Center for Strategic and International Studies (CSIS)

“The Evolving Terrorist Threat and the Importance of Intelligence to Protect the Homeland”

Panel: Homeland Security Intelligence Analytic Tradecraft

Moderator:
Shane Harris,
Writer,
Washingtonian

Speakers:
Mark Lowenthal,
President,
Intelligence & Security Academy

Phil Mudd,
Senior Global Adviser,
Oxford Analytica

Tracy Reinhold,
Assistant Director, Directorate of Intelligence,
FBI

Caryn Wagner,
Undersecretary for Intelligence and Analysis,
Department of Homeland Security

Location: Washington, D.C.

Time: 3:00 p.m. EDT
Date: Wednesday, September 7, 2011

Transcript by
Federal News Service
Washington, D.C.
LAURA MANNING JOHNSON: Good afternoon. It is my honor to get to introduce the people who are going to talk on this panel because there is more talent for analytic ability sitting on this table. And it’s not just the analysis. It’s also these people have not only been the people in their cadre that rose to the top because of their analytic abilities but also for their management skills and their oversight of many, many, many different projects.

So it’s my great pleasure to start by introducing Caryn Wagner. Caryn Wagner is currently the undersecretary for homeland security intelligence and analysis. She started there in 2010. Before that she was on the House Permanent Select Committee on Intelligence. She managed two different things there, almost completely disaggregated. She was the budget director, at the same time being the cybersecurity coordinator.

To her left is – I mean – yes, to her left is Tracy Reinhold, who is the assistant director for the FBI Directorate of Intelligence. He is a 20-plus year veteran of the FBI. He’s held many different positions to include being the director’s special assistant. And last but not least, he is a Marine.

To his left is Phil Mudd. Phil Mudd is currently the senior global advisor for Oxford Analytics (sic). He is a career CIA veteran. He was there for over 10 years and then made one of the most unusual jumps for somebody before 9/11 but an understandable jump now. He went to the FBI to be the deputy director of the national security branch and started that transition of intelligence and law enforcement. He went back to the agency and then went back as a senior intelligence analyst.

To his left is Mark Lowenthal. He is currently the president of Intelligence and Security Academic – Academy. He was the assistant DCI for analysis and production when he was in the agency. Then he went to be Deputy Assistant Secretary for Intelligence. He went to the Congress to be the staff director for the HPSI and as we all know he is the author of “Intelligence: From Secrets to Policy,” which has taught a generation of college students about what that analysis is.

And the moderator for your panel today, I’d like to introduce you to Shane Harris. He’s a writer for the Washingtonian magazine. He also has written a book called “The Watchers,” which was a book about national security professionals and how they did their job and what they did, which is now on my personal reading list. And he has won many awards to include the Gerald Ford Prize for Distinguished Performance.

SHANE HARRIS: Great. Thank you very much. And thank you all for being here. So our task today is to get at the issues of analytic tradecraft for homeland security intelligence. And what I hope to do in the course of this discussion is at least a couple of things at the high level.
One is to better understand what we mean when we say homeland security intelligence, how it’s different from other kinds of intelligence and really how you – what the tradecraft of that looks like. And we’re very fortunate that we have four people here who’ve been practitioners in this field, sometimes in the name of homeland security intelligence but really have been doing it for their entire careers even when it might have been called something different.

So what we’re going to do to start is the panelists will give some brief opening remarks. And then we’re going to move into a question-and-answer period. It’s important that we get feedback also from you all. So there are folks circulating through the audience that have cards on which you can write questions and then those will come up to us and we will make sure we leave plenty of time for your questions at the end of the session which will stop at around 4:15.

So I’m going to turn this over first to Caryn Wagner for some opening remarks and then we will go down with the other panelists.

CARYN WAGNER: Thank you very much. I was actually still looking around the audience and picking out old friends so – which is nice. I’m happy to be here to talk about this topic. I think we’re going to have a pretty lively conversation based on my knowledge of my co-panelists. I hope that’s the case. I just want to say a few short things. I want to try just to hit the wave tops and provide some hooks because I think it would be better to do more discussion.

As was mentioned, I head up intelligence and analysis within DHS. We – you know, it’s a new department. I&A is a relatively new office. We’re a little younger than the department itself since we’ve morphed several times since the department was formed. Probably only been more or less as we are now for the last four or five years. Just to let you know what we’re all about, our primary focus is on information sharing and on information sharing, a two-way flow.

We provide information to state and local law enforcement, to the private sector, to other non-Title 50 members of the federal government. We support the components of our own department. We do do some original analysis but we don’t do a lot of that. We try to focus on the homeland nexus and we try to tailor other people’s stuff, augment other people’s stuff, downgrade and declassify and push it out so that it’s actionable.

And another important mission that I have as the chief intelligence officer of the department as well as being the head of I&A is to try to integrate the intelligence efforts of the other components of the department. Together they’re a pretty capable and powerful bunch. And so, a lot of what I say today will be focused on the DHS intelligence enterprise which is the sum of all of those activities rather than just on I&A.

But just I want to share our mission statement with you because I think it does define what we’re all about. And we say that our mission is to equip the homeland security enterprise with the intelligence and information it needs to keep the homeland safe, secure and resilient.

The enterprise is big. It comprises all those people that I just mentioned plus an alert and engaged American public. And it’s about intelligence and information and it’s not just about CT
because the department’s mission is obviously a lot broader than that – keeping the nation safe, secure and resilient.

So that’s what we’re all about. I did want to comment on the proposed definition of homeland security in the INSA report that was released today – information that upon examination is determined to have value in assisting federal, state and local and tribal and private sector decision-makers in identifying or mitigating threats residing principally within U.S. borders.

And I don’t – I don’t necessarily disagree with that definition. But the one thing I thought I would point out is that we’re concerned about threats to the homeland that emanate from overseas. So and we work those issues closely with our partners at NCTC and CIA and NSA. We’re also very concerned about homegrown and domestic threats to the homeland. We work those in very close partnership with our colleagues at the FBI.

But the one thing that might maybe get lost a little bit in this definition is DHS’s unique role at the intersection of overseas and domestic, the borders, what we call sometimes the transit zone. That is sort of the department’s bread and butter, and it’s one of the things that – one of the main things that we do for the American public which is facilitating the free flow of legitimate goods and services while trying to safeguard our virtual and physical borders. And this analogy works pretty well for cyber too actually as well as the physical world.

What we do is use IC information to help keep out people who would do us harm at the same time as, again, letting the free flow of goods and services happen. And then we collect a lot of information in the course of those encounters at our physical and virtual borders that we then share in a way that is appropriate with privacy and civil rights and civil liberties with the intelligence community and law enforcement to allow them to use that for intelligence and law enforcement purposes.

So that key border element, I think, is very central to what the department does and that’s the one thing that I think may get lost a little bit in the definition.

There is – data is central to what the department does. We have a lot of it. We try to analyze it in new and better ways. We share it with our partners. We’re working on getting new sources of data with our partners. Again, the Department of Justice and the FBI – through things like the National Suspicious Activity Reporting Initiative, the secretary’s “See Something, Say Something” campaign.

We are also sending reports officers out to the fusion centers to work with them on information that they have, things that they know that they don’t have the time necessarily to sit down and write a report on, to share it more broadly, to make sure that that happens.

And we’re also trying to figure out new and better ways to present data, geospatially where that makes sense, and across the whole range of our mission areas. There is a lot of art to producing largely unclassified intelligence. I won’t go into all of that now because I anticipate that that will come up in the Q&A session. And we’ll talk a lot about that.
But there is also – so there’s some art forms there. There are some new forms of tradecraft that I think we need to think through. And the other thing is we are making, I think, new progress and new – sort of breaking new ground in terms of collaboration and coordination in the community, particularly in how we work together with FBI and NCTC to try to prevent – present a unified threat message from Washington to the field.

And while I think it’s far from perfect at this point, we’ve made a lot of progress. And I think that’s something that we owe to our customers. That is in and of itself an art form on how you do that in a way that maintains the freshness of the information and does the job while protecting, again, investigations and sources and methods. So I’ll stop with that and turn it over to Tracy.

MR. HARRIS: OK, great. Tracy, please go ahead.

TRACY REINHOLD: Great, thank you very much. A couple of things, as Caryn alluded to, I am responsible for all intelligence activities in the FBI. And the uniqueness of our situation is that we have sort of a bifurcated mission between law enforcement and national security.

So in order to accomplish both of those missions we have to utilize the intelligence apparatus of the FBI to effectively gather and collect and analyze and disseminate information that provides the opportunity for our operational counterparts to address the most significant threats facing the country.

It’s not enough for us to collect information or intelligence through the utilization of HUMINT or through the analysis of SIGINT or other sorts of INTs. It is more important that what we do collect and disseminate is relevant to the customers that we’re looking to affect. So the very best analytic product, if it doesn’t resonate with the workforce that we’re charged with mitigating threat, is irrelevant.

So one of our big challenges in the FBI as well as the intel community is to ensure that the information that we discern from variable sources is actionable and that it resonates with those operational entities either within the FBI or other parts of law enforcement or the intel community who are responsible for mitigating the threat. In order to do that, we have about 3,000 analysts that are assigned all over the world.

The vast majority of them are either here at headquarters or in our 56 field offices across the United States. We also have intelligence analysts assigned to some of our legal attaché offices abroad to ensure the free flow of information from our international partners back into the continental United States.

I think Caryn hit on it when she talked about the definition of homeland security intelligence when she talked about the difference between threats that emanate overseas and our ability to mitigate those threats before they manifest themselves here in this country. In order to
do that we have to have the ability to collect the information from disparate sources, analyze it and disseminate it as quickly as possible.

I will tell you that the FBI, just like DHS, is incapable of doing this alone. It is a collaborative effort that involves all members of the USIC as well as our 18,000 state, local and tribal law enforcement partners across the country. I will save going through the details of what we do on a day-to-day basis and the definitions of analytic tradecraft for hopefully the Q&A session that goes forward. As Caryn said, that’s the wave tops of what we do for a living. With that, Phil, I will turn it over to you.

PHILIP MUDD: Thanks. We sort of got this backwards, which is why we’re here today and why we’re struggling with this so much. When I grew up as an analyst at CIA, let’s say you’re looking at something like the Iranian nuclear program.

That’s an overseas program where access is limited. The information you’re going to gain is highly classified, at a minimum at a secret level and probably at the top secret level. The customer is at the national level within the Beltway, sort of a vertical customer; that is, going from a place like CIA up to the Oval Office at the White House.

The delivery is going to be sort of a paper product, especially in the most sensitive products that we have. And you’re going to focus, to be blunt, on collection first and civil liberties second. I’m not that concerned about an Iranian scientist’s access to a court in the United States to argue why we didn’t have a reason to put a HUMINT source next to him. So we go to the domestic environment.

Obviously that’s largely within the United States, although as Caryn said there has to be a lot of overlap in the age of globalization. Classification should start at the unclassified level, maybe at the FOUO level and not the reverse. The customer is typically outside the Beltway.

It’s everybody from Disney security after Mumbai, what just happened and what can you tell me, to a police chief to a homeland security advisor. The delivery is almost by definition not going to be paper. And it’s also going to be accessible to an adversary. I’d say BlackBerries. I was going to say Palm Pilots but I think they’re kind of toast. (Laughter.)

And you know, one of the great values of the purple program that the DNI has is people like me who thought foreign intelligence was like domestic intelligence, go to the bureau and realize that common word “intelligence” is really misleading. Civil liberties come first and collection doesn’t. So you go to a case like Mumbai and my view would be, OK, I need a product within 24 hours.

It goes to Disney security. Based on analysis by people like security experts, structural experts saying, here’s a graphic of what just happened, how they breached the walls, what happened on the inside, why Indian security had such problems with the people who got into that building but nothing to do with top secret information about what we were intercepting from the cell, et cetera.
The problem is that people who grew up in the first system are the people who helped oversee the second – people like me. And so as we look forward, and I’ll close here, I think you have to understand the requirement has to be – some of the language is the same.

The requirement has to be set by the customer. Intelligence is simply information that helps you understand a problem. It ain’t secrets. If you go to New York, intelligence is Zagat’s, where do I eat. And I’m not kidding. So intelligence for Mumbai is – for the Las Vegas police chief or for Disney is what just happened in that facility. CIA, NCTC, you can do the cell.

I want to know what happened to the facility and how I might mitigate the threat to the physical environment that I have to deal with. It ought to be delivered on a BlackBerry. It ought to start out at the unclassified level. The analyst might not be a terrorism analyst. It might be a structural analyst. Civil liberties are primary. In other words, if we are looking at human activity in the United States, the first question is what should we do, not what can we do.

Again, as an intelligence professional I can’t tell you the significance of that difference. But we have to sort of think of every category that I grew up with differently and we have to grow people like Caryn who start as homeland security professionals. I said homeland security. I didn’t say homeland intelligence.

I don’t like using intelligence on the homeland because intelligence is pursuing information, not starting out with civil liberties. Homeland security professionals have to grow up in an environment as I did with – at CIA that starts with domestic, no classification, the customer is outside the Beltway. The delivery is not paper. The delivery is on a device that’s probably accessible by an adversary. And the first question you have is what’s right to do in this country. That’s it.

MARK LOWENTHAL: I recommend the Second Avenue Deli. (Laughter.) Except it’s on Third Avenue – it’s on Third and 33rd but you’ll like it. So much for the Zagat’s. Whenever we – in my company whenever we’re teaching a course on the intelligence community and we discuss the definition of intelligence in the FERPA (ph), national intelligence is defined as foreign, domestic and homeland. And inevitably – this happened to me yesterday at INSCOM – somebody says, I’m sorry, what’s the difference between domestic and homeland.

And the answer is yes, because it’s not defined anywhere in the law. So I think I want to agree with Caryn here that I think the INSA paper does a tremendous service in at least trying to attempt to define in a practical sense what we mean by homeland intelligence as opposed to the other types of intelligence.

But this does underlie the basic problem that I think we still have despite having been at this for almost 10 years and that is what is it we mean by homeland security intelligence and what do you do with it. How do you do it functionally? How do you do it as an analytic tradecraft? We do a lot of courses in my company for a mixed audience of first responders and federal homeland security officers of various agencies.
And they are still to my amazement very separate communities. They know each other exist. They’re not carrying around stereotypes of each other anymore. They know that each side is a bunch of nice guys and girls. But they still are in many respects totally separate communities. And I find that a little bit disturbing at this point in this story.

As for info sharing, some of you will remember George Aiken, who was this Republican senator from Vermont during the ’60s and ’70s. And during the depths of the Vietnam War he said, let’s declare victory and go home. Well, I think that’s what it’s time to do with information sharing – declare victory. We got it. And we got it about as good as we’re going to get it.

But to constantly flog this issue and to suggest that, well, if we just have 100 percent perfection, no bad things will happen anymore is absolutely ludicrous. But that is part of the way the conversation goes.

And the thing that worries me most about this in terms of analytical tradecraft is that I think this really begins to breed risk aversion in the analysts because the analysts become so concerned that I haven’t seen everything that I better not file the report because God forbid I miss that one cable that has the variant spelling of Abdulmutallab that would have told me everything I needed to know.

I better keep reading. And I thought it was fascinating that in the aftermath of the Detroit underwear bombing attempt the solution was put more data in the database. I thought at a certain point that had become the problem. But that seems to be the recurrent solution. And that’s not the solution. I really think we need to declare victory on information sharing and move on to something else. Because as Caryn said, I think we’ve got that. What we don’t have is the doctrine for homeland security. What is it really about?

And it seems very often to be don’t let bad things happen. That’s hardly a compelling analytical doctrine. And so we still have to work on what it means to do effective, efficient homeland security. And part of this goes back to something that Suzanne Spalding said during the last panel. We are not going to manage risk avoidance. We’re going to have to do risk management. I thought it was wonderful when Jim Clapper was testifying in front of the Senate committee for his confirmation and Senator Feinstein was back on the information sharing and the Detroit thing again.

And she said, so we’re not going to have any more of those right? And Jim said, well, if that’s the standard, let’s just quit now. And this is the problem is we keep chasing this nirvana, that we can reach this perfect state which will somehow magically bring us back to the morning of September the 10th, 2001. And let me assure you we’re not going back there anymore. The past is a foreign country.

So I think we’ve made some progress in the immigration sharing. We’ve made progress in hiring a bunch of people who I think have pretty good capabilities, beyond the fact that they can’t write very well, which they can’t because they spend all their day doing this, which leads to a sort of Tanto-esque prose – “me here, where you.” (Laughter.) “Eat soon.”
And I see this in my students at Hopkins which is very appalling. But we still have to figure out the doctrine. What does it mean to do really good homeland security analysis and how do you then distribute that, as Caryn said, just to the people who need to know it in a timely fashion so that they will understand what they are reading. So we’re closer but we still have some work to do.

MR. HARRIS: OK, great. Very good opening remarks, Mark. I wish you could have been more provocative, but –

MR. LOWENTHAL: I try.

MR. HARRIS: Maybe in the Q&A. You actually have a great setup for I think where I want to go with my first question and that is to really get into it and some of it involves tradecraft and hopefully we can understand what the state of tradecraft is. We have had a number of near-misses, if you want to call them that, in the past few years. We’ve had the printer cartridge blowup. We’ve had the Times Square plot, the New York subway plot, Christmas Day 2009 – you teed up for that very nicely.

There was a lot of after-action assessment and a lot of looking at what happened. And that was obviously mandated by the White House but I take it that throughout the committee – community, sorry – there was a lot of let’s look at this event and what can we learn from it. So I want to ask about what the lessons learned from that were. What did we get right? What did we get wrong?

And what did, you know, you all as practitioners learn about the tradecraft? Because it strikes me that this goes to the definition that you were talking about with homeland security intelligence – threat emanating from abroad, it comes here, it’s now your responsibility. So talk about that event then and what we have learned or are beginning to learn.

MS. WAGNER: OK. Well, I’ll talk about it from the department’s perspective probably as much as from the intelligence community’s and let Tracy sort of fill in some of the from the FBI perspective. From the department’s perspective, which is really an operational perspective, one of the – some of the interesting things we learned was how we respond to ongoing events of this type when you don’t know if it’s the only one.

And you know, this is a common – a common theme when you see – you know, you’ve seen al-Qaida in the past has had a habit of doing two or three near simultaneous kinds of activities. You never quite know whether you’ve got one or more.

The department had to do a lot of soul searching there to figure out what’s the best way operationally to respond to that and we’ve made it – we’ve made a lot of changes in how we – how we look to the intelligence community to support us in an active, ongoing operational response.

One of the analogies that our deputy secretary likes to use is – for those of you that are military or former military – the “supporting paradigm.” In that kind of a, you know – some
potentially more planes in the air, what – how do we make sure that the intelligence community is focused on DHS as being the supported command and figuring out how to quickly and rapidly feed them anything that they might need to know to manage the ongoing operational scenario.

So we’ve been having those conversations over the last, you know, year or two on how do we do that better. How do we implement sort of quick-reaction capabilities to make sure that TSA, you know, who’s the truly supported command here is getting all of that focus on it and helping it manage the response. So I would say from the department’s perspective that was the number one most interesting lesson learned. And it was new to me as an intelligence professional operating in that environment.

MR. HARRIS: And then as just a follow-up, do you find that it was – the support was where you needed it to be or it was not optimal?

MS. WAGNER: It was – I think that based on how little we knew about this, that I think the support was as good as it probably could have been but it was a new mindset for the community to think about, well gosh, we immediately convened a SIVITS (ph) but the people that were actually running the immediate crisis weren’t on it necessarily.

So those are the kinds of things that we’ve now learned I think to do better and I would say that the connections between the operating elements of the department who need that intelligence focused upon them and the rest of the community have gotten steadily stronger. So I think, yes.

MR. HARRIS: Is it safe to say – and anybody can answer this – that that event was the first big test in terms of how close it actually came and the fact that the threat was nearly – you know, the first big test that we’ve had since how 9/11 of how this entire system functions together or have there been others that have been more or equally instructive?

MR. MUDD: No way, man. No way. I mean, we sat there – when I went back to the agency from the White House in January of 2002 dealing with the threat SIVITS and that was a creaky machine. The real test was in nine years – and what I took away, one of the things I took away from Abdulmutallab, in nine years nothing significant has happened.

And you know, sitting at the threat table for nine years with Director Mueller and Director Tenet, neither of whom is a low energy dude, and you’re dealing with – I’d say in the matrix. I see all this TV crap. There’s probably, I don’t know, 10, 15 a day or something. It’s not50. But you’re tested every day. So we missed one.

What I learned, and I’ll close here, is that in these debates that we’re hearing, and I guess some of this is on TV tonight, you know, should we start pulling away from the war on terror, this country is still so brittle after 10 years of success that one mistake and everybody is going to say, you guys suck. And here’s whose head is going to roll. Unbelievable.

MR. HARRIS: Well, how do you –
MR. LOWENTHAL: Three other lessons learned –

MR. HARRIS: Yeah, and then I want to ask about how you manage that expectation, by the way.

MR. LOWENTHAL: Number one, the enemy has a will of his own. I’m sorry. But he gets to decide where he engages from time to time. And like Phil said, you know, sure, OK, we’ll declare the war on terror is over. Somebody better tell the other guy. (Laughter.) Because if he doesn’t agree that the war on terror is over, you’ve still got a war on terror.

The second – the second lesson learned is they’re still fixated with airplanes. They’re absolutely fixated. They are not that brilliant. (Laughter.) No, I’m serious. They are absolutely fixated with aircraft, which is a good thing. I mean, you don’t want to lose an aircraft. I spend a lot of time in them. I want them all to land safely. But it helps localize the threat. The other lesson learned from both Detroit and the Times Square event is we have an increasingly vigilant, lawful public.

Public citizens in Times Square said to the cops, we’ve got a problem. This car shouldn’t be here and it’s smoking. And on the aircraft the pummeled the you-know-what out of Abdulmutallab. They didn’t lynch him. They didn’t kill him. But they disabled him and that is one of the things that you want to have happen in a war against terrorists, which is a good thing. So I think those are the lessons learned from that.

MR. REINHOLD: A couple of comments –

MR. HARRIS: Sure.

MR. REINHOLD: I think, getting back to your original question, is that what did the Mutallab attack teach us. I think that we all agree that the FBI is incredibly good at hunting what we know. So give us a bad guy, right? And we use Shahzad as an example, right? Fifty-two hours I think is what Commissioner Kelly said, right, soup to nuts. We knew everything about the guy. What reinforces though is that we need to get better at getting ahead of the threat, whether it is through our liaison with foreign intelligence services or whether it is here in the domestic United States.

Our ability to get ahead of those threats through the utilization of tripwires and that gives us the indication that we have problems emerging. You contrast the issue in New York, the Shahzad case, with the recent issue down in Lubbock, Texas.

That’s an instance where tripwires work, where we are able to get ahead of the 4threat. It doesn’t get nearly the media that Shahzad gets for obvious reasons. But to me there are literally hundreds of those success stories that never meet – that never meet the media threshold. And I think that is probably the most indicative sign of the process that the U.S. government has made since 9/11.
And I think Phil hit the nail right on the head. You know, I spend every morning with the
director of the FBI and you’re right, definitely not a low energy guy. And still a prosecutor. He
will drill into the issue like nobody you know. But I will tell you right now that every morning
the volume of threat information that we look at every day and the fact that this stuff doesn’t hit
the radar screen is a testament to the collaborative effort of the USIC and getting ahead of those
threats.

It’s about retraining our 800,000 state and local and tribal law enforcement officers to
think proactively how do we get ahead of the threat, not what do we do once it happens. And I
think that they all have gotten this message from the federal level down to the tribal level.
Everybody understands that and everybody is engaged in what I like to call as law enforcement
INT.

So how do we train our state, local and tribal law enforcement officers to be intelligence
collectors because at the end of the day that is the tip of the spear, the guy that is on patrol that
afternoon who knows that he needs to look for signs that are indicative of something bad going
to happen and takes proactive action to keep that from reaching fruition. And I think that that
reinforces what it is that the transformation that the government has made since 9/11.

MR. HARRIS: Mark, let me ask you, then. You train people for a living is what you do.
You’re an educator. So how do you train – I mean, and we’ve heard lots of people say that this
has to be done down to the front-line levels. Do they get it yet? I mean, has that mission –

MR. LOWENTHAL: Who’s the they?

MR. HARRIS: The people at the front-line levels. I mean, do local law enforcement
understand truly where they fit in this entire enterprise or is it –

MR. LOWENTHAL: Not entirely. In my experience, not entirely because there’s still a
disjunction between them and the FBI and DHS and the other entities, not because anybody’s not
doing their job but they are two different cultures and they speak variants of the same language.
It’s like, you know, British English and American English. You know, the second floor and the
first floor ain’t the same thing in both places. And so that’s part of it.

And part of it also is that, like, we have not been successfully attacked in 10 years. This
is a good thing, as Phil said. It’s very hard for the state and locals to keep a lot of people doing
terrorism when there’s nothing happening. They want to go back and do crimes.

They want to keep the crime level down. And so they get pulled away and they rotate
people in and out. And so they don’t have a cadre the way Caryn has a cadre and the way Tracy
has a cadre because that’s not how their system works. Now, up in New York you can get away
with this.

MS. WAGNER: I want to disagree with you on that.
MR. LOWENTHAL: Because Dave Cohen has enough people. But I just notice too many people going in and out, in and out or having too many other distractions for wholly legitimate reasons because of what they do for a living. If you’re on the, you know, state or local police, you’ve got other things you’ve got to do.

MS. WAGNER: May I give another perspective?

MR. HARRIS: Yes, please.

MR. LOWENTHAL: And now for a different point of view, please.

MS. WAGNER: (Chuckles.) So well, I think that we have – I’m not sure that’s completely true. I think maybe that was true and I would have certainly welcomed Tracy’s view on this.

But I think that we have made – that’s one area where we have made significant progress in the last few years is working very closely with state and local law enforcement, particularly through the fusion centers in the states and the major urban areas to make – to clarify sort of their role as part of the extended homeland security enterprise and to – it to empower them to – we look upon them as being part of our network.

And we want them to create their own network within their states and their urban areas through programs like the terrorism liaison officer program which is something that is being used more widely so that they bring in people, train them and then send them back out to the local sheriff’s office and the local police department. And so that we’ve got – we’ve done a lot of training. We’ve done a lot of outreach. We have conferences.

We jointly – DHS and FBI and NCTC – spend a lot of time. And I honestly believe that if we were to go out and ask them right now if they felt like they understood their role, I think that we would – they would mostly say yes. You’re not going to get 100 percent certainty because we’ve got a lot of different, you know, levels of maturity and personalities and everything else.

MR. LOWENTHAL: Right.

MS. WAGNER: But I think we’ve – I really think that that’s a nut that we’ve pretty much cracked.

MR. LOWENTHAL: No, I don’t disagree with you. They have – we have made progress.

MS. WAGNER: And I would love for Tracy’s view.

MR. LOWENTHAL: No, I’m not saying that there has been absolutely no progress. But I think the state and locals are finding it harder and harder to stay on this in the absence of an event. For example, when so many states are consumed by natural disasters and it’s sometimes
the same people. I mean, state police forces, local police forces ain’t that big. So a lot of people—

MR. REINHOLD: Well, let me ask a – go ahead and I’ll ask a question.

MR. LOWENTHAL: – get pulled in many directions. They’re going to defer to – Tip O’Neill was right. All politics is local at the end of the day. And so a lot of these people just find it hard to hold on to this other mission which is of concern but not as compelling as something that’s actually happening in your locality.

MS. WAGNER: But there’s a surprising amount of commitment.

MR. REINHOLD: Yeah. So let me just – one of the things that you said sort of made me kind of chuckle a little bit about the cadre of resources that the FBI has at its disposal. First, let’s put this into perspective. We have 56 field offices. If I am in Biloxi, Mississippi, the cadre that you speak of is tiny. So without the relationship that we have with our state and local partners, those are part of that cadre. There is – we don’t make a distinction.

We’ve got 102 joint terrorism task forces across this country that are comprised mostly of state and local law enforcement officers who have been secunded to the FBI to address this mission. We also have the same relationship with the state fusion centers and with our field intelligence groups where we leverage the local and municipal police officers and their sworn and non-sworn members to make sure that we get that message out.

So if I am in a resident agency in a small town where I have three FBI agents, if I don’t have the relationship with my state and local partners, there is no way that I can keep touch with the threats that emanate there. So what makes this work is that it’s not counterterrorism-centric. The FBI’s mission crosses both criminal and national security. And one of the challenges that we have is this cross-programmatic look at threat.

So if a threat – so I’ll give you a quick example. If the Sinaloa drug cartel is moving narcotics up into Middle America and they’re using Somali street gangs to disseminate those drugs for them, it’s not much of a stretch to talk about what’s about the rest of the Somali population in that AOR – area of responsibility – and what sort of penetration do we have for that community to determine whether or not there’s a threat because you’re right. Everything is local and guess who has the best contact there?

MR. LOWENTHAL: Mm-hmm. (Affirmative.)

MR. REINHOLD: So it’s that collaboration between state, local and federal that allows us that visibility into a threat community to determine whether it actually exists or not. And I think that the fact that there hasn’t been a significant issue since 9/11 is not a fluke. It is through that collaboration and through the training and the partnership that we have across the country that has allowed us to at least keep at bay the threat that faces us. I’m not saying that it’s perfect.
And I think, Phil, you hit it earlier. There have been near misses. There have been issues abroad against U.S. interests. But at the end of the day, I will stack the partnerships that we have up today against anything we had. Having worked these issues before 9/11 it is a night and day difference out there, the relationships that exist today versus the relationships that existed pre-9/11, understanding that the FBI has, you know, been involved in state and local law enforcement since we began in 1909.

But the relationship has morphed post-9/11 and I think that it has made us a better organization and it has made the community safer.

MR. HARRIS: Well, I want to ask a question to Phil, then, to follow on this. Let’s say I’m a local police officer in Topeka, Kansas, and I see something suspicious that I think might be related to terrorism. Am I calling you at the FBI first or am I calling Caryn at the DHS first? I mean, on a practical level, where is the interface? Where does that data get gathered up at that very granular level and how does it move and then eventually get to the people who need to act on it? And does it matter who they call first?

MR. MUDD: My judgment is that’s an investigative issue and I would call JTTF. You’re seeing – you’re seeing – you’re not just seeing suspicious activity. To me, you’re seeing something a step above that. And the JTTF has a classic responsibility to deal with it. They also have state and local representatives so you can get what Tracy was talking about, the interface. I would argue that you’re making this a little too black and white.

If I’m sitting at the table, one of the questions you’re asking is what kind of activity do we see and do we have to put out a bulletin to other state and locals. That’s going to be a joint DHS/FBI, maybe even NCTC bulletin that says, here’s what we’re seeing. You know, we’re seeing alterations in gas canisters. So to me, you know, you have an investigative responsibility that has to mitigate threat. The first question you have is security of people.

So I want to mitigate that threat immediately. I want to get somebody on that and figure out if we’ve got to take this guy off the street. But I also have responsibilities in terms of fusing. Do we see this kind of threat elsewhere in terms of informing? So I’m not sure I see the world that black and white.

MR. HARRIS: OK. Let me bring it up a bit with a question from the audience. Someone points out that a lot of this discussion has been about operations and reaction about tactical issues. This person wants to know what has this type of work that we’re talking about done to affect strategic and national intelligence analytic tradecraft capabilities. Does anybody want to take it? And you know, it’s a broad question obviously but –

MR. MUDD: Let me take a quick shot.

MR. HARRIS: Yeah. Go ahead.

MR. MUDD: When we’re sitting at the threat table in about – I’m going to back to – shoot, I don’t remember – maybe ’06 or ’07 or so. We knew we had a fundraising problem for
Shabab in this country. It’s pretty interesting investigative work. I thought it was actually brilliant. The question that came up over time was your responsibility is to ensure that you’re preventive. The quality of your investigation of Somali fundraising for Shabab in this country is nice.

The real question is, as Tracy would say, why didn’t you know that there was also some recruitment that led to kids, now several dozen, who went to Mogadishu? So you know, I think one of the real changes has been expectations.

And some of them are subtle because people will say at the same time, well, make sure you don’t spy on us but make sure nothing bad ever happens. That’s pretty cool. I would go to that example as one of the classics that explains or that really characterizes some of how expectations and changes have happened. Why didn’t you know?

MS. WAGNER: Can I add to that?

MR. HARRIS: Yeah, please.

MS. WAGNER: One of the things that I think is different that we do that I find is sort of spreading a little bit is that, as Tracy said, the point of the stuff that we point out is it has to be actionable. It has to be useful. It has to help law enforcement or the private sector plan on where they’re going to allocate their resources, what kind of countermeasures they’re going to pay for or employ. There has to be a so what to it. So every product that we put out does that.

But that’s not necessarily the norm for the rest of the intelligence community’s analytic products. But as we team more with – particularly with NCTC but we’ve even done a joint seal product with the CIA which I’m pretty proud of – only one, but it was col. But it was – we blended those two things of OK, what’s the threat here and now what are we telling people that we can or should do about it. It was a new thought process. And I think people are starting – the point Phil makes is very valid.

People are starting to take it to that next level, the so-what and dig – it’s not just why didn’t you know but why don’t you dig a little deeper and maybe ask some of the other people like the fusion centers or the folks that are out even in the communities about is there more to this.

And one of the – we’re actually learning some interesting techniques from the production that’s coming out of the fusion centers themselves, some of which are producing some really interesting products that are combining national information and local information with a strong nexus to, you know, why should my local law enforcement care and what should I do about this. So I think that is a change.

MR. REINHOLD: It’s the same from a little bit of a higher level. If we have 56 field offices, if the country decides AQAP is a significant threat to the homeland, so if an office wants to tell me, we don’t have that threat, the first question going back to what you said is, well, how do you know that? How do we establish the methodology from a national perspective that
allows our mitigation centers, our 56 field offices, our 72 fusion centers to say, I know definitively I don’t have this threat.

So what we’ve done is, you know, historically we’ve been very reactive in nature. So now what we want to do is, well, look at the demographics. Look at your critical infrastructure. Look at your – the issues that you have in your area of responsibility and then come back and tell me this is why I know I don’t have this.

This is why I know this is not a threat or this is a threat but I am unfamiliar with it and now I need to take action that then informs the national picture about what the posture is of this country to collect against a specific threat. It’s one thing to say you have an AQAP threat.

The bigger question is that’s great. Now, how are you going to collect against it? Where are your population centers? Where are your specific targets of interest? If we have airplane threats, for lack of a better term, what are the areas that we need to look at? Which agency is best postured to collect against that collectively and then bringing that back in for a national collection strategy that tells us, you know, we send this out and it tells us from our 56 nodes that we have these pockets of the population.

So if you’ve got 6,200 Yemenis in your little town, the next question if what do you know about them. Are we utilizing madrasas for radicalization? Do we have nodes of radicalization there? Do we have any penetration in that community that gives us the visibility inside of that threat to either say yes or no as opposed to yes, we have it.

If you remember early after 9/11 the utilization of hawalas – there was a misconception if you were utilizing a hawala you were a terrorist. That’s ridiculous. So educating the workforce about the relevance of issues and then providing that posture that allows us visibility into that threat so that we can position our resources to the most effective manner. I think that’s one of the things that it’s taught us collectively.

MR. HARRIS: So you both have described a way the system sort of optimally performs. Now, I want to ask people who are outside the system, is it working that way? I mean, is it working that well where all of these fusion centers and the field offices and the task forces are completely collaborating and we see the threats in a way that you’re describing.

MR. LOWENTHAL: Nothing works optimally.

MR. HARRIS: Well, how close are we, then? Is it good enough?

MR. LOWENTHAL: No, I mean, look –

MR. HARRIS: I mean, should we declare victory as you said?

MR. LOWENTHAL: I think Caryn and Tracy misunderstood my earlier remarks. I agree with them that we have made a lot of progress. We really have. But I still – what I’m
seeing this at the teaching level, I still see two distinct communities that are still having trouble totally comprehending each other for reasons that I think are totally understandable.

So I think we, you know – it works pretty well a lot of the time. And the fact that we have not been attacked and there have been a lot more near misses than most people know about, some of which have been hinted at in the newspaper, is a sign of success. And the number of attacks that get disrupted is a sign of success. The operations that have succeeded overseas are a sign of success. I think it’s premature to declare any strategic victory like the secretary of Defense did.

But clearly we have done a lot of damage to the original inspiring group that hurt us. But I mean, but one of the things we learned is that these people morph. So you have to morph with them. So the real question is are we morphing at the same rate that they’re morphing or are we back, as Tracy said, and are we reacting.

And I think it’s probably a little bit of both. But I think we have some reason to take some pride in what we’ve done, knowing it’s always an imperfect system and we can never assure the American public never going to happen again.

MR. REINHOLD: Right. I mean, I think that Mark’s spot on. And here’s the issue that you have, and to address whether we’re treading water or are we moving forward. One of the challenges in transforming the FBI, for example, to being this intelligence-led, threat-focused organization is that in times of crisis human nature is that you will always revert back to where you’re the most comfortable.

And where you’re the most comfortable is what you came up with. If you are a reactive law enforcement type, that’s where you’re the most comfortable. So our challenge is to continue to set the bar higher and higher and make sure that we push every day. We like to say that every day is a vest day because if you cede any ground at all, you never gain that back.

So every day you have to fight to solidify the gains that you’ve made in transforming the organization and to integrating the community. Are there frictions? Of course there are. Is it optimally positioned? Probably not. But I will tell you right now that the relationship is better than it has ever been. It wasn’t too terribly long ago that Phil’s former home and mine didn’t really see eye to eye. And I will tell you that bringing Phil into the bureau really opened a lot of eyes.

MR. MUDD: It was a brave step on your part.

MR. LOWENTHAL: It was a good time too, I’ve got to tell you.

MR. REINHOLD: Well, you said it best. It’s about risk management. It’s not about risk avoidance. And in order to manage risk you have to assume something. And the problem is government as a whole is relatively risk averse. That’s being kind. And pushing the edge of that envelope every day is what makes us successful and it is a very uncomfortable position for people to be in.
But it is critically important that we push that a little further every day because the people that are depending on us don’t want to hear about risk avoidance. They want to go to bed and they want to wake up in the same world they went to bed in last night without any horrible things happening. And that’s our job. So I think that we’re way – way further than we have ever been. We still have a ways to go but I would say we’re definitely making progress.

MR. HARRIS: Let me switch gears a bit and tighten in on the tradecraft question. We’re getting a number of questions that have to do with technology. Some are touching on civil liberties issues. I want to talk about a potentially valuable source of information; that is, social media. This is obviously something that you all as analysts are having to grapple with, talking about morphing, right.

So we know that in many of the cases of homegrown extremism and foreign plots as well, some of these perpetrators have posted on Facebook hints about what they were about to do. There is sort of a signal trail that maybe we pick up later.

I mean, obviously law enforcement and intelligence agencies have various authorities that they can use to monitor social media, to try and learn from it. Talk to me about the role that that is playing in this whole mix because it seems to me that that is sort of – if you’re talking about modes of communication, the threat is migrating in that direction. You’re shaking your head.

MR. MUDD: Yeah, this is a problem because the American people think that security services are pervasive. In my experience as an intelligence officer, the gap between what a security service can do in terms of collection, whether it’s Facebook or whatever, and that relates to gangs. Gangs are up on Facebook. And what they actually do is growing.

I could look algorithmically at activity around the world. Who’s accessing websites? I want a rotating every three month list of the most active websites. I want people who are on at least three of them at least nine times a month. I want to see if those people have ever bought a ticket to Pakistan. I want to see if they’re between the ages of 16 and 40.

By the way, none of those criteria, which are pretty sound criteria, represents illegal activity. That’s – so I think, as General Hayden made a great point at lunch, when you walk out of this building and somebody says, I want to look at your bag, you’re going to say – I’m not going to use what he wanted to say. (Laughter.) You’re going to say, heck no. If you – you know, I’ll be in an airport Monday and I’m going to say, you know, what do you want to see?

On this highway, I suspect a lot of people are saying, well heck, why aren’t you looking at websites? I assume you’re looking at websites seeing who’s talking about jihad. Well heck, a lot of people are. That’s a free speech issue. But if you’re involved in procuring explosives for a group, then I can look. People – we haven’t defined what lanes we can look at.

Those lanes of data are getting bigger and bigger and I think at some point there’s going to have to be a national dialogue, as there is on physical security. You go to an airport, you’re going to take your damn shoes off. That dialogue’s not there and we are not even close to
exploiting what we could. I’m not saying we should. I’m saying I think people probably radically misunderstand where we are.

MR. HARRIS: In terms of thinking that we’re farther ahead than we actually are?

MR. MUDD: Yeah, not farther ahead but more aggressive.

MR. HARRIS: And more pervasive, as you said.

MR. MUDD: Yeah, and that the reaction of people on the inside isn’t – I mean, I found it very cautious, as it should have been.

MR. HARRIS: Caryn and Tracy, address where this – you know, this, you know, social INT or whatever you want to call it fits into the whole mix.

MS. WAGNER: Well, I mean, there are differing, as you pointed out, levels of authority. And ours are quite different and more limited than the bureau’s. And we have the authority to do sort of overt collection of open source which is, you know, not pretending to be somebody else and not going into, you know, password-protected sites.

But Phil raises a good point is that it’s very difficult sometimes to connect what you see on those sites with actual intent or anything that anybody is actually going to do. We’ve had an interesting time even figuring out, for example, you know, the Inspire magazine that’s put out by AQAP. People want to know, well, how is that resonating? Well, the community has had a hard time trying to figure out how that’s resonating. We don’t know how to measure that and we don’t know what it means if someone, you know, hits “like” on Facebook. You know, I liked it. Well, does it resonate or, you know – there’s still a lot of art I think that needs to be figured out here.

We also, frankly, haven’t figured out, well, how to source things when we’re doing all-source analysis that we find out in the, you know – how do we know when something is citable as a source. We don’t have a lot of tradecraft or doctrine. Someone used that word – there either. So I think this is a – it’s a growth area but there’s a lot of pitfalls here.

And what we try to do is focus the work that we do in the open source realm on specific requirements that are tied to our analytic and production authorities and go look and then we’ll report on what we find as HIRs and that becomes sort of grist for the mill. But I think the FBI obviously does a lot of more interesting and fun things.

MR. HARRIS: Well before – let me ask before you get to that, are DHS –

MS. WAGNER: (Chuckles.)

MR. HARRIS: I just want to be clear. Are DHS analysts reluctant to rely on social media as sources?
MS. WAGNER: I think that the tradecraft sort of rules of the road there are not particularly clear. So we are – I wouldn’t say that we are reluctant because we use it quite a bit. But we’re careful in qualifying what kind of conclusions we draw from what we see and it’s just – it’s what I would say is a growth area.

MR. HARRIS: OK. And you’re on Twitter, so that’s a step.

MS. WAGNER: Not me personally, no. (Chuckles.)

MR. HARRIS: So go ahead, yeah.

MR. REINHOLD: Yeah. So here’s the issue. The FBI is responsible for the protection of the civil liberties of the American people. And just what I want to say about utilizing social networking is this – is that if the FBI loses the trust of the American people, we are incapable of doing our job. So with that as the premise, we are very, very careful about the way that we exploit social media and whether or not – and whether or not the person is a U.S. person or a legal permanent resident.

Those sorts of issues all come into play and when we look at obtaining court orders that allow us to do this. We are not surfing at will. It’s probably a really bad practice I would suspect. And our ability to penetrate social networks has to be predicated by something.

We have to have the underlying premise that allows us to move forward. We can’t just decide that we’re now going to monitor all social networks in the country. First of all, it would be physically impossible. And secondly, I don’t think it would be a good return on investment for work on that.

MR. HARRIS: So you can’t have an analyst sitting in a counterterrorism center set up a Twitter account and just sit there and watch what people are saying?

MR. REINHOLD: No. We have safeguards in place to make sure that we follow the letters of the law and we follow DOJ policy to make sure that the rights of the American people are protected. I mean, and it’s important to do that. I would rather protect the civil liberties of the population than to abuse the trust that has been given to us because once you do that, you can never get it back. You can say you’re sorry but that’s not going to cut it.

I mean, we’re very, very, very careful in that respect. And I think appropriately so. It’s a delicate issue with the FBI and with law enforcement, not just FBI. I mean, if we’re looking at NYPD, these are huge issues that have far-reaching consequences that sort of take precedent over the issue of the day. The issue will come and go. But if you lose the trust, you’ll never get that back.

And we will – and I think, Mark, you hit it earlier about saying we have a well-informed and cooperative public. If we lose that, we will not be successful.
MR HARRIS: Well Mark, you talked earlier about students in your class and on, you know, obviously texting and using communicating through social media. I mean, so talk about its value obviously as an intelligence source but also, I mean, this isn’t just the future. This is now. I mean, they are not going to relinquish –

MR. LOWENTHAL: This whole century is such a disappointment. (Laughter.) I mean, I don’t think we know yet how to successfully use it as an intelligence indicator. For one thing, it’s too large. It’s too amorphous.

So even if you were watching social media overseas, which you could do in the foreign intelligence community, you know, if you wanted to watch what’s going on in Cairo or in Tunis, even in a place like that where it’s not California, it’s not the United States, it is so large and so amorphous that I’m working with a colleague of mine on creating a model for how to do this. And we’re really at the beginning of the story here because it is a very amorphous kind of target.

And you’d have to do an awful lot of filtering. For example, you’d have to do traces. All right, this guy has how many followers? Is this guy just a lone nut who’s busy, you know, tweeting away and nobody’s listening to him or does this guy got 40,000 people listening to him? So I mean, I think we have some of the basic understanding of it. We don’t really have our hands around it.

But it is obviously going to have – is going to be something we’re going to have to use more and more of. Overseas will be fine. We’ll know how to do it, although you’ll get into this interesting conversation, who should do it. Should this be people overseas? Should this be done by somebody here in the United States watching it? Should it be an open source? Is it a different source?

Once you’re in the United States though, you’re in the land that Tracy and Phil are describing, different set of rules. So I just don’t think we have – you know, it’s not that – it hasn’t been with us that long. Let’s be serious. I mean, Twitter is how old? Is it 10 years old? I don’t think so.

MR. HARRIS: No, a couple of years.

MR. LOWENTHAL: OK, so I mean, so the fact that we’re still catching up to the technology isn’t that surprising and understanding its value and how to mine it. I mean, there are people working on it. Like I said, I’m working on it.

MR. HARRIS: Somebody will tweet the exact date as we’re talking, so.

MR. LOWENTHAL: Yes, they will. And I won’t get it since I don’t tweet.

MR. HARRIS: I’ll get it and I’ll call you up on the phone

MR. LOWENTHAL: Yes, call me because I don’t text either, so.
MR. HARRIS: OK, all right. (Laughter.) Someone raises a good question. I want to use this to then lead in to another question to stir up some debate here. And this person remarks the commission of a terrorist act is a crime. Do we still have a cultural (or legal) issue for law enforcement that counterterrorism is anticipating a crime that has not yet been committed?

And along those lines, I want to ask about what I know is one of you all’s favorite metaphors for describing what it is that you do, which is connecting the dots. It’s a useful metaphor. I’ve certainly made great use of it.

But I want to know, keeping in mind this audience member’s question which I think is a good one and gets to this issue of prevention and preemption versus investigating, why doesn’t connect the dots describe what it is that you all do? And if it doesn’t, then what is it that you do and what is the metaphor we should be using to describe it?

MR. MUDD: You know, I connected the dots when I was 4-years-old.

MR. LOWENTHAL: Thank you. The defense rests. (Laughter.)

MR. MUDD: Not well.

MR. LOWENTHAL: What was your error rate when you were 6?

MR. MUDD: What is Twitter?

MR. LOWENTHAL: He used to sit next to us at those 5 o’clock meetings.

MR. MUDD: But you know, I don’t want to be facetious. We’re not stupid sitting around the table. We’re not stupid. So give an example that links your two questions together – going back to the Somali example. So we see fundraising. You know, suppose somebody said, well, look dummy, you know, there’s somebody who just traveled to Mogadishu. You should have known his travel records and everything. Well, you know, there’s thousands of investigations underway every day.

Let me open the door a little. What I should have said at the table, and this is one of the things I flog myself about aside from going over to the bureau in the first place – (laughter) – but I should have sat there and said, you know, maybe we have to start thinking about among all the subjects we have getting into whether, you know – linking up the foreign question.

You have African troops coming in to a domestic environment in Somalia. U.S. policy is backing African troops and first-generation kids in Minneapolis are reacting to that. Should have thought of that. That’s not just – that’s not a simple proposition.

MR. HARRIS: It’s not a linear progression.

MR. MUDD: That’s right. It’s not. And then the question would have been among all of the cases we have, for example, since we already have access to them, maybe I should start
talking or looking at issues like has any of this person – any of these people been using travel agencies in these areas and are any of the tickets from those travel agencies one-way cash tickets and is that concentrating?

Maybe I should geospatially array the purchase of those tickets. Is that concentrating in any particular areas of the city? Do we have access to a community leader who might say, yeah, by the way, when people talk about Shabab, that’s the kind of – if that’s connecting the dots, then I was pretty damn smart at four years old.

MR. LOWENTHAL: And you were. All right, too many people in this room have heard me rant about this. But I’ll do it really fast. It’s not the way our intelligence comes. When you connect the dots, you get only the dots you need. You don’t get extra dots. You’re not missing dots.

Well, the world that I lived in, the world these guys live in doesn’t look like that. And the dots are numbered sequentially. Well, isn’t that convenient. (Laughter.) Somehow the incoming that I used to see every day that Phil, Tracy, Caryn see, don’t work that way.

MR. MUDD: And somebody twittered the conclusion.

MR. LOWENTHAL: And there you go. My thing – the two mosaics that I like best for what we do in analysis, one is we’re in the pearls business. We slowly accrete data over time day after day, month after month, year after year and we build a pearl. I mean, think about the Soviet pearl. As Jim Clapper once said, this is the mother of all pearls. I mean, this was a 50-year pearl. It’s a Dom pearl. It was a 20-year pearl. And we still got stuff wrong in both cases.

Or we make mosaics. You come into the office in the morning. They give you a tray full of colored glass, different sizes, different shapes, different colors and they say, make a coherent pattern – not make a picture, make a coherent pattern. At the end of the day, you have to give them the glass back because it’s classified colored glass. You can’t take it home. (Laughter.)

And you come in the next morning and they give you the tray back and they say, we changed 30 percent of the pieces last night. Have a nice day. That’s basically the metaphor. But it ain’t connecting the dots.

MR. REINHOLD: Right. So let me get back to the originally question. (Laughter.)

MR. LOWENTHAL: That was the original question.

MR. REINHOLD: Because I cannot do justice to what these two guys are talking about. So let’s talk about the anticipation of a terrorist act and how it affects law enforcement real quickly. So that is a huge problem because you need a statutory violation in order to put somebody in handcuffs. You can’t do it because you think he’s going to be a bad guy. You have to build a case with him. Now, this is the big challenge for us is law enforcement and intelligence collection at the same time.
And this is something that’s really hard to get a handle on because you can’t just unilaterally decide I’m going to pursue a criminal case because this is what I do. I put bad guys in jail. That no longer works. The challenge is how do you build a case at the same time that you’re using that same platform for collection of intelligence because it may never reach the level.

But the question is where is that intelligence collection going to lead you and it may not be the guy that you originally thought was a bad guy. He may be a third-tier facilitator. But that collection platform that you’ve established leads you to other individuals engaged in nefarious activity that you can build a case on. So the key is if it’s not there, it’s not because it’s not there.

Maybe you don’t see it and do you need to develop the tools necessary to do that. Not every case is going to end in prosecution. The first challenge for us is how do we collect the intelligence so that we can mitigate threat. If it means we break up this issue before it becomes a criminal violation, that’s great. There’s nothing wrong with that. It’s not – it’s about changing mindset.

It’s not about quantitative statistics – how many arrests did we have, how many indictments did we have, how many convictions did we have. The real thing is how does this impact the lives of the people that we’re supposed to protect. And in order to do that, it’s sort of a fuzzy science. So you have to be able to train your employee to say you need to be looking at the criminal violations but at the same time you need to be looking at collection opportunities.

And this is where fusion centers, joint terrorism task forces, field intelligence groups working with their state and local partners sort of change that mentality so that they understand that it’s not just about that. One of the challenges when I used to run task forces was, you know, you’d get the beat sergeant that would say, what have you done for me today.

And it takes a long time to build these cases. So really we need them from that – you know, I need to see what you’ve done today because today you may not have shown any progress. It’s that pearl analogy, like that, yeah. OK, so that’s kind of what we’re talking about here. And our challenge for us on the law enforcement and intelligence side is how do we marry those two up and not miss something. And it’s a tough nut.

MR. HARRIS: OK. We only have just a few minutes left because the DNI is here. So we’re going to cede the platform to him. But I want to very briefly ask for each of you a closing question. I want you to tell me what you think is one of the great strengths – it doesn’t have to be the greatest or the worst – but one of the great strengths and also the great weaknesses among what I’m going to broadly call our homeland security intelligence corps, the analysts who are out there doing this.

And I’ll let you go last because you speak for them most directly. But if you could just very, very briefly give me what you think is one of the great strengths and one of the greatest weaknesses among that group now.
MR. LOWENTHAL: We’re hiring really good people who are very eager. They’re very dedicated but they have no experience. So the strength is a weakness. These are really wonderful people. I used to be the graduating speaker at each class of CIA analysts. They were fabulous.

But the numbers have worked in such a strange way that we probably have the least experienced analytical cadre that we’ve had since 1947, not because they’re bad people but because the numbers of new people are so much larger than the cadre of veteran people that there’s a disproportion of experienced/inexperienced that isn’t in our favor right now. So that’s sort of a strength and a weakness combined I think.

MR. HARRIS: OK.

MR. MUDD: Yeah, what he said. The talent I saw at the bureau and at the agency and when I was reading in at DHS and at NCTC, these 24-year-olds, they’re really good, just inexperienced a bit. They lack experience. They also lack training. The last thing I’d say is – I shouldn’t say it in this audience but my experience with first-line and midlevel management is that they are not that strong. Moving people up too fast so when you have a new untrained workforce they’re learning from people who I thought were mixed at best.

MR. HARRIS: And will that – I mean, does that improve over time?

MR. MUDD: I think we should fire them all. (Laughter.)

MR. HARRIS: OK, all right.

MS. WAGNER: Oh dear, applause.

MR. HARRIS: Briefly, yeah, go ahead.

MR. MUDD: I tried it with Tracy and failed.

MR. HARRIS: Settle that later, yeah.

MR. REINHOLD: One of us still has to go? So integration of intelligence and operations – I will tell you right now that’s our greatest strength and it’s our greatest weakness because it’s our biggest challenge is making intelligence relevant to the people that we’re asking to mitigate that.

The fact that we have made that transition as far as we have speaks volumes about the caliber of people we have both on the outside and on the intel side, figuring out how it is that they mesh and how it is that they add value and relevance. That is still our biggest challenge. But it’s also I think our biggest success.
MS. WAGNER: I agree with Mark that the dedication to the mission I think is the biggest strength. We have people who are just unbelievably motivated and find the mission challenging and energizing.

I also agree with what pretty much everybody else said about the weaknesses is the midlevel management not probably all it needs to be and the bigger – the bigger challenge associated with that is that the midlevel and even the upper level management grew up in either a CIA traditional analytic culture or a defense analytic culture and there’s nothing wrong with either of those.

But we’re trying to kind of come up with a new thing here. And it’s merging law enforcement and intelligence. It’s operating at the intersection of classification and unclassified. It’s national. It’s local. It’s a new thing and we don’t – we don’t yet have the doctrine. We don’t have all the tradecraft. We do – we have a lot of enthusiasm.

We sometimes have people who either don’t get it or don’t want to get it because it’s not the way they grew up. So that’s basically a leadership challenge and also a challenge for all of us to put our thinking caps on on how do we grow this new, you know, homeland security intelligence whatever it is, so.

MR. HARRIS: Perfect. OK, that’s all the time we have. Please thank the panelists with me for an excellent discussion. (Applause.) And I guess you’ll stay in your seats. We’re going to move off and the DNI will join us momentarily.

(END)