



INTELLIGENCE



for a NEW ERA in AMERICAN
FOREIGN POLICY

Conference Report
January 2004



Sponsored by:
CENTER for the STUDY of INTELLIGENCE

All statements of fact, opinion, or analysis expressed in this report are those of the conference participants. They do not necessarily reflect official positions or views of the Central Intelligence Agency or any other US Government entity, past or present. Nothing in the contents should be construed as asserting or implying US Government endorsement of the study's factual statements and interpretations.



**Center for the Study of Intelligence
Conference Report**

Intelligence for a New Era in American Foreign Policy

*10-11 September 2003
Charlottesville, Virginia*

**Washington, D.C.
January 2004**



Introduction

The terrorist attack on the World Trade Center in New York and on government facilities in Washington, DC, irreversibly altered the foundations of US national security policy. It also reshaped the imperatives that drive the work of the US Intelligence Community. On the eve of the second anniversary of that attack, the Center for the Study of Intelligence (CSI) assembled a group of approximately 85 experts at a conference in Charlottesville, Virginia, to think through the implications of this new world for our profession. CSI sponsorship was in keeping with the Center's original mandate from DCI James Schlesinger—assemble the best minds and bring them to bear on the most critical challenges to the Agency and to the Intelligence Community.

Within the Community, far-reaching changes were well underway during the decade that preceded the 9/11 attacks. They stemmed from the collapse of the Soviet Union and the pressures for adaptation to the post-Cold War environment. As the bipolar confrontation receded and a more fluid, chaotic world of diverse threats emerged, intelligence programs were refocused and resources were realigned to a new set of priorities. In important respects, evolutionary and adaptive changes were indeed beginning to create a more flexible, agile, and responsive Intelligence Community. But the tidal wave generated by the shock of 9/11 soon overtook and broke over the Community in a way that has led many observers to question the adequacy of evolutionary changes. Existing organizational arrangements, legal authorities, institutional cultures, business practices, and support architectures are all being reexamined with a new intensity. The importance of timely intelligence is indisputable, and the consequences of failure are unthinkable.

The conference opened with a broad-ranging consideration of the evolution of the international security environment, the changing American role in it, and the best stratagems for ensuring that intelligence priorities and guidelines conform to the needs of policymakers. It also examined in detail the changing intelligence needs of specific user communities and the ability of intelligence to meet them. Most importantly, it considered possible procedural and institutional changes that might enhance the capabilities of the Intelligence Community in this new era.

Conference participants included former and serving senior government officials from the national security policy arena, academic specialists, and experienced intelligence professionals from across the Community. Sixteen of the participants contributed formal presentations that served as catalysts for lively and informative discussions. The presenters were:

- Walter Russell Mead, Senior Fellow of the Council on Foreign Relations and author of the recently published *A Special Providence: American Foreign Policy and How It Changed the World*
- Eliot Cohen, Director of the Strategic Studies Program at the School of Advanced International Studies (SAIS), The Johns Hopkins University and member of the Defense Policy Board

-
- Brent Scowcroft, National Security Adviser to Presidents Gerald Ford and George H. W. Bush
 - James Steinberg, Deputy National Security Adviser to President Bill Clinton
 - Greg Treverton, former Vice Chairman of the National Intelligence Council and faculty member at the Kennedy School at Harvard
 - Russ Travers, Deputy Director of the Terrorist Threat Integration Center (TTIC) and former Director for Policy at the Defense Intelligence Agency (DIA)
 - Major General John Kimmons, Commander of the US Army Intelligence and Security Command
 - Major General (ret) Robert Scales (USA), coauthor of the recently published *The Iraq War: A Military History* and former Commandant of the Army War College
 - Ellen Laipson, President of the Henry L. Stimson Center and former Vice Chairman of the National Intelligence Council
 - Leon Fuerth, Research Professor of International Affairs at the Elliott School of International Affairs of George Washington University and National Security Adviser to Vice President Al Gore
 - Lt. General (ret) Bill Odom (USA), Director of National Security Studies at the Hudson Institute and former Director of the National Security Agency
 - Larry Kindsvater, Executive Director for Intelligence Community Affairs, CIA
 - Richard Betts, member of the DCI's National Security Advisory Panel and of the National Commission on Terrorism, and Professor at the Institute of War and Peace Studies, Columbia University, and former member of the National Security Council
 - Bill Nolte, Deputy Assistant Director of Central Intelligence for Analysis and Production
 - Kevin O'Connell, Director of the Intelligence Policy Center of the Rand Corporation
 - Fritz Ermarth, security policy consultant and former Chairman of the National Intelligence Council

The following summary of the conference proceedings focuses on the most innovative and thought-provoking ideas surfaced at the conference. It does not attempt to recapitulate the discussions in detail. As a result, some of the Intelligence Community's achievements, as acknowledged by speakers at the conference, have been given short shrift. Those interested in capturing the flavor of the discussions at the conference may refer to the italicized presentation excerpts that follow each section of this summary. Asterisks separate the remarks of individual speakers.

Contents

	<i>Page</i>
The Changing International Political-Strategic Setting: Driver of Change	1
Presentation Excerpts	2
Meeting the Challenge of Change: Assessing the Intelligence Community's Performance	3
Presentation Excerpts	4
Diagnosing the IC's Difficulties: Identifying the Root Causes	7
Presentation Excerpts	8
Reforming the IC: Proposals for Change	13
Presentation Excerpts	15
On Restructuring the Community	15
On Exploiting Technologies and Methodologies	18
On Improving the Intelligence Product	18
On Fine-tuning the Relationship to the Intelligence Consumer	20

The Changing International Political-Strategic Setting: Driver of Change

Conference participants were strongly of the view that the most serious challenges to the Intelligence Community were the product of fundamental and irreversible changes in the global environment and not the result of changes in political goals or priorities at the national level. As the tragedy of 9/11 has demonstrated, mortal threats to American lives and interests are no longer confined to a single superpower adversary. Not only nation-states, but much smaller and more amorphous organizations now possess the means and the motivation to inflict major damage and casualties on the United States. These terrorist groups constitute the most immediate threat to US security. This new threat environment has been in the making since the collapse of the Soviet Union. It has erased the bipolar division of power that had dominated the world and the threat horizon of the United States for decades.

The principal drivers of the ongoing changes in the international threat environment are the forces of globalization and the associated processes of technological progress and diffusion. By eliminating barriers to the spread of goods, capital, and ideas, the former process subjects more traditional societies—such as those in the Islamic world—to social, cultural and economic stresses they are ill equipped to handle. These stresses have given rise and will continue to give rise to violent extremist movements. They draw their support from groups and individuals who find themselves economically and politically disenfranchised, or who consider their traditional values to be threatened. The US has become, and will remain, the main target of the animus and actions of these movements. One speaker suggested that the US economy and the global institutions and networks

that it dominates are driving the changes whose consequences these movements and their supporters find so objectionable.

The rising tide of social and economic disruption has been paralleled by an accelerating pace of technological change and an ever-widening access to the innovations that have resulted. The erosion of geographic and communications barriers to the diffusion of knowledge has given relatively small groups, and individuals as well, access to new and more lethal technologies capable of causing massive casualties and damage. At the same time, the complexity and intricate mesh of economic, financial, trade, and human contacts characteristic of advanced societies make it more difficult for them to shield themselves against the attacks of small and amorphous groups.

Confronted with these changes in the global threat environment, intelligence must radically revise the perspectives and procedures that served it well in the bipolar world of the Cold War. The requirement now is for a broad rather than a narrow focus, flexibility rather than concentration of forces, and a fundamental reorientation of the Intelligence Community's reserves of area knowledge and expertise. Plumbing and addressing the religious motivation and inspiration of some of the most dangerous terrorist movements poses particular difficulties for both the policy and intelligence communities in the US. We are both unfamiliar and uncomfortable dealing with religion as a driver of violence and hostility. Religious rationales for violent acts are not unique to Islam but have taken on particular importance in the Muslim world.

You no longer need to be a large country with a powerful industrial complex to [undertake] acts that fundamentally compromise the security [of democratic countries].

Presentation Excerpts

There really has been a fundamental change in the world environment, and I don't think you can understand how you need to adjust without knowing that. The world of the Cold War was a world of intense focus on a single center of threat That fixed the way we looked at everything, the way we organized It was replaced by almost the polar opposite For the Intelligence Community, you went from a pinpoint focus to [needing to have] a panoramic view.

You no longer need to be a large country with a powerful industrial complex to challenge the liberal democracies, to [undertake] acts that fundamentally compromise their security or economy. You can be an NGO [a non-governmental organization] and do the job.

The technological society and technological enhancements that we are straining every nerve to accelerate are creating new . . . international dangers Smaller and smaller groups of people disposing of smaller and smaller resources will be able to cause greater and greater damage.

The more the American project of creating a world in which the dynamic productive capacities of capitalism are unleashed . . . [and] generate a more dynamic and faster [changing] society, the more we're going to have a world at risk.

It's a considerably more dangerous world [It is] entirely conceivable that some state or rogue actor . . . could one day do something that could destroy our capital city.

You have to think about [terrorism] as part of a broader set of global phenomena, [which have] broken down barriers between states [and] have made individual actors, NGOs, non-state actors, . . . more capable of acting across borders in an effective and organized manner. [These global developments] have created new opportunities for growth, but also for destruction.

An historian looking back on September 11 and our reaction to it will be struck by . . . the difficulty we have in talking about religion and in acknowledging religion as a source of violence in the world [Religious extremism] is going to be a large, multi-decade, quite likely multi-generational set of issues that are going to involve large parts of the Islamic world.

Meeting the Challenge of Change: Assessing the Intelligence Community's Performance

Speakers noted that the Intelligence Community has not performed as well as needed to meet the challenges posed by a world characterized by diffuse and rapidly evolving threats. It has failed to develop the flexibility and resources to cope, not only with terrorism and the associated threat of WMD proliferation, but with other new, as yet unidentified, threats as well. Neither collection nor analytical organizations have performed well in identifying and meeting these new challenges.

The warning function is chaotic. The failure to establish an effective warning system that would have correlated strategic warning (the recognized threat represented by al-Qa'ida) to tactical warning (indications of al-Qa'ida's operational capabilities and intentions) represented a "failure of intelligence." So did the unsuccessful efforts to develop a comprehensive overview of the status of Iraqi and North Korean WMD programs.

The IC as presently structured evolved to deal with the massive threat to US security represented by a nuclear-armed superpower. The Community performed well in meeting that challenge, but the conditions inherent to that environment—a known adversary, enduring intelligence challenges, clear priorities, and a narrow focus—no longer apply. The IC now confronts a security environment that is almost the mirror image of that: one characterized by rapid change and multiple new threats.

Although the most significant threat to US security today is that posed by the terrorist and extremist movements within the Islamic world, it cannot be assumed that this will still be the case in 10 years. Other threats whose outlines are already visible include the fallout from civil conflict in other

states, the dangers posed by failed or rogue states with access to WMD, and the implications of China's rising power. Success in meeting the challenges posed by this array of potential threats will require a panoramic vision, flexibility, and innovative approaches to intelligence collection and analysis.

A major weakness of the IC is its difficulty in providing strategic intelligence—the comprehensive overviews that put disparate events and the fragmentary snapshots provided by different intelligence sources into a contextual framework that makes it meaningful for the intelligence consumer. This criticism applies to intelligence prepared both for a national policy audience and for more specialized audiences, such as battlefield commanders.

We excel in missions susceptible to technological solutions—"counting tanks"—but do not perform well in those that require a subtle understanding of the goals and perspectives of our enemies and other potential antagonists. We lack the depth of area and linguistic expertise that would enable us to put their actions and intentions in the context of their own culture, and allow us to better anticipate their actions.

This deficit in cultural expertise is associated with another negative trend highlighted by conference participants: We increasingly report rather than analyze. We are good at the "who" and the "what," but bad at the "why" and the "so what." One result is that the usefulness of our threat analysis is limited. What we present as threat analysis is really vulnerability analysis and of little use in identifying real threats. These shortfalls have had a negative impact not

Is American national and strategic intelligence up to the demands of the global environment? . . . I think there is a prima facie case that the answer is no.

only on our record in dealing with terrorist organizations like al-Qa'ida, but on our performance in Iraq as well.

Speakers emphasized that the difficulties confronting the Community will not diminish. To the contrary, the bar has been raised. The emphasis on preempting terrorist threats in the New National Security Doctrine places a premium on intelligence. If intelligence is to be used to justify a military attack or other preemptive action against a state, organization, or individual, it must be virtually flawless. It must provide not only a fine-grained assessment of a potential enemy's capabilities, but be founded on the analytical expertise and human intelligence sources needed to support an accurate assessment of his intentions. Intelligence support that falls short of this exacting standard can lead to policy decisions that will undermine the moral authority and credibility of the United States and inhibit its ability to exercise influence in the world.

Presentation Excerpts

We are in a new era . . . This means that we have to assess whether our intelligence mechanisms are adequate . . . Is American national and strategic intelligence up to the demands of the global environment and our national policies and strategies? I think there is a prima facie case that the answer is no.

[Intelligence] has less competitive advantage than we've ever had . . . We're competing against high class academics, think tanks, and the press, many of whom have

far more access to [good resources] than we in the Intelligence Community. That's a huge problem. Policy is less trusting of us. We've had enough mistakes over the last four or five, six years. You couple that with the natural self-assuredness of the policy community and they're not necessarily willing to listen to the Intelligence Community when it comes forward.

It does seem to me that 9/11 has driven home to us just how mismatched many of our organizations and processes were to the world even before 9/11 . . . We had based our Cold War arrangements for intelligence and for its connection, or lack thereof, to law enforcement on a series of distinctions. We said intelligence is one thing and law enforcement is another. We said foreign is one thing and domestic another. We said public is one thing and private another.

There are a lot of people in Congress who have given up trying to get the Intelligence Community—FBI, CIA—working together. They are saying, "We're going to recreate the Intelligence Community inside Homeland Security. You guys go ahead and do whatever you want. You're never going to solve the problem. We'll solve it by creating a new outfit. If TTIC fails, that is what is likely to happen."

Terrorism is our number one problem . . . That is a fact of the environment now. Beyond terrorism, interstate conflict, which is traditionally what foreign policy has been about, is being supplanted [by] internal conflict, within states. This is a very differ-

ent kind of problem to deal with Plus [we have] a handful of rogue states with modest military capability, but possible access to weapons of mass destruction Finally, [technological] changes have reduced the target intelligence cycle . . . to minutes in many cases. This changes . . . what kind of intelligence you need.

As a Community, we've become increasingly focused on reporting rather than analyzing We've been relatively good at the "who," the "what" and the "when" We're less good at the "how," and I think we're positively miserable at the "why" and the "so-what."

[September 11] was a failure of intelligence. It was a failure of intelligence because, in the face of a strategic threat that we recognized, that three DCI's and a lot of . . . other authorities testified about, we didn't set up a real warning system. A real warning system should have . . . correlated strategic warning (that is, there's the enemy) . . . with what I call operational warning . . . (here's what we think, what we have evidence he's thinking about doing.)

[As to] Iraq WMD, the real scandal is not what's in the newspapers about cooking the books, spinning, exaggerating, manipulating The real scandal is that the books were so thin, that there was so little in them on a target of what was professed to be the highest priority through the 90s Iraq was not a closed society. It was not a North Korea. It was not even a Soviet Union. There were Iraqis coming and going, not to mention Ukrainians and Dutch-

men and Germans selling you know what Why didn't we get in there? . . . North Korea—it is said they may have . . . one to two nuclear weapons. The difference between two [or] five nuclear devices that are untested and may be as big as refrigerators . . . and 10, 15, 20 weapons that . . . are the size of breadboxes that will fit on . . . missiles . . . is enormous Our strategy requires an appreciation of where they are on that spectrum. We don't seem to know.

I think you all know [that] despite considerable investment both at the strategic and at the tactical end—especially at the tactical and operational end—there's not enough [HUMINT], certainly for the environment that we're in now. Access is key. We need our partners, our Allies, to help us with that Access is something that takes decades to grow Even though we've been looking at Iraq a long time, we weren't where we needed to be in terms of what the leadership was thinking and doing. [HUMINT is] also, as you know, the least automated and well-linked of all the databases, although we're moving in the right direction.

At the end of the day, what [CENTCOM Commander General] Abizaid confronted me with is, what are they thinking? What are they going to do? Why are they doing what they're doing? I was very hard-pressed, and the Community was hard-pressed, to give coherent answers.

As a Community, we've . . . been relatively good at the "who," the "what" and the "when" We're less good at the "how," and positively miserable at the "why" and the "so-what."

If you're talking about preemption, you pretty well have to have perfect intelligence.

We have the ability to count tanks, [but] we don't have the ability right now to get inside the head of the enemy, to follow the cycles and patterns of decisionmaking, to understand the nature and character of the enemy and divine what he's all about.

The commanders in [the Iraq conflict] had plenty of information. It was the human element that was the bottleneck—the [inability] to absorb and pass along information, and perform that fusion at the lowest level— [that] is what got us into trouble.

Dick Kerr did a study . . . of all the analysis that was written on Iraq [by the CIA] He said . . . it was very good, there was a lot of detail, there was a lot of information, but he came away from all of that analysis having no real sense of what Iraq, the country, was all about.

My greatest frustration [as a former intelligence consumer at the NSC] was trying to get political intelligence, particularly of a strategic nature And I got very, very little of it. The best stuff I saw was military intelligence that had to do with arms control and weapons systems and so on. What this gets to . . . is the distinction between strategic intelligence and tactical. The more strategic you get, the less of a

data dump. The data dump is the easiest thing to do [but it's almost always of a tactical nature].

If you're talking about preemption, you pretty well have to have perfect intelligence if you're really going to operate on [that basis], because what you're saying is, "We have to do this because . . ." I think what has happened in Iraq with the WMD is a good example of the morass that we have gotten ourselves into with the preemption idea How are you going to decide whether somebody is seeking domination over the United States . . . [and whether] you need to preempt?

The intelligence response to the policy of preemption also means, I think, that intelligence has to bear scrutiny, not only from the public but from our allies as well. I think intelligence has to have an analytic method [that also can bear scrutiny] A method that we have often used in the past, which I suspect may have taken us down the wrong path on the Iraq-WMD issue, is the worst case method. We take facts, and we interpret them in the worst possible [way].

Diagnosing the IC's Difficulties: Identifying the Root Causes

Conference speakers cited several factors as major contributors to the IC's difficulties in dealing with the new security environment. Foremost among these were the institutional and organizational holdovers from the Cold War that continue to inhibit intelligence sharing and rational planning and management within the IC. They also obstruct contacts between the IC and external sources of information and expertise. Another major problem is the decline in analytical capabilities and basic intelligence that has taken place during the decade of the 1990s.

Many speakers pointed to the limitations on the authority of the DCI as a major obstacle to long-term planning and coherent management within the Community. He lacks the fiscal and personnel authorities to shift resources and establish priorities within the Community. In contrast, the DOD, which commands 80 percent of the resources of the IC and dominates the collection requirements process, is an "800-pound gorilla." There is no effective central planning and direction. From the perspective of the DCI's ability to establish priorities for the Community, the situation has become worse with the establishment of the Department of Homeland Security, which will become another equally imposing obstacle to the DCI's ability to manage the Community and establish clear guidelines.

Another organizational weakness highlighted by conference speakers, and one closely allied to the limitations on the authority of the DCI, is the rigid distinction drawn between intelligence agencies with domestic or law-enforcement responsibilities and those with an international mission. Both the constraints on the DCI and the legal barriers established to limit coop-

eration between agencies like the FBI and CIA have their roots in historically justified concern over the implications for civil liberties if security and intelligence powers were concentrated in the hands of a single individual or organization. Nevertheless, they have seriously hampered counterterrorism efforts. Terrorists do not respect borders and domestic-international distinctions. In addition, the development, as a result of this legal distinction, of two bureaucratic cultures, the law-enforcement and the intelligence, has further inhibited efforts to develop an effective response to the terrorist threat.

Beyond the dividing lines drawn between agencies with domestic and international responsibilities within the IC, some saw a more fundamental problem in the Community's organization on the base of collection disciplines—NSA for SIGINT, NIMA (now the National Geospatial Intelligence Agency [NGA]) for IMINT, and CIA for HUMINT, among others. Rather than concentrating the resources of the Community on crucial intelligence needs, its existing structure encourages individual collection disciplines to focus on the information they collect best, rather than that which is most crucial to meeting priority needs.

Apart from the misapplication of limited intelligence resources, organization on the basis of collection disciplines has worsened another chronic problem within the IC, the gulf between analytic and collection functions. As a result, limited analytical resources have been overwhelmed by vastly larger collection capabilities. Information overload is an ever-more serious problem for intelligence analysis within the IC. Moreover, it has harmed collection as well

From an Intelligence Community perspective, planning and direction are fundamentally broken.

as analysis. As one speaker put it, you have to know what you are looking for before you can collect.

Yet another problem which some view as a by-product of the Community's current organization is the obstacle it presents to the crucial efforts to achieve the goal of analytical fusion, the ability to survey and integrate information from a variety of sources to identify patterns suggestive of emerging threats. The proliferation of special compartments and access restrictions—particularly for HUMINT, but for the other INTs as well—runs counter to the need to integrate information from disparate sources in order to put it in context and to derive maximum benefit from it. One former senior intelligence consumer whose own access had been virtually unrestricted was among those complaining most sharply about the practice of delivering HUMINT and other sensitive intelligence in "manila envelopes," segregated from other information and lacking in context. Security and accountability, in his view, have defeated efforts to integrate knowledge.

Access restrictions imposed by "collection discipline" agencies also hobble efforts to disseminate crucial counterterrorist information to state and local authorities. These officials are crucial to efforts to maintain the security of the homeland against terrorist threats. Similarly, intelligence sharing arrangements with foreign allies whose interests—particularly in combating terrorism—are congruent with our own are limited by the security controls and access limitations imposed by individual collection authorities, each of which imposes its own rules and controls. Speakers questioned the validity of the NOFORN restriction in an era when the most immedi-

ate security threat arose from non-government organizations like al-Qa'ida, and some of the best sources of intelligence are controlled by friendly services.

In addition to institutional and organizational weaknesses, speakers cited an erosion of analytical capabilities as a factor in the IC's difficulty in coping with issues like terrorism and proliferation. They pointed to a decline in investment in analysis in the decade of the 1990s as a major strategic error. The problem was compounded by the division of collection and associated analytical responsibilities between various members of the IC. This promotes specialization and helps to defeat the cause of contextual analysis.

Presentation Excerpts

From an Intelligence Community perspective, planning and direction are fundamentally broken.

The DCI has very little more authority than he had in 1947. The biggest consumer of intelligence in the government is the Department of Defense. It also pays 80 percent of the [intelligence] budget . . . and the Community works for them When or if [Homeland Security] gets really operating, you're going to have two 800-pound gorillas [for the DCI to deal with].

The Intelligence Community, at least in an organizational sense, is pretty much the way it's been since the creation of the National Security Act . . . since 1947 . . .

We do not focus on missions. We focus on how we collect stuff We organize everything we do by INT.

We have a new world . . . threats we haven't anticipated before, and yet we're organized much the way we were organized when we really had only one major threat . . . the Soviet Union.

I think one of the major problems facing the Intelligence Community is that we do not focus on missions. We focus on how we collect stuff We organize everything we do by INT How much money do I want to throw at SIGINT . . . MASINT . . . HUMINT? That's an interesting question, but the first question ought to be how much do I want to throw at terrorism.

Are we doing business the way we should be doing it? For example, we're organized by collection units. We're not organized by threat or anything. You've got an electro-optical satellite, so what do they do? They go out and look for all of the intelligence business that you can use electro-optical for rather than say, we've got a China threat here and start from that as a basis of organization.

We have a huge American problem, and it starts in the National Security Act of 1947. It divided the Intelligence Community into two parts, foreign intelligence and domestic intelligence It didn't matter too much during the Cold War, because most of the problems were overseas Then comes terrorism The terrorists don't care about national borders.

It is a fiction, a complete fiction, to pretend that the world is organized into what is happening here and what is happening

there and that you can accurately describe the world in two chunks In the real world, these things are tightly woven together, and . . . the separation . . . makes what you do increasingly artificial.

It's important to distinguish between structure and process on one hand, and the reasons for Intelligence Community failures on the other. The former may often be the cause of the latter, but not necessarily. If present structures and processes don't produce the proper functioning, is it because of the structure, or because of other things like the political mandate or the material resources?

There are . . . these two philosophically different bureaucracies—the law enforcement bureaucracy and the intelligence analyst bureaucracy. They look at problems . . . from opposite ends. [For] the law enforcement professional . . . you collect information with the goal of bringing someone to justice. What is not involved [in an] investigation you throw out The intelligence analyst, on the other hand, looks at a whole world of information of different sorts, different qualities, [from] different sources [and looks for patterns].

Who's responsible in the National Foreign Intelligence Program for going against terrorists? It's not CTC. It's not the JITF-CT. It's not TTIC. Who brings together all of the collection and analytic capabilities

Our whole classification [system] . . . needs very thorough examination.

that we have to go against the terrorist threat facing the United States? . . . We don't have anybody.

The distinction between open and secret needs to be rethought . . . We need to create processes for sharing information . . . Many of the things that are secret are, if we're honest, not [secret] for very long.

We organize ourselves around a group of people who've got security clearances . . . In this world where the cop on the beat may be part of the front line of both intelligence collection and action, is it credible to think we're going to be able to define that Community in advance, decide who gets the clearances . . . ? In this new world of "unknown unknowns, [specifying] a priori who needs to know is not only difficult, its also contrary to the basic problem that we have. We don't know who will need to know in advance.

Why [do] all the [HUMINT] reports arrive in separate envelopes? Because they're part of a separate, hermetically sealed security and accountability system. To serve accountability and security, you defeat integration of knowledge.

Our whole classification [system] . . . needs very thorough examination, because we are both extending [sensitive information]

to too many people at one level, and not giving [essential information] to the police at another level.

NOFORN . . . As long as that word exists, I think we're going to be crippled in terms of releasability . . . If we can't get beyond it, we're not going to be able to leverage fully our best allies and friends.

We force fit analysis into the existing functions . . . [We developed] incredible specialization, but it was absolutely anathema to contextual analysis . . . To make matters worse, we not only divided up analytical functions, but [created] . . . a very complex management structure [that] . . . pulled more and more people in [and away from core functions].

The distinction between analysis and collection [is beginning] to break down. To be out there looking at masses of data, you need to know what you're looking for. You need to be an expert.

It seems to me that downsizing analysis significantly after the Cold War was to a fair extent penny-wise and pound foolish.

People are the core of the intelligence business. We've made a number of decisions as a nation in the past decade that deemphasize people. I consider that one

of the biggest strategic mistakes in US intelligence Language is a critical part of this. Unfortunately, we've been working the [foreign] language problem for decades now, and it still doesn't seem to be improving.

The DI is grossly overstretched. Frankly, the DI was grossly overstretched on September 10, and since then we have created an 800-pound gorilla in Homeland Security and [another] in CTC.

We've made a number of decisions as a nation in the past decade that deemphasize people.

Reforming the IC: Proposals for Change

The conference surfaced multiple proposals for improving the performance of the IC in meeting the challenges it faces. They ranged from a sweeping institutional overhaul to more modest proposals for improving the depth of expertise and the range of analytical tools at the disposal of the IC. Responding to the widespread—albeit not universal—feeling that the IC's organization on the basis of collection disciplines inhibits its ability to respond to new and rapidly evolving crossborder threats like those posed by terrorism, the most far reaching suggestion was a proposal for a sweeping overhaul of IC structures and procedures.

As outlined by one speaker, this scheme aims at restructuring the Community on the basis of 10-to-15 major missions, such as counterterrorism and China. The current lineup of IC agencies, including the DI and DO, would remain in existence, but primarily as pools of specialized talent and expertise on which the proposed mission-oriented Community Centers could draw to support their personnel and other needs. The centers would have full programmatic and operational responsibility for a given mission.

The centers and the existing agencies would all be incorporated in a revamped Central Intelligence Agency that would function as such, in fact as well as in name, replacing the loose confederal structure of today's Intelligence Community. The overall structure would be under the control of a DCI with greatly enhanced personnel and budget authorities. Specifically, this more muscular version of today's DCI would have the power to appoint and replace center and agency heads, as

well as the authority to transfer personnel and resources from one agency or center to another.

Other, somewhat less far-reaching proposals, also focused on what most saw as a key weakness of existing IC relationships, the DCI's limited authority over the Community. Although not endorsing a ground-up restructuring of the Community, they made a strong case for eliminating many of the current constraints on the authority of the DCI by giving him full budgetary authority over all member agencies of the IC and converting him into a Director of National Intelligence.

A third proposal supported by several speakers zeroed in on the IC's difficulties in meeting the threat of domestic terrorism. These speakers backed the creation of a US equivalent of the British MI-5, a domestic intelligence agency with overall responsibility for counterintelligence and counterterrorism. One speaker argued that concern about the potential threat this might pose to civil liberties was misplaced. Concentrating responsibility and authority for these issues in one agency would facilitate Congressional and public oversight, which is currently fragmented.

Another speaker called for revising our definition of the Intelligence Community. With reference to the counterterrorist problem, he pointed out that much of the expertise and collection capabilities against this target were to be found beyond the confines of the IC, in the ranks of police, other local and federal government officials, and academics. He argued in favor of a fundamental rethinking of the institutional and

procedural barriers to the exchange of information between the IC and these groups.

Other speakers did not go this far, but there was strong support for an overhaul of the security and classification procedures that inhibit the exchange of information with other governments, non-IC agencies, and groups with particular expertise or relevant responsibilities. NOFORN restrictions that inhibit the exchange of information and intelligence cooperation with friendly services came in for particularly strong criticism. Several speakers argued that the number of truly sensitive items of intelligence information—originating, for example, with unique sources—did not justify the proliferation of special compartments and restrictions.

Along with those who supported institutional reforms and makeovers as solutions, others looked to technological or methodological innovations as ways to improve the IC's performance. Speakers saw new technological and software solutions as essential to coping with the ever-increasing masses of data that are deluging analysts. There was particularly strong support for technology-facilitated approaches to data mining and pattern recognition as ways to identify emerging threats—the "unknown unknowns."

Another speaker argued that technological aids also could be important in retrieving the "unknown knowns." Equally important, in this speaker's view, were new methodologies and a willingness to reconsider discarded hypotheses and alternative analyses. He envisioned technology as a means of facilitating this reexamination of old data and hypotheses, and avoiding the

pitfalls of short-term, event-driven analysis that have been characteristic of much of the IC's production.

Others saw the remedy to the Community's problems in a return to basic principles of the intelligence craft—such as a revival of emphasis on the classic intelligence cycle—rather than new approaches. Most of those holding this view stressed the importance of reemphasizing area knowledge—"understanding the enemy"—as a fundamental building block of the Community's analytical capabilities. One called for a national program to build a knowledge base on the Islamic world akin to the government's support for the Soviet studies programs that had dramatically improved our understanding of the Soviet system. Another warned against singling out any one region of the world for emphasis at the expense of other regions, arguing that we could have little confidence in our ability to identify the threats that would exist 10 years from now.

Conference participants recognized that the development of broad area expertise would be a laborious process. Some called for innovative approaches to tapping outside expertise, such as the development of a reserve intelligence corps of academic and other outside experts. This would be used in much the same way that the military relies on reservists to expand its capabilities in time of need.

Panelists also examined ways to improve the interface between the intelligence and policy communities and to ensure that the product meets the needs of the policy makers. There was a general consensus that formal policy documents, such as the new National Security Doctrine, were an

inadequate guide. At best, they provided a snapshot of an Administration's intentions, and could not take into account the constraints and pressures that would be imposed by time and circumstance. Polling the policy community for its interests and priorities was also dismissed as virtually useless as a guide to future needs, most sharply by a former senior policy consumer.

There was a strong consensus that an institutionalized dialogue—one embedded in standard practices—offers the best means of attuning the IC to the needs of the policy community. Speakers warned, however, that to be useful the DCI would have to initiate the exchange by inviting a reaction to his proposed priorities, rather than relying on the policymaker to look beyond his or her short-term needs.

Presentation Excerpts

On Restructuring the Community

Whatever management philosophy you may think is good, you wouldn't come up with the Intelligence Community the way it is. Almost any change, even random change, would probably improve it.

If we assume a rate of change in national security affairs over the next 10 years at least equal to what we've seen in the previous 10 years, we had better be prepared to make radical changes in the way we do intelligence.

How do you create a mission focus in the Intelligence Community? I think you need to create . . . Community Centers. We have Centers. We just don't have Community Centers. We have a CTC, a Counterterrorist Center, at CIA. Most people like to call it the DCI Counterterrorist Center, as though giving it the DCI nomenclature makes it a true Community Center. [But] CTC does not organize the way the Intelligence Community goes against the terrorist threat facing the United States.

You need to put these Centers someplace. I'd propose someplace called the Central Intelligence Agency. It's not today's CIA, so don't think CIA. It's the Central, emphasis on Central, Intelligence Agency. Some organizational structure . . . central to bringing together all these activities across our existing Intelligence Community.

If we had these Centers, the Community's programming and budgeting process would rely on the Centers to help us figure out where we need to put dollars and cents in programmatic activities against the missions . . . NSA, or NIMA, or DO, or what have you.

[These Centers] need to report to some sort of corporate center. You still continue to have NSA, NIMA, etc. . . . as subsidiary spokes to the central corporation. Those subsidiaries provide services . . . people who support the Centers The Directorate of Operations and the Directorate of Intelligence would be treated the same way . . . as NSA or NIMA . . . as supporting functions to the overall mission orientation of the various Centers.

If we assume a rate of change in national security affairs at least equal to what we've seen, we had better be prepared to make radical changes in the way we do intelligence.

Our current system is based on drawing a balance heavily in favor of security versus the flow of information. . . . We're going to have to draw that balance differently.

This overall central organization . . . needs to be headed by the DCI. Some people want to call him the DNI. I don't care what you call him. [There] needs to be somebody in charge.

If we're ever going to get NSA, NIMA, DO folks, DI folks, people from DIA together in Community-wide Centers, somebody has to . . . be able to move people across the Intelligence Community, anytime, anywhere. . . . You need somebody at the top who actually is responsible for picking, employing and, when necessary, firing the heads of the major [subsidiaries] I think the DCI ought to be given the ability to pick the heads of these organizations in consultation with the Secretary of Defense, just the opposite of the way it is today.

The DCI needs to control the money . . . into, out of, and around the Intelligence Community At the moment, that's not the way it works at all Some 80-to-85 percent of the Community's budget is not appropriated to the DCI. It's appropriated to other people.

[Reorganization on the basis of mission would] centralize management of the Intelligence Community in an organization that actually has a Community function You actually end up with somebody responsible for intelligence; somebody who ought to be held accountable.

We need . . . a new definition of what the Intelligence Community is, because the Intelligence Community isn't just the group sitting here in this room It's a very undefined and broad group of people who exist in and out of government in the United

States and abroad. In particular, we need to begin to think about the role of the state and local governments, private sectors, and civilians as part of this.

Our current system, based on security clearances and the need to know, is based on drawing a balance heavily in favor of security versus the flow of information. . . . We're going to have to draw that balance differently. We're going to have to be prepared for more leaks, for more compromises of information, to make sure that people who need . . . information have a way to get [it.] . . . There'll be some kinds of sources that are of such great value that we have to protect them, but I think we're going to have to draw the balance very differently.

We're going to have to have a much more decentralized system in place [We] have to recognize that there are going to be lots of different nodes and different ways in which networks develop to deal with intelligence information.

Both because of the nature of the [intelligence] challenge . . . and because we need to find a way to break down the domestic and international lines, it seems to me that we need to look at the MI-5 model. . . . Many of the critics of the MI-5 proposal [have asked whether it poses] . . . an unacceptable threat to civil liberties . . . [but] we should not try to solve our problem with civil liberties by having a less effective domestic security strategy. . . . I think it's possible through a very serious [debate] and explicit . . . set of guidelines to deal with what we want such an organization to do; to have clear rules, strong accountability, and strong oversight.

**The challenges
for the intelli-
gence world will
not continue
. . . to conform
to a few
standard
formats.**

It does seem to me that an MI-5 or domestic intelligence organization probably is the right ultimate outcome From [the perspective of] accountability and oversight, it seems to me it probably would be preferable to have a separate agency, separately overseen, than to have domestic intelligence continue to be the tail of a law-enforcement dog. I think that would make for cleaner lines of accountability and oversight. As it is now, the oversight committees . . . oversee [only] part of the FBI.

[I think] the ability to mix and match specialties according to the issue [rather than a massive restructuring is the way for the Intelligence Community to go]. . . . The challenges for the intelligence world will not continue . . . to conform to a few standard formats. They will require an ability to move blocks of knowledge and expertise together in new combinations, possibly for interim periods, possibly for long periods if the problem is durable and the need for coverage is durable. They will need the application of networked approaches. In particular they are going to need networking into the outside world—networking into outside expertise—because you can't possibly have what you need inside the building for all the kinds of issues that you're going to need [to deal with]. But above all, it needs networking within the system. This implies . . . the need for crosstraining, crossassignment, and, of course, for having people spend time in the policy world . . . so they can acquire an instinct for what that's about.

On judging plans for reorganization, we need to balance the clear short-term costs, disruption of work, against uncertain long-term benefits Both centralization and decentralization offer important benefits, because they're good for different things Centralization helps us against the Pearl Harbor problem, but it's less open to dissent, challenges to dominant views. . . . It promotes layering, delay, sclerosis, stifling of unconventional views . . . like any huge hierarchical bureaucracy. Decentralization has the advantage of pluralism and competition that helps to surface disagreements; it copes with politicization by making a clearer market for competing views, but it makes units more responsive to their parent department's interests than to national intelligence. It promotes duplication, confusion.

[Can] covert action become a more important part of what we do? . . . It is certainly true that we need to be able to mount operations that allow us to disrupt [terrorists] and be effective in dealing with them. The question is whether that is the same as what we have traditionally understood to be covert action. And second, whether we have the right institutions to cope with it in its new forms. I would suggest that the kinds of secret operations that we're talking about are different in character from traditional covert action. [There] the goal was to hide the hand of the actor and, in effect, create deniability for the United States. For the most part, the kind of secret operations that we need to do now are operations for which we need secrecy [to carry out], but not necessarily deniability after the fact.

We need to think about tools and techniques that will help us see patterns that we haven't seen before.

On Exploiting Technologies and Methodologies

Is there any way we can replicate that [success against the Soviet target]? . . . I don't know the answer . . . but I think I know where the answer is to be found. . . . The answer is going to be found in the space between aggressive human operations, close-in surveillance technology, and deep data mining.

How do we begin to think about these "unknown unknowns"? How do we get the kind of peripheral vision that sensitizes us to things that haven't been on our screen, that don't fit the models that we have? Here's where this very challenging question of pattern recognition, of data mining, comes in. Notwithstanding the very bad publicity that TIA [Total Information Awareness] got and . . . deserved because it was cavalier about the potential civil liberties implications, we do need to think about tools and techniques like that that will help us see patterns that we haven't seen before.

There are enormous possibilities for technology to help us in these tasks Technology is not a panacea. We're not going to find the algorithm that allows us to find hidden terrorists in the weeds, but at the same time, technology does allow analysts to do their job better, more effectively, to communicate better with others, to disseminate better It also can provide a lot more accountability by keeping records, by letting us know what we're searching for Analysts can be held to account, policy-makers can be held to account.

Finding ways to put analysts and technology together to mine enormous amounts of data [is important]. More important, it seems to me [is being] open-minded about patterns, [resurrecting] hypotheses that were discarded, [looking] at data again and again and again. [We have what] seems to me to be a real opportunity to think about methodologies more generally.

On Improving the Intelligence Product

What strikes me about the run up to 9/11 was how important the things we didn't know we knew were Reminding ourselves of the "unknown knowns" is an important part of the challenge in front of us. We'd known from about 1990 on about planes as bombs. We just forgot we knew it Keeping alive what we've known in the past but may not be attentive to at the moment . . . calls for a kind of methodological sophistication, a use of technology, that really offers opportunities.

Since everybody is pressed for manpower and time, especially on the part of people who are [area] experts, this may be an area where a few experts on the inside, plus some contractor support, could be of help. [They could] look through a carefully crafted list of targets or topics where we know we really have to be up to snuff. . . . Are we? It's worth knowing why we're not, if we're not. Is it a question of funds, people? . . . More important, though, can we close the gaps? . . . How might we do that?

Since the volume of data is getting larger, we're going to have to rely on better automated solutions with brilliant software tools

One of the emerging challenges for intelligence . . . [is] intelligence sharing . . . across national boundaries.

to help us slice, dice, manipulate, and profile those signatures. And I'm talking meta-data, as well as internals, to do the keyword searches to make the interrelationships apparent quickly so that we can focus and try to understand significance and relevance to the tactical problem, or to the operational problem, or the key read at the strategic level.

The current buzzword . . . is "multi-INT," which has lots of features in common with all-source analysis or fusion. If it has distinctive features . . . there are really three. One is a lot of understanding of what the various INTs can do. Second is a very iterative process that keeps going back, over and over existing hypotheses and data. The third is a degree of technological sophistication that lets that happen rapidly. Those seem to me to be features that need to characterize intelligence analysis in the future. It needs to be much more interactive; it needs to be much more open-minded about hypotheses. . . . [It should be] less event driven. Events are important . . . [but less so than for] Cold War intelligence.

[My experience at the NIC] made me realize just how much expertise is out there in society that is tappable [if we are] creative enough. Lots of people we wanted to get with sophisticated technical or financial expertise, we couldn't have hired for a career, but we could get [them] for a couple of years with some combination of [appeals to] patriotism and [the opportunity to see] how the other side worked. I think the possibilities for doing that and for all kinds of less formal relationships with NGOs, academics, think tank, and Wall Street peo-

ple—which the Community is starting in some small but interesting ways to tap—is going to be critical.

One of the emerging challenges for intelligence . . . [is] intelligence sharing . . . across national boundaries. Certainly the war on terrorism has shown us that. . . . My sense is that some countries still believe that the asymmetry of both political power and intelligence capabilities still put them at a great disadvantage. Either what they have is not valued by the United States or they don't feel they're getting anything in return. . . . So I don't think we've got the politics and the culture of a new concept of sharing down right. We are essentially using the old model of bilateral liaison relationships, when perhaps something much broader, more inclusive, is called for.

We've got to be imaginative, [perhaps] internationalizing espionage [against the jihadist target]. . . . We [already] rely heavily on foreign liaison. Most of our agents, operatives, and collaborators are non-Americans. There must be some way to parlay this

One of the most important reforms, at least for the mission of counterterrorism and a lot of associated questions about political instability, world order and so forth, is the cultivation of much larger numbers of real area experts in this country, who are genuinely bilingual, really bicultural, who haven't just taken a few courses, or learned how to order from a menu in an exotic language,

I've been struck by how much we really have to return to basics. Back to basics really means understanding the adversary.

but can really operate abroad . . . and get inside the skins of people who are not like . . . Westerners.

Having a revolution in intelligence affairs does not mean that every single thing has to change. In fact, I've been struck in the last day and a half by how much we really have to return to basics. . . . Back to basics really means understanding the adversary. . . . In Iraq, there are people reading thousands of messages a day and writing sitreps every four hours. What they are doing is very, very important, but it's not analysis. Analysis means having the luxury of time to think about your adversary.

We need vastly simplified management, and a significant increase in the number of core functions people that we have. . . . There's so much overhead in the Community that that's doable within current numbers, but it does require a simplification of structures. I think SIGINTers and imagery analysts should be collocated with other analysts far more than they are now.

The bottom line on analysis is that we need to get people more time to think. [Time] is one of the things that the people in the Community have very, very little of. . . . Some of that you [may be able to] solve by linking to outside expertise.

My instinct is to err on the side of throwing money at a lot of things, because I have very little confidence that we can know now what we're going to need five or 10 years from now. One simple answer . . . is to invest more in analysts with regional expertise.

One of my few specific recommendations for reform [is] to create a systematically organized and serious intelligence analyst reserve corps . . . using these people for first coverage of apparently low-priority areas. And secondly, as a pool of mobilizable, smart, well-grounded people who can be used to beef up other accounts in an emergency. . . . It's a good opportunity to use people with expertise in universities, think tanks, businesses that operate abroad, and so forth, the way the [military] services use military reservists.

The US government was a big actor in creating the broad and institutionalized knowledge base necessary for conducting the Cold War. Could we replicate that in some way today? We need to create, among other things, an atlas of Islam . . . a knowledge base. We ought to do it as a national project.

On Fine-tuning the Relationship to the Intelligence Consumer

The fundamental responsibility of intelligence to power is to tell truth. . . . If you don't do that, if you trade in your independence for the sake of greater intimacy and access, then you have violated what should be a fundamental ethic of the Intelligence Community.

**The
fundamental
responsibility
of intelligence
to power is to
tell truth.**

The first relationship, the closest bond between the intelligence services, has to be between them and the President. You cannot be in a position where the President asks, "Who are these guys working for anyway?"—where he looks at his DCI as a potential interloper rather than as someone to turn to for the most sensitive information. What does that mean about the Congress? Well, it may mean there has to be something of a lag [in getting information to them].

Most of the time the intelligence consumer . . . doesn't know what [he] wants until [he] needs it. So [the responses to] the questionnaires that you send out . . . [are] hogwash. . . . What I would do is have the DCI, once a year, present a document to the National Security Council, "Here's what I think you need, and here's what I'm planning to do." Give the consumers a document [to which they can respond]. . . . I think then you would get a dialogue. There is no dialogue now.

You still need to be able to anticipate things that are not on the current Administration's agenda at all, but that are the responsibility of the Intelligence Community to highlight and draw attention to.

There has to be . . . [a dialogue between the analyst and the intelligence consumer about priorities]. The question is, how do you induce that? How do you create the structures to do it? . . . We need some way of building this into the system so that it becomes part of what people do.

[We need to] rethink again the distinction between policy and intelligence. . . . [Our situation] requires a process by which analysts and policy people work much more closely together. Intelligence [should] help frame hypotheses . . . hear what hypotheses are on the minds of policy people, [try] to understand their worries . . . mixing up policy and intelligence much more than we have traditionally done is all the more important [now].

