THE ASPEN INSTITUTE

ASPEN SECURITY FORUM 2016

SEEING AROUND CORNERS: THE INTELLIGENCE PROFESSIONAL'S CHALLENGE

Doerr-Hosier Center
Meadows Road
Aspen, Colorado

Friday, July 29, 2016

LIST OF PARTICIPANTS

Brian Bennett
National Security and Intelligence Reporter
Los Angeles Times

S. Leslie Ireland
Assistant Secretary of the Treasury for
.Intelligence and Analysis

John Scarlett
Former Chief, Secret Intelligence Service,
United Kingdom

Gregory Treverton
Chairman, National Intelligence Council

* * * * *

SEEING AROUND CORNERS:
THE INTELLIGENCE PROFESSIONAL'S CHALLENGE

(3:00 p.m.)

MR. BAKER: Good afternoon. I am Stewart Baker, member of the Aspen Homeland Security Group by -- and Washington lawyer, and I am pleased to say someone who has been fielding calls from Brian Bennett, who will be leading this panel for at least a dozen years. This is probably a good time to take up those misquotations -- no, maybe not.

(Laughter)

Brian is a remarkable reporter. Had worked for *Time*, covered Afghanistan, covered Pakistan, was covered the war in Iraq from Baghdad and was a member of the team that won a Pulitzer for coverage of the San Bernardino killings and the investigation that follows. He will be leading the panel through its paces and without further ado, Brian.

MR. BENNETT: Thank you very much Stewart, and thanks for always returning my call on deadline. So, this panel is called "Seeing Around Corners: The Intelligence Professional's Challenge" and particularly honing in on the puzzle of the unknown unknowns, a famous Donald Rumsfeld phrase. And as DNI Clapper said yesterday, "The country is currently facing the most varied number of threats that he has ever seen in his many decades of security work." And so this panel is particularly topical for right now, and fortunately, we have three people who have spent their careers thinking about intelligence and how to keep country secure.

First, we have -- I will introduce the three of them and then we will have a discussion about what the intelligence community should be thinking about in preparing for the future. So, first we have Leslie Ireland, who is the assistant secretary of the Treasury for Intelligence and Analysis. Leslie has been the head of the Treasury's Office for Intelligence and Analysis since 2010. She also wears another hat. She is the

intelligence -- the national intelligence manager for threat finance for the DNI.

So, what that means is that she has to do the thinking about how an entire intelligence community should be using threat intelligence, financial information intelligence. So, it's a really interesting person to have on the panel. Leslie also has a full career as an intelligence officer. She has been intelligence officer for 30 years. She was the intelligence briefer for President Obama. She was the Iran mission manager for the DNI and she has spent many years at CIA as an analyst and manager on the Middle East and WMD and other issues, and particularly topical for now, she has a masters in Russian area studies from Georgetown.

Next we have John Scarlett, who was the head of British Secret Intelligence Service; also known as MI6, from 2004 to 2009. And also during John's career, he had postings for MI6 in Russia, East Africa and France. He speaks French and Russian and I assume he's very familiar with how Russian intelligence services think and operate, which is particularly topical right now.

And on the end here we have Greg Treverton. He was the chairman of the National Intelligence Council. Now, the National Intelligence Council reports to the Director of National Intelligence and it's like an internal think-tank for the DNI. Greg's job is to think long-term about the intelligence needs for the intelligence community and for the country and what's coming next. This is also the body that produces the country's national intelligence estimates. So, it's going to be very interesting hear things that he's thinking about.

I will also mention that Greg's office produces a report every four years that we will be asking him about that's called *Global Trends,* it just so happens that that report, which often comes out right around the time of an election is due out in December. So, we will get to hear --

MR. TREVERTON: Safely, after November.

MR. BENNETT: And then you know that's report that will be on the next President's desk. So we will be able to hear from Greg some of the deep thinking that they have done; his office has done about what the future of intelligence and the intelligence services needs are for the next 10 and 20 years.

So, with those introductions I wanted to start on the news. Obviously, we have the DNC hacks. There is a report last night from Reuters that we had yet another hack that's -- cyber security officials have attributed to the Russians on the DNC. This time it was the DNC donor information. And what I wanted to bring up -- bring this up is, we are now at a point in our history, where Russia has become more aggressive in its actions to goad the United States and project its power.

So let's just review the basic facts of what we know so far. We have a cyber security firm, CrowdStrike, reputable cyber security firm that has -- said there's a high degree of confidence that Russian intelligence is behind the hack of DNC e-mails several months ago. Then those e-mails appear on the Internet and then a senior official, the head of a major political party of the United States resigns as a result of those e-mails.

And so that brings us to where we are now and the question is you know what should US and Western intelligence agencies be doing now to adapt to this new reality from Russia and what tools does the intelligence community need to prevent Russia's actions and better understand what Putin is going to do next? And I am going to refer that first to Leslie.

MS. IRELAND: So, the first thing I would want to assure the audience is that cyber activity is a high priority for the US intelligence community. For those of you who aren't aware, we annually sit down and develop something called the National Intelligence Priorities Framework. And we work with the policy community to identify where the intelligence resources capabilities need to be focused. And I can assure you that cyber takes some of the highest priorities that we've got.

I am looking at that question a little bit more from my perspective, within the Treasury Department and looking at how we work with our Office of Domestic Finance to work with the financial sector and help protect them in terms of cyber activity against an array of actors, not just perhaps Russia, but against the full array.

And one of the things that we've been able to do is to help leverage what the intelligence community has through the Office of Domestic Finance with the financial sector itself. And I think as an intelligence entity we need more broadly to look at how do we help the broader infrastructure inside the United States and the DNI has a group that has partnership engagement and I know they are looking at that and I think that's something they need to continue to do.

The second thing I would say and this I think is to your question of tools. I would want the analysts as well as the collectors who are looking at this problem to understand that we have an executive order that was signed last April of 2015 that would allow sanctions against actors involved in malicious cyber activity. And obviously that gets into a whole array of questions about being able to prove the identity of the actor and having the right information and then moving forward on a sanction package, but I know that's something that we would be prepared to do.

MR. BENNETT: So, I want to just follow up on that. Financial intelligence has become more and more important in finding out the weak points for adversaries, particularly, you know, when it comes to an adversary like Russia, what kind of information is useful in finding out how sanctions could be effective.

MS. IRELAND: So, I am going to give you a vignette. I know we talked about this beforehand. A colleague of mine received in the mail his hotel honors card. You know the one that you flash when you want to get points for staying, a royalty card for staying at a hotel. He opened it up and it had a picture of people whitewater rafting. He thought that's cool, I love

whitewater rafting. He looked again and he saw a guy that he had been rafting with and when he looked the third time. He was in the boat too. And that program is run by a major U.S. financial institution and what I would contend to you is that what they were able to do is to follow his financial activity, follow purchases that he made, follow travel that he might have made.

That trip was in West Virginia and he didn't stay at that particular hotel. So, it wasn't a case where they knew because he stayed there. And I think they also probably used facial recognition software at the same time to create that picture of him as a customer. I believe that within all of the legal authorities that we have in the intelligence community and the law enforcement communities we can create that kind of picture as well of our adversaries by watching that financial footprint that whether you like it or not each and every person in this room stepped into it today.

MR. BENNETT: That's incredibly creepy.

(Laughter)

MR. BENNETT: To think that a private company is collecting that much information. I hope, obviously, that's not being used on American citizens, but I can see it as a useful tool against intelligence adversaries.

MS. IRELAND: Right. Before this becomes the tweet that's heard around the world --

(Laughter)

-- I am not talking about the intelligence community using this as a capability against US citizens. I am talking about it with our foreign adversaries.

MR. BENNETT: John, I want to ask you a little bit about how intelligence services need to get better at getting inside the mind of the other side and the adversaries if there are new tools available, if there are old tools that we need to use better. Can you talk a little bit about that?

MR. SCARLETT: Right. Well, it's looking around corners, getting into the minds of the other side, I mean, there are a range of basic tasks I have learned or I think I have learned over the years that intelligence can achieve that maybe it is very difficult for any other arms of government in society or government to achieve and that can be done in various ways. At the end of the day it's just being very well informed in quite a deep and complicated way. So, it's not just of having items of information. It's understanding and looking at the world or a problem or a confrontation, whatever it might be and in the way that somebody else looks at it, not yourself or some other society looks at it and not yourself.

It's an obvious point. It shouldn't need a stressing, but of time and time again I have found in my career in the past when I look back on it and I find now that we're not very good at it, and maybe when particularly not very good with this in our sort of society, because we sort of live with the belief that we know best and we're more advanced than everybody else and we have universal values and all this kind of thing.

And then, there are various ways in which you can obviously do this, and I can cite examples I think, both from my own experience, but also from history and recent experience probably of where it's been, you know, particularly effective and different techniques have been used.

So, in the final stages of the Cold War for example and understanding exactly what thinking was going on at the very top of the Soviet leadership and in the Politburo, you know, there were examples and there are examples of us learning that and being surprised by what we learned and as learning it through good old fashioned human agents, human sources.

Nothing else was telling us exactly the way the Soviet leadership in the early '80s was thinking for example about the possibility, in fact, probability of a US policy under President Reagan to launch a nuclear first strike against the Soviet Union. And indeed when that

intelligence came through we found it unbelievable and policymakers just simply didn't believe it, but it turned out to be true.

MR. BENNETT: Were you producing from the human source? Were you producing some of that intelligence in Moscow in the early '90s yourself?

MR. SCARLETT: Well, I wasn't in Moscow at that time, but without going into too much detail it's been quite well written about and publicized and there was in fact a very good German TV series, *Deutschland 83,* about it, well based on it a few months, that the key intelligence came from a extremely brave human source inside the KGB that I was involved with, yes. So I know I about that. Okay.

But that's -- you know, that's just -- that's one example there where we succeeded because we had intelligence. But if you take another example -- sort of technical example going about back a bit in history to 1944 in the May -- May 25th, I think it was, 1944; when the Japanese ambassador went to have a three-hour conversation with Hitler in (inaudible) Garden and Hitler told him what he thought what was going to happen when the invasion across the Channel inevitably, that was inevitably coming, was going to come, that it was going to come in Normandy or maybe somewhere else along the Western French coast, but it wouldn't be the real thing.

The real thing was going to come a couple of weeks later in the Pas-de-Calais, which is what we had been trying to convince the German high command. It wasn't really going to happen and we knew from that and so the Japanese ambassador went back to Berlin and sent a very long report. As Japanese ambassadors did in those days, back to Tokyo and gave a full account of the conversation and through -- but actually (inaudible) and all that, we read that report within a few hours of it being sent.

So we knew from that what was in Hitler's mind critically, yeah, less than two weeks before one of the most important events of the 20th century and of our

society's existence. And that enabled us to double up on the deception and put it, you know, large numbers -- German armored troops were kept in the Pas-de-Calais area for two weeks after the invasion of Normandy and until the beachhead was secured in Normandy.

Now, if that's not important I don't know what is, but that came from technical intelligence, that you are seeing into the mind of the other side. And just finally and I am not -- a more mundane example, where I think we haven't succeeded, sticking with Russia for a minute, but one could go into other areas, of course. And I was in Moscow in the early '90s, '91 to '94 and the moment of the collapse of the Soviet Union so -- and I was the service representative. It was a quite interesting job to have in those days, and partly of course, because my service was one of those that was blamed for the collapse of the Soviet Union, and it's annoying now when I find CIA blamed for it, because I find --

(Laughter)

MR. BENNETT: You want the credit for it.

MR. SCARLETT: Yeah. Right. And the -- I saw then, you know, the impact of the collapse of the society which had many tragic aspects to it I have to say. But I don't think I did understand and I think hardly anybody understood the humiliation that it involved for the leadership and the society generally in the Soviet Union and then Russia at that time. And we live with the consequences of that humiliation now. But if we had understood it better at that time perhaps we might have managed it better.

We thought we were doing a really good job of managing it, but in retrospect perhaps we didn't really understand how the new world looked to the population and the leadership of Russia at that time.

MR. BENNETT: So to pick up on that. I mean, that -- it's taking us into the mind of Vladimir Putin a little bit, who obviously seems to be acting on a certain amount of that resentment from that time. My next

question is, in the last 10 years the US, and I imagine the UK and other intelligence services, have become so focused on terrorism and to retool themselves, I wonder if they took their eye of off the other great powers like Russia and China and didn't have enough resources focused on looking at those countries and whether there is currently a calibration going on and what should be done in the next 10 years.

Greg, can you pick that up?

MR. TREVERTON: Sure, absolutely. I mean, I think that -- yeah, that you are right. There was -- obviously, counterterrorism is for obvious -- very obvious political reasons. Very top of the pops, it's always dominates my day every day. Sometimes I feel like I do all ISIL all the time. And so it is really important, particularly from where I sit to try and remind people that there are lots of other important issues out there. And I think Russia is an example of us, not exactly taking our eye off the ball, but as Jim Clapper put it yesterday, it is a kind of a zero sum game, particularly given declining resources.

So, if you are doing a lot of something, you are probably doing less of something else. And so I think the community -- the American community did a good job of keeping its eye very much on China. Recognizing that China was the main game out there, but it did, I think, resources devoted to Russia did go down fairly dramatically. And so we are now trying to rebuild a bit, our capacity, to even understand basic order of battle things, to understand their technology.

And as John said, "We spend a lot of time trying to get inside Putin's head," which isn't so easy, but it -- and that -- the, the kind of you can't understand I think his actions without understanding the kind of humiliation he feels. And that makes me if you ask the, what-keeps-you-up-at-night question, mine would be that, Putin would miscalculate in some way that took us to an Article 5 crisis and therefore to a very different world. That means we do spend a lot of time trying to get inside Vladimir Putin's head. Not so easy.

MR. BENNETT: So, Greg, your office is currently writing the *Global Trends Report*. It's going to come out in December. This will land on the desk of the incoming President. Can you bring us through sort of what the critical issues are that you and your office have seen over the last 10, 20 years?

MR. TREVERTON: Absolutely happy to. We try, in *Global Trends* -- it's obviously completely unclassified. We try and look at 5 years and then 20 years. The great thing about it is if you are trying to look at even 2 years, none of that stuff on your classified computer helps. You really need to be out talking to experts and others. So, we will have been in about 35 countries and touched about 2,000 people by the time we finish *Global Trends*.

Let me just give you the highlights. I don't want to scoop us and indeed it's not yet entirely written, but the big uncertainties. I start with two big uncertainties even over 5 years, but particularly over 20. And no surprise -- I think those two big uncertainties are China and us. What kind of role China and the United States are going to be playing in international politics, both 5 and 20 years out.

I don't get to talk a lot about the United States, but in this case we will some. And if we look at the 5 year look, the 5 year look is really mostly the playing out or how it might play out the kinds of issues we've talked about the last couple of days. Top of the list is China, cyber, then Europe's troubles and Russia, and then for me Middle East, terrorism, how does ISIL morph, those are very much on our minds. We're trying to think creatively about how those might play out even in 5 years is a big piece of the task.

I always remind myself we think history sometimes goes slowly and sometimes it does, but if you think the amount of time between Mr. Reagan's evil empire speech and the fall of that empire one decade a rather short time even in human life.

Then for the 20-year look, let me just tick off the kind of big trends we're trying get our arms around in the 20-year look. First would be the increasing empowerment of individuals and small groups. Again, not new, but striking previous versions of global trends we talked about the power shift to Asia that's still continuing. But the empowerment of single individuals is striking in the case of terrorists, but it's also striking in the case of the Gates Foundation, which spends more on health in Africa than the World Health Organization.

Second on this list is the structural change in the global economy. We imagine, like many other people do that there'll be a period of slower growth than we're used to that's going to make almost everything harder to solve, increasing inequality and create a kind of scramble for middleclass jobs, because so many a billion people have been risen out of poverty in the last generation they'll be in danger of falling back into poverty.

Third will be clashes of values. The most striking to me is, we Americans have a kind of prosperity presumption that says, "Prosperity makes everything better, makes people happier, more democratic, less likely to go war," and then we bump into ISIL that cares none about that. There's no such presumption, doesn't care a bit about it. Less striking are the Chinese attitudes towards international financial institutions and others. They see those as made in America or made in the West, but clashes of that, of values, will be a piece of the future and how that plays out.

Two more. One is technology. There we're going to focus I think on artificial intelligence and on bio. The artificial intelligence the first effect there will be, I think significant disruptions in job markets around the world as more and more jobs are vulnerable to are actually taken over by technology.

Bio, we know we're on the cusp of something enormous. Bio, I think is about today where IT was 25 years ago. The kinds of advances we'll see will be wonderful. Life extending, life improving, but we're intelligence analysts and it is said of intelligence

analysts that when they see flowers they think of coffins. So we're -- needless to say also mindful of how bio advances might lead to designer bio-weapons targeting ethnic groups or even single individuals.

Last on this list would be really what seems like the growing disconnect between people and their governments around the world -- often it gets labeled populism, sometimes nativism. Now, we've seen it in our country. We've seen it strikingly in the Brexit vote in Britain. And so thinking about the implications of that 20 years out. Will that mean that societies that are now tolerably well governed fall into bad governance or will there be new forms of public-private partnership that supplant our existing arrangements.

MR. BENNETT: So thanks for that, Greg, inside overview. One of the things that the intelligence community is tasked with is predicting events and be having the leaders of our countries prepared to handle unfolding dynamic events like the Arab Spring for example. The US intelligence community has been criticized for not predicting the Arab Spring and a recent event was the coup in Turkey for example.

I spoke with a senior US official, who first started seeing information about the coup in Turkey breaking on Twitter. He told me in an anecdote, where he called his counterpart in the intelligence community who hadn't seen the information on Twitter popping up. It had just been out for about 20 minutes and he had to go and find out what was going on.

So that brings us to how is this social media feast of information going to change the way that the intelligence community looks at information, all the information that's available there on the open source. Leslie could you talk a little bit about that?

MS. IRELAND: Sure, and then I'm going to ask Greg to chime in. So one of the responsibilities, as an intelligence analyst, is to be able to evaluate the information that's in front of them. Frankly, not all intelligence is created equal. Some of it sourced better

than other parts of it and as part of our tradecraft we train analysts who look at the sources, evaluate them before they come to a judgment.

So, what I would say is on social media I have often heard, but it was on Facebook. It was on Twitter. It was here. It was there. Why didn't you take that into account and I don't think it's a case where they didn't take it into account, but in fact there is a whole new science that's going to have to be developed and is being worked on in terms of how do you evaluate the information you get on social media, because you don't know the identity of the person who is putting a post on Facebook or who is putting out a tweet. It could be somebody right in the middle of things. It could be a foreign intelligence service, who is trying to mislead you. It could be any number of things, but I think we're growing in our capability of being able to take that social media information and integrating it better with the classified sources that we have.

MR. BENNETT: Greg, you want to weigh in?

MR. TREVERTON: Yeah. I think that's exactly right. I mean, the case you mentioned Brian is there what you'd hope is you get a tip. You know, we know about all the open source stuff, particularly social media, it's hugely voluminous and completely unreliable, right? And so trying to make some sense of it, but you probably could get a tip and say, "Well, maybe is a coup entirely unthinkable?"

What we've been doing in my Africa work for example is, there is not a lot of great intelligence on Africa, but there is a lot of data. So, we have a data scientist looking for data, not all Big Data, but just databases and there what you find is that data is plenty good enough to help you foresee famines or disease, but beyond that what I hope is we can get out of it sort of tips like the one you suggested.

Shouldn't you look here, shouldn't an analyst take this connection that he or she hasn't thought out before seriously. So, I think it's a really big deal for

us, but it does have the huge challenges of reliability and just processing, because the volume is so enormous.

MR. BENNETT: While we are in this new world do you want to weigh in on that?

MR. SCARLETT: Well, I just like to challenge to some extent, what you just said there about what's expected of the intelligence community and also distinguish between predictions of some events. Let's say a coup in Turkey that of course is clearly a role for a security service or an intelligence service starting with the Turks one has to say --

(Laughter)

MR. BENNETT: I mean if Erdogan didn't know that a coup was coming too.

MR. SCARLETT: -- to predict that that might happen, and given the number of people apparently involved it is quite surprising that it came as a surprise. That's a particular kind of event. The Arab Spring is a completely different kind of event. I personally would pushback very strongly against the idea that, that was some kind of intelligence failure. It is not the job of intelligence to predict events when they are not no events. I mean, there are enormous movements, trends.

It was not the job of the intelligence community to predict the fall of the Soviet Union. That was lucky because nobody did really predict it. I mean, it's a much broader to think about that is the political analysis is for diplomats, it's for a whole range of capabilities that this sophisticated global government will have. And there were some events, by and large my experience, has been that the biggest changes and most strategic changes certainly that I have seen like, fall of Soviet Union, the Arab Spring, actually 9/11 is sort of almost by definition unpredictable.

The job of a really well informed and skilled government machine is to be able to understand very quickly once the event has happened, to be able to

understand it and then to behave in order to react to it and to manage it. I think that's a much more realistic way of looking at things, because it's the idea that somehow or another these really big things are -- it's the responsibility of intelligence to predict. It is not the responsibility of intelligence to predict in my experience. And we need to be clear about the different kinds of events we are talking about.

MR. TREVERTON: Can I just? If you look back at the intelligence record before the fall of the Soviet Union, the particulars were all pretty good. We understand how bad -- what bad shape their economy was in, military. We all understood all that. What we didn't do, what they didn't do or my predecessors, is put it together in a story and say, "This is leading to the fall of the Soviet Union."

So, we knew the specifics but it's always creating the story, creating a credible story and indeed the first people who created a story about Gorbachev didn't believe it, because they were people like Bob Gates who said, "He is destroying the Soviet Union." He can't mean to be doing that. So, they created a story, but didn't believe it.

I always think it's the story that's critical, because if there is no story then the individual bits of information are just kind of factoids, what you need is some credible story. But imagine intelligence analysts in 1980s trying to write a story about the fall of the Soviet Union, probably would have found himself or herself counting submarines on Kamchatka Island right?

MR. SCARLETT: That's exactly right

MR. BENNETT: So social media presents this opportunity for understanding the world better. It also presents a liability for human intelligence for intelligence collectors, for people trying to operate covertly. We all walk around the world and we have this digital exhaust as we use social media, we use credit cards, we have financial transactions. Can you talk a little bit about both the benefits of that from an

intelligence collection perspective and the difficulties it presents for doing covert actions, getting people moving around the world without being traced by adversaries?

MR. SCARLETT: Yeah, well obviously, you know, as somebody who did used to move around the world, sometimes not being me as it were, and obviously that's much more difficult and more complicated than it used to be, but nothing is impossible.

MR. BENNETT: You're going to tell us what your favorite disguises were?

(Laughter)

MR. BENNETT: Moustache --

MR. SCARLETT: They wouldn't be difficult to guess actually, yeah.

(Laughter)

MR. SCARLETT: But I think again we need to be so careful in understanding as we categorize different kinds of information flows and what they can -- what we can reasonably expect from them and what we can't. So again going back to your story about the Turkish coup and it coming up on Twitter that of course is completely -- you know that's really interesting. It's really interesting that that should have been available, you know, 20 minutes whatever it was before the US government sort of picked it up. And there are other examples of that I think the same is true about the Brussels attacks back in March.

And that is telling us something that we need to think about and we really need to think about, because there are other things that social media can do -- the sheer scale of it, around 500 million tweets a day means that there is actually a global pattern of activity.

So it's not just the individual items that might come from let's say a coup, but it's also the overall

picture of events, if you suddenly get an outbreak of violence over a few -- a half an hour or an hour in a certain part of the world, which is politically sensitive then, you know, you might pick it up from watching that. And of course that's the kind of area where lots of companies and so on are now engaged, and governments have got to learn how to incorporate that into their analysis.

And it's an example of where if you like private sector capability is relevant to government analytical capability, in a way which was never true, you know, for much of my career and it's one of the changes taking place in this area.

MR. TREVERTON: I know it's a wonderful opportunity. One of my colleagues in the defense intelligence agency says, "Selfies are our best friend," because boys will boys and they take pictures of themselves in the back with their girlfriends and so therefore it makes it hard for them to say, "No, I wasn't there or for Putin to say, no, there wasn't any Russians there."

We've actually seen selfies that had in the background weapons that we hadn't seen before. So it's a great opportunity. The real challenge I think is as we move to where there is more pictures than words then the challenge we all face is trying to figure out how to interpret those pictures, make use of those pictures that I think is the challenge in front of all of us.

MR. BENNETT: And Leslie, I wanted to talk to you a little bit more about how financial intelligence is driving the future of intelligence collection and also policy recommendations from the IC. You know you've got a huge new amount of information about people's financial transactions, about countries' economies. Can you talk a little bit about how that has given the intelligence community new opportunities to find weaknesses in our adversaries to find pressure points to bring people to the table, find pressure points on Russia, find pressure points on Iran to bring them to the negotiating table?

MS. IRELAND: Sure. So, let me back into it

first and talk about the Iran piece and that is. So the sanctions program depended upon a huge amount of intelligence and that's because when the Treasury Department works to sanction an entity, an individual -- a financial institution what have you, I mean Treasury currently has over 30 sanctions programs.

There's intelligence that's marshaled that identifies vulnerabilities and provides that useful information to the policymaker, who can then implement the sanctions that a package is built -- it's called an evidentiary, and it is actually reviewed from a legal standpoint, because the Department of Treasury, specifically the Secretary or the Director of the Office of Foreign Assets control can be sued by an individual or an entity that it sanctions.

So, you really need to have a very, very strong case to take forward in order to implement sanctions. It's not done on a whim. It's not done on a -- well, I think they're doing this. It's done on a -- with a reason to believe that this activity is going on.

The reason I think that's important is that sanctions are not designed to punish for past behavior. They're designed to encourage a change in future behavior. And so, to get to your point the information that we were using on Iran to come to a point, where I genuinely believe the sanctions brought them to the negotiating table, because of the impact on their economy, because of their -- that they were isolated within the international financial sector. That information is still very important to us moving forward.

We have to keep a very close eye on Iran, both from the perspective of the implementation of sanctions that still remain on terrorism, on ballistic missiles, on human rights abuses etcetera, but also because the JCPOA includes the opportunity for snapback sanctions if they do not follow with the agreement, or that actually can confirm that they are behaving in a way that we wanted them to behave with the sanctions in the first place.

Getting to the broader question about financial

information. When I started six years ago and Jim Clapper asked me to be the national intelligence manager for threat finance, I found that people tended to see financial information solely through the lens of sanctions. And I took a lot of time as manager for threat finance to help -- show people that you can use it for other things.

Now, I knew I'd been in the job too long, when I'm driving down the Dallas toll road in the morning and I drive through the tollbooth and I look up and I look at the transponder and I think, where are we collecting those overseas. Think about the information you can get from a tollbooth transponder. You've got pattern of life. You've got somebody's vehicle. You've got access to their financial accounts, whether it's a credit card or bank account. You've got access to their driving records.

I think that information is out there and it's a matter of pulling it in, pulling it in a way that the entire intelligence community can use that's something that are working on right now.

And I think that eyesight, so this cloud-based integrated IT infrastructure that the DNI is building the IC toward, will be part of that. Part of that is having the right tools to sift through that data, because some of it is structured is in spreadsheets and some of it is very unstructured.

We've worked on that with DARPA to develop specific tools to be able to work through the financial information and a lot of it is training and educating people that you've got a cyber group, maybe the way to understand how that group is interrelated is to follow their financial activity, and to see the connections that are made through the financial activity, because the fact is people only transfer money, because they know who they're sending it to. This is not like a wrong number when you pick up the phone -- money is transferred intentionally.

MR. BENNETT: Let's hone in a little bit on Iran and the Iran deal. Your office has been tracking the --

you know financial intelligence coming out of Iran. Have you seen any indication that any of the money that's gone back into Iran in -- result of this sanctions coming have gone to the Quds Force or the IRGC that was -- as it was a concern?

MS. IRELAND: And so I can't answer that directly, but what I will tell you is that it's our belief that the Iranian government certainly recognizes that they have got economy difficulties on their hands. So in other words they've got high rates of unemployment. They've got high rates of inflation. They have a rial that is struggling. They have an oil industry that they have neglected for decades that they really have to bring on line since oil still remains their primary source of hard currency earnings, and is our belief that the money that they are gaining access to now primarily will go towards the funding for the economy.

That's not to say they couldn't want to prioritize some of that and put it into the nefarious activity that they've been involved in, but our basic expectation is that the vast majority of it is going to go back to the economy.

MR. BENNETT: As we move into the information age the demands on the workforce and the intelligence community have changed -- we're going to open it up to questions shortly, but before we do that I was just wondering if any of you had any thoughts on ways that the intelligence community can find the right people to hire to do the work that they need to do?

MR. TREVERTON: I'll just make two points on that score. One is I think we've done an okay job by beginning to respond to the needs of Big Data. So, we've now various -- the agencies have created new positions for data scientists or data analysts heard, because in the first go round the data folks weren't sure what the regular analysts needed or did and the regular analysts weren't sure what the data folks could contribute, but the second round is getting better. So, I think we're doing relatively well there.

We've also done a decent job at making the workforce look more like America, but I think for me the real challenge is the next level down taking advantage of diversity, so we get advantages from the number of languages and ethnic backgrounds in the country, so we get some differences of view.

Our challenge is that once you've put people through a polygraph you may have homogenized the people you're getting. You don't get a lot of wild and crazy people, who might have wild and crazy ideas through the polygraph and that's a real challenge. So, trying to -- from my perspective as an analyst trying to increase the diversity of thought that's a challenge that's much harder for us.

MR. BENNETT: John, do you have any thoughts on that and how --

MR. SCARLETT: Well, I was at one stage, a few years ago, responsible, in our service, for security and vetting and counterespionage and so on; and one of my job was to stop us recruiting wild and crazy people. And if you did recruit one wild and crazy person, you know, the lesson was -- any professional colleagues here would, you know, what I'm talking about they could do untold damage across the organization. So, you couldn't afford to do that, but you've got to be careful because homogenous issues are of course a threat, and if you -- I mean when I joined a long time ago -- I'm not going to say how long -- in my first interview they wouldn't tell me what it was that I was being interviewed for.

And when I asked at the end of the interview, well, what is it that I maybe joining, it's a government service. Well, what does it do? Well, it provides support. And then, I'll say, well support to who? Support to people who provide support. And that was as far as I got, you know, after an hour or so and then it got better. Now a great change has been when people are recruiting into a career service and, you know, these are career services still, which is an issue too actually.

MR. TREVERTON: Absolutely.

MR. SCARLETT: And then it's on publicly; so it's all open and that is the best way to avoid copycatting yourself. And it's not difficult to attract people to work for a service like MI6, because everybody wants to do that, but the problem is filtering out, you know, getting the right people and not the wrong people and so on. But reflecting the diversity of society and of course an increasingly complicated and not least, because of course apart from everything else you have nationalities also, and they certainly apply in the United States, they apply in the UK too.

I was once asked by parliamentary committee, why was it that we had to insist on recruits to the service career being British. And I sort of said, to my amusement, one of those left-wing MPs on the committee thought felt this was a great joke and laughed out a lot. And the obvious answer was because it's a British intelligence service, yeah.

I can't easily discuss this any further, but you can see that that brings with it issues about diversity and homogeneity and so on, and of course we've got to get out there, and recruiting new skills, particularly data skills, analytical skills which originally, you know, a long time ago we didn't have to think about.

MR. BENNETT: Well, let's see if there's any wild and crazy people out there who want to ask some questions. Please raise your hand and identify yourself, ask a question and wait for the microphone. Thank you very much. Here in the blue blazer. That's you, yeah.

MR. NEBRI: It's black, that's why I was confused. This is a question that -- Mark Maybury director of the National Cybersecurity, FFRDC. My question is for the director of the NIC, but really it goes to all the panelists. One of my favorite things about the *Global 2030 Report* was the glimpse of hope. You actually predicted -- forecasted the growth of the Chinese middleclass and their desire for increased -- a reduction in corruption, improvement in the environment, improving education, the same kinds of things that the US

middleclass cares about. And you predicted -- forecasted, I should say that that we would have increased stability globally.

So I'm curious if you have updated that forecast, but equally importantly for the other panelists, what is your glimmer of hope for the future?

MR. TREVERTON: On China, as I said it, it for me is one of the two big uncertainties as I look out and the question there is whether they will get through their current political difficulties and the middle income trap they're in and get to a point of decent if not very plural governance and decent economic growth. So that's the big uncertainty about them.

I realize when I did my run through the trends it's a pretty dystopian view of the world and therefore trying to look for glimmers of hope -- I keep asking everybody, since you look at the Middle East and all of the trends are going in the wrong direction, I keep asking, "Does anybody have a hopeful sign about what's going on in the Middle East?" So far the hopeful signs turn out to be places like Iran, right. So it's not -- well, not your hopeful sign that it's not great, but it is I think incumbent on us to -- as we do this, to make clear that a lot of this future we're trying to shape is really in our own hands.

The things we can't -- we don't run the world or control the world or -- the dominant power, as we once were but we're still absolutely necessary to make things happen. So trying to find what my colleagues call, "opportunities" -- I don't much like that idea but opportunities, places where there are silver linings where things might get a lot better. That's obvious in the technology area, but in other areas as well that's a big challenge for us.

MR. BENNETT: So Greg just to follow up on that. When you talk about the big things the intelligence community needs to think about in the next 10 years; China was on top of your list and what -- and give us the opposite of that, the doom and gloom, why is China so

important for the intelligence community to think about in the next few years? What could go wrong?

MR. TREVERTON: Two things. One is, as I said earlier, I think it's pretty uncertain and the bumps in the road for China which we knew were coming. We knew economic growth was going to slow that's happened, but now the combination of slower economic growth, with the backlash against the corruption campaign, with the stalled economic reform that makes me think that its course is pretty uncertain.

The worry is that as its internal sources of legitimacy get less that it will turn even more towards South China Sea and nationalism abroad that's sort of the five-year future I foresee and worry about. Obviously, the other reason for thinking about China is that it is the second most important country in the world and therefore it deserves a place at the top of the list no matter what.

MR. BENNETT: Before we go to the next question any glimmers of hope?

MR. SCARLETT: Well, of course the difficulty for intelligence professionals, analysts or operational officers and so on and you look at the world, your job is to look for problems and for things that go wrong. So inevitably you are Mr. Gloomy Boots that is --

(Laughter)

-- and I have this problem the whole time and I'm asked to -- because I'm good at spotting problems and so on. But actually you find at many intelligence operational people and analysts they are actually within themselves natural optimists, and so you have to be, you know, resist that temptation.

(Laughter)

And a purely personal reaction is that and I would say -- I don't want to sound like a US presidential candidate, but I am -- China maybe the second most

important country in the world, but by a long distance, the United States is the most important country in the world, and it will continue to be so.

And then the community of nations around that is fundamentally powerful, resilient; able to exploit opportunities, technology for example in a far more imaginative and expressive way than we have seen happen elsewhere. If you stick with that you can be an optimist.

MR. BENNETT: Let's take some more questions. Over here, in the blue shirt.

MR. STEPHENS: Bret Stephens from the Wall Street Journal. This is a question for Mr. Scarlett. A few weeks ago there was a YouTube video, which had been leaked in Russia and caused a small scandal when recent graduates of the FSB toured around Moscow in $100,000 Mercedes SUVs, what does this tell you as an intelligence professional about the culture and caliber of the FSB today?

MR. SCARLETT: When I was in Moscow working with FSB colleagues in the early 1990s, the monthly salary for a lieutenant colonel was $130. I remember that well. So, that would suggest that there's been a bit of a change in their salary profile. Actually, I suspect there might not have been that much. Yes, I read of course that story and -- somebody interfering there -- and I was very interested in it, you'll probably find the whole evening was funded by somebody -- I don't know the story. It didn't actually say that, but those officers will not have that kind of money at their personal disposable, I'm quite sure.

And it's important to remember too that a security service like that has lots of good professional people in it. They're not just there to sort of throw money around and be boastful and do whatever their bosses tell them and so on. It's a much more disciplined and complex structure than that. So one has to be sort of (inaudible). So I would say in other words, put that story into some kind of context. It was probably an oligarch.

MR. BENNETT: Next question? Yes.

MS. HARMAN: I'm Jane Harman. I'm a wild and crazy supporter of the intelligence community and I would observe that it's stronger because of its diversity and because of our strong liaison relations, especially with Britain. My question is this. Traditionally, at least, as I understand it intelligence is not the same thing as policy. Intelligence professionals try to project an accurate picture of what's happening and to some extent predict what will happen and get into the minds of the big actors, but then policymakers make the policy; they're not the same thing.

And so my question is with respect to the US presidential campaign, what degree of confidence does the intelligence community have that intelligence will be used seriously by our next president, whoever she or he may be?

MR. TREVERTON: I suppose the easy answer is it's up to us to demonstrate they were useful. We do -- intelligence draws this line between intelligence and policy. Most policymakers in my experience don't have any similar line. They're just looking for help and often the kinds of questions we do a lot of intelligence support, we do the intelligence work for the Principals Committee and the Deputies Committee as you know and out of those high level policy deliberations come just the right sort of questions from my perspective they'll ask us, "If we do X how will Putin respond? How will it affect his entourage?"

Those are really trying to ask for assessments of possible policies and that's exactly the kind of conversation I'd like to have. Whether we'll have it for the next administration obviously depends a lot on personalities. My guess is they'll also be interested in help and discover that the intelligence community is a pretty good, pretty professional, pretty sensible place to find help.

MR. BENNETT: Yeah, go ahead.

MS. IRELAND: So just a couple of observations

on my part and one of the things that I found very important. I started briefing President Obama, President-Elect Obama right after the November 2008 election and I walked into that understanding that I had been steeped in intelligence for years but he hadn't. And so it was really incumbent upon me and I think any other briefer is to help the President, whoever it is, understand exactly what intelligence means, and understand what we mean by some of our statements, because the way we speak in intelligence language is not normal.

(Laughter)

MS. IRELAND: It isn't. If I were writing this as an intelligence analyst I would have phrased this quite a bit differently, but the bottom line is to help them understand what the capabilities are, what the limitations are, just what they can expect from the intelligence community.

And then to part of your point regardless of the party that is elected, it is the job of an intelligence professional to provide the best and the most objective information they possibly can. You have to have that severe line between intelligence and policy. You cannot be preparing intelligence analysis, you cannot be skewing collection, you cannot be doing any of that in any way to try and influence the course of policy.

MR. TREVERTON: Just to reinforce Leslie's first point. When Mr. Obama was elected, Mr. Bush wanted him to get the same President's Daily Brief, the document that Bush himself got, and one of our colleagues observed that Mr. Bush had been doing this for 8 years by then, while for Mr. Obama it was like opening new listees at random to try and understand what this President's Daily Brief is all about. So it's --

MR. BENNETT: John, as an observer of the American political process, do you have concerns that one or two of the presidential candidates might not use intelligence appropriately?

MR. SCARLETT: Well, I'm going to sidestep that

question completely and make a slightly, I mean related but a different observation, maybe. Of course, it's absolutely correct the dividing line for an intelligence professional between intelligence and policymaking must be rigid and it's not just the individuals who have to recognize that the whole system has to recognize that and the structure has to be built around that and, you know, by and large it is in both of the countries I know best, which United Kingdom obviously and the United States.

I think that the challenge for a US president coming in and to some extent that's true also for a prime minister actually, but maybe particularly for a US president is that although the intelligence community, of course, doesn't know everything and it has lots of gaps it knows a huge amount, and the difficulty and the challenge is knowing how to form policy -- in a way accept that you can't get everything right and you might know the truth of what is happening in a particular situation, but you may not actually be able -- and then maybe an obvious right thing to do.

I mean, you know, that somebody -- some of head of state is coming to you and it's just lying, you know and telling you something which you know is completely untrue, but you can't actually behave as a human being, right. In response to that you got to have a clever and thought through policy response and that's very difficult.

And if you are not -- obviously for anybody, however, good and clever and honest they are, if they come in without experience and there's a very high number of political leaders in both our countries do, then that's a real challenge. And it's often not understood just how much the US government in particular, but my own government too, how much they actually know, but they can't say.

MR. BENNETT: So I just saw the five minute card and so we'll take two more questions and then have the panel answer it. So let's go with this gentleman here and this woman here with the black and -- black, yeah, that's right.

MR. SMEATON: Hi Joe Smeaton (phonetic) from Santa Clara County, California. And I'm just curious, are there noteworthy differences in the philosophy or approach in the British system and in the American system of intelligence gathering? They're different cultures, they have different legal systems. Does that manifest itself in a way that means you have a different perspective if you're a British intelligence professional as opposed to an American intelligence professional?

MR. BENNETT: Let's take one more question and then we'll have them both asked at the same time.

MS. HARRIS: Okay. Dale Harris, Foreign Policy Association. My question to you concerns intelligence support to the military side of the House, as you know military strategy is often revolved around there. I'd like you to talk about the criticism that the intelligence community needs to get ahead to understand the new forms of warfare -- hybrid warfare that particularly Russia and China are taking advantage of not just with cyber, but with movement of forces. And for the British gentleman I'd like to know who the next movie James Bond is going to be?

(Laughter)

MR. BENNETT: So well, let's start with the differences between the cultures of American intelligence services and British intelligence services.

MR. SCARLETT: Well, the biggest difference is one of resource, I mean, in our terms in fact in anybody's terms the resources available to the US intelligence community and it's 17 agencies is what are -- are vast. And they're on a completely different scale and from everybody else. And I'm not sure everybody in America always quite understands that.

And of course there is a legend; if you like out there that -- and I often hear it -- that the US is very good when it comes to technology and technological collection and old fashioned signals intelligence or whatever it might be and the British let's say are better

at human intelligence. I mean that's the sort of legend. It is a legend. It is a myth. Both sides are very good at both. And I can back it up with lots of examples if I had to. It's not completely surprising since they have worked extremely closely together famously since 1941, this is the 75th anniversary year of the special relationship, I can think, I couldn't claim.

And obviously therefore you know a lot of capability and knowledge and understanding and so on is a shared, although there is a difference of scale and if you are from my side you therefore got to prioritize in a way otherwise you wouldn't do and you'll have slightly different -- I mean you will have different interests and so on. And so you'll be perceiving that. Fundamentally, I don't think there is so fundamental structural or cultural difference -- that means I can't -- I wouldn't immediately pick on it.

MS. IRELAND: And I would just echo that from an analytical standpoint. I came up through the analytical ranks is that we will have intelligence exchanges and it's oftentimes you understand that a service by virtue of their threat perception or their national security concerns may have focus on an area that you're interested in and so maybe you go and you talk to one service in one area and you may talk to another service in another area because you know that's where they have to specialize, because their resources are so scant and because frankly the global perspective in the United States is that we need to be on top of everything and it is through those partnerships that we are more successful.

MR. BENNETT: Okay. So the final question was how does the intelligence community adapt to these asymmetrical threats from China, creative things being done by Russian intelligence services to destabilize different -- the political discussion in United States, asymmetrical threats through terrorism?

MR. SCARLETT: So, did you want?

MR. TREVERTON: Happy to start. Intelligence is something that's very much on our minds. It is -- I think

it's a task for all of us -- the military, there's a big military intelligence establishment. The services have their intelligence agencies so I think it's a task for us all. What we're trying to do at the NIC is really think about the future of warfare in an era when all the technologies we have, our adversaries are going to have from nano to drones to all of the rest, when the line between combatants and non-combatants is gone and these are really since war is between societies. So cyber there's no difference between the kinetic and the cyber realm; they're interconnected.

So trying to think of our way through the really fundamentally changing nature of warfare and sometimes even warfare doesn't sound like the right term for that if we want to encompass grey zone war, hybrid war, all those things that I think that are a real challenge for us, but something we're working hard at.

MR. BENNETT: So I'm getting the zero minute card, John --

MR. SCARLETT: Well, as a non-American and you mentioned for maybe a second or third time the DNC point. I think advice just calm down, yeah. It's become a frenetic atmosphere around it. And yes, of course, technically we can work out almost certainly who did it; the original hacking. It shouldn't be that big a surprise, you know, these sort of things have been going on one way or another in the pre-cyber age and the post-cyber age, and to imagine that it can distort an entire political process like the American political process.

I just -- I'm influenced by what I experienced back in the late cold war days when -- I see it's minus 3 minutes probably, yeah -- late cold war days when we were told to get really worried about Soviet and KGB activity enacted measures and interference in our political process and so on, and it all turned out to be rubbish, and it had no influence at the end of the day at all, because of the strength of our own systems. So keep things in proportion.

MR. BENNETT: So keep calm and carry on and that

brings our panel to the end. Can we have a big applause for the panelists? Thank you very much for joining us.

(Applause)

* * * * *