

INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

**Defense Intelligence and Transformation
William G. Boykin**

Guest Presentations, Spring 2007

William G. Boykin, Richard J. Danzig, James A. Baker,
Warren G. Lavey, John D. Bansemer, Michael J. Sulick,
Robert A. Fein, Darryl R. Williams, Rob Johnston

May 2007

Program on Information Resources Policy



Center for Information Policy Research



Harvard University

The Program on Information Resources Policy is jointly sponsored by
Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

Copyright © 2007 by the President and Fellows of Harvard College. Not to be
reproduced in any form without written consent from the Program on
Information Resources Policy, Harvard University, Maxwell Dworkin 125,
33 Oxford Street, Cambridge MA 02138. (617) 495-4114

E-mail: pirp@deas.harvard.edu URL: <http://www.pirp.harvard.edu>
ISBN 1-879716-98-4 **I-07-1**

Defense Intelligence and Transformation

William G. Boykin

February 15, 2007

Lieutenant General William G. Boykin, U.S. Army, became the deputy under secretary of defense for intelligence for warfighting support in June 2003. Previously, he was commanding general, U.S. Army John F. Kennedy Special Warfare Center at Fort Bragg, N.C., after having served as commanding general, U.S. Army Special Operations Command (Airborne) at Fort Bragg from 1998–2000. He was commissioned as a second lieutenant in the Army in 1971, and eventually became a member of the Delta Force. In 1980 he was the Delta Force operations officer on the April 24–25 Iranian hostage rescue attempt. He was an operations officer during Operation Urgent Fury in Grenada, served in Panama as part of the mission to apprehend Manuel Noriega, and led a mission to hunt for Colombian drug lord Pablo Escobar. In April 1993 he helped advise Attorney General Janet Reno regarding the standoff at Waco, Texas, between the federal government and a religious sect. In October 1993, then-Colonel Boykin commanded the Delta Force tracking down militia leader Mohamed Farrah Aidid in Somalia. He was later assigned to the office of the Joint Chiefs of Staff as chief of the Special Operations Division. He served at the Central Intelligence Agency as deputy director of special activities, and was made deputy director for operations, readiness, and mobilization on the Army Staff. General Boykin attended Armed Forces Staff College, Army War College, and Shippensburg University (where he received a master's degree). His badges include the Master Parachutist Badge, Military Freefall Badge, Ranger Tab and Special Forces Tab, and his medals and awards include the Service Medal, Defense Superior Service Medal (with three Oak Leaf Clusters), Legion of Merit (with Oak Leaf Cluster), Bronze Star Medal, Air Medal and the Purple Heart (with Oak Leaf Cluster).

Borg:¹ We are delighted to welcome as our first speaker of the year Lieutenant General William Boykin. As you know, he is a visionary and an architect of the current intelligence transformation process. I know you have a lot of questions about that process and about what's being done on issues such as the development of the Joint Intelligence Operations Centers [JIOCs]. General Boykin is also a combat veteran and has unique and interesting experiences in a number of

¹ Lt. Col. Lindsey J. Borg, U.S. Air Force, is the 2006–2007 National Defense Research Fellow at the Program for Information Resources Policy.


operations, including the Iranian hostage rescue, Grenada, and Panama, and he was key to the command and control and Special Forces direction in Somalia. You can all relate that directly to the movie and the book *Black Hawk Down*.² General Boykin, thank you for being with us. We look forward to the information you will share with us.

Boykin: Thank you very much. I have with me Mr. Tom Matthews, who works with me. He’s a retired colonel from Army aviation. Like me, he served in the Special Operations community. Tom and I have been in a number of hot spots together. Tom will be giving part of the briefing here today.

If you have any questions, just go ahead and ask as we go through this. It will be fresh in your mind and it will be a little easier to keep it in context. So just stop me and let’s hear your questions if you want to talk about something that I’ve said, or if something pops into your mind related to intelligence.

There’s probably no element of our government that has received more scrutiny than intelligence. There’s probably no element within our government that has received more congressional attention and more congressional effort than intelligence. A lot of changes have occurred in the intelligence community. A lot of changes have occurred just within the Department of Defense.

Before we get into the presentation, I want to give you a little pretest to see how much you know (**Figure 1**). How many organizations are there in the intelligence community?



Remodeling Intelligence Quotient (RIQ) Test

1. How many organizations comprise the “intelligence community?”
2. How many of those organizations are subordinate to the secretary of defense?
3. How much of the intelligence budget of the United States goes to the DoD?
4. Is a qualified “all-source” analyst authorized access to all available intelligence?
5. Does the DNI have authority over all U.S. intelligence?

Figure 1

² Mark Bowden, *Black Hawk Down: A Story of Modern War* (Washington, D.C.: Atlantic Monthly Press, 1999). The book was later adapted into a 2001 film directed by Ridley Scott.

Student: Sixteen.

Boykin: You're right. Go to the head of the class. How many of those organizations are subordinate to the secretary of defense? It's eight. Now, the key is: how much of the intelligence budget of the United States goes to the Department of Defense? The actual amount of money is still a classified figure, so I'm not going to say how much it is, but it's tens of billions. I told you that of the sixteen elements in the intelligence community eight are subordinate to the secretary of defense. How much of the budget does that represent? Trust me: it's disproportionate. You could make a case that it should be 50 percent, since it's exactly half of the intelligence community. In fact, it's 80 percent.

When you go back and look at the way the law is written, the secretary of defense is specifically tasked by law for the collection of intelligence. If I asked "Who collects signals intelligence [SIGINT]?" most of you would answer "NSA" [National Security Agency], and that's right, but the one tasked by the statute to collect it is the secretary of defense.

How about the next one: Are qualified all-source analysts authorized access to all available intelligence? This is an important issue. The fact is, as you already figured out, they're not authorized access. What that means is that in most cases nobody sees the big picture. Then you have to go back and ask the question "Is that one of the reasons why we didn't get it right on the issue of weapons of mass destruction? Is that one of the reasons why we did not foresee the events that occurred on 9/11—that no analyst gets access to all the information available?" That's one of the things we're working on.

What about the fifth one: Does the DNI [director of national intelligence] have authority for the management of all U.S. intelligence? He does actually have budgetary authority, but he cannot hire and fire, and that is one of the issues. Here's the key thing you must remember: the DNI, who was Ambassador Negroponte and is now Admiral McConnell—a great guy, a good choice—does not have authority over military intelligence. Remember that: the DNI does national intelligence, not military intelligence. The secretary of defense is still responsible for military intelligence. We'll talk about what's national intelligence in a few minutes.

I want to say a little bit about the Department of Defense here. Secretary Rumsfeld came in. We got into the post-9/11 activities and the secretary had people saying "Mr. Secretary, sign this piece of paper right here, and this will authorize you to put military people under CIA [Central Intelligence Agency] control and send them to Afghanistan." He said, "Hold on a second. I'm the secretary of defense. I'm going to put American military people on the ground in Afghanistan, I'm going to put them in harm's way, I'm going to be responsible for what happens to them, but I'm going to do that under the authorities of the CIA?" He was told "Yes. The CIA has the infrastructure and the network inside Afghanistan, and you don't, Mr. Secretary." He said "Then in reality it's not an authorities issue, is it?" No, it's not an authorities issue. What it means is that the Department of Defense had not built an infrastructure inside Afghanistan that would allow it to put people on the ground who could start dealing with the Northern Alliance and organizing a resistance movement, and the secretary of defense said "I don't want to be in this position again. I respect and recognize the authorities of the CIA, but I don't want the department to be in this situation again."

That's the point at which he said "We're going to reorganize the intelligence effort within this department" (**Figure 2**). What you wound up with is the secretary of defense; an under secretary for acquisition, technology, and logistics; an under secretary for policy; an under secretary for personnel and readiness; and an under secretary for comptroller, and Secretary Rumsfeld added a fifth under secretary: an under secretary for intelligence.

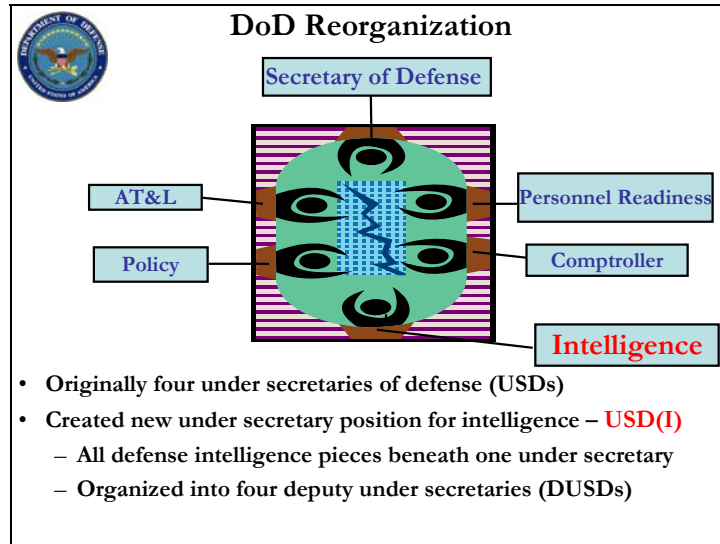


Figure 2

Matthews: Here is a basic wiring diagram for the Office of the Under Secretary of Defense for Intelligence, or OUSDI (**Figure 3**). This is the way we're currently arranged. There are four deputies. We do not currently have an under secretary of defense for intelligence, other than the acting one: one of the deputies, Bob Andrews, who has counterintelligence and security.

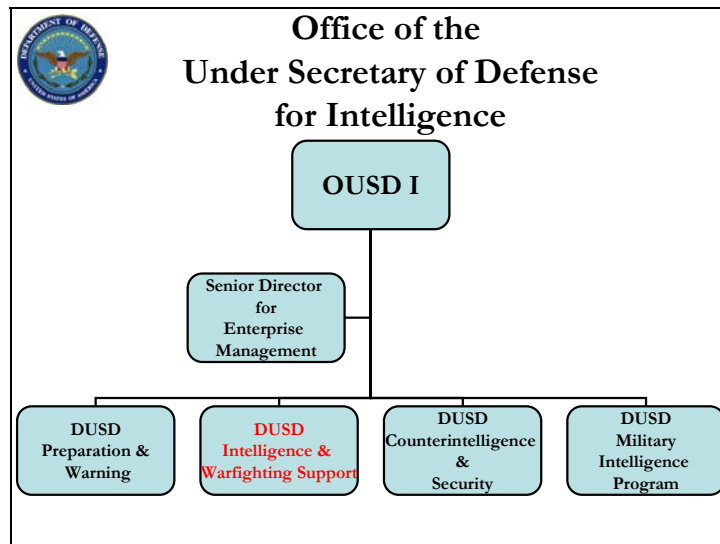


Figure 3

Dr. Cambone resigned on 31 December and there is a nominee, Jim Clapper, formerly head of the National Geospatial-Intelligence Agency [NGA] and of the Defense Intelligence Agency [DIA]. We'll probably see corporate action in a few weeks or months before he gets confirmed, and then we'll again have an official full-time under secretary for intelligence.


General Boykin is the deputy under secretary for intelligence and warfighting support. When was this office created? Does anybody know? You'll see a slide later that gives the chronology of events, but I'll say it right now: the major structural change in the Department of Defense in probably almost the last fifty-plus years was really made post 9/11, because of the nature of the problem and the threat. It created in law, in the authorization act of 2003, two new offices. One was an assistant secretary of defense for homeland defense—domestic stuff. We never used to have anybody officially in charge of it from a military perspective, but they created civilian oversight and created a combatant commander for the United States. The second structural change was creation of the under secretary of defense for intelligence, and that was Dr. Steve Cambone. That was the point that General Boykin just made.

Not only that, but because of the nature of the fight, because it's so human-centric and network-centric, the arrangements that deal with the human intelligence [HUMINT] community in the intelligence community revolve heavily around a relationship between the DNI, the CIA, and the Department of Defense. The under secretary of defense for intelligence is really pivotal in the relationship and the construct we currently have in the nature of the fight we're in today. It never existed before. It was spread out across the department. There never was anybody at the OSD [Office of the Secretary of Defense] level, in terms of civilian oversight, who specifically had a requirement to cover all the intelligence.

Boykin: Let's take a historical look at intelligence (**Figure 4**). First of all, in 1947 Harry Truman sent his national security advisors to Key West and said "Write legislation for how we're going to do national security in the future." The bottom line was that Harry Truman believed we had failed at Pearl Harbor. Who was responsible for intelligence for this nation on December 7, 1941?

Student: The military services.

Boykin: That's right, the military services: Army and Navy. There was no Air Force. Truman said "You guys failed to predict the events at Pearl Harbor. We're not going to be surprised again. He sent them down to Key West and they wrote Title 50, or the National Security Act. Unfortunately, it created the Air Force. The Army has been struggling to get it back ever since. It created the CIA, and it made the director of central intelligence also the CIA director. You should keep in mind that from 1947 until 2004 the CIA director was dual-hatted as the head of the intelligence community, or DCI—director of central intelligence. Even though the cold war ended in 1989, we never changed that structure. It was a cold war structure that was developed there, and I will tell you that we stayed in that cold war structure until the legislation of 2004, which was driven by failure, or at least a perception of failure.



National Security Act 1947 Key West Conference

- National Security Act / Title 50
- Created:
 - United States Air Force
 - Central Intelligence Agency
 - Director of Central Intelligence
(*Also director of CIA)
- Driven by failure at Pearl Harbor
- Cold war structure

Figure 4

There are lots of changes going on today within this country, and within the Department of Defense. What's driving those changes? First of all, the threat (**Figure 5**). Now stop and think (and you military folks will understand this): What we were focused on during the cold war? We were focused primarily on formations—conventional forces—which were easily identifiable from overhead platforms. That's why our satellite technology was held so secret for so many years. We didn't want the Russians—the Soviet Union writ large—to know just how sophisticated that technology was so they wouldn't know exactly what we could see. We could tell where their strategic rocket forces were. We could tell when they were doing exercises. We could tell when they were uploading nuclear weapons on submarines. We had a whole structure that was built around being able to see what the Soviet Union and to a lesser degree China were doing.



Driving Forces Behind Change

- Change in threat – (conventional vs. asymmetric)
- Change in the political / military situation
- War-driven requirements
- SecDef/USDI direction
 - Taking stock of defense intelligence
 - Defense HUMINT reform
- Perception of failure
 - 9/11 Commission
 - WMD Commission

Remodeling
Defense
Intelligence

Figure 5

That was the cold war. That has gone away. Now we are literally searching for one man. I don't mean that's the sum total of what we're doing in intelligence, but think about trying to take that structure and turning it so that it is in fact manhunting—looking for one guy, probably in the hills of Pakistan. There's a substantial difference. So the threat has changed, and we're changing the way we do business.

There are lots of changes in the political and military situations. Here's a good example. What was NATO [North Atlantic Treaty Organization] created for? It was a counter to the Warsaw Pact. Now there is no Warsaw Pact, so what's the relevance of NATO? Does anybody know what just occurred in Afghanistan?

Student: NATO took control of operations.

Boykin: NATO just took over in Afghanistan, even though an American is the NATO commander there. NATO now has thirty-seven nations participating in that operation—they're not all NATO nations—and NATO is running the command and control for these thirty-seven nations in Afghanistan. So, changing political and military alliances are driving changes.

You may not be aware of this, but the combined defense budget of all the military forces of NATO is less than the Army budget in the United States. So, as NATO draws down its maneuver and strike capabilities, I would make this case: One of the things that should grow to offset them is the intelligence capability of NATO, so that when NATO applies its force, whether its strike or maneuver elements, it can do so precisely at the right time and right place, with the right effects.

We've got a lot of war-driven requirements coming out of Afghanistan and Iraq right now. The secretary of defense directed Dr. Steve Cambone back in 2003 to do a study called "Taking Stock of Defense Intelligence" and another one called "Defense Human Intelligence Reform." We combined those two studies into a single study called "Remodeling Defense Intelligence."

What else is driving change? Another perception of failure, like in 1947, when Harry Truman sent everybody to Key West. He believed we'd failed. There are at least two commissions now that said we failed. What did they say we in the intelligence community did wrong?

Student: The agencies didn't talk to each other.

Boykin: That's exactly right. And you know what agencies primarily? The military and law enforcement. The military community, with its capabilities to collect, wasn't talking to the law enforcement community. Then what did the WMD [weapons of mass destruction] Commission say? It said we'd missed the boat on the issue of WMD. So again we had perceptions of failure driving us back to substantial changes.

Matthews: To kind of walk you forward to 2004, I told you that not everything was done simultaneously. Change was incremental, and a number of forces were working in Washington to implement change. A lot of people didn't think we'd actually pass a law and directives. There were other things, as I've mentioned: the reorganization of the Department of Defense, the creation of the Department of Homeland Security [DHS], some shuffling around of things to

respond to the focus on the homeland. But because those commission reports came out on 9/11 and through the summer of 2004, the White House thought they could get ahead of the power curve and implement change by putting in a series of executive orders.³ They did that in August. To the surprise of a lot of people, it still wasn't good enough, and the Congress, in less than sixty days, passed the Intelligence Reform and Terrorism Prevention Act of 2004. Lo and behold, it was the law, and it had to be enacted.

There were some pretty big muscle movements in there, and they're listed on the chart (Figure 6). That second hat the director of the CIA wore was now moved to the director of national intelligence as a mechanism, it was hoped, to pull the entire intelligence apparatus and intelligence community together. He would by definition be in charge of everything.

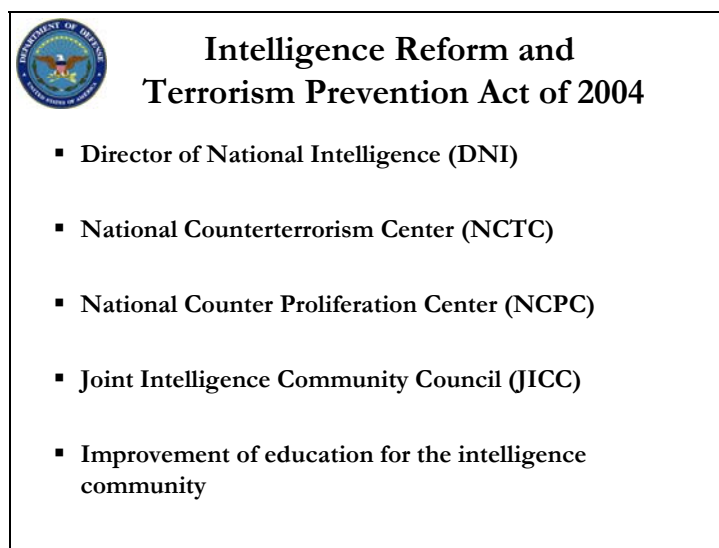


Figure 6

You all remember Ollie North, right? One of the big negatives, and the thing the American people didn't like, was that operations were being planned inside the White House. The White House and the National Security Council are supposed to be about policy, not about conducting operations per se. But the reality is that our government didn't have in one organization a location where the entire interagency—the departments and agencies of government, as appropriate—sat across from each other every day and planned and coordinated (synchronized if you will) the policy decisions to be executed for the country. You might get the Department of Defense planning to wage war or you might have a CIA operation, but who was really synchronizing and then prioritizing to direct the execution of the nation's business? There was no such place.

In the law there was this National Counterterrorism Center [NCTC]. Again, we get back to the point about information sharing and planning and how do we do that. I'll speak to how the

³ For a discussion of the intelligence reforms of 2004, see John D. Bansemer, *Intelligence Reform: A Question of Balance*, P-05-2 (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, August 2005), [On-line]. URL: http://pirp.harvard.edu/pubs_pdf/banseme/banseme-p05-2.pdf

intelligence gets shared in a bit. The law also created the National Counterproliferation Center, and that speaks to the WMD issue. That language kind of scratched the WMD Commission's itch.

The Joint Intelligence Community Council is where the heads of all the intelligence agencies can convene as the seniors to talk about business.

There's a new approach to education in the intelligence community. For example, in the 1990s, when the Army downsized after the first Gulf War, the armed services had already been downsizing. They put in a "stop loss" and a freeze to fight that war, and then they said "Thank you very much for your service to the nation." A whole bunch of people were let go, and the force structure of the Army was reduced by about 35 percent. Guess what they reduced? They couldn't get rid of systems that quickly. At the time there wasn't a perception of what the real threat was. It was perceived, out of old habit, that technology could provide us the intelligence we needed, so what we did was draw down the manpower for intelligence. Congress mandated the strength reductions, and we did that. The human dimension of intelligence took a big hit in that arena. So the end strengths came down and the numbers in the service came down: we were going to rely on technical means to gather intelligence. When the threat changes and becomes human network-centric it's very difficult to have only technology to provide you the level of fidelity and clarity that you need. That's a HUMINT task.

We're in the process of building that back up now, so this intelligence education for the community at large is a big deal. We're having to revamp, modernize, and change the community.

This depicts the law (**Figure 7**). You have the NCTC, you have NCPC, and they work for the DNI. The law says "You're going to have in the NCTC representation from all the appropriate agencies and you're going to have a Directorate of Intelligence and a Directorate of Strategic Operational Planning. How do you define "strategic operational planning"? Is it strategic? Is it operational? Is it supposed to be doing operations as opposed to planning? What is that all about?"

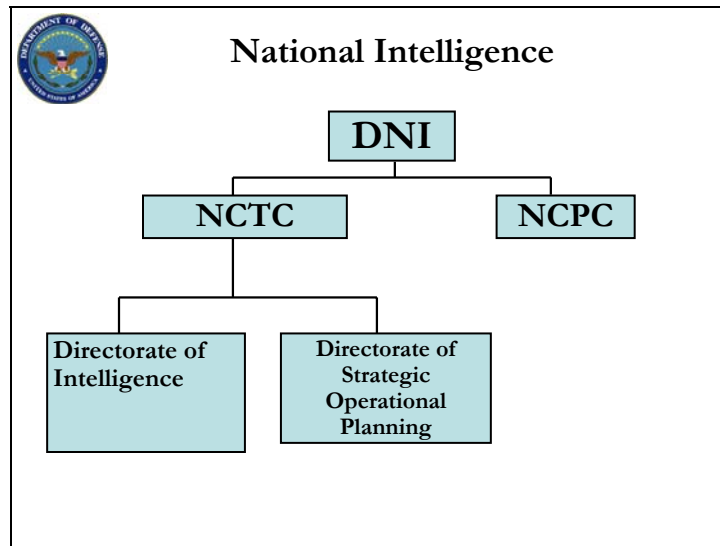


Figure 7

We spoke to the folks who wrote that language in the law as we moved to try to implement this, and they said “We don’t know. We just know that you have to tie the strategic to the planning and operationalize that stuff. You need to do it coherently across the government. You figure it out. We just know it needs to be done. We can’t define it exactly, but we know that it’s needed.”

So that’s how the NCTC began. It is an up-and-running enterprise now, with representation from all the appropriate agencies that deal with intelligence, obviously with a focus on counterterrorism (**Figure 8**).

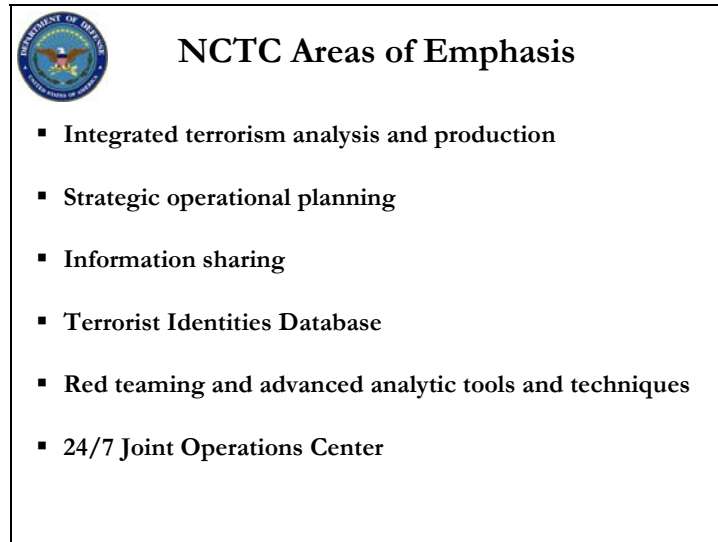


Figure 8

Student: Does the NCTC do any actual tasking of operations, or does it just receive information from CIA, DIA, and the defense collectors in the field?

Matthews: What it’s supposed to do is government-wide planning, where it directs the prioritization of efforts. Does it direct operations? No. It’s supposed to synchronize them, but you still have a bit of a problem there. The problem is that it really can’t direct the Department of Defense to do X, Y, or Z. When you move to the direction of the resources of the different departments and agencies, you need to transition from that center to the forums that we use today, which are the deputies’ committees or the principals’ committees that no-kidding make the decisions and represent the leadership of those organizations.

In theory, the NCTC is supposed to be empowered by the departments and agencies it represents to speak for them. The staff go to work every day in the same place, which we never had before in our government. We would have PCC—Policy Coordinating Committee—meetings at the White House. They were kind of like your class. People come in, everyone’s together for a while, very intensely discussing things, the meeting ends, and you go about your business. What is the coalescing mechanism? When you go back to your parent organization, with whom do you coordinate the plan you made with the other guy? There was no such thing. You now have that,

but there's still difficulty in implementing the execution of a comprehensive program across our government. A couple of shortfalls are more apparent than others.

Student: Is the NCTC domestically or internationally focused, or both?

Matthews: It has representation from all, but the reality is that it's focused on the international more than the domestic. It views the international with an eye toward whether there's a threat that will manifest itself in the homeland. You have the DHS there, you have the FBI [Federal Bureau of Investigation], so you have people who are worried about the homeland. The lawmakers planned the NCTC activities with a global perspective to do things in the away game, as they say—away from our shores—to disrupt and preempt things that could manifest themselves back at home.

Boykin: The earlier question is the most fundamental to this whole thing: does the NCTC run operations? The answer is that the law specifically says no. Having said that, the idea, as Tom pointed out, is that it should be in a position to have situational awareness, to know what's happening around the world, and to be able to say to the different departments within the intelligence community, "DoD: here's a mission we want you to take the lead in planning. Department of State, Treasury, Homeland Security: you guys will be in supporting roles." Then they go off and they plan and execute under the authorities of the lead agency. It could be State or Justice in the lead, particularly if it's domestic. That's the way it's supposed to work, but the law says it cannot run operations. That goes back to what Tom said earlier, which was that in the 1980s, when Ollie North and John Poindexter were running operations out of the White House, everybody said "Never again." The law says the NCTC will not direct operations, but it is a place to plan, coordinate, synchronize, and make recommendations on the operations to be conducted.

Student: What mechanisms did the law give it to facilitate that synchronization?

Matthews: It has a thing called a national implementation plan. It's essentially a national plan with input from all the departments and agencies on what they're doing and can do to help fight this terrorism network. So, first, they have to develop the strategy. Second, they have to essentially survey what everybody can bring to the table, what their core competencies are, what tasks have to be done, whose resources will be applied against this task, and what sequence of implementation will be used. Then it's up to the departments and agencies to do it.

Now, the other reality of it is that the NCTC does one other big thing on a daily basis: it prepares the President's Daily Intel Brief. It is like a twenty-five-meter target. That means it eats their lunch every day. They put a lot of resources on it every day, and all night. Formerly Ambassador Negroponte, now Admiral McConnell, is responsible, and he is the guy briefing the president every morning on what's hot: what's the intelligence, what's the threat, what's the problem that we've got here, and what's the consensus of the intelligence community about this? That's the other big item it does, and that tends to consume it. If you deal with everybody rushing to the soccer ball on a daily basis, that doesn't allow for a very good strategic view. So the NCTC has to balance both of those things.

Student: Do you think there is an appetite for further reforms in the near future? It doesn't sound as though you're happy with the organization as it is now in some respects. I've heard the criticism before today that the 9/11 Commission's recommendations were implemented after a bunch of stuff was already in the works. Is the intelligence community ready for more reforms? Are they in the works?

Matthews: I'll be blunt with you: I think it would take another event to require us to jump: to raise the bar or that threshold to the next level. It has sought its own level of advancement, and that threshold has gone to where it's gone. Absent another external catalyst, in my opinion, we're going to have some degree of where we are already.

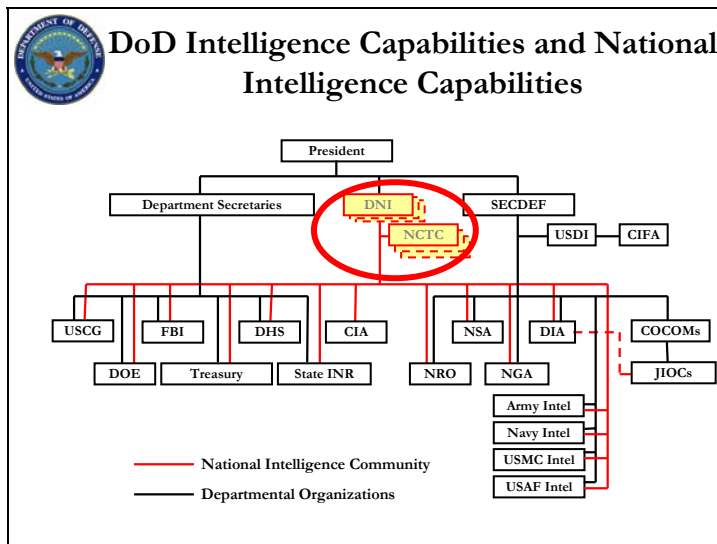
Boykin: How many of you here are intelligence professionals? Lots, I see. I'm going to make a statement and see what your reaction is. The most inflexible entity within our government is the intelligence community. It's resistant to change. Does anybody disagree with that? Now, lots of change has occurred, and it's because there are some visionaries within the intelligence community, but institutionally intelligence is a very conservative organization, with a very conservative ethos. By nature, conservatives are resistant to change. They like the way it used to be and never was, if you will.

It's been tough getting the intelligence community to make the changes that have occurred, because in 1947, when we built this intelligence community, we built it as individual organizations. In 1953, for example, NSA was organized as ASA [Army Security Agency], but nonetheless it's what we know as NSA, to collect signals intelligence. It became an entity unto itself. It did its own analysis, it did its own production, and it retasked itself. That was okay during the cold war, because of what we were looking at, but it doesn't support the dynamics of today's threat or of today's operations. That's why it's been such a struggle getting organizations that for years have invested in technology that will allow them to talk to themselves now to divest themselves of that and start investing in technologies that will allow them to talk to other intelligence entities—particularly analysts—and other coalition partners. It's been very difficult to get the community to change. That's my assessment of it; you may not agree.

Matthews: If you look where the red lines go, there are your sixteen agencies (**Figure 9**). The DNI is both an office and a person, but he doesn't generate intelligence. The red lines and where they run show the intelligence community.

The ones that the secretary of defense has a direct line to are highlighted in yellow (**Figure 10**). I'll point out one other thing: we have the Coast Guard listed there, as well as the Department of Homeland Security. When they reorganized and the Homeland Security Act was passed, the Coast Guard became part of the Department of Homeland Security. They are shown separately because they used to be part of the Department of Transportation, and they had their own intelligence apparatus. No one stood that down and told them to do away with it, so they came into this organizational structure with an intelligence capability already established, and then the Department of Homeland Security established an additional intelligence office within the department.

CIFA is the Counterintelligence Field Activity. It's kind of unusual, because it actually plugs right into the office of the under secretary of defense for intelligence.



CIFA = Counterintelligence Field Activity COCOM = combatant command DOE = Department of Energy INR – Bureau of Intelligence and Research NRO = National Reconnaissance Office USCG = U.S. Coast Guard

Figure 9

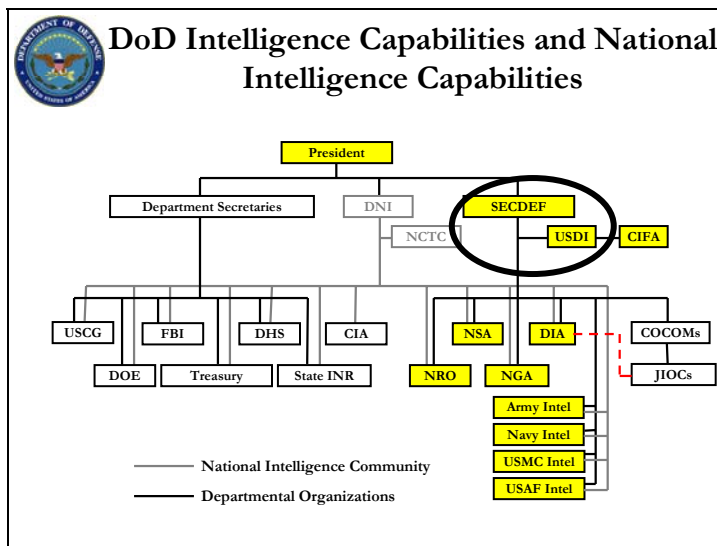


Figure 10

Boykin: Let’s talk about analysis. Executive Order [EO] 12333 says that the DCI—now the DNI—is responsible for competitive analysis. The first question is: What’s an executive order? Is it a law? In fact, it is not a law by strict definition, but it is treated as such. It is an executive proclamation, signed by the president, that says “This is how we will operate.”

What do we know most about EO 12333? What do we hear the most references to?

Student: Assassination.

Boykin: It says we will not assassinate. There's a huge legal debate as to what that really means. That executive order says other things too. It says how we will run intelligence in this country. One of the provisions is that the DCI—now the DNI—is responsible for competitive analysis.

What is competitive analysis (**Figure 11**)? It's a pretty simple term. Does it mean I give everybody here all the information available, they do an analysis, Person A doesn't agree with the rest of the group, and so I give that person a footnote in the analysis? That is not competitive analysis. Competitive analysis says I give this group over here all the data available, I give the exact same data to the group over there, they go away without collaborating, they come back, and I compare their analyses.

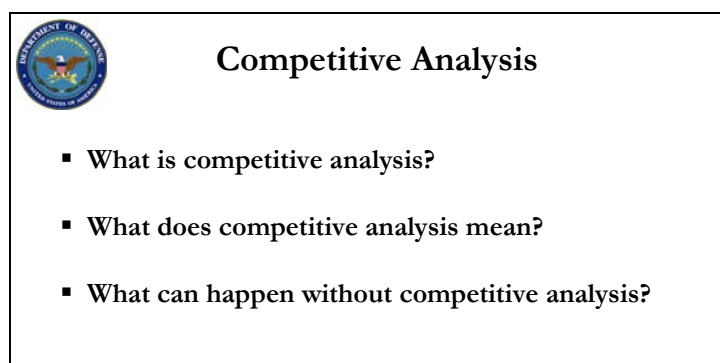
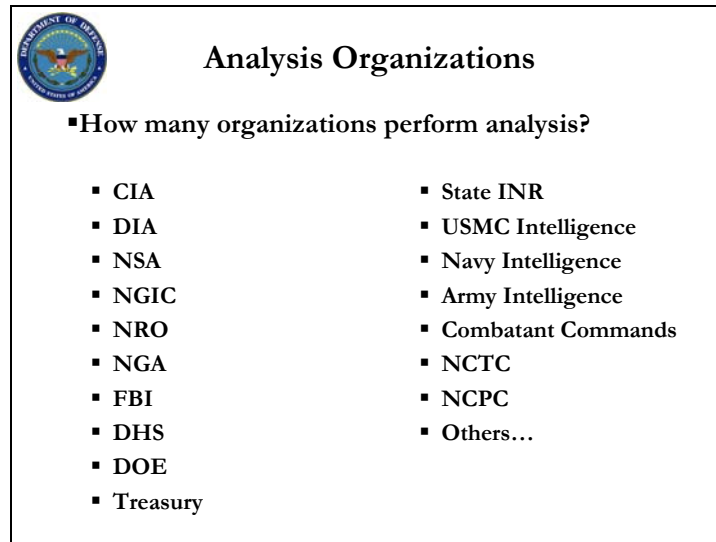


Figure 11

Let's go back to the run-up to the invasion of Iraq. Where was the analysis done on the issue of WMD? It was done at CIA, at the intelligence directorate of CIA, which is their analytic center. Where else could it have been done? In fact, all of these organizations do analysis (**Figure 12**), and that's not everyone who does analysis. What's the primary one that could have given a competitive analysis of the issue of WMD? The Defense Intelligence Agency—DIA. It has a huge, very good analytical capability. But the criticism in the WMD Commission was that we had a DCI—George Tenet (great guy; I used to work for George when I was assigned to the CIA, and he is a great American)—who was also the CIA director. When your whole staff and your whole surroundings come out of one organization it's hard for you to be objective and to do what the executive order calls for, which is competitive analysis. That is the primary reason that they separated the DCI from the CIA.

Now, on the other hand, were there WMD in Iraq? Let's be clear on that. Yes. We found enough already to kill tens of thousands of people, but it wasn't what was supposed to be there. It wasn't what the analytic community said was there, or at least we haven't found it. So we just missed it on analysis.



NGIC = National Ground Intelligence Center

Figure 12

To do competitive analysis, and the kind of focused analysis we need to do, we have to have the ability to share the data that's available with the analyst. We cannot do that today, for two reasons. The first is that because these intelligence organizations have grown up as individual entities they have built communications systems that basically communicate with no one but themselves. They do that very effectively, but they don't have architectures to share their data with analysts from other organizations.

The second thing is that we don't have the policies within the intelligence community that allow us to share information. Why is that? The policy issue is one of sources and methods. Under the same executive order, 12333, the DNI is responsible for the protection of sources and methods. What does that mean? You're going to hear it a lot if you're going to be in the intelligence business.

Student: It means the way you collect the information. For instance, if you're collecting it with satellite technology you don't want anyone to know how accurate it is or how that satellite collects the intelligence. They could possibly spoof it or defeat the intelligence collector.

Boykin: Exactly right. When they talk about sources and methods they talk about protecting how we got that information, because in many cases it could only be one way: Maybe it's one human source, or maybe there's a SIGINT device in a specific location monitoring diplomatic communications and we don't want anyone to know we've got it there.

The policies in our country do not allow us to share that information with the analyst. That's one of the things that we're in the process of changing right now.

Matthews: I'm now going to fall back to where I left off. In the Department of Defense we got the first-ever under secretary of defense for intelligence. He came in and he did the same thing you would do if you got the task. You essentially have to figure out what the organization is

doing, if there are any gaps and seams, and what it should be doing given the nature of the threat, the nature of the problem, and the world we live in today.

That’s essentially what he did. He started off by looking at HUMINT, because that was obviously the most critical. He quickly realized it’s an all-source world, and the information comes from everywhere, so what he did was went about this thing on an earlier slide (Figure 5) called “taking stock of defense intelligence.” That meant going out with a team, surveying everybody, listening to them, finding out what was broken, and coming back and setting a way ahead to fix these problems that everybody has to deal with in the field and that need to be fixed now that we’ve got one guy in charge.

This defense intelligence survey is what has led us in this last year-and-a-half journey to do what we’re doing today. The first thing (and we’ve touched on it) is that there’s strategic intelligence, there’s tactical intelligence, there are all the various INTs—SIGINT, HUMINT, you name it—whatever you’ve got, and it’s in these piles in organizations everywhere. In some it’s up here, and in some it’s down there, and it’s in stovepipes. The overarching concept in remodeling defense intelligence was to have an enterprise that crushes the strategic down all the way to the tactical and connects everybody and all those INTs in some common IT [information technology] architecture so that everybody is able to share with everybody else (**Figure 13**).

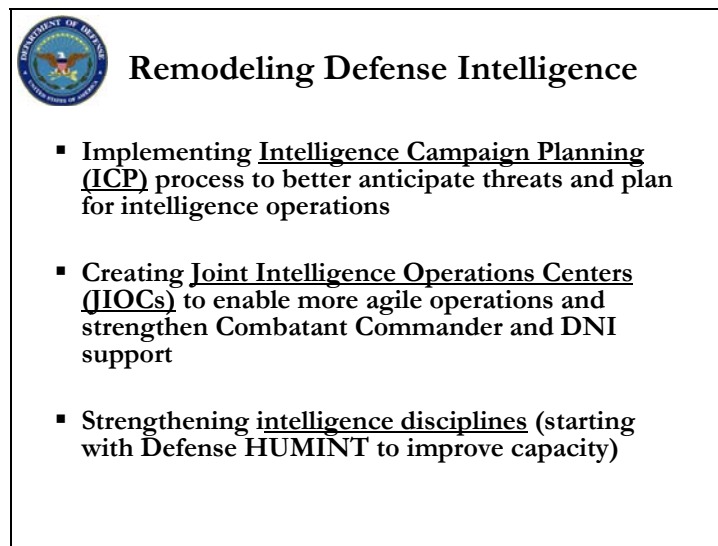


Figure 13

We had to change the whole paradigm about sharing: the inability to share and the way we build our systems so that we can’t share. When you gather this intelligence, for years and years it’s been about protecting these sources and methods. But if you’re the only person who knows about it, it’s not very useful to the rest of the community.

The paradigm shift is figure out how much of this information and intelligence you can share, and hold back or restrict by exception. That’s a huge change. It affects everyone, from the individual analyst who writes something down and puts “ORCON”—originator control—on it or puts “NOFORN” on it, which means you can’t share with an ally.

There are thirty-seven countries fighting in Afghanistan today. We talked about all the problems we have in our government; take that and figure out how to share intelligence and information with thirty-seven coalition partners. By the way, the military has decided to set up a command called Africa Command in the future, and we're in the process of doing that. We're going to have all kinds of other coalition partners that we never dealt with before, and to enable the effort we're going to have to share information and intelligence. We are not designed to do that. That was one of the glowing findings of that survey. So, remodeling defense intelligence, in a nutshell, means crushing it down, breaking down the stovepipes, and using an architecture that enables us to share as much as we can as often as we can.

The first thing up there is an item that came out of this as well. It's called an intelligence campaign plan. You ask "What is that? We do campaign planning all the time." But we don't do intelligence campaign planning. Without boring those of you who don't know a lot about individual military plans, we've got a thing called an Annex B, which used to give us the order of battle of the enemy. But it didn't say how we were going to marshal your intelligence resources, figure out how to plan to employ them at any phase of the fight we were in, and prioritize the effort of those (quite frankly) few resources that we had to get the information and intelligence we needed. We didn't even have a planning vehicle to do that, believe it or not. That's what this intelligence campaign plan is: the idea is to look at every source we have that can gather intelligence, figure out what sources we want to apply in what phases of our plan to support that operational plan, and then do that detailed campaign plan to support our operation. This is about operationalizing intelligence, which you'll hear more about.

I explained to you about crushing down the strategic. We've got to have an organizational construct, just like the NCTC, where we're collocated, have access, and have the ability to share among ourselves. We need every intelligence agency that's in the fight, or at least their representation, sitting around so we can leverage anything and everything that each one in that room can bring to the fight. The JIOC is the organizational construct by which we're implementing that. It's tough, because we're doing it at all commands at the same time, and at the DoD level at the DIA, and we've got to build that apparatus with a war going on at the same time. A laboratory, if you will, has been under way for about two-and-a-half years in Iraq, trying to net together over 200 databases that have developed on information and intelligence in Iraq alone and figure out how to share it to continue the fight. The same is true in Afghanistan.

The last bullet is kind of an education piece, and I've already touched on it. By the way, we have to redo how we recruit the right kind of people, entice them to come in, reward them for their efforts, and keep them focused in their disciplines. You might get an analyst in PACOM, the Pacific Command, who works on Korea for five years and then, because he's been in PACOM too long, it's time to move him to DIA, where he works on something completely different. We've just lost five years applied to the problem that person was an expert on, because it's time to move that person on to some other area for professional development. That's not the professional development we're looking for. We're looking for something that's more focused on that subject matter expert and a career progression for an entire career.

This shows what the ICP will do (**Figure 14**). Every one of the combatant commands will get a JIOC, or has a JIOC. Each of them will set up that JIOC and each JIOC will do an intelligence campaign plan for its particular campaign. It's all an effort to congeal the entire intelligence apparatus for the Department of Defense.

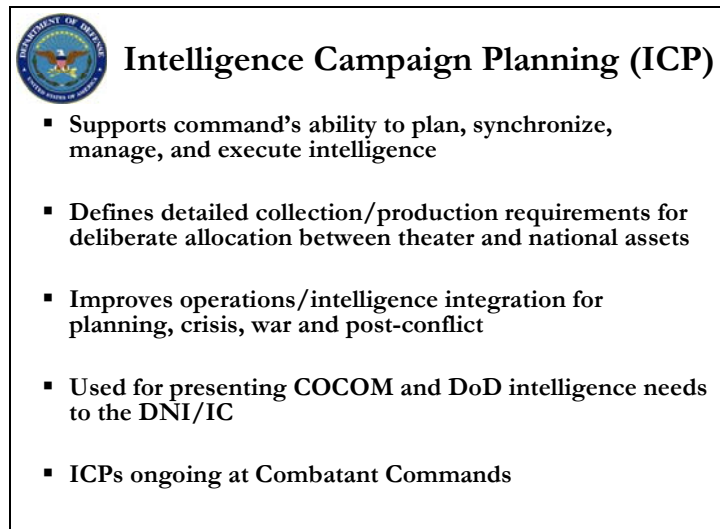


Figure 14

Boykin: We've talked to you briefly about these things called JIOCs (**Figure 15**). The centerpiece of the JIOC is the analyst. What we're talking about here is analysts literally putting a puzzle together. We've created this structure out in the combatant commands that allows analysts to solve problems and facilitates their being able to talk directly to the entities that have to collect intelligence.

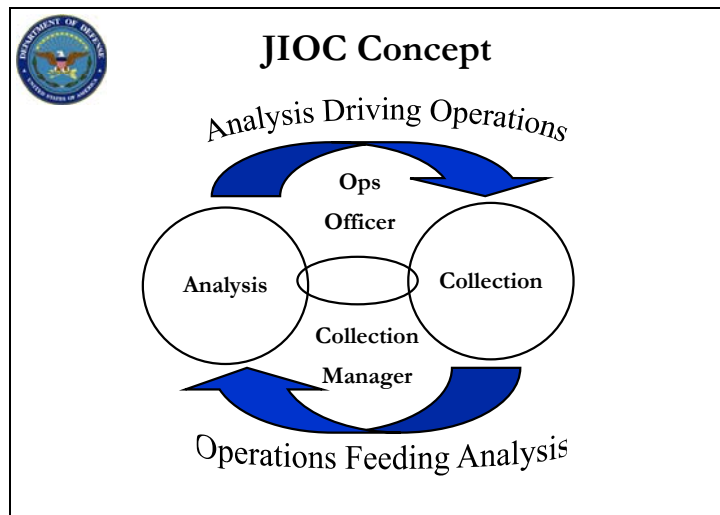


Figure 15

If you look at the way the Department of Defense is organized today, out in the theaters—Southern Command, Central Command, European Command, Pacific Command, Special Operations Command, down the line—you have disparate chains of command, if you will, for all the different elements of their intelligence apparatus. For example, most of DoD’s analysts belong to DIA. Your collectors belong to about five different organizations. Both CIA and DoD have HUMINT collectors; your signals collectors belong to NSA; your geospatial collectors belong to NGA; and you have chains of command out there, none of which is under a single entity. What we tried to do here is bring them all together under a single chain of command and make the senior intelligence officer—the J-2—in that theater the director of the JIOC. The analysts are the focal point. They and all of those around them are putting a puzzle together.

Let me give you a vignette. On December 5, 2003, most of you saw an elated chain of command in Iraq when we captured Saddam Hussein. Remember Saddam’s two boys, Uday and Qusay? How did we catch them? Somebody came in and said, “I understand there’s a \$25 million bounty on these toads. Well, I know where they are, and I want my money.” That’s exactly how we found them. Somebody came in, got the \$25 million for each of them, and we went to them and killed them.

Saddam and his capture were a different story altogether. There were two analysts, enlisted, one Marine and one Army, sitting in the Joint Special Operations Center, which at that time was not a JIOC but looked an awful lot like it. They were putting a puzzle together, and they were literally across the room from the folks doing the collection operations for them. The analyst would say “You know what, Joe? If you can capture the following individual—and here’s his last known location—and interrogate him, ask him these questions, and let me know what he says, I’ll have another piece of this puzzle put together.” Joe would saddle up, get in his helicopter or his Humvee, and go capture the guy who’d been identified. Joe would interrogate him on the scene, provide the information directly back to the analyst, and the analyst would have another piece of the puzzle. Eventually we had it all. It came together. There was no golden BB on Saddam’s capture: it was hard analytical work. Finally these two analysts had a complete picture. We knew where Saddam was and went right to him.

The point was that when this analyst said “I need the following information” to the collectors, there was nobody in between who was saying “Well, what the analyst meant to say was.... What he really needs is...” and that happens in the intelligence community all the time. There’s somebody who’s smarter than the analyst who’s always deciding exactly what the analyst really needs. We’re eliminating that, and, by the way, when the collector gets that information he gives it directly back to the analyst and there’s nobody in there filtering that and saying “You know, he doesn’t really need that information.”

Has anybody here heard of a tearline? It’s a common phrase. What it means is: “Below this line all this information is releasable, but only a very select group will ever get to see what’s above the line.” It protects the sources and methods. That tearline itself occasionally prevents that analyst from getting the kind of information he or she needs to solve that puzzle. We’re trying to eliminate that, so that the analyst talks to the collector and the collector talks to the analyst: a closed loop. That’s the JIOC. It’s operationalizing intelligence.

Now, since most of you are not intelligence professionals I'll just tell you that one of the problems we're having is that within the Department of Defense we have always considered intelligence to be a staff function rather than a line of operations. CIA considers it a line of operations; they have a Directorate of Operations. They put people out in harm's way in Baghdad, Moscow, or Kuala Lumpur, and they consider them as running operations. When the department does the same thing we consider it to be intelligence preparation of the battlespace—IPB—a staff function. We're changing that paradigm: we're making intelligence operations. For example, the operations directorate in Korea today is concerned about readiness and training. The intelligence directorate in Korea today is running operations twenty-four hours every single day, trying to figure out what Kim Jong Il is about to do. That's operations. We're trying to operationalize intelligence within this department and take it from being a staff function to being a line of operations. That's what part of this JIOC organization is all about.

Matthews: We're talking a lot in military terms. We're referring to the interagency, but this problem and threat network have components that we in the military do not have core competence in. Treasury deals with the flow of money. That's not something that we are experts in. You go to a target, you take down an objective, and you arrest some people, and if they're not high-value individuals whom you need to interrogate—if they're just criminals who have been killing people, and there are a lot of them out there—then you can transfer them to the legal system in Iraq to get a jail sentence for those individuals. You then have to present a case that can stand up in court. In the operations centers in Iraq today there are over sixty FBI agents, and they had to help train operators who were kicking in doors so they didn't destroy evidence. They were teaching them how to gather evidence—not a skill set that they were worried about—so that they could have a criminal case to put someone away. A foreign fighter caught in Iraq will automatically get twenty years in jail, but you have to present a case in front of somebody in the legal system to get there. So how we do what we do is very different, and the intelligence that we need today is a lot different than your father's intelligence.

Boykin: Nowhere have we made greater improvements than in HUMINT (**Figure 16**). In about 1973, when the Church Report came out, it said that the Department of Defense was spying on Americans, and the Department of Defense got risk averse. From about 1973 to 1975 the Department of Defense fundamentally divested itself of clandestine human intelligence. Now we're in an environment and up against an enemy where we must rely heavily on human intelligence and we are rebuilding our human intelligence capabilities. The Army alone—and you see the first bullet up there—is restructuring its human intelligence. In fact, the Army is taking about 8,000 spaces, primarily from artillery units, and restructuring to have a more robust intelligence capability, specifically human intelligence. That's happening in all the services. We are putting a lot more money into human intelligence for cover support, technology, training, and manpower as well.

We're also decentralizing the authorities for human intelligence, so what was once controlled at the very highest levels of the Department of Defense is now being controlled down at the combatant command level. These combatant commands have the authorities to run clandestine human intelligence on their own.



Figure 16

Then we're writing new doctrine, and what we're doing is legitimizing the concept of clandestine human intelligence within the military. There are those who would tell you that the Department of Defense does not have the authority to run clandestine human intelligence; that it's all governed by the DNI. We have done a complete and total legal review, and that is simply not true. It's an urban legend that grew out of the seventies that we've lived with for a long time. The secretary of defense has every authority to do clandestine human intelligence. What does that mean? It means recruiting spies, for example.

Student: Even outside a combat zone?

Boykin: That's a good question. The fact is that in order for the secretary of defense to do clandestine human intelligence outside Iraq or Afghanistan one of two conditions must exist. He could do it as part of his Title 10 preparation for combat, under the rubric of the global war on terrorism. If he anticipates a problem in the future, he could say: "I believe that there is a high probability that the department is going to be engaged in combat activities in this area. Therefore, I'm conducting clandestine human intelligence in this area in preparation for that eventuality." The second condition would be that it is being executed under the authorities of the DCI (now the DNI) through the process that is called DCID 5/1. At that point, when you do it under the DCID, it becomes a Title 50 activity, even though the military is doing it, and it's the DNI's responsibility.

Regardless of what you might read in the *Washington Post*, we do not have issues with the CIA over this. The *Washington Post* would like very much to create issues, but we are working hand in glove with the CIA to coordinate this clandestine human intelligence. We've signed two memoranda of agreement [MOAs] with them. Secretary Rumsfeld signed the basic MOA and I signed the implementing instructions, along with the director of operations at CIA. We are working together to make sure we can all work in the battlespace.

Matthews: We're at the point where we're supposed to get to the questions and answers. I think we've touched on everything there (**Figure 17**). We've kind of got the point where we're trying to shift from the left side over to the right side. I think we hit pretty much everything up there, with the possible exception of actionable intelligence. Jerry, would you like to comment on that?

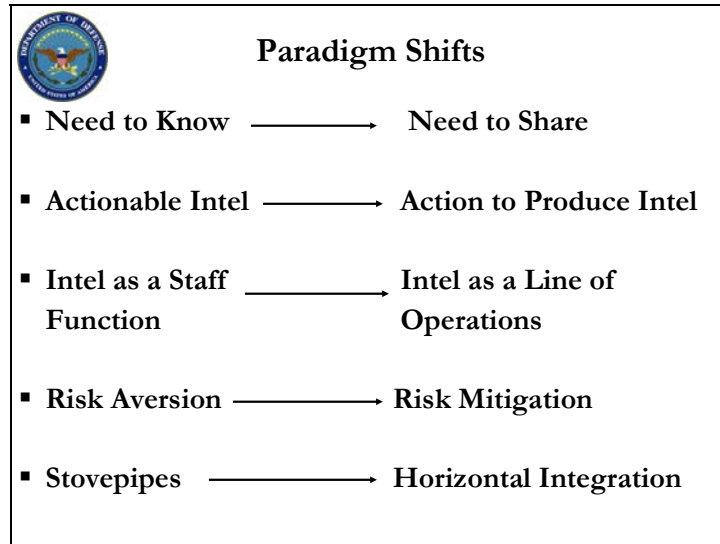


Figure 17

Boykin: Does everybody understand the concept of actionable intelligence? Giving me intelligence that I can act on? I think that's nonsense. I think that for too long we've used that as an excuse for not doing things, and then blamed the intelligence community because we didn't have actionable intelligence. My view is: Get out there and take some action and you'll get some intelligence. The best units on the battlefield are the units that make things happen, and they get a lot of intelligence.

Matthews: That goes back to risk aversion. If you give me perfect knowledge it's pretty easy to go forward. There's no ambiguity and so on and you don't have to worry too much about risk, because it's just clear as day that everything you need to know is right there and what you need to do is clear, so you just go do it. Particularly against this threat, you have to get into the battlespace. The Army says now "Every soldier is a sensor." The nature of this fight is that you are seeing, touching, feeling, and smelling the environment. You've got to be sensitive to it and you've got to report on it, because it's in that environment that the threat exists. It's a different world out there—very different.

Boykin: We've got a couple of minutes for questions, so what's your question?

Student: Sir, you mentioned a lot of paradigm shifts within the intelligence community. Have you been able to affect the community management in the specific branches of the intelligence community in the services?

Boykin: Yes, we're working that right now. One of the areas where we really hope to affect the services is, for example, the management of attachés. The only one of the services that has a professional attaché program is the Army. All the services should have one, and have better ways to manage their attachés. I told you earlier that the Army, for example, is adding 8,000 spaces for intelligence.

Student: You mentioned a lot of ways to make intelligence officers more sensitive to operations, but have you addressed how to make the operations types more sensitive to potential intelligence requirements, specifically at the junior officer level? Both of you had significant operational experience before you came to the intelligence community. Special Operations probably works more hand in glove with the intelligence community than with the conventional forces.

Boykin: Yes, we're working that as well. We would have called the JIOC a Joint Intelligence Operations Command had it not been for pushback from the "operational" community. They just could not come to grips with intelligence having another command, particularly one that would be operational. We just have to beat them down. They're paradigm shifts; we just have to whittle away at them one at a time.

Matthews: For what it's worth, the way you direct things, the secretary of defense can sign a number of documents. One is called an "execute order." He directed and signed an execute order for all the commanders out there. These combatant commanders have the world divvied up. There are five of them geographically who are responsible for every square inch of the earth. We poll them and communicate with them about how to do the department's business. The secretary signed out an order to all of them, coordinated with the interagency, about where we as a department need to go with this remodeling of defense intelligence. The order told them that we need to establish these JIOCs, and telling them the concept and the vision. Implementing them is tough. Some of them are doing it a bit better and faster than others, but we just have to keep the momentum going.

Fein:⁴ General, would you say a little more about national intelligence and military intelligence and how you see your role and your office's role in both of those areas?

Boykin: "National intelligence" is defined in the 2004 legislation as "intelligence of value to two or more national organizations within the intelligence community." There's very little intelligence today that isn't of value to multiple organizations, so then you have to go back to the purpose of collecting it. If the purpose is to satisfy a national-level requirement, then it is national intelligence. On the other hand, if the primary purpose is to satisfy a Department of Defense requirement, it's military intelligence.

Matthews: In this day and age it can be strategic and tactical intelligence at the same time. There is a DNI representative in each of these JIOCs, along with all the combat support agencies and the military structure. So everybody is there. With scarce resources, if there is a national requirement that can be serviced or acquired by somebody in the field at the tactical level, we do that. We

⁴ Dr. Robert A. Fein is director of the National Violence Prevention and Study Center, and a member of the DNI's Intelligence Science Board.

never had the means to convey that, identify that need, and have that resource go get it if they happened to be able to. There's a JIOC at the defense level, at the DIA, which has a DNI representative who connects to the rest of the interagency and then is connected to each of the combatant commands. You now have an enterprise architecture to allow that.

Student: With the shift in structure of the intelligence community to fight global jihad do you have any concerns that we might not be able to gather intelligence on conventional forces, or do you think that all these steps help the intelligence community to be more effective?

Boykin: The primary change is the development of and the enhancements within our human intelligence community with regard to looking at the global war on terrorism and what we need to be successful. We're tracking the money and developing better human intelligence. All the apparatus that was designed to look at conventional forces is still there and being modernized, so I am not worried about that.

Student: Are there any structural changes for getting information from intelligence agencies outside the United States, for instance, from allies, and getting it to those centers?

Boykin: We have great allies. Unfortunately very few of them made much of an investment in intelligence. The British have; the Israelis have; the French have done a pretty good job. The Canadians haven't done much. As a cold war carryover we have certain relationships, particularly with four of these countries, and they are being optimized as much as possible. There are any number of other arrangements, given our new partners in this fight.

Matthews: I'll just tell you that on the ground, at the tactical level, is where it's always the best. You have the most intelligence shared, because they're in the same battlespace. They're all facing the same problem, and normally it's all about one mission focus by that same group of people. So if you're organized correctly and you have a presence there, they will work it out on the ground. The higher you go away from that, and the closer you get to Washington, the more bureaucratic it gets, and obviously the more resistance and friction and cultural bumping into each other you find.

Student: What we've seen in the last couple of years is a lot of policy-level integration and a lot of analytical integration at places such as the NCTC. As conflicts become more unconventional there might be more of a need for integration at the operational level, conceivably a kind of operational unit where you bring in people from both civilian and military agencies. Do you see a need for groups like that? If so, do you think the government might respond by actually creating integrated operational units of some sort to handle intelligence?

Boykin: That's what NCTC is supposed to do. Tom mentioned that we're standing up a new regional command called Africa Command. It's interesting that there's a concept on the table that says that ultimately Africa Command could be commanded by the State Department, so there is a strong view that it needs to be an interagency organization. Part of what NCTC is supposed to do is try to help organize an interagency effort with lead and supporting agency designations.

Student: Sir, you talked about how the cold war structure is being replaced by this new structure. Do you think we need the new structure because the challenge of gathering data from entities that are not states is simply greater than the one we had before? We could have had this structure in the cold war. Do you think we would have done better than we did in that time, or do you think there are trade-offs between the type of structure we needed to gather intelligence in the cold war and the type of structure we're developing now? In other words, is this an improvement or are there some alternatives?

Boykin: I think we're achieving a better balance now. That's the way I would characterize it. For many years, the only entities within the Department of Defense, for example, that really had an intelligence apparatus that would allow us to focus on individuals, linkages, and all of that was Special Operations, the community that Tom and I came out of. We did that because that was our mission: chasing people like Manuel Noriega in Panama, Pablo Escobar in Colombia, and Mohamed Aidid in Mogadishu. We had that kind of intelligence structure built into Special Operations. Now the whole country is facing that challenge, so we're having to make improvements and achieve a better balance between the old cold war structure and what Special Operations Forces do.

Matthews: The reason is because the threat changed. It's a function of the threat, and you have to adapt and do measure, countermeasure, counter-countermeasure. It's a cat-and-mouse game, and with humans in it who are innovative, learning all the time, watching what you do, and then changing what they do it's a constant dynamic. If you have a set piece of twenty divisions lined up that's relatively simple. We have the systems that can identify all those, and we could apportion our resources with precision-guided munitions, but we don't have that as our primary threat today.

Boykin: I'm going to have to go, because the flights are so squirrely out there at the airport.

Borg: Sir, it's been a pleasure having you here. We very much appreciate your taking the time to travel here and brave the cold weather that Boston has to offer. We'd like to send you home with a little memento of your time with us. We look forward to hearing more good things out of your world.

Boykin: Thank you very much! I enjoyed it.

Borg: Are there any other questions? Mr. Matthews was going to grab the same plane as General Boykin, but he's willing to stay behind and answer some more questions.

Matthews: "Leave no man behind" is our motto, but I'm ready to stay.

Student: You talked about the importance of information sharing. I couldn't agree more. Certainly in my experience the one place that has it more right than wrong is the NCTC. All the data is coming in there. We've been able to work through some of the systems and intelligence architecture issues, so everyone there sort of has access to the same type of data. I guess the problem then is the interpretation of the policy. You have to be physically in that environment in order to have access to that pile of data. That I guess gets back to how the DNI interprets his

information sharing responsibilities, based on the 2004 legislation. How do you work that policy issue from this point forward, or does that fall into that bucket you mentioned earlier about how you have to wait for the next big bang before you make progress?

Matthews: You can only take this thing so far given the inertia, and then there's enough resistance that it just plateaus. At the NCTC, the ground rules are that not everybody has access to everybody's information, but some number of people from every organization have access to everybody else's information. The sharing ground rules to the best of my knowledge are that you can have access to it at a senior level in a program. If you need to distribute it back to your parent organization, as opposed to keeping it in house and working with it at the NCTC, you have to get permission from the person above you. So that's still a bit of a problem. If the boss says no, then the ground rules are that you can't send it home. If you send it home, they'll send you home, because you broke the rules. That's happened.

Student: I'm curious about your perspective on some of the changes that were made regarding interrogations. That gets a lot of press. The authorization to do waterboarding was packaged with that memo in 2003. I don't know if you are part of that....

Matthews: I've never waterboarded anyone in my life.

Student: Was there much debate and discussion? How did that transpire? I'm an interrogator. I was in school at the time at the FBI, and we were all surprised when the classified memo that authorized it came out in public. How did that decision even come about?

Matthews: Are you talking about how we expand what we're doing? Is that what surprised you?

Student: Just the authorization to do it. In the Defense Department, was that a significant change?

Matthews: Basically, it was consensus, but it depends on how you define the problem in today's position. It was a new problem. We weren't prepared for it, so they tried to define it in newer terms that would allow us essentially to deal with the frustration. If these individuals were part of a terrorist network, or part of Al Qaeda, they were not lawful combatants. It was a stream of logic: if they're not lawful combatants, then they're not subject to the Geneva Convention. If they're not subject to the Geneva Convention, and they're not U.S. citizens, then what are our limits? The Geneva Convention provides our ground rules going in. If we're not dealing with a nation-state we're facing some other category of animal. I think that the issue of how we deal with it is what the hand-wringing was about. As a result, the logic was that we could do additional things with this problem set, because they were an exception.

Student: Were you surprised at the backlash that resulted?

Matthews: It's difficult when you're fighting an enemy and a threat that doesn't have your society's values. What you risk in the end is denigrating or compromising the values you stand for: "the end justifies the means" kind of thing. At the same time, we were not, and still are not, totally organized correctly for this problem set. There are no bounds and no rules for them;

anything's in bounds for them. So how do we behave? It takes a lot of discipline, and if you know where to find new ways of doing things legally we need to look at them.

We never perceived that was going to be our problem set. We went in with a cold war construct, mentality, and approach. With the peace dividend from the Wall coming down we weren't supposed to have some big existential threat to the country. It wasn't out there anymore, at least not in the near term. Maybe Korea if they got some capabilities; maybe China down the road, but a clear and present danger that was going to shake our foundations wasn't imagined.

These are the ways things change. In 1979 you did not seize an embassy. That was hallowed ground. It was out of bounds...until it wasn't out of bounds anymore. The posture of our most focused counterterrorism forces was about how to take down an airliner if there were hostages. If they don't care about hostages and are using the airplane with the people on board to send a message, and the airplane is just a missile, then they're on a suicide mission and you're not going to have much of a chance to take that airliner down. The whole nature of the threat and the problem took us by surprise. It really did, and at the end of the day we weren't prepared for that.

Student: Are you seeing a new incorporation of open source reporting or material?

Matthews: There's a whole open source center. We have an office at the DNI level to manage that. One of the biggest fights they have is that after they do all this open source analysis somebody wants to classify it, because they connected too many dots. What's wrong with that picture?

At the same time, there's so much information out there. That is an area that is very tough to bound and focus on, because we don't have enough resources to data mine, and unless we build IT tools that do all this for us, at the end of the day it's a human having to look at an awful lot of stuff. What we're trying to enable at the JIOCs are data mining tools that automatically associate any piece of intelligence that's out there and pull it in to you when you initiate the query. You hear analysts say that they can do in five minutes what it used to take them five hours or five days to do: conduct research, pull all the information in, and make an assessment. Now it's geospatially oriented. There are associations in there. The tools we have now to pull up intelligence rapidly are tremendous.

Student: Is this center set up as a competitive analysis center, completely separate from classified material?

Matthews: It certainly does competitive analysis. It's another way to look at things. We have run a few experiments with some very sophisticated IT tools to see what we could find out through competitive analysis on an existing problem, without going to classified sources in the intelligence community to make our assessment. We found some new and different things there. But how many resources would it take to do broad and comprehensive all-source analysis? I don't know, but it's huge. My gut reaction is that it would be a black hole for resources. You have to figure out what your priorities are and focus that effort, but it's clearly necessary.

Student: The process that General Boykin described for the JIOC sounds like it would work really well for getting the analysts to support operations. It would work really well for the organic

intelligence collection assets of the command. But the collection managers they took out of the picture are supposed to be the guys who know how to convert the analysts' needs for national collection assets, so I'm wondering if there is a danger of creating yet another stovepipe for potential military intelligence that isn't connected as well as it should be with the national assets and what they provide.

Matthews: I guess theoretically there is, but the example he used is on the ground, inside a JIOC, with a task-organized entity that's already in contact, if you will, in Afghanistan or in Iraq. That's where they're doing it. Do we still have collection managers at NSA and the other agencies? Sure we do. We have more demands and requirements than we have resources to do collection, so they have to manage and do the same things they were doing before. But do we have access to that information? Do they have access to the information we have down there? Can they ask their representative in that JIOC "By the way, do you already have this?" Could they then refocus a collection asset and apply it to something else? It's about trying to get more efficient as well, but we hope not about building another stovepipe.

Student: Does the DNI in fact have power over the purse for the agencies under Department of Defense?

Matthews: He's only gone through one budget cycle. The intent is that he would have oversight and at some national level be able to level the playing field, set some priorities for the nation at large, and not have somebody saying "No, I'm going to spend all my resources just on what I want." So you have to submit those budgets to him and he sees them. The military piece of it is the military piece, and that's for the services and the troops, but the national piece and the rest of it the DNI does have visibility into and he can take exception.

We haven't had a huge fight yet. They've been taking baby steps with it. They've been trying to package the first submission and get a process where when the DNI reviews this stuff he knows enough to make an informed recommendation or decide he wants to stand on a detail or have a fight over something. It's still a work in progress.

Student: Could you say a little more about efforts to improve access for intelligence consumers outside the intelligence community? For instance, I spent the summer at OSD SOLIC [Special Operations and Low-Intensity Conflict]. I consider myself to be pretty good with computers and search engines, but it would take me hours of trawling around to find and access all those great intelligence reports and products that the IC is coming up with. I know that there are better tools available on JWICS [Joint Worldwide Intelligence Communications System], for instance, which I didn't have access to, but even in OSD Policy most of the action officers who were cleared for it didn't have access to it. There are a lot of different ways to improve intelligence. One is by getting more and better information, and another is just by getting that information to the right decision makers so they can make better policy.

Matthews: JWICS is a nice system. It's at a high level, which is also a problem. What system are we going to have the bulk of our intelligence information on? The intelligence community built JWICS, but the rest of the department was either on an unclassified or a Secret network. Okay, great, but meanwhile the intelligence community had built special systems, not unlike

NSA, et cetera. They built them with no intention or vision that the information would have to be shared with a whole bunch more people. It's a huge structural problem. Short of breaking it down and creating a new system that shares across the agencies, you're going to have to proliferate JWICS to more people. That's the simplest solution.

The intelligence community is still its own worst enemy on that. I can't tell you how frustrating it is to have a piece of information on JWICS that is totally unclassified, but because it originates, let's say, from DIA I can't take it and move it to SIPRNET [Secure Internet Protocol Router Network]. I can't send that email or that file to you here for an unclassified briefing, because I can't take it off that system. I've got to get some IT manager who will take about a week to clear that for me and make sure it doesn't have any hidden or embedded things in it that will divulge the nation's secrets. So it's very frustrating. We built some things to be very secure, but it's a really negative factor for us today.

So, again, organize and collocate where at least some people have access. Not everybody needs access to everything, and if you're organized correctly and you have everybody present you should be able to get to the information in one or two steps—maybe not most efficiently or most easily—if you have the need to know.

Fein: You suggested that it might take some awful event to move to the next level of intelligence reform. If the president and Congress came to you after some event and asked what should happen next, what recommendations would you have to move to the next level?

Matthews: There's still, no kidding, not enough transparency and visibility on all the intelligence. The originators still get to hold back what they decide they really want to hold back more than they need to. So I guess it would be another barrage of better information sharing, and a system design that allows you to get people culturally amenable to sharing. You almost have to destroy some of it to rebuild something new and better.

It's like a closed architecture, let's say in the cockpit of an aircraft. The Army had a helicopter program that they finally canceled a couple of years ago. It was supposed to be the be-all and end-all. They built a closed architecture. They didn't have the vision to understand that you have to have an open architecture, because the technology is advancing so fast that you have to be able to plug in to a common architecture. It was the death of that program, and it should have been, because it could not keep up with the environment as fast as it was changing.

Better information sharing sounds so simple, but it is unbelievably bureaucratic and hard to do. There are people whose lives are invested in those systems, and some of them need to retire or go away and find their own line of work. At the end of the day, the bosses can say a lot, but the same people are still controlling the levers, and if you don't get inside their head and they don't have the vision and the understanding, you're sunk.

It's kind of like lawyers. Whenever you do anything in the department you've got to get a legal chop, a legal opinion, on your action. If you're an action officer trying to get an action through, the joke is "If it's not illegal I don't need your opinion, I just need your signature. Thank you very much." Everybody's got an opinion, but we'll never resolve anything. We'll just go round and round and round. Those are my first blush thoughts.

Student: Are there mechanisms that you want to improve that would translate individual capacity into institutional capacity?

Matthews: I mentioned before that we don't have skill sets resident in the department. It's part of the "JIOC after next" concept. We need access to anthropologists, to people who understand cultures, to things that are not resident in the department. How do you leverage that? We need access to academia, and to go to really smart people who have spent their whole lives doing what they do and can give us what we need to know to be informed. That's part of the vision for the JIOC after next and the Joint Forces Command that does our experimentation and the future stuff down at Norfolk.

We have a guy who has one of these fifty-pound brains and we have always have to tell him to keep it simpler. His vision is to have the JIOC working and then be plugged in to all the intelligence resources that people might possibly need and tap them as they need to tap them: pull them in virtually, give them the request for information, and let them come back and tell the analysts at the JIOC. But guess what? They'll have to get on the computer system, and do they get access? That's where the bureaucracy starts to kick in. We have to have access to tap into those people's minds and get their insights to what is going on out there when it is a human-centric problem, because we don't have the necessary skills in the department. We never recruited them. It wasn't necessary, because that wasn't something we had to worry about.

Someone briefly touched on one of my big recommendations about what we ought to do next that fits the operational and tactical level. In every agency of government, in this day and age, who deploys? Does the Department of State, the CIA, Treasury, or the FBI deploy? Do they have a deployable capability? Have they organized, trained, and recruited people into those organizations of our government to deploy? That's not who they are. That's not their nature. That's not the skill set most of them advertise to bring people in. But across our government I believe we should have deployable capability, because of the nature of the problem we have.

Now we ask people to volunteer. "Okay, I can go for ninety days." "Great, we've got somebody going for ninety days." We need people who can deploy and immerse themselves forward for an extended period of time. Suppose the Department of State, Treasury, or the other departments told people "If you come with us, if we hire you, we're going to train and equip you. You'll be in an organization that's going to have to deploy and work in an interagency environment to better share intelligence and work problems on the threat to the world we live in." I submit to you that it would take a long time to build that capacity, but I think we sorely need that in our government today, because we're asking people to volunteer for stuff they never signed up for. It's not their ethos or culture. I believe we have plenty of Americans who would do this in our departments if they were trained and recruited that way from the get-go, but we don't have them. It's a pick-up game.

Student: Earlier you talked about the need to touch, feel, and smell the field. Is part of this reform designed to get the analysts closer to the field to get this interaction?

Matthews: That's where NATO and the ISAF [International Security Assistance Force] have a tough challenge. We're saying "Put the analysts forward where they're in the environment and

can see what's going on in real time." We're trying to turn that cycle faster than the enemy cycle. The only way we can do that is to be able to turn as rapidly as possible.

NATO was constructed for the cold war. They thought they would have to fight on their own terrain. They weren't going anywhere. Now NATO has got to deploy. Guess how they're organized and guess what their systems are like? They've got legacy profiles, systems, and ways of doing business that do not match the world they're asked to participate in today. So it's a problem. Very few of those countries can do that, because they never saw themselves as having to do it. So we are constantly telling them that they have to push their analysts forward. It's really important.

The problem is that they still rule nationally. The intelligence always has to go home before they can send it back out. Do you know how much time you lose with that little circuit drill? They aren't on a twenty-four-hour wartime footing at home, so you hit the weekend and it's not really efficient. They've got to change the way they do that. We sent that message to ISAF. We've been to the Hague. We've been to Brussels. We said this to the NATO Intelligence Board, and they're very interested, but they're not organized for that, so I see it as a deficiency.

You've worked with NGOs [nongovernmental organizations]. Part of the problem is that there are certain civilian organizations that absolutely will not work with the CIA or the Department of Defense. They do not see themselves involved in, nor do they want to participate in, the things that those organizations do. Yet they have information and intelligence that in and of itself is just information. Are we organized correctly to have some mechanism to leverage what the NGOs know and feed it back into all-source analysis or whatever to round out the rest of the picture? It's a void there.

Borg: Sir, to that end, is there work being done with the private sector to improve the flow of information; for instance, as they work with foreign governments and businesses?

Matthews: There is work going on, and there are certain NGOs who are very willing to work with us, but they can't tell others they're doing it.

Borg: Is there that same exchange at the corporate level?

Matthews: No, the challenge with the corporate sector is one of the big challenges that the Department of Homeland Security has. They are not just protecting intelligence and information; they're protecting their business secrets, and if their competitors get the edge on them and get access to their secrets they go out of business. That is one of the main reluctances in industry. Industry does a lot in a collaborative fashion, but it's a lot more difficult if we're trying to get at how we can bring industry all together so that everybody's well informed and our national economy isn't affected. It's about profit. There's corporate espionage now, and there has been for a long time. That's a tough one, because they see the potential for misuse as a life-threatening activity.

Fein: You and General Boykin have described some very substantial changes in how the DoD approaches the whole intelligence function. With a new secretary of defense, with General Clapper coming in as the new under secretary, and with a presidential election coming in 2008,

would you anticipate changes in that direction, or continuation, or is what will happen in the future very much up in the air?

Matthews: Here's what I see going on. If you want to determine intent, watch behavior. We have a saying about the enemy: "If you want to know what he's up to, watch how he's behaving and acting, and that will largely dictate intent." What we're seeing right now is a swing. Frankly, and to be perfectly blunt about it, Secretary Rumsfeld was disliked by a lot of people. Dr. Cambone was his right-hand man. So there's a swing in that pendulum and it's important not to appear as if it's more of the same, just as you saw with the change of leadership in Iraq and in CENTCOM [U.S. Central Command]. Essentially, the idea is to clean house, because what we had was old think, old school. We've got to have new ideas, new folks, and a new way ahead, because the old way was just unacceptable. It's largely political.

There is not a lot of rush to engage with the under secretary of defense for intelligence piece of this, because "under secretary of defense for intelligence" translates to Dr. Cambone, which translates to Secretary Rumsfeld, which translates to the last guys we had. We have a new team. If they behave the same way they'll get labeled with "Just more of the same" and they'll run into a lot of resistance. That's just the Washington bureaucratic reality. So I don't see happening what used to happen. We don't have a full-time under secretary yet, so it's hard to say.

The new secretary of defense has not told us to do anything different. On the things that he has dealt with that touch on the under secretary of defense for intelligence and the intelligence community nothing has been a problem at all. I believe the secretary's mission right now is not to rock the boat a lot; take over the helm and keep her steady as she goes. He's essentially coming in as a lame duck. It's a two-year tenure (less than that now) at the helm of the ship. He'll make minor course corrections, but he's not going to turn to and do a 180. He's in there to maintain a sense of calm, move ahead, and accomplish missions.

I think that we may well see more change inside the intelligence community initiated by General Clapper than we will or have seen from Secretary Gates. Clapper is from the community; he's got vision; he has a whole bunch of thoughts on things; and I think he'll want to take what he sees as the next logical way ahead.

There's an informal series of in-briefs with him tomorrow in preparation for his testimony on the Hill. We can't tell him anything classified; it's kind of vanilla, one-on-one, about who we are and what we're doing, to get him prepared for his testimony. Technically we can't deal with him in any detail or in a classified manner until he's confirmed. It would be an assumption of Congress's prerogatives, and that would be bad.

Student: General Boykin mentioned a defense attaché service. Is there a move to create a true defense attaché service where the growth, care, and feeding of attachés are handled in the joint world rather than within the services and then they come in and are managed for the time they're in that service?

Matthews: I don't think we've gotten to that joint service yet. We're at a point where we're trying to convince the services that they're not as well equipped in the attaché business as they

need to be in this day and age. Attachés need to have a career path, an opportunity for progression and promotion, and a chance for flag billets.

Interestingly, the Air Force never invested very much at all in intelligence from the standpoint of people. There wasn't an intelligence officer flag inside the Air Force. It was all the pointy-nosed-fighter kinds of guys who ruled, and that had to change. They've redone their staff and they now have an A-2 [deputy chief of staff for intelligence]. He's a fighter guy, but he clearly understands it's a different world he's trying to operate in, and his deputy is an intelligence officer, a one-star, Paul Dettmer.⁵ So the message to the Air Force internally is "This intelligence thing is becoming more and more relevant and important, our bench is really thin, and it's something we have to work on." The same message is coming out on the attaché thing, but the services will have to take initial steps before we can get to a really good joint approach.

Student: Have we outsourced too much of our intelligence capacity in terms of analysts and collectors?

Matthews: I don't think so, because it's based on supply and demand and immediacy of the need, and we've got to put somebody onto the problem right now. Simultaneously what we're trying to do is systematically structure it organizationally to build more capacity. But if we've got a problem that needs fixing today, and there are people out there with a particular skill set and we can hire them, we're going to have to hire them. I think there will be a leveling and a balancing of that, but when you get a bunch of civilian analysts—maybe former military and maybe not—and they're around for a few years proving their worth, their value, and their insight, they've become a trained resource for you, so are you really going to get rid of them? I don't know. We'll try to maintain them, I think, as we continue to grow the capacity inside the uniformed services. There are so many things outsourced that require clearances that I don't see that ever drying up. I don't know how it would.

We outsourced because we had nothing taken off the plate when we downsized. We had to get to the lower numbers, but keep doing everything we were doing. How do you do that? You outsource. You contract for it. Until we're not required to do certain things, or are told "That's no longer a priority, so get rid of them," they could stay forever.

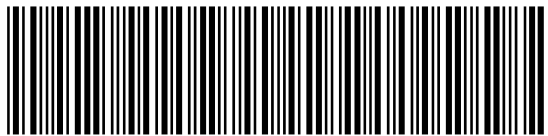
Borg: Sir, thank you for being here today, and for slipping your travel plans to allow us to go on with questions. We appreciate it very much. Please take this memento home with you. We hope to see you again, and we wish you luck in all these endeavors.

Matthews: My pleasure. Study hard!

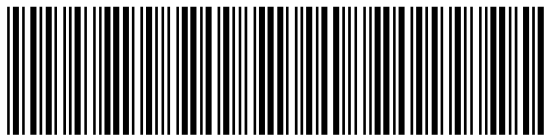
⁵ The Air Force A-2 is Lieutenant General David A. Deptula. His deputy is Brigadier General Paul Dettmer, vice director of intelligence, Joint Chiefs of Staff.

Acronyms

CIA	Central Intelligence Agency
DCI	director of central intelligence
DCID	Director of Central Intelligence Directive
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	director of national intelligence
DoD	Department of Defense
EO	Executive Order
FBI	Federal Bureau of Investigation
HUMINT	human intelligence
ICP	intelligence campaign plan
ISAF	International Security Assistance Force
IT	information technology
JIOC	Joint Intelligence Operations Center
JWICS	Joint Worldwide Intelligence Communications System
NATO	North Atlantic Treaty Organization
NCPC	National Counterproliferation Center
NCTC	National Counterterrorism Center
NGA	National Geospatial-Intelligence Agency
NGO	nongovernmental organization
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OSD	Office of the Secretary of Defense
PACOM	Pacific Command
SIGINT	signals intelligence
WMD	weapons of mass destruction



INCSEMINAR2007



ISBN 1-879716-98-4