through the door, these small groups, whether they are embedded in Yemen or in North Africa, in the FATA Pakistan or Afghanistan. What we can't do is to let down our guard for any one of these. It's not binary. It is, you have to be looking at some of these smaller groups that have tremendous capabilities because of the technologies that are available today to carry out such destructive attacks with tragic consequences.

MS. DOZIER: So are we exaggerating the threat too much? (Laughter.)

ADM. ROGERS: Can I ask two other questions?

MS. DOZIER: Go for it.

ADM. ROGERS: If I could just make two other points.

MS. DOZIER: Yeah.

ADM. ROGERS: Two other things come to mind for this in this. Another aspect that concerns me about ISIL is the fact that – don't underestimate how success can breed change in others. And if ISIL is perceived increasingly among those around the world who would try to do us harm through violent extremists behavior – if the perception becomes that the ISIL vision of the future and the tactics they use to implement it is successful and, hey, we want to get on that train, that's really bad – not that ISIL isn't bad, but if this idea expands beyond a single group, right now rather geographically focused in terms of their disposition, is something even broader. That's really bad.

And then the second point I would make is when we're working these threats as targets from an intelligence perspective and attempting to generate insights that support policymakers and operational commanders, I'm also struck by – and it's a dialogue I have internally with our team out at NSA – is, like John indicated, if we acknowledge that we're not going to kill our way out of this, then part of our challenge as intelligence professionals is not only generate insights that provide tactical options to commanders and policymakers, but we've got to help generate the insights that answer some of the more fundamental underlying questions that allow the other elements of power to be applied effectively.

And that's a real challenge at times when you can be very tactically focused on a particular target, a "generate me actionable intelligence that I can execute today" versus the desire, "hey, how can I help understand the underpinnings and the more broader aspects of this so we can respond and deal with it in a broader way?" I just – I always feel that tug at times, at least for me.

MS. LONG: And so to that point – those points, it's not only the top threat.

MS. DOZIER: It's the layers underneath.

MS. LONG: Yes.

MS. DOZIER: So I would like to move the conversation to something we were discussing in the green room, the idea of trust and the American public's trust in the intelligence community. Now, that's taken quite a dent over the past couple years through media coverage, partly from the Edward Snowden leaks and also other issues. So I'd like to start with the provocative question: If you all feel that what was

done was done legally in whichever agency, what do you do to win the public's trust? Do you need the public's trust to do your jobs effectively?

DIR. BRENNAN: Well, I certainly believe that having the public's trust makes our jobs much easier and better. And I think what we all want to do when we engage in sessions like this is try to explain – because, quite frankly, the narratives that I see floating around in the media, domestically and internationally, there are so many mischaracterizations about what the intelligence community is doing, what individual agencies are doing –

MS. DOZIER: What's one –

(Cross talk.)

DIR. BRENNAN: You know, there are a lot of reports that the – that each of our agencies are rogue agencies and we're trying to sort of undermine the law and do things around the law. We are a community of dedicated men and women from throughout the 50 states, those who have public service in their blood, who are trying every day to keep this country safe and do good by their fellow Americans.

And so are we infallible? Absolutely not. Have we made mistakes? Yeah. We've made some big mistakes over the years. We need to learn from them and then move forward, because our plate right now, in the international arena, is so overflowing that I think it's good to be able to explain to the American people what we're trying to do, some of the things that we are doing, but also there needs to be a sharp distinction between that which is, I think, OK to be able to talk publicly about and some of those very, very important and sensitive source and methods that keep this country safe.

And unfortunately there has been too blithe an attitude on the part of many to put some of this information out and they don't know the consequences of it. So I do think the narrative is important. I do think the trust of the American people is important, and we need to be able – we have to work better at it. We have to work harder at it.

MS. DOZIER: So while we're on that subject – and you knew this question was coming – one of the last times I saw you speak publicly you talked about the Senate investigators who were looking into the enhanced interrogation program, and at CFR you had said, no, my people didn't access their computers improperly. And in the interim you put out a statement saying, actually, after our investigation it seems they did access it, and you apologized to Senator Diane Feinstein.

DIR. BRENNAN: Yeah. With all due respect, Kim, this is part of the mischaracterizations. At the Council of Foreign Relations, Andrea Mitchell said: Did, in fact, CIA officers hack into the Senate computers to thwart the investigation on detention and interrogation – thwart the investigation hacking in? No, we did not. And I said, that's beyond that scope of reason. I also said during that same session that if our folks did something wrong, I'm going to make sure that they're held to account.

And so I submitted this issue to our inspector general. I said, I want to know exactly what CIA officers did. And when the inspector general determined that, based on the common understanding between the CIA and the SSCI about this arrangement of computers, that our officers had improperly accessed it, even though these were supposedly CIA facilities, CIA computers and CIA had responsibility for the IT integrity of the system, that I apologized then to them for any improper access that was done, despite the fact we didn't have a memorandum of agreement.

And so what I've said to the committee and to others is that if we do something wrong, I'll stand up in a minute, but I'm not going to take, you know, the allegations about hacking and monitoring and spying and whatever else. No. Do we make mistakes? Yes. When we make mistakes, we're going to raise our hand and say, OK. And that's why I've asked former Senator Evan Bayh to head up an accountability board. And, you know, when I think about that incident, I think there are things on both sides that need to be addressed, and I'll just leave it at that. (Laughter.)

MS. DOZIER: Have you – have you managed to –

DIR. BRENNAN: Just saying – just saying –

MS. DOZIER: – but just 2,000 of your closest friends –

DIR. BRENNAN: Yes.

MS. DOZIER: Just us. Have you managed to reach out to Senator Feinstein? There's also friction over the upcoming – their push for the publication of their report on –

DIR. BRENNAN: We're working very closely with the White House and the Senate committee. This is a committee report and we continue to work on it, on that issue, and I'll defer any questions on that to after this report comes out, as well as to the committee itself.

MS. DOZIER: Thank you.

MR. SHEDD: Kim, this question on trust is so vital. It's a sacred trust. And when we raise our right hand to protect the Constitution, we do so with heart, soul and mind. And the men and women of this community do so all alike.

When I think of the risks that our men and women are oftentimes placed in, often with imperfect information, to make decisions day in and day out, they do their level best to do so on behalf of the American people, because that's what they're – that's who they're sworn to protect. Our representatives in the House and the Senate are that manifestation of that relationship.

And so when I think of trust, if we break the trust with the American people, we cannot actually do our jobs. That's how strongly I feel on this particular topic – deeply emotional topic. I'm a product of Iran

Contra. I have history in this area. And it is an issue that we must continually talk to the American people through our oversight committees, and where we do our level best to represent for the security of our nation in what we do.

MS. LONG: And talk to the American public through venues like this. This is a great setting and a great opportunity for us to have a dialogue. And that's really what it needs to be, a dialogue. We can talk more about what we do. We cannot always talk about how we do it, nor should we, but we can talk more about our capabilities and how we can apply them to protect the nation.

MS. DOZIER: Admiral Rogers.

ADM. ROGERS: Can I add one? Clearly this is a topic as the director of the National Security Agency that has been front and center for me for the five months that I've been in this job. And one of the things I talk to the team about is – and it goes to what you've just heard from my two teammates in their remarks – the challenge for us in some ways are the mechanisms that we put in place to execute the oversight of our functions – were largely for us a court of law and congressional committees.

And how do you achieve a level of trust in a nation when those very mechanisms do no longer enjoy the high confidence that they perhaps have previously or historically in our society? And if those are going to be the venues that we traditionally had counted on to ensure that the American populace was comfortable with what we were doing, because their elective representatives had the specific details on what we do and how, and a court oversaw it and gave us legal authority in many cases specifically to do what we do, how do you create an environment of trust and confidence if those mechanisms don't necessarily enjoy the same confidence and trust that they have historically?

So one of the things I have talked to our team about – and it goes to Tish's point – we have got to not only ensure that we continue those traditional mechanisms for compliance and oversight, but we have got to expand this dialogue beyond them. We have got to talk directly to the citizens we defend as well as our key allies and friends around the world, because if we're only going to rely on the established mechanisms, I don't think we're going to get where we need to be. And that doesn't mean we're going to walk away from them. Far from it. We have a legal and a statutory requirement to do that, but I'm just talking to the team about, we've got to learn to think beyond that.

MS. LONG: And it is "learn to think beyond that." This is not second nature for us – (inaudible).

MS. DOZIER: So what is your – what is your plan, specifically with the NSA, to win back the public's trust?

ADM. ROGERS: So for me it's a couple things. I've talked about I want to bring in an outside perspective and I want to take a look at how effective we are in our current communications strategy, because I don't think we are where we need to be.

Secondly, I've said I want to engender a broader dialogue about what do you do and why do you do it, and why should I, as a citizen, feel comfortable that that capability you have is not going to be misused or will be used against me? We've had what I think is a very incomplete dialogue to date. I would argue it's not even a dialogue. We've heard details about amazing technical capabilities that people then assume, well, you must be using these indiscriminately against us.

What we haven't talked about is, so what's the legal framework that's in place that drives what you do? What are the controls and the compliance mechanisms you've put in place to make sure these technical capabilities are not misused? Why should we feel comfortable with these capabilities? That's the dialogue that I am interested in having over time, and that to me is what has very much been lacking.

And then the other point I find frustrating – and “frustrating” is probably too close a word, but I don't think it gets us to where we need to be – don't ever forget that part of this equation needs to be a discussion about what's the right balance between risk and our inherent freedoms. We've got to do both. It's not either/or. It's both. But there's a good room for what's the right balance, and it is amazing under what – under some scenarios makes perfect sense versus other scenarios you would say we would never do.

I mean, you look at what we did in immediate aftermath of Pearl Harbor in 1941. I mean, we made a government policy to intern U.S. citizens purely on the basis of their ethnicity, for example, their race. You look now in the rearview mirror and you say, how could we ever have done that as a nation, made that a policy? And yet if you go back and you look at the polling data from the time, the immediate reaction of the majority of the nation was it seems like a reasonable thing to do, given what just happened to us on the 7th of December.

You know, we need to have that dialogue about what's the right balance. Don't take from this, boy, he's arguing it's December the 7th, 1941. That's not the point I'm making. The point I'm trying to make is you need to understand the context and we have to make a choice as a society, as a nation, what's the right balance, always mindful it is never, never either/or. I just would never agree to that as the director of the National Security Agency. I have no desire as a citizen to be in that environment.

MS. DOZIER: So I have to ask – the follow-on question to this is, you know, we have heard a lot in testimony that the disclosures – the recent disclosures not just of – from Edward Snowden but some of the disclosures about the drone program – not the Title 10 one but the Title 50 one – that it has harmed intelligence operations and it has threatened and endangered people in the field. Can you say, have lives been lost because of these disclosures? And how much money has it cost to change things because of them? Can anyone put a number on that?

ADM. ROGERS: What I'll say for me – and I'm not going to talk about a number – there should be no doubt in anyone's mind that the National Security Agency has lost capability because of this. There should be no doubt in anyone's mind that I am watching groups change their behavior as a direct result

of these revelations – groups that represent a direct threat to the citizens of this nation and those of our friends and allies.

Now, I have also, as a result of this, had to spend time and money as an organization dealing with an – with a series of things. Quite frankly, I wish we didn't have to deal with them in many ways. So one of the questions I get is, well, what's the opportunity cost in the fact that I've had to strip a lot of people to go do something as a result of this and not do their regular jobs? And I haven't quantified that in terms of, hey, here's how many millions, but it's in the millions, and here's how many people. But those who think that this has had no impact are sadly mistaken.

MR. SHEDD: For our partnerships, it has seeded distrust in where they questioned, first and foremost, can we keep a secret? And secondly, can I trust you with sensitive issues in a relationship that may blow back politically or otherwise in a host country? And we've had a direct correlation to the leaks.

MS. LONG: And I would take that a step further to the economic impact to this country, where foreign countries no longer want to deal with U.S. industry. So there is a wide spectrum of very real impact from this.

MS. DOZIER: OK.

DIR. BRENNAN: Very significant, very consequential, devastating to a number of our efforts to try to keep this country safe. But I think the intelligence community has shown that it is resilient, and we're trying to adapt now to some of these compromises. But again, there is this irresponsible disregard for national security by this information getting out.

MS. DOZIER: So I'm going to go to the questions from the audience – have quite a bunch. I'll start with: Some of our intelligence counterparts in Western Europe maintain much lower levels of transparency with their citizenry, yet they don't receive the same amount of public backlash. Why does the U.S. intelligence community struggle to find a similar balance? Along the lines of, do you think that European citizens are more warm and fuzzy about their intelligence services? (Laughter.)

DIR. BRENNAN: I think the premise of that question is questionable, because there has been a lot of backlash against the intelligence services throughout Europe right now because of some revelations and also mischaracterizations of what some of those services are doing. And so we're seeing, throughout Europe, that there are parliamentary investigations and other things, so the – and the media has really sort of glommed onto this in Europe.

So I think the – when we meet with our counterparts from Europe or other parts of the world, they're having to work hard to strike this balance as well in terms of what's the engagement with the public? How do you optimize both one's national security as well as one's protection of civil liberties and privacy rights? So this is something that is not just sort of endemic here to the U.S. intelligence community. I think it's worldwide.

ADM. ROGERS: I would agree with John. In fact, one of the discussions, quite frankly, I have with my counterparts around the world is, if you are going to lead an intelligence organization in a democratic society in the 21st century, I would urge you to ensure that your senior executive leadership and your elected representatives have an awareness of what you do and why you do it.

It is a strength to me in our structure that our policymakers have a level of awareness of who we are and what we do and why we do it, as well as those in our legislative branch, the elected representatives of our citizens, in their oversight role, have a level of awareness of what we do. I think that is a real strength for us.

I do not – like John, my view would be my experience has been quite the opposite in dealing with many of our partners. And so when they find themselves in trouble and you're trying to deal with leadership that doesn't necessarily know how you're structured, what your focus is, what you do, what your relationships are, whether that be in executive leadership or that be the elected leadership, that's a tough place to be in as an intelligence leader in this day and age. So I constantly urge them. I think that's one of the take takeaways.

MS. DOZIER: Now, have some of the bruised feelings gone away since the revelations that U.S. intelligence agencies were spying on Angela Merkel's cellphone, et cetera? Is that in the rearview mirror? Have people managed to talk about these things behind closed doors and repair those relationships?

DIR. ROGERS: I mean, clearly we are working our way through this at a policy and a nation state level. I would say I think most of us at the intelligence-to-intelligence level, we have worked our way through it. We continue to partner strongly with our key allies. It hasn't had a major effect globally for us in terms of countership (ph) relationships. Some clearly are more concerned, but in general the point we've always tried to make with people is remember what brought us together in the first place. We have a mutual set of shared interests. The reason we created this relationship – these relationships with counterparts is because we felt they generated value for both of us. Don't ever lose sight of that, even in the midst of all of this. We want to continue to generate value for both of our nations or when we work collectively as a group.

MS. DOZIER: Now here's another question. Based on efforts this past year, how has the insider threat problem increased or decreased or stayed the same, and why? I know that the Counterintelligence Executive has been putting in some new policies to try to spot insider threat. I'd also let – like to add a corollary to that. I know that post-Snowden, a lot of your agencies have tried to teach people, here's the right way to blow the whistle. Have you seen a rise in that? So have you seen a rise in capturing insider threats and have you seen a rise in people saying I think there's a problem here?

DIR. ROGERS: : I mean, for us, clearly it's an issue that we're working. I don't think that's different for anybody. But the challenge I find at times is – again, I'll only speak for our workforce – I have parts of

the workforce going, now let me understand this. Because of the actions of one individual who violated the trust and the authority that was granted to him, you want to impose fundamental change, greater oversight, potentially more restrictions on the rest of us? And I'm – so as a leader, I'm trying to strike that balance, because I don't want one of the takeaways from all this to be, well, you know, you just fundamentally can't trust your workforce and you fundamentally can't share information and you can't create open architectures designed to provide people, analysts, professionals the opportunity to share information on a timely basis, in a global manner. I don't think that's in our best interest. So for me, I find part of the challenge is, how do you strike that balance?

MR. SHEDD: Mike has hit on an interesting issue about how do you trust your people yet at the same time message the insider threat? And what we're doing is opening that aperture to the larger counterintelligence threat awareness. And NCIX, the National Counterintelligence Executive, is clearly assisting with that, but that – it is the responsibility of every officer in the intelligence community to have a counterintelligence awareness of what our adversaries are after. In a world of technology where IT is the backbone of that technology and threat, that is certainly part of the increased training, back to your question, Kim, that we're focused on. And so there really is a balance between the two with a model of trust, but verify.

MS. DOZIER: So a question from today's headlines. The Australian government detected a domestic terrorist attack that included a plan to publicly behead a random victim. What impact does this have on your organizations? Is this something that has made you reframe what you're looking for when you look at the threat?

DIR. BRENNAN: I think when we look at these organizations, whether it be ISIL, al-Qaida or others, we look at what is the threat that they pose to the region, to include our personnel that are in the region, as well as what type of threat do they pose outside, including in our homeland? And I think what Australia experienced is the ability of groups like ISIL to – able to use technology, Internet and other things to be able to communicate, to be able to encourage, incite, recruit individuals to carry out their heinous attacks. And so this is just one more demonstration that this is an international challenge, this is something that we have to work together on, and this is something that we have to destroy not only from the standpoint of their ability to carry out the attacks, but the drivers that are sustaining them and also allowing them to gather more adherents. This is something that is going to be with us for a generation.

MS. DOZIER: So can – here's a question that we haven't even covered at all. Can you talk about where cyberthreats currently fall among your priorities, particularly when you've been talking about hot areas like ISIL, Russia and Ukraine? In other words, I guess they're saying are we – are you guys like we in the media looking at the bright shiny objects of ISIL, Ukraine and Russia and ignoring cyberthreats? How does it impact you?

DIR. BRENNAN (?): Yeah, we're ignoring cyberthreats. (Laughter.)

DIR. ROGERS: Well, as command – well, as the commander of United States Cyber Command, I spend no time thinking about – (laughter) – cyber-associated challenges and with NSA's mandated information assurance mission I spend no time thinking about cyber challenges. No, clearly, again, as you heard from the very beginning, we recognize that the inbox is huge, and it can't be just – we're focused on one thing, which is why I thought, you know, John attempted to characterize this from the very beginning as that's part of our challenge as intelligence professional: how do you ensure that you never forget you've got a global set of interests out there. You've got a global set of challenges. There are clearly spikes and shifts in prioritization, but you can't lose sight of the global aspect of the global aspect and the broad diversity of the challenges out there. We can't be like kids running to the soccer ball.

MR. SHEDD: The other mistake is that – it's to think of it as a binary problem. Every one of those has a cyber component to it. And so the capabilities that the community, Cyber Command are focused on oftentimes overlap with the nation state threat, as well as the nonstate actors and – when it comes to cyber.

MS. DOZIER: So is the leading cyberthreat a retaliatory attack by a sophisticated nation state cell, or is it a terrorist cell that hires a smart radical from a top university in the West who's done cyber all his life and is hacking?

DIR. ROGERS: I mean, either scenario is plausible. It's one of those I would argue, hey, it's not either/or.

MS. LONG: It doesn't matter. It doesn't matter.

DIR. BRENNAN (?): It's all of the above.

DIR. ROGERS: Either scenario is plausible.

MS. DOZIER: You're really not making it easy for us who write about this subject.

DIR. ROGERS: We're here for you.

MR. : That's our intent. (Laughter.)

DIR. ROGERS: Yeah, we're here for you.

MS. DOZIER: So in Afghanistan, something we haven't touched on that much, can you address how the announced drawdown of forces affects the willingness of local people to speak up and produce information on the adversary? (Inaudible) – tackle that one?

MR. SHEDD: I think you have to place Afghanistan in a larger context in that question, and that has to do with coming back to trust: the belief by the Afghan people that the United States, along with the coalition partners, will be there for the long haul in some capacity in terms of the amount of risk that

they're prepared to take in the relationship with us as opposed to what they face day in and day out in their own neighborhood, with the Taliban, the Haqqani Network and so forth. And so as such, their willingness to talk, I think, was the way the question was posed with us is, I think, another larger risk calculus associated with the conditions on the ground.

MS. DOZIER: OK. Anyone else want to talk about their sources on the ground in Afghanistan? Probably not. (Laughter.)

DIR. ROGERS: Could you tell me your number-one source on the ground?

MS. DOZIER: We've got lots of them. OK. Moving on – well, OK. But there is a larger question to when you shrink a footprint in a country, how do you maintain the relationships and the trust of the local population? Is it – it must be something that you're looking at in Afghanistan, or is it that you've had a relationship for 10 years so you don't need so many quote-unquote "boots on the ground" to have the presence all over the country?

DIR. BRENNAN: Today is CIA's 67th birthday. I have the best job – (inaudible). (Applause.)

MS. DOZIER: (Inaudible.)

DIR. BRENNAN: (In the United States government ?).

DIR. ROGERS: You look very young.

DIR. BRENNAN (?): (Laughs.) Yes. It's also the Air Force's birthday, too. (Applause.)

MS. DOZIER: (Know that ?).

DIR. BRENNAN: I have the best job in the United States. And CIA, throughout its 67-year history, has been able to work in many different parts of this world, all over the world, and getting individuals to work with us – CIA does symbolize the United States in the eyes of many, and so whether or not we have a large military footprint or we have a small diplomatic presence or we only have in fact a fleeting presence, we are very fortunate that there are a lot of people worldwide who seek the U.S. intelligence community, the U.S. government out because they believe in what we believe in, which is allowing people to live in free and stable societies.

So as footprints and the military shrink in Afghanistan or any other places, we, CIA, just like other organizations, are going to adapt and try to carry out our mission the best we can, and we will.

MS. DOZIER: OK.

ADM. ROGERS: But I do think, like the Iraq scenario, again, it's part of our jobs as intelligence professionals to ensure our policymakers and the operational commanders that we support understand – so given the different presence in Afghanistan, what are the implications for us from an intelligence perspective, and what can our policymakers and operational commanders expect realistically, again, is part of the dialogue we need to have, because we've got to ensure everyone will understand the Afghanistan in 2015 is not the Afghanistan of 2010. It's not good or bad. It's just going to be different, and there's implications for us in that in terms of our ability to provide timely insight.

MS. DOZIER: I have actually had quite a few questions in here asking, is the intelligence community – and this will be one – just the last couple questions – is the intelligence community too focused on counterterrorism, or is it the threat that we in the media portray? It gets a lot of the headlines, but when you look at numbers of people killed or businesses affected, there are other parts of what you guys are looking at, like the cyberworld, that have a lot greater impact.

MS. LONG: And so you haven't heard any of us talk about how much time or how many resources we spend on the wide array of issues that we have been talking about. As you opened up, Kim, with your first question, our inboxes are overflowing, and it is our responsibility to make the best judgments that we can on continuing basis to balance what we are investing those resources in versus the extent of the threat, as well as what's happening at any given moment. And we do that individually within our organizations, we do it as a community, and we regularly have those discussions to ensure that we are, to the extent we can be, focused on that which we should be.

ADM. ROGERS: If I could, the bigger challenge I find in the CT arena is not – when I'm looking at it from a resource perspective, is not necessarily have we applied too many resources. It's what are those mission segments – and I'm sure it's the same for all my teammates, but when I look at that segment of our workforce, we have pounded the heck out of it for over a decade. We have just driven it like there is no tomorrow.

And one of the questions, as the new director in my organization, I'm talking to the team about – this isn't going to change, so how do we sustain a workforce that has literally been at a sprint for a decade? And this challenge ain't going away, so how do we keep them energized? How do we get them rejuvenated? How do we potentially look at rotation, expanding their skill sets, ensuring they're maintaining their edge, because I watch them and I think to myself, they will literally destroy themselves, their health, their well-being, in many cases their family relationships. They become so focused on this, because they see it as such tangible, immediate threat that if I don't do my job, the implications are a citizen, an ally, a soldier, a member of an embassy is going to die somewhere, and I need to drive at 150 percent, and I need to do it all the time. I find that, for me, at least, in talking to our team – and I'm sure it's the same for all of you, because we all work the counterterrorism challenges together; we do this – this is one area where we have become particularly integrated – I worry about the long-term resiliency of the workforce, because we have just driven the heck out of them.

MS. DOZIER: And you know, that's a great question to end on, because, as you all know, I'm working on a book on resiliency and special operations and intelligence officers. So to the other three directors, what do you all do? You have had people running at a sprint for a very long time, thinking that if they stop for a moment, someone will die.

DIR. BRENNAN: It certainly keeps the adrenaline running in our agencies, knowing that if we miss something, it's going to result in somebody's death or it's going to lead to – a government to collapse or it's going to lead to the undermining of vital national security interests.

And it is that adrenaline that allows the intelligence professionals to keep running. Twelve, 14, 16 hours a day is not that unusual.

And every month I swear in a new class of CIA officers, and I can tell you this. We are getting, like the other agencies, the cream of the crop in terms of Americans who want to come and be part of this very important community. And they have the enthusiasm and the energy.

What we need to do as directors is to make sure that we're able to balance those resources appropriately against all these different things we have to deal with and also make sure that we are mindful that we are nothing if we don't take care of our workforce. We can have the greatest technical capabilities, we can have the greatest accesses, whatever, but if our workforce is not well-trained or well-cared for, this nation's security is going to suffer. So I think all of us take that obligation probably the most seriously of all of ours.

MS. LONG: And it's something that I often say, because if you take care of the people, the people will take care of the mission. We are so very fortunate, as a nation, that we have many, many more high-quality applicants than we have positions for. People are drawn to this, not that they're adrenaline junkies, but they are drawn to this mission. They care about our nation, and we're fortunate that we have that.

And it is our responsibility to take care of them, to sometimes tell people to go home, to ensure they have what they need to do their jobs so that we can carry out the mission.

MR. SHEDD: Our effort is to continue to allow that CT – counterterrorism – professional to find opportunities outside of the several or perhaps, in some cases, many years of doing that to refresh.

One of the great findings in the WMD commission report of 2005 was that the functional side didn't have enough interaction with the geographic side, right, in assessing whether Saddam Hussein had weapons of mass destruction.

So one of the things that I'm driving is that those CT professionals take an area, a region, a country and really go deep on that. So take Boko Haram in Nigeria. Go do the Nigeria rest of the account as a Boko Haram CT specialist, as an example, and try and get that refresh.

The other thing I would say is joint duty, the opportunity to serve with JSOC, SOCOM, CIA, NSA, NGA are all areas that again refresh in a way. They may still work 12 hours a day, but I think there is – there's a renewness (ph) that comes with that.

MS. DOZIER: Well, with that, I want to thank all of you for coming – (end of audio).

(END)