

THE BROOKINGS INSTITUTION

A NEW MODEL FOR DEFENSE INTELLIGENCE

Washington, D.C.

Wednesday, November 20, 2013

**PARTICIPANTS:**

**Opening Remarks:**

DAVID R. ELLISON  
Rear Admiral, United States Navy (Ret.)  
President, National Intelligence University

**Moderator:**

BRUCE RIEDEL  
Senior Fellow and Director, Intelligence Project  
The Brookings Institution

**Featured Speaker:**

LIEUTENANT GENERAL MICHAEL T. FLYNN  
Director  
Defense Intelligence Agency

\* \* \* \* \*

## P R O C E E D I N G S

MR. RIEDEL: Good afternoon and welcome to the Brookings Institution. It's my great pleasure to have Lieutenant General Flynn here today speaking as part of the Brookings Intelligence Project. Today's event is a joint event between the Brookings Intelligence Project and the National Intelligence University, and as I said we're very proud to have the director of the Defense Intelligence Agency here, and you'll all see his biography already. We'll have more to say about that.

Let me explain the event format. Very simply we're going to have Admiral Ellison introduce the director. The director's going to give a talk. At the end of the talk I'm going to interview him for a few minutes, and then we will close by opening it up to the audience and taking your questions. For today's event we have a hashtag. If you'd like to tweet, the hashtag is #DEFENSEINTELDNI.

To introduce our speaker today is Admiral David Ellison. He's a 34-year career Navy officer, then went on to become president of New Mexico Military Institute until he came to what is now NIU and what was then the Defense Intelligence University in 2009. He's a graduate of the U.S. Naval Academy at Annapolis and has a Ph.D. from Pennsylvania State University.

ADMIRAL ELLISON: Good afternoon, ladies and gentlemen. One need only span the globe to readily observe the complexity and instability, and the uncertainty, that characterizes today's global security environment. The challenge of preventing the proliferation of weapons of mass destruction, the challenge of defining and combating the cyber threat and the challenge of defending against the danger posed by ever-present terrorists combine to characterize an immensely complex national security environment.

Instability is evidenced by events such as those surrounding the Arab Spring and the recent turmoil in the countries of Syria and Egypt. Together this

complexity, this boundless regional instability, define a future of extreme uncertainty. This is a national security environment that demands an intelligence professional with unique characteristics. Protecting and defending our national security interests requires intelligence professionals who are adaptive, agile, and forward thinking, ever endeavoring to anticipate the future, anticipating the future rather than reacting to the future.

It is no longer enough to focus attention on one area to the exclusion of others. Intelligence professionals no longer have the luxury of slowly and deliberately refocusing their attentions, and no longer can they succeed as an intelligence professional with just understanding the past and the present. Today's intelligence professional must be able to anticipate future events.

Preparing intelligence professionals capable of meeting such an enormous challenge demands that we place them in an environment that fosters creativity and innovation and one in which exploration, collaboration, and integration are commonplace. That environment is the National Intelligence University. It is NIU where former directors of national intelligence and distinguished war fighters sharpen their critical thinking skills. They produced value-added research enhancing their innovative capabilities. They collaborated within the intelligence community and most importantly, across its boundaries, expanding and broadening their knowledge, and where each developed those very special personal and professional relationships that today continue to stimulate the integration of the intelligence community team.

As president of the National Intelligence University it is a distinct pleasure to join with Bruce and Brookings to co-host this afternoon's event. One of those adaptive, agile, and forward-thinking intelligence professionals to whom I previously referred is unfortunately not a graduate of NIU, but he is an individual to whom NIU can attribute a great deal of its success. He is the director of the Defense Intelligence

Agency. A stalwart supporter of the National Intelligence University, he is a proven warrior having served at the tip of the spear in both Iraq and Afghanistan. He is an astute scholar, having earned three graduate degrees and having been awarded an honorary doctorate of law. And he is a servant leader as demonstrated by the priorities, principles, and values he has set forth to the DIA workforce. People, integrity, and service are front and center among them. Ladies and gentlemen, it is my distinct honor to present the 18th director of the Defense Intelligence Agency, Lieutenant General Michael Flynn.

(Applause)

GENERAL FLYNN: Okay, and if you can, just somebody way in the back just give me a hand wave that you can hear me way back there. Yeah, great. Wonderful.

Okay, couple things. First Bruce, I really, really appreciate the partnership with the National Intelligence University and DIA and what Brookings does and brings to the, really, the national security conversation that our country needs right now, and has always brought that, but I think for all of us part of why I'm here and part of why what you just heard Dave Ellison, Dr. Ellison just talk about is also an approach to how all of us need to think about how we outreach, how we partner, how we collaborate in different ways.

In the past you wouldn't find intelligence agencies or personnel at something like this. You really wouldn't. I mean, maybe the leader, maybe the director level, maybe, but certainly not in an engaged way at other levels, and I think that that's a sign of the times for the kinds of things that we are involved in, particularly sort of what I call "this open world," and I'll talk a little bit about that.

So, what is today imperative? And I'm not going to walk you through slides here. I may go to them on the Q&A just to maybe help answer some questions or

help me answer some of your questions. But I think today's imperative and it's really for me and me collectively, for the DIA, it's about two things that are going on in the environment, and the first is the skyrocketing intelligence requirements that are out there on the world stage today, far more than they ever were or certainly they're far more apparent than they ever were in the past. Maybe it's because of the amount of information that's out there today. That is certainly, when you start thinking about a cause and effect, so the range, really the exponential increase in what I would just call sort of these skyrocketing requirements that we have placed on us as an intelligence system in really in defense of the United States.

The second major effect or impact is the fiscal environment that really not just the United States is facing, the Department of Defense is facing, but also what the world is facing. I mean, we have to come to grips with how we partner, how we collaborate, how we invest, the kinds of things that we invest in, the priorities that we have. For the United States intelligence community it is a huge conversation that we are all in right now. We are in this constant debate and give and take about what is really important, what's not important, what's the here and now versus how much do we invest in in really the next generation of ideas and the next generation of capabilities.

And then what I would tell you is that there's really sort of four megatrends that are occurring, and I think the megatrends are - they're playing out now. I just briefly or I just sort of implied a little bit about a couple of them, but I'll state them here in a second. But these trends, for the most part, as you look at where we have been since really post-World War II and where we can project ourselves maybe out into, like, 2050, these are trends that we can judge pretty accurately.

We can judge them pretty accurately, and the trends have to do with economic trends, what I would call sort of resource trends, and that's the resource trends

are the idea or the need for access to what I would call food, water, and energy markets.

And then the other two which is really where I want to spend some time is on the information trends, the kinds of trends that are occurring in the information world.

And then the fourth area is population trends, and I think the population trends have a lot to do with what it is that we are facing today in the world and definitely over the next 20, 30, certainly in the first half of this century. And I always like to start out these kinds of conversations with sort of my own personal situation.

I have a granddaughter who is one year-old. I have a mother who is 90. She's thriving, alive, she's got all of her wits. So, she's lived for 90 years, so she's seen back 90 years ago.

If my granddaughter lives to the age of my mom, my granddaughter will live into the next century, so I'm only trying to talk about really 2020, maybe 2030. I may touch on 2050, but this is a person if, God willing, she could live into the next century, so you begin to think about how much change - as I listen to my mom talk about - that she has seen and experienced in 90 years to what my granddaughter is likely to experience certainly in the next 90 years.

The changes are stunning, and we have to come to grips with a century of the past, right, that was really defined by sort of the "isms," the Nazism, the fascism, the capitalism, communism, whatever, and in a century that I think that's going to be defined in the future that is really going to be about how we understand the environment that we are walking into.

We're already into the second decade of the 21st century, and I just briefly described four, what I would call, these megatrends. And so how are we dealing with them? How does the intelligence system deal with them? Ten, fifteen years ago I

used to walk into my commanders, my military commanders, and mostly what I gave them was intelligence, was signals intelligence, human intelligence, imagery intelligence. And a little bit would be sprinkled with what was maybe reported in the *Early Bird* at that time.

Today it's almost 180 degrees flipped. The open world and the knowledge that exists and is available to all of us -- you know, at the push of a button, you know, really smart -- I mean, and this is some really smart analysis that's out there that's being written by people that are on the ground seeing it for how it is instead of getting a bunch of reports and trying to figure out well, what does it mean; someone who is culturally attuned to what the environment is, and they're able to post it. Some can post it in 140 characters or less. Some can post it in a really meaningful, thoughtful piece of analysis, and we cannot sit idle in our -- in sort of our worlds of the intelligence agencies and the system that we have and not pay attention to that.

We can't go, well, it's not properly sourced or whatever. We have to be really smart about how do we apply the open world to a world that's really a closed-loop system? And I think it's really important that we think broadly about how we need to move in the future with our intelligence capabilities.

For me, and when I say me or I, it's always in a collective sense because we're, you know, my world is the defense world. The Defense Department, the defense of the country, and my enterprise is about roughly 17,000 people. A little bit more than 50 percent of them are out in the field, what I call at the edge. Some of them are at combat and command, some of them are in-countries operating, and so how do we leverage the edge? How do we make the edge the center? When we think about the center we always think about the center here in Washington, D.C., and we can get into our own little cocoon of knowledge and sort of cross talk here and begin to believe what

we're saying to ourselves and it's not necessarily -- it's sort of intel for intel's sake.

I think it's really important that we use, we leverage the technology that we have in a smart way to understand what is happening at the edge and make, to a degree, make the edge the center, make that the place where the best, clearest, cleanest, most relevant, most timely knowledge can be gained, and then you bring it back to help really shape the conversations that are happening here.

And that's why I think as I look at the make-up of a Brookings, Brookings has that kind of a feel, a much smaller, obviously, than what a DIA has, but we have to take what I call "this fingertip feel" that we can get of the operational environment and actually bring it to bear on the decisions that we are making.

When I talk about DIA, when people ask me what does DIA do, DIA provides knowledge for decision-making. That's what we do. We have a mission statement, prevents strategic surprise, provide early warning. I mean, we've got a, you know, very straightforward military mission statement, but really at the end of the day we provide knowledge to support decision-making.

So, three things that I think that are components or capabilities that we're seeing today, and I believe as far out as I can tell, as I can see, I think will be capabilities that will be applied much more so than we ever thought of in the past primarily because we are really, really, all of us, and internationally -- so today I've talked to our U.K. partners. I've talked to our Pakistani partners. I've talked to some folks in Afghanistan, and I've talked to certainly one of our senior leaders that work on the African continent, just today.

So, what are these three capabilities that are going to be - that are I think are exponentially rising in need and desire to have more of. Number one is special operations forces. Special operations forces by far have the requirement -- and I'm not



talking about the -- you know, what we have really done very, very well over the last decade with our counterterrorism efforts. But the other aspects of special operations forces, you know, the foreign internal defense operations, the unconventional warfare, the partner capacity engagement and the building that is so necessary. Why? Because we have an extraordinarily talented workforce in our special operations community that can help other countries help themselves. And at the end of the day to stay in this left of bang pre-conflict, we really want to help other countries help themselves.

The second capability is cyber. Cyber is a new domain. It's a new domain, and over, I think, it's a third of the world is connected, you know, somehow. Five hundred million people that have Twitter accounts, over a billion on Facebook, all these datapoints that are out there, all this volume of activity, a lot of noise, and in the world of cyber people, I think, particularly the discussions that I have inside of the military, inside of those uniform-wearing folks is that there's still a tendency to believe that cyber is some function of intelligence or intelligence and cyber are the same. It's not at all. It's not like that at all. Cyber is a capability that allows us to understand an operational environment far better. It allows us to see each other. It allows us to communicate. It allows us to defend. It allows us to exploit. It allows so many other things. It definitely allows us to partner better.

If we as a nation, the United States has great capabilities to help other countries in a variety of fields with applying cyber techniques and capabilities, and we need to do that. I think there's a tendency to think it's all about war fighting or some negative, and we have to look at it as how it can be turned into a positive.

And then the third capability is intelligence. I mean, intelligence is a capability that post - shoot, even post-World War II would -- certainly post-Vietnam, post-Desert Shield, post-Desert Storm, you know, the tactical operational actions that we've

had in previous times where the intelligence system was -- the whole adage about it's behind the green door. You know, it's behind the green door.

Well, now it's the looking glass. I mean, it's a sliding glass door. There's so much transparency going on between the intelligence community and all others, and there has to be. There has to be more of it. The need for intelligence is important. Intelligence is the analysis of information. It's what it is. Intelligence can come out of an institute, just like it can come out of an agency, and so we have to understand how to use the intelligence that's out there.

It's not all going to come from the Defense Intelligence Agency or all going to come from the Central Intelligence Agency or some intelligence structure, but how can we help ourselves and our own national security environment? We can help bring that together because we do have systems and processes and capabilities to be able to do that, and I think that that's really important.

So, just in terms of sort of what I would kind of, you know, some words to use for success is really agility. We have to be a very, very agile capability. So, as an agency we have to be agile. As a capability we have to be agile. I would say that we have to have a far better, far deeper understanding of the operational environments that we are operating within today.

We have to understand the societal challenges that are underlying the challenges that many, many countries are facing or regions are facing today. I mean, some of the regions that are out there in the world are facing extraordinary challenges, and we have to have a much deeper operational understanding of that. That means understanding the culture, understanding just the humanity that's out there.

I think that partnerships, partnerships are really important, so talk a little bit about NIU and Brookings and DIA and Brookings as a partnership, partnerships with

other countries, partnerships with regions, partnerships with other academic outlets, partnerships with industry. We have to have new ways to partner. If you look at our national security strategy and our national military strategy, it's really about partnerships, and it's about increasingly being more collaborative.

Integration: integration is the word, you know, in the intelligence community right now. We have to integrate better. That's what we -- big lesson learned from a decade of wars is integration. So, in order to -- we have to be better integrated. That means we have to team together.

A subset of integration is creating ways to collaborate better, and again, if you have the tools and the technologies to collaborate, use them. Not everything has to be physical, right there. We have to be smarter, and definitely our military and our IC have to be smarter, and I see a lot of this. Part of what I'm saying is we're doing some of these things, but we can do more.

And then I think the last sort of key to success is about technology, but it's not to lose sight of the human being in the loop, the human in the loop when it comes to technology, but it's definitely -- we have to understand and we have to innovate better on technology because it's like I said about what DIA does. If we provide knowledge to influence, shape decision-making, the technology is moving so fast, I mean, over half the world is going to be connected here. I think the gauge is about 2017. It's only a couple years; about half the world is going to be connected somehow in some sort of Internet. So, there's technology that we can't allow to pull us, and it does. It still does. So, if that's the case then we have to figure out how do we stay in front of it. How do we use technology to be able to get the kind of information that we need to get to our leaders to be able to make better decisions?

And again, it's not all about, you know, I'm standing up here as the

director of the Defense Intelligence Agency. It's not all about defense these days. It's not all about what we're going to do. Now, we have to be ready to support our war fighters on a moment's notice, tonight.

But we also have to engage in a different conversation about all the underpinnings of the challenges that many in the world are facing today, and we have to understand how to help those. What are the kinds of needs that these societies have? So, with that I'll stop there, Bruce, and maybe open up for any questions. Thank you.

MR. RIEDEL: Let's see if I can self-mic. Nope, I don't trust me for a minute, and smartly so. Thank you very much. That was a fascinating overview of the world that you live in.

I'd like to take something you said at the end about agility and bring it to the war that we are fighting today in Afghanistan. We are on the cusp of the transitional year, 2014. I want to ask you two questions. First, your estimate for how well you think that's going to go most broadly. Secondly, your challenge of collecting and analyzing intelligence in an environment in which we have far fewer U.S. forces and allied forces on the ground becomes a much more difficult intelligence challenge and one that's going to require a lot of agility, and I'd like to get your thoughts on both the big picture and then the intelligence picture as you deal with the AfPak theater post-2014.

GENERAL FLYNN: Great. So, there's a lot going on that -- in terms of what our force structure might be, and so I won't speculate on a lot of discussions and decisions that are pending.

I think that there -- if I was to sort of describe it, there's really two transitions going on in Afghanistan. The one transition is that the transition of our forces out of Afghanistan with whatever residual capability that remains for whatever purposes; training, advising, assisting, maybe some counterterrorism-type forces. There's the --

and part of this sort of first transition, there's the elections that are going to occur in April. I think that there's a lot of lessons that are being applied to this next election that were used and certainly known in 2009. I think that for Afghanistan they certainly look at, I think, the transition from the election process that we just saw in Pakistan, which I think is a really positive thing, so there's some lessons. So, there's a transition going on, to use military vernacular, sort of at the tactical level that's in the here and now.

The second transition is really the big question which is what does it look like as we look out to, like, 2018, 2019, 2020? And that's more difficult. It's really more difficult to tell. I think that from what I believe and what I see and the way I understand it, I think if we stay engaged, the international community stays engaged with the people of Afghanistan and the government of Afghanistan at some level that I believe that we will see more contributions than anything coming out of that theater, primarily Afghanistan, from the government of Afghanistan instead of things that will be more viewed upon a negative things and negative behavior. So, I think the bigger transition that's going to occur is really going to occur over the next five or six years, and I think that really does take us through, like, 2018 maybe, maybe 2020, and that's the broader, more difficult transition that all of us are going to have to pay attention to.

On that and part of your question, for intelligence there's a principle of war called economy of force, and you use that principle of war when you have less force or when you have more uncertainty. So, if you have less capability or you have greater uncertainty, you apply the principle of economy of force, and when you apply that principle that requires far more intelligence capability. So, I believe that the requirements, the need for more intelligence support for our partners in the region and certainly by what we are going to be called upon to do, is going to be greater.

MR. RIEDEL: You very kindly -- I think everyone got a copy of this --

provided a brochure. I took the liberty of reading it, and I looked at your requirements. And the top of your requirements, whether they're supposed to be in order of priority or not, it's got the top as terrorism. We've spent the last 15 years in a war against al Qaeda. We've had some notable successes. We've had some failures. I would characterize the situation now as the enemy is broadening the battlefield. We're now dealing with al Qaeda in places like Niger and Mali that we didn't deal with them, while we're still dealing with them in Afghanistan and Pakistan. And we're dealing with a huge al Qaeda surge in Syria and Iraq.

I look at your job and think about collection priorities, and special operation forces. There's a finite number of all of those things, especially in an environment where the Congress won't come to decisions about financial matters. How are you managing to figure out where the biggest threat is and therefore to deploy your most important intelligence assets? Is there a way to do this without ultimately ending up with some crack in your zone defense?

GENERAL FLYNN: Yeah, and there's always going to be a crack, and there's always going to be a gap. Any smart enemy and the enemies of those that are involved in terrorist activities are smart, savvy, cunning, guile, whatever word you want to use, and they will find the holes no matter how many resources we put against it. That's why we have to be -- you know, in that world, the world of countering terrorism, if there's something that keeps me up at night it would be our inability to work together as a group of national security intelligence, law enforcement, the nations that we partner with, together. And so, if there's a crack out there it could be in one of those places where if somebody decides we can do this alone, and if there's one thing that we know, we cannot do any of this alone. And that absolutely requires kind of what I talked about, Bruce, is, you know, you look at the continent of Africa as an example, you know, I mean

just in terms of scale. I mean, you can take three of the United States, the CONUS-based United States and put it inside of the African continent to give you some idea about scale.

So, we have to work together, and you kind of -- the sort of the concentric circle approach, if the center is those capabilities and resources that we have align with other intelligence agencies and other intelligence capabilities, the services, you know, the NCTC, and then you go out from there. You know, some of our closest partners that we have in this challenging environment, you go further out to other bilateral, other multilateral regional partners that we have, and even further out is new partners that we haven't developed yet that we need to reach out to and ask for help in support of it because they're the ones that are actually living in that environment.

So, it's a really difficult way to prioritize it, but like I said, if we work together I think we're far better off than working apart, and I know that if we've learned a big lesson from the last decade, it's that. It's that we must work together to be able to challenge this ideology that's out there.

MR. RIEDEL: Couldn't agree more. Of course, we have a new challenge to our partnership relations. It's the two words Edward Snowden. You knew it was going to come up sooner or later. He has revealed in great detail some of our partnerships. Our partners are not happy. The head of British secret intelligence service, John Sawyer, has, I think, put it in a nutshell the other day when he said, "al Qaeda is lapping it up." How do you describe the effect of Snowden, and how it's made more difficult your working environment?

GENERAL FLYNN: And thanks for asking the question. First, a lot of people listen to these kinds of conversations, are the men and women, the professionals in the United States that work at the National Security Agency are

extraordinary. They are talented. They have done unbelievable work and continue to do unbelievable work for this country, the United States of America, in support of our national security. And I would tell you that it's -- I know it's a challenging environment for them these days because of the scrutiny and the pressure that they probably feel that they're under, but they are just -- they continue to save lives out there on the -- certainly on the battlefield today.

I think that the impacts are -- they're very, very serious. They are still not totally understood, not totally known. There's a lot of sort of information gathering stages that we are still in. I think we're still coming to grips with what is known, what is unknown, what are the second, third, fourth order consequences of what he did.

I do think, and it's out in the public domain, is the challenges, the impacts of relationships around the world, and I think that those are things that we have to pay very close attention to. I know our administration is doing that. We've been asked -- all of us in the intel community at our own levels of responsibility have been asked to reach out and make sure that we engage our partners around the world. And I think that that's an important aspect of what we have to continue to do, so there will be sort of more to come, but definitely it hurts us.

MR. RIEDEL: I'd like to, on that, open it up to you, but I do want to take the opportunity to second what you said. I spent 30 years working with the National Security Agency. We used to have a little proverb in the CIA, "SI doesn't lie." It's not always true, but sounds good, and certainly NSA provided unique and critical information on so many cases that I can think of.

I'm going to ask you to please put your hand up. When I call on you, please identify yourself, and let's not have statements. Let's have questions. Right in the back here.



MS. VARGAS: Hello. Thank you for being here. My name's Christine Vargas and I currently work at Abisent, and I'm a graduate of Johns Hopkins SAIS, and my question has to do with counterterrorist intelligence. As we're seeing al Qaeda move from a tiered, big-picture leadership position under al-Zawahiri to more of a flat lone-wolf organization under people like the Syrian, how are you tailoring your defense intelligence to serve communities like law enforcement internationally since the push to handle counterterrorism moving towards law enforcement and a little bit away from military in certain environments?

GENERAL FLYNN: Yeah, great question. In fact, when Bruce was talking I wrote down -- because I wanted to hit it today. It was law enforcement and intelligence, the interaction between international law enforcement and international intelligence capabilities, organizations, is by far -- it's the closest lash up that I'm aware of and that I have ever seen. And we -- you know, I've been part of it. I think that it's -- we have some great relationships. We have some great processes. We have some great forums that we interact in. We move at a much faster speed these days than I think we ever did, and we are getting better and better every day.

On your sort of description of the threat or the description of sort of the terrorist structure, I think we've always seen them as being a bit flat, as you describe it. And people talk about flattening organizations these days. Flattening organizations has nothing to do with the line and block chart. It has everything to do with, really, speed of decision-making, speed of doing actions and activities out there in the world, and I think technology enhances that speed to a degree, so when we talk about how do we place ourselves on top of that, I think one of the things that we really do have to learn and to really to get inside of or to think more clearly about is the thickness of the relationships between the different disparate groups that are out there.

You see these organizations plastered on maps and they have lines between them. What do those lines really mean? Are they really talking to each other? Are they financing each other? Are they sharing ideas? Are they sharing lessons? There's a thickness to that that I think gets misrepresented sometimes, and I hate to -- I learned many -- at the beginning of my time in the military, never make an enemy 10 feet tall because I think as good as we are, we're not. And so, they're not 10 feet tall. They are defeatable as an organization.

What we have to understand is what's the true nature of it? What are the -- again, one of the underlying conditions that allow them to thrive in these environments where we see them thrive, and those are kind of some of the stuff that I talk about. It's some of these underlying societal issues, and all somebody wants to do at the end of the day is go home, be happy. They want to be with their kids and really give their kids something more than they have. I mean, I've had many, many tribal leaders tell me that. That's what I want. I want something better for my kids. So, I think that's what most people want.

When you have this cancer inside of these systems out there that does not allow for that, then that's where we have to come together as partners and try to figure out different ways to combat that. And so, it's a great question because it is a sign of the times, and it's not going to be something that's going to just suddenly go away.

MR. RIEDEL: Right here.

SPEAKER: Hi, General Flynn. Amber (inaudible), Federal Computer Week. You touched a little bit on the intersection of cyber and intelligence, so I wanted to ask you about that. I was wondering how you see a potential split of NSA and cyber-comm impacting intelligence, and what do you think needs to happen there to make that transition happen as seamlessly as possible, and what do you think that post-split

operational picture looks like?

GENERAL FLYNN: Yeah, so I'm not going to speculate on where our national security leadership is going with your question on cyber and NSA.

From an intelligence standpoint, what does intelligence do? Intelligence enables things. Intelligence enables decisions. It enables operations. It enables ideas. It enables new technologies that we have, so intelligence definitely enables cyber. There is a really, really close lash-up between intelligence and cyber. Cyber operations, cyber whatever that you want to extend that phrase out to, so there's a very close relationship between the two.

And I think that as we go forward and we -- like I still believe we're still at the bit of the sort of the infant stages of how we will grow cyber capabilities in the future, and I do totally believe that our U.S.-based private industry has to be part of that conversation to be able to ensure and assure the critical infrastructure of this country. And that's to go back to intelligence, we do a lot of intelligence assessments and input into many of those kinds of conversations, so it's really important, that lash-up. Thanks.

MR. RIEDEL: How about right here, this gentlemen. This lady right here. You, yeah.

SPEAKER: Otto Criser, reporter for SeaPower, Semper Fi, and a few other magazines. General, I want to talk about the problem of there's so much intelligence coming in. The Air Force Chief of Staff and other people have complained frequently there are RPAs out there, UAVs, whatever, and things are collecting a lot more information than you can analyze, so there's a difference between noise and knowledge. So, how are you guys handling this flood of information you're getting in order to get some knowledge out of all the data?

GENERAL FLYNN: Yeah, I used to be a lifeguard at a beach years ago,

many years ago, and this one guy used to always find -- you know, the guys that come out there in the morning at a beach, and they're sifting through the sand and they're trying to find a lost wedding band or some old coin, you know. You got an entire beach. The beach I worked at was giant. This guy always found stuff. He always found stuff because when I talked to him -- I used to talk to him all the time because he'd be there at like 6:00, 7:00 in the morning. I'd say how come you're so lucky. He said, "I've been doing this for 25 years." And so he kind of knew because he used to watch where people sat at the beach is how he described it to me. And he would look for places on the beach where people would be, and he kind of knew, well, whether they lost something or he would be very observant. And so, he'd go back and he'd scour around and the guy actually made a living doing it. So, the metaphor or to take it to an analogy is we have to really be very observant of the things that are important to us, and then ruthlessly prioritize where we put that sand basket to sift for the right types of information that we need.

And even when we do that, even when we pull that sand basket up and we shake it, is it actually what I need? Does it mean what I wanted it to be? Is it the gold ring or is it just a shiny rock? And so, I think that we have to understand what it is that we're looking for. We have to know where to look, and we have to, like I say, we have to ruthlessly prioritize those collection requirements, those intelligence collection requirements. And I think we -- I believe we do a very good job at that because we have to. We are -- it's been said before, we're sort of drowning in data, the velocity of which is just exponential, so we really, really, have to be better at how we -- where we put that sand basket.

And we have to be smart about how we do that, and frankly we have a capability to put multiple sand baskets out there, so it's not just about one place on the

beach. We have special operations forces. We have conventional forces. We have intelligence capabilities. We have partnerships. We have to be smart about where we ask those different elements that are part of our national security structure, where we ask them to go place that sand basket and start sifting some sand. Hope that helped.

MR. RIEDER: Maybe one aisle forward of the last question.

MS. DOZIER: Kim Dozier, AP. General Flynn, as we've been sitting here, Secretary of State Kerry has said that he and President Karzai have reached an agreement on the terms of a security deal in Afghanistan, so ideally how long would you like to stay in Afghanistan and support Afghan troops there? What do you think can be accomplished, and how long do you think the U.S. is going to have to stay in a support role to keep al Qaeda from coming back?

GENERAL FLYNN: And again, Kim, I mean, it's a -- I'm not going to speculate on the broader geopolitical issues in play. I think what our President said a few years ago when he talked about the Afghan strategy, you know, we are there to help the people of Afghanistan create the conditions and an environment to be able to live in a relatively free and fair system. And we also want to ensure that we take all necessary measures that are within our realm to be able to be able to defeat al Qaeda, and I think that we have done an extraordinary job at those two things; at helping the people of Afghanistan, and really working very hard to defeat al Qaeda.

I think as we go forward, whatever decisions are made, I do believe that we will see engagement by the United States of America, certainly with Afghanistan, and frankly any country that wants to contribute to the greater good of the world. And I think that -- in fact I know that there are so many good things that are going on in Afghanistan right now, so many positives, many more positives than there are negatives, and I believe that the outcome will be one where we will continue to stay engaged with the people of

Afghanistan. I'm actually -- today, sitting here versus over the last 10 years of being in and out of that place, I'm excited about it. I actually am upbeat. I'm far more upbeat today than I ever was.

MR. RIEDEL: Right here.

SPEAKER: Hi, General. James (inaudible) from (inaudible). Good to see you again. Shift your focus to another hot spot which is Syria. There have been reports that you're old adversaries, al Qaeda in Iraq, have sort of sprawled offshoots into the Al-Nusra Front and the Islamic State of Iraq and Syria. They've captured territory apparently. Congressman Rogers from the Intelligence Committee said that there have been indications they're already plotting external operations, if you will. I mean, when that sort of dynamic seems to coalesce, it usually means trouble for us. I'm just curious of your threat assessment on what's going on in Syria.

GENERAL FLYNN: Oh, how long do you get? The situation in Syria as everybody sees is incredibly not only very serious for the region, but I think it's serious for the international community. It's caused the international community obviously to engage in an international dialogue which is think is very healthy. In terms of the various threats that exist that range the full gamut, I mean, from the threat to internally displace people, refugees that have had to leave the country. I mean, so there's those aspects of what we're facing as well as the fighting ongoing inside of the country itself.

It kind of goes back to one of the questions about terrorism just writ large. We have to be concerned about it. We have to be concerned about those individuals who have the notion that perpetual violence is an okay way of life, and we cannot have individuals that see perpetual violence as a way to live, and there are some that are like that.

And we do have to be concerned about the flow of these foreign

elements into the country and in the flow of these elements out of the country because while they're there one of the things that we -- and I'll take it to my experiences in Iraq -- one of the things that we clearly saw was they improved. You know, they got smarter. They got better. They were -- they kind of got their combat skid marks, if you will, and they also were developed in other ways, too, you know.

Not just some young male with nothing better to do, and he's given a rifle or an IED, but also they were trained on other aspects of how to engage in a war fight; you know, information operations and all the other pieces. To create an IED, in some cases you can say, well, it doesn't take much. I will tell you it takes a lot to some of these, so they have to train people like that. Those are the kinds of things we should be concerned about, not only to help those in Syria to try to resolve this thing peacefully, but also if they take those skills elsewhere around the world. I am very worried about that.

MR. RIEDEL: We're nearing the witching hour, so what I'd like to do is take three questions really quickly, and then you have the final, final word. All the way in the back.

MR. BOYER: Hi, thanks so much. Spencer Boyer with John Hopkins SAIS. Just a quick follow-up question on NSA. What is the way forward so that the scandal or at least a bump in the road doesn't have long-term collaborative effects with our European allies? Is it just a matter of time? Is it about doing a better job of explaining to our publics why this intelligence cooperation is so important, or is it really about us developing some kind of code of conduct to help our European government partners have some political cover? Thanks.

MR. RIEDEL: Two more. Right here.

MS. BERTELLS: Ellie Bartells, National Defense University. As you're sort of laying out these future threats I wonder if you could state what the educational

experience or skill set that you wish that your workforce had moving forward that you feel is either not present or lacking right now?

MR. RIEDEL: Last question right here in front.

MR. FASIANO: Nick Fasiano. I'm an intern here at Law Fair at Brookings. You talked a lot about intelligence writ large, and so much of that intelligence was changed between military and civilian intelligence agencies post-911. Where to you see DIA fitting into the intelligence community moving forward, and what space do you see it best occupying?

GENERAL FLYNN: That's great. So, I want to go backwards because the last question is real easy to answer, or the first question is really easy to answer. I'm sorry.

So, where does DIA fit? DIA, the Defense Intelligence Agency -- we have transformed ourselves into what I call a centers-based model, and that centers-based model, we have five centers; four are regional and one is functional. And I did not -- I decided, we decided, collectively to not align along the boundaries of the combatant commands because we do support the war fighter, right. We're defense. So, those regional commands, they actually support our combatant commanders. Those regional centers support our combatant commanders by covering down gaps and seams and responding in a much more agile way to crises around the world that many of our combatant commanders are dealing with. So, this regional and functional centers-based model is part of that.

The other component is to get more of our capability out into the field, so whether that's analysts working in close cooperation with our special operations forces or our human intelligence capabilities working in close cooperation with our national partners and our special operations forces to get more of that fingertip feel out in the



operational environment. And I think the third is just being a very innovative organization to try to -- don't just think of innovation when you think about technology. You can innovate people. You can innovate processes. You can innovate systems. You can innovate technology, so that's kind of in a broad brush where I think DIA is going.

On the second question about the future workforce, one, I loved the question, and we also have a great partnership between DIA and NDU.

So, I'll just talk about one quick aspect of it. Analysis, because we all all-source analysis agency, defense all-source analysis agency, so the future analysts. What is the future analyst? The future analyst has a range of capabilities, needs to have a range of skills. They can't just be analysts, somebody who can connect dots. They have to be collection managers. They have to be targeteers. They have to be open-source collectors or collectors of the open-source environment. That's a skillset. That's not just going and doing research to answer a question and doing a Google. They have to be smart about foreign disclosure activities. How do we rapidly foreign disclose in a military environment where we are so reliant on our coalition partners? And the fourth or probably the fifth thing, I think, is the world of data science. And it goes back to the questions that I got on the volume of data that we're getting, the analogy that I gave you.

So, we have to have people who understand, I think, data science. I've been researching data science lately to study it and to talk to some of our younger analysts about their thoughts on it because it does have to do with everything that we're doing with data. When people throw out the phrase big data, well, big deal. What does it mean? It's the science of data as well as the art of the knowledge that's between your two ears, and your ability to put it all together. What I just described in a minute and a half is what I believe is a future analyst.

And on the first question which I left till the third, great question. Major

league challenges, but I cannot and am not going to speculate on what's going on right now. It's a sensitive issue. But I would add -- I would finish with my point that I said about our work force at the National Security Agency. I know personally that that organization has saved lives, not only U.S. lives, but many, many lives around the world.

MR. RIEDEL: Thank you very much, General. Thank all of you. I want to thank the National Intelligence University, and Admiral Ellison and his team for making this happen. I want to thank my own staff for making it happen, and we welcome you back as many times as you want to come in the future.

GENERAL FLYNN: Great. Thanks a lot, Bruce. Appreciate it.

(Applause)

MR. RIEDEL: Can I ask all of you to stay in place while we try to get the General to his car expeditiously.

\* \* \* \* \*

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016