THE ASPEN INSTITUTE

THE ASPEN SECURITY FORUM 2016

THE NEW NORMAL?

Doerr-Hosier Center
Aspen Meadows Resort, 845 Meadows Road
Aspen, Colorado 81612

Thursday, July 28, 2016

LIST OF PARTICIPANTS

SCOTT A. MONTGOMERY
Vice President/Chief Technical Strategist
Intel Security Group

WILLIAM BRATTON
Commissioner, New York City Police Department

ROBERT GRIFFIN
General Manager, Safer Planet, IBM Analytics

PETER NEFFENGER
Administrator
Transportation Security Administration

MICHAEL STEINBACH
Executive Assistant Director
National Security Branch
Federal Bureau of Investigation

SHANE HARRIS
Senior Correspondent
Intelligence and National Security, *The Daily Beast*

* * * * *

THE NEW NORMAL?

(3:00 p.m.)

MR. MONTGOMERY: Give everybody a moment to sit down and we'll get going. So again, good afternoon. My name is Scott Montgomery. I'm with Intel Corporation in the Security Division. I've been building and designing information security and privacy solutions for the intelligence community and the defense community since I had long brown hair. And one of the things I'd like to do and echo some of the other folks who introduced sessions is to echo my thanks, may heartfelt thanks to the Aspen Security Forum and to its organizers for having us.

This is always a very compelling event, very informing event, and this year is no exception. I have the privilege of introducing this next panel that's discussing "The New Normal." And one of the things that we've heard during the course of this conference is the frequency increase and the new normality of this horrendous physical terrorist attacks, whether it's San Bernardino or Orlando, whether it's a lone wolf, whether it's organized. And in my lens, in cyber we see a new normal as well.

We see incursions that are espionage-like as we did over the last 10 days, if that's your perspective on the event. We've seen a cavalcade of breaches where trillions of dollars of value is taken out of the G20 and other GDPs. And also, in the new normal we're seeing a new kind of attack where the physical, critical infrastructure is attacked for the purpose of disruption by state-sponsored adversaries as we saw in the Ukraine over Christmas.

With that, it gives me great pleasure to introduce Shane Harris who is the senior correspondent of *The Daily Beast* for national security, intelligence, and cyber. He's also the author of two fascinating books *The Watchers* and *@War: The Rise of the Military-Internet Complex*. With that turn it over to Shane. Thank you.

MR. HARRIS: Great. Thank you very much. Thank you all and thank you to the Aspen Security Forum. Very excited about this panel. We have to say sadly it could not be more timely, I think, this discussion as so many things have been here today and to the list that we put in the program when the panel is put together, of Paris and San Bernardino and Brussels. Of course now we have to add Orlando and Istanbul and Nice and so many other places as well.

So hopefully our panelists here are going to help us illuminate in a very big level what in the world is going on here. And we're going to sort of talk in detail about this new threat environment that we're facing, which perhaps is not so new. Maybe it was something that was anticipated as well. We'll talk about that. Let me first make brief introductions. Here to my right is William Bratton, the commissioner of the New York City Police Department, probably one of the most storied careers in law enforcement in the United States, one of the most experienced law enforcement officers and leaders. Welcome.

The administrator of the Transportation Security Administration, Peter Neffenger. You all know him because he flew to get here. So you interface with his agency on a regular basis. So thank you very much for being here. Michael Steinbach who is the executive assistant director for the National Security Branch at the FBI and very apropos to this discussion. Michael has spent a lot of his career working on terrorism issues and has worked with the Bureau in Iraq and Afghanistan on their efforts as well there.

And at the end of panel (inaudible) here is Robert Griffin, the general manager of Safer Planet at IBM Analytics. And for those of you who've worked in law enforcement investigations, you will know Bob's previous company i2 of which he was the cofounder and CEO, which is -- if you work in this domain you're probably very familiar with the software and products that they developed. So what I want to start with is an observation, a bit of a reflection.

As I was thinking as we were getting ready for this panel, shortly after the 9/11 attacks, what seemed to me first and foremost in the minds of people I was talking to in the security world in the national security space was not so much when the next attack was going to be, because it seemed like everybody I talked to in government anticipated that would soon, but when terrorists would start hitting soft targets.

When would they start picking up automatic weapons and going into restaurants and the shopping malls, to amusement parks? When would they start blowing up gas stations? When will they start blowing up buses? All of these sort of seemingly totally vulnerable targets that were just right for the picking, when would that happen -- when we see that kind of environment where all these attacks would just proliferate.

And that really didn't happen. I mean putting aside attacks like in London and Madrid, we never really saw sort of the rapid succession of attacks that we seem to see today happening in so many countries and here now. And so what I want to start with -- and then I want to go first to Administrator Neffenger on this is, is the threat environment that people seemed to be dreading 15 years ago that I'm laying out there, has that finally come to pass and is that now the environment that we're living in? I'd like to get your thoughts, but also the panel's thoughts on this idea.

MR. NEFFENGER: Okay. Well, thanks, Shane. And first let me just say thanks. It's a pleasure to be here with colleagues I've worked with for a long time. It is about the threat. And I like the fact that you opened with a question about this threat rather than calling it the new normal, because I think labels tend to detract from what's really happening. What I see over the past year in particular is disaggregating an evolving threat.

I don't know that we're seeing anything especially new, but the way in which it is occurring, the unpredictability of its occurrence, and the proliferation of its occurrence, I think is new. And the way -- and the repetitive which people can share information and move

information amongst themselves I think has changed. So really it means that we have to -- as you go back -- as you think about 9/11 we've been -- become very good at stopping that next attack.

I think General Clapper hit it right when he said there were a lot of signatures to large attacks like that. What we have to understand is that we have an enemy that is creative, it's adaptive, and it evolves. And we have to do the same thing. So in my world as I look at -- if we take the aviation environment, for example -- as an example, rather than thinking in terms of perimeter, things outside the airport or public area of airports, at checkpoint, in a secure area and you're producing things that are secure, things and people that are secure as they go through, I think we have to rethink the whole security environment, the ecosystem, if you will, of securities so that you don't think in terms of handoffs from one to another, but look in terms of the whole system.

I know Commissioner Bratton will have a lot more to say about that. When you look at managing security in a large city, you don't think in terms of just the handoffs but how they go together. So I -- from my perspective what it teaches me is that you have to -- we have to learn to evolve certainly at the speed at which the enemy is evolving, their tactics and techniques, but more importantly to get ahead of that and to not do what Secretary Johnson said, which is just pay attention to the last attack but think about what it is. So what it tells me is that we have to look forward continuously and try to read where we might be going with those.

MR. HARRIS: Commissioner Bratton, how do you see the environment based on, you know, compared to where we were 15 years ago?

MR. BRATTON: Several thoughts falling out of your question and the admiral's comments. The term new normal, there is not a new normal. The normal is going to keep changing much more quickly than it has over the past 12, 14 years. Then the threats have multiplied exponentially that for 12 years after 9/11 the principal threat as we know was al-Qaeda. Al-Qaeda was focused on

the big attacks, largely multiple attacks if they could do it, take down multiple planes, multiple attacks on embassies.

And then just as I came back into the business again in 2014 with John Miller in New York kind of taking over as my counterterrorism chief, ISIS, ISIL, whatever you want to call it, really began to come on to the stage as al-Qaeda really went backstage. And ISIS was able to take advantage of something that al-Qaeda was slow to recognize and still has not been able to really fully understand and use, and that's the whole social media world. Different from 9/11 now we have the social media which changes everything.

And the threat picture isn't just the -- if you will, the radical Islamic threat al-Qaeda, ISIS. We're now seeing it, the attacks on police officers -- that's a new element -- began in New York in 2014 with the murder of two police officers sitting in a car. We saw an exponential expansion -- Baton Rouge, Dallas recently, as well as other attacks that are occurring more frequency on police. So the world is changing. In terms of your question or comment about the soft target, effectively everywhere is now a target.

There is no area that is not potentially a target. And we have to recognize that and understand that. And that is the new normal right now, but that's going to change also very quickly as we go forward. So how do you protect all of that? For the life of us in the law enforcement world, intelligence world, we don't know why in this country with more guns than people. And as we clearly understand, a very large, improperly cared for population that have mental illnesses, a variety of illnesses, why there are not many more instances of mass shootings and incidents like we've seen recently, we just don't know.

But what is disturbing is that we're seeing more of them. And the challenge for us now in law enforcement, certainly in the federal level on the intelligence side, the multiplicity of threats that we have to deal with -- terrorism, the idea of the whole racial issue in the

country at the moment that's generating so much discussion, tension, frustration, the large number of emotionally disturbed, the incredible number of fire arms in this country have contributed to the numbers of incidents.

We're in uncharted waters. I used that expression of speech several days ago. And we're really trying to get a full understanding of what are all those potential mines in those waters, where are they, so we can prepare to deal with them. Mumbai changed everything very quickly a few years ago -- Mumbai attacks, multiple attacks, soft targets. In LA when I was chief of police at that time literally within 30 days we totally changed how we were prepared to deal with that.

And in New York just over the last 2 years John Miller and I have created now a series of rings of protection to deal with what we saw coming with ISIS, but what we're also starting to see with the attack on our detectives that new types of threats. So in New York now that I've got at any given time several hundred officers in the field equipped with the long guns, the heavy-duty armor, et cetera, so that we can get to any location in New York within 5 to 7 minutes.

As the FBI did an analysis of all these attacks, most of the deaths occur in the first 5 to 7 minutes. Similarly that -- I just this week announced we were purchasing as a result of what happened in Dallas and Baton Rouge, 20,000 ballistic helmets and 6,000 heavy vests so that one of my police guys will now have that. Every one of our police guys is now going to have basically bulletproof doors on the vehicles.

So we have an obligation -- we have officers with the uncertainties at the time we're facing to equip them, prepare them, active shooter, protect them against active shooter so they can protect the public. And then the balancing act that we're dealing with right now in the race issue -- how do we at the -- on the one hand train them to go toward the danger, but how do we also at the same time try to train them to deescalate many of the other situations we find ourselves in. There's never been

in the history of policing and I've not been involved in since the last 45 years a more challenging time and a more potentially disturbing time.

MR. HARRIS: Right. Michael Steinbach, you've seen not only the evolution of the threat, but the Bureau's response to that threat as well. I mean going from a traditional law enforcement agency to much more being on the footing of proactive and preventative with these kind of things. And so talk about how you see it, how we got here in this, this environment that we're in. And then do you agree with the idea that this has sort of been a long time coming maybe?

MR. STEINBACH: So I agree with the administrator and the commissioner's point that it's an evolution. It is very much an evolution of the threat and that evolution is driven by technology. Technology is driving the evolution and it continues to drive the evolution. So when I look at it I bucket it into three paradigms. The first paradigm was 9/11 and going from reactive to proactive. The second paradigm being the Internet and the anonymity of the Internet and all those things that the Internet allow for.

You no longer had to travel and the tripwires that we used with the travel were gone. But we still have the ability with the Internet even though it was anonymous to kind of look towards watering holes where they gathered online. This third paradigm shift, which is where we're at now is social media and smartphones. It has changed the face of the game. It allows for the bad guy like never before to reach into our local communities, to radicalize, to recruit, to operationalize like never before.

So when we look at the tools that are out there now, two things with smartphones and social media, the issues behind them are volume and encryption. Volume and encryption are the new normal, the latest evolution of the threat. Social media is volume, the way the horizontal nature of the social media works. It pushes out and it's not pushing out in hundreds, it's pushing out in thousands

and thousands. And then once you've sort through the volume now you're stuck with an encrypted piece.

I know we don't like to talk about that, we think it will go away, but it's not. The encryption piece is there. Once we sort through volume and it starts with an online anonymous moniker and we drive to and identify as the bad guy, now we're stuck with encryption. So it's not just about being more efficient, it's not about throwing more resources out, it's not about just working harder. It has to be about being more agile, being more adaptive through -- to volume and encryption.

And how do we do that? With tools and training. New tools and new training that are not just the same old thing, but are adaptive and agile -- tools and training to combat volume and to combat the encryption piece.

MR. HARRIS: What if we were to discuss what percentage of cases are we seeing where encryption is creating essentially an insurmountable obstacle to solving a case or getting a breakthrough that stops an attack if you had to quantify it?

MR. STEINBACH: Sure. So it's easy to quantify. So I'll take 2015. So we had about 70 arrests in 2015 -- 70 arrests -- of the 70 arrests, the vast majority of them, if not all of them, had a social media piece to it. And of that, a large portion of them began with an anonymous online moniker. In other words, we started with somebody we didn't know -- @mikesteinbach -- we didn't know who he was, where he was, just an anonymous online moniker who we had to then take from the digital world and move to the physical world so that we could disrupt.

And of that volume a percentage, probably a quarter, were using encrypted communications for operational parts.

MR. HARRIS: Okay. So Bob Griffin, we've been talking a lot about technology and its role in this new environment. You are the career technologist, you're the serial entrepreneur as you describe yourself on the panel. React to some to this too and talk about how you see this

threat environment. You've interacted with law enforcement investigations supporting them, building the tools they need to do these investigations for -- throughout your career.

MR. GRIFFIN: Yeah, I have for a long time. So a couple things. You know, I think as we moved from, you know, nation-state terrorism to kind of market-state terrorism the battle space changed. And I think it's drawing more and more of my clients to that battle space and that's an open area that we're going to have to continue to be focused on. I've watched my clients ask and make requests of us that I've never heard of before.

I mean I get requests not only about, you know, could you come in and help us do things like active shooter training. Can you come in and help us build an intelligence unit. More and more folks are leaving from the IC world and starting to build intelligence units at commercial client basis, whether that's at a city bank or at a retailer or wherever. And they are looking for training around TTPs and how these technology can help, really help and assist.

The power of technology is it can move faster than the speed of threat. You know, the problem with technology though is how quickly can people assimilate what it's telling you. You know, the challenge is it is incredibly not only an enabler both good and bad, to your points, but it's an incredible asset. I had the privilege years ago working with the commissioner when he was at LAPD. You know, he said something that's always stood with me.

He said the power of technology is it can be the second or third person in the vehicle. It can help assist, it can help provide us more capabilities that we can and that we need to take advantage of. I think we've really just started to scratch the surface of what technology can do, especially as we enter the cognitive era around allowing technology to really start to help define and take care of some of the mundane issues that we just can't deal with 24 hours a day, 7 days a week, 365 days out of the year from a human perspective.

You know, the ability to make recommendations to say, gees, you know, I know this person is not necessarily on a watch list currently, but they have been in the past. And from a pattern of life perspective, they just walked into a gun store and bought 250 rounds of whatever. And that's unusual. Maybe somebody ought to pay attention to that, you know. And that's the things that technology and cognitive --

MR. HARRIS: Michael Steinbach, let me get you to respond to that too, because obviously after the Orlando shooting there were a lot of questions that got raised about the shooter in that case and we're maintaining the fact that he had been on a watch list, he'd been investigated a couple of times. I mean can you address this -- both -- I mean not maybe the role that technology could play in it, but from a policy perspective should we be keeping people under some kind of permanent watch that if they have been on a list like this before, they've been investigated, that somebody ought to know when they go and on buy an AR-15?

MR. STEINBACH: So I don't think it's appropriate for me to discuss policy. So we will -- the FBI in conjunction with our JTTF partners and state and locals, we will take the tools, the authorities you give us, and we will go to the extent possible. We will go to -- right to the edge of what those authorities allow and stop. And the case in the world we live in today, that meant going, investigating, closing, and pulling off the watch list.

So if the American public through a Congress decides, hey, we want to keep people on the watch list, we will change our procedures. But we follow the policy and the legal processes that are in place.

MR. HARRIS: In a generic case, if somebody was off a watch list, but there were a way to notify the FBI if that person had bought a certain category of weapons, would that be a helpful tool?

MR. STEINBACH: So I think that you've given a very hypothetical question. So you're asking me somebody's -- we investigate somebody, we determine that this individual does not need a predicate, is no longer a threat to the community, we close him, and now he goes and exercises his right to buy a weapon. Do -- what we do? I think in some cases it may affect, in some cases it won't, but it's a very hypothetical question.

MR. HARRIS: Okay.

MR. STEINBACH: Thank you.

MR. HARRIS: Sure. That's a fair try. This is with journalists too, we love hypotheticals. Administrator Neffenger, I want to ask you the question about -- specific on the transportation system. And I mentioned in the beginning of my remarks that this idea that soon buses would be being hit and these kind of soft targets. I mean we have now 15 years of experience of securing the aviation system, that's what we're all most familiar with, that's how we interact with DHS and TSA on a most regular basis.

When does this threat though migrate into the buses, the subways? How concerned are you about that and how prepared is both the agency, but also the local jurisdictions to deal with that?

MR. NEFFENGER: Well, first if you look globally it it's in that system already. I mean you had the Madrid train bombings, the London Tube attacks --

MR. HARRIS: Knife attacks, recently --

MR. NEFFENGER: -- knife attacks. We've had bombings in Israel for many years on buses. The Brits dealt with it for many years with the IRA. So it's not as if that's a new thing, but it is -- it would be relatively new in the U.S. I think that there's a couple of things to think about. First of all, it's a very different system as you look at the surface transportation world from the aviation world -- much more open, open by

definition, open by necessity, because it works most effectively.

You could not impose the kind of security in a transit system or a bus system that you do in the aviation world. So that said, how is it approached? I think to some extent there are some lessons we can learn about cooperation and connectivity and sharing of intel and information. It's done very effectively in that surface world.

There are any number of groups that work collectively on a daily basis to -- not only to share information about the tactics, techniques, and procedures and to think about the ways in which those systems could be attacked, exploited, or otherwise taken advantage of, but how you might respond in the incident that they do. Some entities do it better than others, but because no one entity, no one agency, no one police department has all of the capability and the resources it needs to do that, you're sort of forced to work together.

And there's a general recognition that it's a vulnerable system by definition. In the states we still say that the relative threat is low in there -- does mean there's no threat, it just means that there's no specific evidence to suggest that there's anybody out there right now trying to do something. But I worry a lot about this unpredictable nature of things.

And as you see, the Thalys train attack, for example, or the attempt in the Thalys train attack and then some of the other more recent attacks -- I worry that somebody will just look for an opportunity. And I think that it will be challenging to prevent that. The key is that you are prepared to respond and that you keep people aware of the possibility there.

MR. HARRIS: What's your -- go ahead, sir.

MR. BRATTON: Yeah. The idea that there is no capability anywhere in the world on the part of law enforcement or the various state agencies to protect everything, all the time, everywhere, and particularly our

transportation systems that -- New York City subway system carries 6 million riders a day and if we were to screen them with TSA types of systems --

MR. HARRIS: Subway wouldn't run the way it is run.

MR. BRATTON: -- the city would just lock down. Lot of what we try to do in the law enforcement world is the idea of -- with the resources we have, certainly the improved collaboration we have with the JTTFs, as well as -- New York, for example, we really believe we have seamless collaboration with our colleagues. That the idea is to be unpredictable in the sense of -- we have the benefit in New York fortunately with this largest department I had, 36,000 officers.

We have a lot of personnel now who are out there for spontaneous assignment that they will go to this subway station for an hour, they'll go to Times Square for a couple hours. And these will be with the bomb dogs, the vapor wake dogs, the heavily armed officers just moving to some of the more significant potential targets, but also the softer targets, so-called softer targets. We have that capacity and capability. I have almost 2,000 officers that I can use each day that are armed and equipped and trained for that function. Most police departments don't.

So a lot of it has to do with the prevention side, the information, intelligence that the JTTFs provide, that the fusion centers provide, and the scanning of social media, et cetera. The algorithms fortunately are getting stronger and stronger all the time. They can link a lot of this information together. The idea that somebody who was on a watch list goes off the watch list by law -- we can only keep on it for so long -- but then basically pops up buying a firearm.

You put the linkage back together again And so it's a needle in the haystack that you're now focused on. So we're in a world of discovery, in some respects, about how do we use what they're using -- social media,

technology, cyber, and use it to our benefit and to their detriment.

MR. HARRIS: And New York has obviously one of the most sophisticated intelligence organizations in the world. And we're talking -- you're -- many people would regard it on the level of a national intelligence organization and sophistication. Most local jurisdictions don't have that.

MR. BRATTON: That's correct.

MR. HARRIS: So when we're talking about these other itself, we're talking about soft targets everywhere. So I mean -- anybody feel free to respond to this -- but you know, New York is up here, the learning curve for cities is, they're somewhere way down here, places like Dallas, Orlando which may have their own community policing, I doubt have that kind of a sophisticated intelligence operation. So what do they do? How do they get ahead of that?

MR. BRATTON: That's the JTTFs that -- they're in most of the major cities -- that's one layer. You have the fusion centers which are -- they form a JTTF that -- intended to take all streams of information, crime as well as terrorism-related so that -- because we clearly understand that oftentimes we get some of our best intelligence out of crime reports that will give us an avenue into a terrorist potential plot being developed so that -- we've got at this time a lot more than we had before 9/11.

And the sophistication of it, the collaboration levels of it is much more than we had. But clearly as these new threats are morphing and we're going to have to do more of this, there is no denying that, we're going to have to do more.

MR. STEINBACH: Let me --

MR. HARRIS: Sure, please.

MR. STEINBACH: So I think you're asking the wrong question. So I think we struggled over the years to build an information-sharing network that's -- it's pretty good. We've had a lot of bumps and bruises and made a lot of mistakes, but like the commissioner mentioned, through the JTTF, the fusion centers, we're pretty good. The problem now is Europe. So how do we now apply that to the next level? How do we develop the same processes and speed of information-sharing that we developed here in the United States with Europe?

Because as you know -- you've heard the media reports, we've seen the intelligence, it's very easy to get from the Middle East to the Levant, to Europe, to Europe, to United States. So how do we prevent that from happening? How do we look at information-sharing and what is information-sharing? So it's okay that the CIA is sharing great amounts of intelligence with MI6, but if somebody gets on a plane in Dulles and flies to Heathrow and TSA doesn't have the information, is pushed down from the intel agencies to the border control agencies, we're not any good, right?

So the European partners, we have to develop better -- we have to define information-sharing, first of all, what is -- we're talking about high site threat information, we talk about law enforcement, are we talking about border control. Once we define it, we have to develop mechanisms to robustly and quickly share that information faster than the speed of a train or a plane.

MR. HARRIS: So we have the TSA administrator here, so how do we that?

MR. NEFFENGER: Well, I think Mike makes a good point. And we do a really good job in -- domestically at sharing information. And I think commissioner hit it on the head. And you can't overstate how much has changed since 9/11 in terms of the way information is moving, how quickly it moves, and how many layers it moves through in that repetitive. JTTFs are a big reason that that happened and all the fusion centers that they created after that. But where we really break down is right outside our borders.

And from my perspective, this is a global system and anyplace you enter the system you're in the system. We do as good a job as I think we can right now under current -- to at least know who's coming into this country. So in my case if they're coming in by air I'll get passenger name, data, I'll get master crew list data, we'll vet all that, we'll vet that through the various FBI databases and other databases of concern.

But I have great concerns about the entry into the system globally, because it's quite possible to -- even with all of that, you can still have somebody you don't know anything about that's relatively clean that comes into the system, because we don't have, in my opinion, the same sort of sharing globally that we do domestically.

MR. BRATTON: One of the benefits we have in New York -- my predecessor, Ray Kelly, using actually private funding, the police foundation funding, established an overseas liaison program -- 9 to 10 detectives in critical areas around the globe. We've since then expanded that into Australia and several other areas, Europe whole.

Police officers working with police agencies stationed overseas -- Paris, London, Singapore, and Jordan and Israel and Abu Dhabi. The idea being when an event occurs, a terrorist event, that we have the ability to get a detective in there very quickly. So the case of Paris, the incidents in Belgium, that we go in as fast as we can. And relationships we have along with the sharing with the FBI, what they will do, to learn as much as we can about what just happened, what is new about this attack, what can we then bring back into our environment -- and not just the environment in New York because we quickly look to share with our colleagues.

We have a network in 75 major cities, the top counterterrorism intelligence offices. In each of those agencies there is a network that they're able to share information very quickly. So John Miller's overseas liaison people come back with you need to be aware of this element that's new in this terrorist attack, we're able to

disseminate that very quickly into the major cities. And so that's something that has been morphing and expanding.

And you're correct, the European areas, other areas, they have intelligence services, are not collaborating, I don't think as intimately as we've been able to do over the last 15 years here. It was a struggle in the early days to -- from the local police angle to get the federal agencies to understand we're partners. We've got 800,000 sets of eyes and ears that can work with you. But I think we're over that hurdle finally, the Europeans are not. They still have state police agencies, local police agencies, and they're just not oftentimes working together.

MR. HARRIS: Bob Griffin, you want to add to that?

MR. GRIFFIN: And Bill makes a great point. You know, the information-sharing paradigm has been going on -- conversation for years. And you know, in the early days, you know, when you talk about information-sharing people would look at you like you were the green banana, you know, why would I want to share information. The reality is it's table stakes -- we have to share information, and we do. And it's not a technology problem. If content is king and information is king and we all know that, access and distribution is King Kong.

The ability to get that information to the right people, at the right place, at the right time, as close to the edge as possible, this stuff is going to make a major difference. And the folks up here have broken down a lot of those barriers to do that. But to the commissioner's point, there's more to come, there's more to have happened and lot of that's happening now. And it is struggling not based on technology, but based on policy and in some cases based on will.

MR. HARRIS: Commissioner, I want to go back to something you said and then I'm going to put you on the spot here too, so I apologize. But you know, you talk about a country with more guns than people and the prevalence of guns and the ease of buying guns. And

obviously in New York that must be a concern for you. If there were stricter gun control laws, would countering this threat be easier in New York?

MR. BRATTON: It would reduce the potential for it. I've been long -- in the '90s was the face of American policing and a lot of the campaigning we were doing for more significant gun control, not gun abolition, that's not going to happen. It's -- we're a country that is fascinated with our guns, but more meaningful control over who gets them, the ammunition, what type of ammunition. And the great frustration is that we've --are losing that issue and it's resurfaced again in this national election.

It would appear that the Democratic Party is willing, based on all the carnage that was recently experienced, to once again raise the banner and bring it into a national presidential election. And I salute that, because I think we need to have that attention, that visibility, and that discussion.

MR. HARRIS: And it would -- well, people then maybe would take a different position on this, on gun control. And anybody answer -- feel free to answer this. Look at what happened in Nice and say here's an instance where he didn't need a gun. He got behind a truck and he mowed down 80 people, that they're always going to find a way. Is that an argument that, you know, goes against limiting access to guns, because we say they're going to find some way to do it one way or the other?

MR. BRATTON: Well, it's the idea that so much of what happens in the United States is a direct result of guns -- Orlando, Baton Rouge, Dallas. There is a mass murder in the United States every day, four more people everyday and that, you know, the guns is still the leading cause of death in this country. Sure we have couple of million trucks riding around. And certainly ISIS, the use of social media to inspire, get an axe.

Every time they go out with one of those messages, we will see someplace in the world somebody going out and responding to that, whether inspired or

enabled -- the FBI coined the term, I think Director Comey -- inspire, enable, or direct. And we're seeing many, many more inspired now as well as enabled, that are becoming with much more frequency.

MR. HARRIS: Okay. I want to turn to audience questions now. I'm sure you all have many things that you'd like to ask the panel. So please raise your hand if you have a question and the mics will come over to. Yes, right here, sir. There's probably mics on both sides. You got one coming your way right here.

SPEAKER: Thank you. You all mentioned the JTTF and the fusion centers. And one of you mentioned distribution of shared intelligence directly to the edge as quickly as possible. My question is do you regard the FirstNet initiative for -- that's designed to provide interoperable communications to first responders as part of that network of both receiving information and delivering information?

MR. BRATTON: Its intention initially is actually emergencies. FirstNet is the idea of finally having dedicated space for communications, particularly for technology rather then voice. And it's been a very slow process, it's still kind of limping along. It is a source of great frustration. But that's one component of the ability when an event does occur, to be able to have interoperability and that's what it's designed to do -- to ensure we have that the wave, the bandwidth for all of that. But it is not a panacea, if you will.

Certainly the advance over what we had as recently as in the LAPD back in 2009. And so it's a good thing, but it's not happening fast enough. And it's going to prove to be an essential element of everything that we're working on for communication sharing.

MR. HARRIS: There is a hand up in the back here and then we'll go over here to the middle and we'll work our way over.

SPEAKER: Thanks very much. Bill Trillo (phonetic) from Canada. I just want to come back on the

title, "New Normal," because new normal implies there was an old normal. And of course, couple of the experts were real quick to say, well, it's not a new normal. But for our grandchildren it's normal. They become desensitized and it is what they are growing up to be amongst -- death, violence, the challenges of today.

And I'm just wondering as we look ahead a couple decades, the social costs of this in terms of community values, trust, privacy, health implications of everything we're talking about here. What are we seeing now? What are we projecting and? And how do we prepare for the social cost of what is normal for our grandchildren and their children?

MR. HARRIS: Very important question. Who would like to tackle that? It's a big one.

MR. STEINBACH: I'll try. So you're right. First of all the threat is not static, we just stop talking about what was normal. It's an evolving threat, it'll always be evolving. So what's going on today, I guarantee, will not be what's going on in a year or 2 -- 5 years. I think the key to the community piece is making sure that communities, the local governments, and our state and federal governments understand the reasons. We show transparency and the reasons why we do what we do and why we need the tools we need.

Ultimately, it'll be up to our children and grandchildren to decide what tools they are comfortable with providing to law enforcement, to the intelligence community to protect them. So I think that -- I'm not so worried about that. I think as long as we recognize that it's up to them to balance national security versus privacy versus all the other civil liberties that we hold dear and that we make it clear that it's people through our elected officials who decide what tools we will be allowed to use. And going forward with that I have no problem with our children and grandchildren.

MR. HARRIS: Yes, sir, right here in the middle.

SPEAKER: Hi. Brian Zimmer. This question is directed either to the gentleman from TSA or the gentlemen who represents FBI. I presume that you're monitoring the darknet in regard to counterfeit IDs. If so, does it concern you that more and more counterfeit ID vendors are featuring testimonials of people who have successfully gone through TSA using counterfeit IDs?

MR. NEFFENGER: Actually that's a good point. One of the challenges that we face in aviation security, which is what you're talking about, is ensuring that the individual who presents themselves is in fact the person that they claim to be. And that's a lot more challenging than one might think at times. So an ID is one component of that. Another component of that is other verifications that happen as your name gets tumbled. So -- but when you make a reservation for a flight now you go into something called the Secure Flight system and that is a system that bounces your name against databases of interest.

So that's one way in which we begin to look to see whether there is -- this is a name of some concern. Ideally then when you present yourself you present an ID that we try to validate as a real ID, as a valid ID and then we try to connect that to the individual. The challenge right now is that we don't currently have all the systems in place we need to verify the validity of that ID. We've been working very closely with FBI and with vendor, people like Bob and others, to begin to think about how do you -- how you actually ensure yourself that this ID is not a counterfeit and the like.

We're getting much better with that and we've got some pilot systems out there that do that, but it has to be part of a larger system. It doesn't stand by itself. As you know, many of you are used to the -- walking up to the guy who just scribbles all of your boarding pass and he holds your ID underneath an ultraviolet light. That is not the most effective way of determining whether or not somebody's ID is valid. So we have to do -- we're working on additional things.

We're actually working very closely with some of the airlines themselves, because if you think about it

they've got those kiosks everywhere that read IDs. CBP does that. And so I think that what I hope to see over the coming months is a dramatic improvement in our ability to validate, because you point up a very real concern. It's the -- you know, it's a number one issue. You want to find out that the person who presents himself is in fact that person so you can determine whether or not they are somebody of interest or concern.

MR. HARRIS: Just a very quick follow-on to that. How long before -- for average passengers going through TSA is like what it is now with PreCheck or it's just -- you just go through? Is that a goal?

MR. NEFFENGER: Well, there is actually.

MR. HARRIS: No taking off the shoes, no laptops on?

MR. NEFFENGER: You know -- I mean you take off your shoes for a very real reason, as annoying as it is and I recognize that. I mean I was really annoyed by TSA before I became the TSA administrator --

(Laughter)

MR. BRATTON: Now you're just angry.

MR. NEFFENGER: And I'm still kind of annoyed, but it's partly because -- if you think about it -- well, when we have a -- we have a system that's been relatively static for a long time. That's a problem. So it has to evolve and transform. If we had more time, I could talk about what we're doing to really dramatically transform this system. But part of that transformation is in transforming the way we think about individuals moving through. I mean it really is, you do have to do risk-based.

And I -- so I think we're not far -- I believe this -- we're not far from a system where you can do large numbers of people that get relatively little screening. It depends on your willingness to opt into a system. And I think that there are levels of opting in with biometrics

and other things that would enable that. But there's also -- there are also technologies out there and we've been working with the private sector to look at ways to incentivize the private sector in ways that we haven't done before.

And I think that some of that is on TSA to incentivize the private sector to really rapidly develop some of those things that would allow us to keep shoes on and the like. Dogs do that to some extent now. If you haven't signed up for PreCheck, well, shame on you. But if you haven't and you want to go through faster, find a dog and walk past one of those dogs. You won't take your shoes off. You won't pull out your stuff out of your bag, because the real key is to find nonmetallic explosives, and they are very challenging to find as they come through.

MR. STEINBACH: Don't forget though, this is a threat. So we're not talking about something abstract. The bad guys have figured out ways to insert and build stuff that's hardly able to be detected. So I'll take my shoe -- I'll do whatever I have to do to make sure the plane doesn't blow up --

MR. HARRIS: Yeah, these are not arbitrary measures that we're taking --

MR. STEINBACH: No, not -- in fact no --

MR. NEFFENGER: You know, I'm very uncomfortable when I travel overseas that those things aren't being done, because as Mike said, these are -- there's a very real reason, we just -- really not just to annoy you, but it's to keep you safe.

MR. HARRIS: Yeah. Sir, right here. You had your hand up, yeah. Thank you.

SPEAKER: Hi. My name is (inaudible). I'm a reserve officer with the D.C. Police. You know, post Ferguson there was a lot of call, public outcry about the militarization of our police departments. And I think San Bernardino was a case in point about why we need tactical

weapons, tactical abilities in our police departments. But how do we message that with the public in a manner that they become advocates for us to be able to do more than take out a peashooter and try and pick him up with a 9-millimeter handgun?

MR. BRATTON: Well, I think the issue with Ferguson was one of the problems with small police departments is when you have something on a scale of what was going on in Ferguson. We had the mutual aid situation where officers from many different departments with very different levels of training, very different equipment, now come together oftentimes for the first time. And Ferguson is a clear example of what can happen in the sense of what would be arguably inappropriate use of certain equipment, display of equipment. And that is a challenge.

And I think the recent events, however, in Baton Rouge, Dallas and other communities that have been losing an officer here, an officer there, the attacks on officers increasing. When we announced this week all that we're doing to give our officers protection against attacks directed against them or protection when they're going in harm's way to the active shooter or actually the normal shooting call, which is all too common in many cities, that I didn't hear a single objection to that.

Maybe with the understanding of why we were doing it and the training we were going to apply to use it appropriately, use it in a way that it's not seen as a militarization of the police, but a reflection of the reality of what our police are up against today. So it's the constant trying to find balance. And Ferguson's would -- way out of balance. Recent events -- terrorism issues, attacks against police -- bringing it back more into balance.

Challenge for us, government and police is to what we acquire, use it appropriately, train appropriately, and your comment -- explain it appropriately as to what we have it for and to use it for those purposes only.

MR. HARRIS: Great. That's the end of the panel. Thank you all for being here, for sharing your insights, and thank you for the work that you're doing. Thank you.

* * * * *