

Central Intelligence Agency  
The Work of a Nation. The Center of Intelligence

Search 

## CSI

# Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm

---

**Roger Z. George**

### ***The Challenge***

*Post-Cold War and post-9/11 challenges raise questions about the effectiveness of the traditional intelligence paradigm.*

In the six years that have passed since the shock of the attacks on 11 September 2001, a great deal of change has occurred within the US Intelligence Community (IC). Legislation created a Director of National Intelligence (DNI) with authorities to develop overall strategies and promote integration of intelligence activities; specific intelligence units have been established within the FBI and as part of the newly created Department of Homeland Security, as well as new IC-wide centers like the National Counter-terrorism Center and the National Counterproliferation Centers.

The Intelligence Community is revitalizing clandestine collection of human intelligence and enhancing the cadre of intelligence analysts and their foreign language capabilities.<sup>1</sup> These and many other changes are occurring at a time when the United States is facing entirely new challenges unmatched since the end of the Second World War.

The essence of many such efforts—all necessary and long overdue—is to improve the effectiveness of what has been the dominant intelligence paradigm for the past half century. That is, a paradigm which develops critical information through a national, classified system of collection and analysis. This paradigm has been effective in organizing US intelligence—as well as many other national intelligence systems in other countries—for what have been largely state-centric challenges.

Despite occasional surprises, the United States and its allies did a good job of monitoring the Soviet Union's domestic, military and foreign policy activities for most of the Cold War. While crises occurred, intelligence helped policymakers avoid going beyond the brink into a nuclear

Armageddon.

At the Cold War's end, there were many critics who claimed the IC—perhaps most especially the CIA—had outlived its principal adversary and its *raison d'être*. Like it or not, this assertion proved sadly incorrect as the series of terrorist attacks culminating in the 9/11 attacks brought home to the American people the enduring need for organizations focused on anticipating and warning about major threats to our nation's security.

What has been less well understood, however, is that many post-Cold War and post-9/11 challenges raise questions about the effectiveness of the traditional intelligence paradigm. In fact, many of the post mortems which followed the 9/11 attacks pointed directly to the need for an entirely new way of developing insight and anticipating surprises, one which places less emphasis on secrets or restricted channels for sharing information and more emphasis on open source information and creating networks of expertise that connect diverse thinking across disciplines as well as continents.

Indeed, the DNI's July 2006 Intelligence Community Directive 301 on "National Open Source Enterprise" establishes the goal of making open source "the source of first resort."<sup>2</sup> What follows here is a description of a new way of thinking about intelligence collaboration that is designed to leverage open sources, multi-disciplinary and multi-national sources of expertise, and pooled international resources. The objective is not to eliminate the old paradigm, but rather to complement it with a new way of handling 21st century transnational challenges.

[Top of page]

## ***Transnational Issues***

*The world is now confronted with a host of border-spanning trends which challenge our traditional intelligence and law enforcement practices.*

What distinguishes today's tests and makes the traditional intelligence paradigm less effective is the transnational and global character of many trends. As Tom Friedman's "flatness" metaphor notes, the compression of time and space and the easy movement of people, weapons, toxins, drugs, knowledge and ideas have transformed the way threats emerge and challenge the way intelligence must operate.<sup>3</sup>

Many of the major international terrorist attacks, including those of 9/11, follow the pattern of having been conceived, planned and launched from many different countries, making the individual actions of any single government or intelligence service ineffective in detecting, deterring or preventing those attacks.

It would be short-sighted, however, to focus exclusively on the "terrorist" threat, as the world is now confronted with a host of border-spanning trends that challenge our traditional intelligence and law enforcement practices. International organized crime, narcotics trafficking, illicit sales of weapons—WMD as well as conventional—not to mention the spread of disease, internet-driven jihadist and other militant forms of radicalization, and the geo-political implications of climate change head the list of new transnational challenges we are collectively facing. In his excellent book, *Illicit*, Moises Naim calls many of these the international community's "blind spots," which our current analytical lenses are not to make sense of. <sup>4</sup>

Not surprisingly, many of these transnational issues are becoming central themes of intelligence organ a series of workshops in 2004, the CIA and the Rand Corporation examined what could be done to ada to better address threats coming from the transnational realm.<sup>5</sup> Among the many insights generated fi meetings was the idea that such issues could be better understood through a process of “sense-making a continuous, more free-wheeling, creative and collaborative process of questioning assumptions and e one’s ideas to inspection by experts who do not necessarily share the same background, training, or na

Simultaneously, within CIA growing attention has been given to so-called “strategic research themes” : Islamic extremism and radicalization, terrorism, strategic threats emerging from transnational drug, c illicit finance groups as well as proliferation of various weapons technologies.

<p>This is not a uniquely US concern.</p>	<ul style="list-style-type: none"> <li>■ The globally stored information produced annually equals more than 37,000 new Library of C collections (Global Business Network)</li> <li>■ Four million people are smuggled across international borders each year (UN)</li> <li>■ The illicit global economy accounted for \$500 billion in world trade (Interpol)</li> <li>■ Over 80,000 computer viruses exist today, with 80 new ones per month (Symantec Corp)</li> <li>■ Over 80,000 computer viruses exist today, with 80 new ones per month (Symantec Corp)</li> <li>■ SARS, Marburg virus, Avian flu, antibiotic-resistant bacteria are on the rise (WHO)</li> </ul>
---	---

For example, writing even before the 9/11 attacks, the German Foreign Intelligence Service’s president, Er noted that his service’s mission was to provide early warning of transnational issues, including weapo proliferation, international terrorism, organized crime, trafficking and money laundering.<sup>6</sup>

### Slices of the New Transnational Reality

Other intelligence services are likewise faced with monitoring threats to their national security interest homelands that are far more diverse, interconnected, and dynamic than ever before. One of the rationa creating a European Union’s Situation Center, which now includes an intelligence cell, is to cooperate : of transnational security.

As the 2003 European Security Strategy makes clear, the issues of international terrorism, proliferatio organized crime, and state failure head the list of what it calls “new threats which are more diverse, les and less predictable.”<sup>7</sup> It is also encouraging that—despite the many reports of growing rifts in Europe American views—there is a surprising consensus among publics on the importance of terrorism, Islam fundamentalism, immigration, global disease and environmental changes; as the German Marshall Fu “Transatlantic Trends” study showed that “large majorities—topping 70 percent of Americans and Eur continue to agree on a wide range of international threats in the next ten years.”<sup>8</sup>

*Other intelligence services are likewise faced with monitoring threats that are far more divers interconnected, and dynamic than ever before.*

The question, then, becomes how can our intelligence services make better sense of these boundary-le state, often global phenomena that are not explained adequately by the collection of “secrets?” To be si secrets still remain regarding the actions of specific terrorist or proliferation networks. However, muc transnational phenomena are in “plain sight,” but might not be visible because those insights are not fi among US government experts who hold security clearances or are generated by the few non-US exper intelligence services with whom we hold classified exchanges. Both the 9/11 Commission and Iraq/WMD Commission reports singled out IC’s use of open sources and outside views as areas where more impro are needed. In particular, the Iraq WMD Commission noted:

*The need for exploiting open source material is greater now than ever before. Regrettably, the Intelligence Community’s open source programs have not expanded commensurate with eithe*

*increase in available information or with the growing importance of open source data to today's problems.*

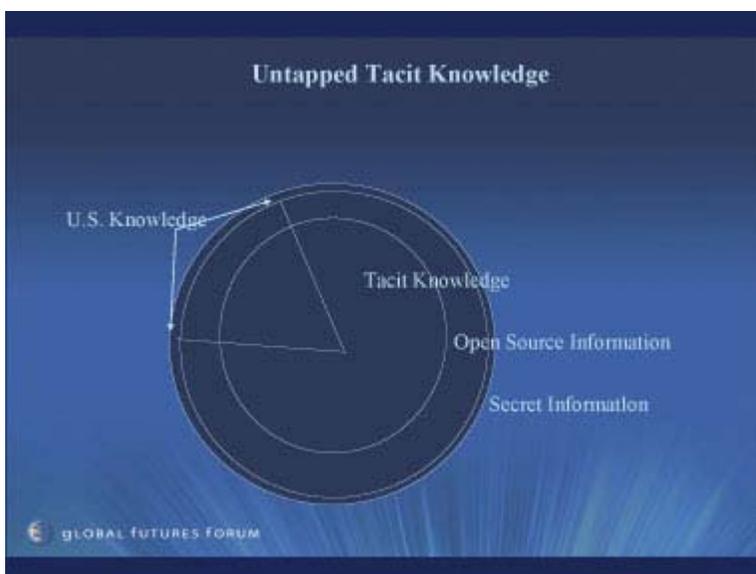
*During the Cold War, the Intelligence Community built up an impressive body of expertise on Soviet society, organization, and ideology, as well as on the Soviet threat. Regrettably, no equivalent talent pool exists today for the study of Islamic extremism...Non-clandestine sources of information are critical to understanding society, cultural and political trends, but they are insufficiently utilized.*

*Many of the intelligence challenges of today and tomorrow will, like terrorism and proliferation, be transnational and driven by non-state actors...The Intelligence Community needs to think more creatively and above all more strategically about how it taps into external sources of knowledge.<sup>9</sup>*

*"Open source," in the sense of not being classified, is not always to be found in a broadcast, a book or journal, or other media form.*

Though much of this knowledge is "open source" in the sense of not being classified, it is not always to be found in a broadcast, a book or journal, or other media form. In fact, much of that knowledge is "tacit," meaning it resides largely in the minds of experts who have collected knowledge through study, experience, or other special skills. How can we access such "tacit knowledge" when the paradigm in which intelligence traditionally operates is based on controlling access, limiting contact with foreign nationals, and focusing only on the most important, "hard" targets?

As the figure below illustrates, the knowledge that the United States can directly leverage is remarkably small in comparison with the global information environment; even granting that the IC has the best "secret" information, this amounts to a very small amount of knowledge (e.g., merely the thin outer "crust" of only one section of world of knowledge); in comparison, the open source information (e.g., various media forms) and the even larger amount of tacit knowledge (e.g., in the minds of experts) available globally dwarfs the world of secrets.



Speaking to an international audience in December 2006, Scottish innovation specialist David Robson remarked to an audience of intelligence experts that "all the smart people do not work for you," nor would you want to employ them; however, research shows that "nobody is as smart as everybody," so using a more open, network-centric model would enhance one's knowledge the faster the network grows.<sup>10</sup> If we do not

work to leverage this vast resource, are we not consciously blinding ourselves to much that can be learned about transnational challenges?

[Top of page]

### ***The New Paradigm: Collaborative Intelligence***

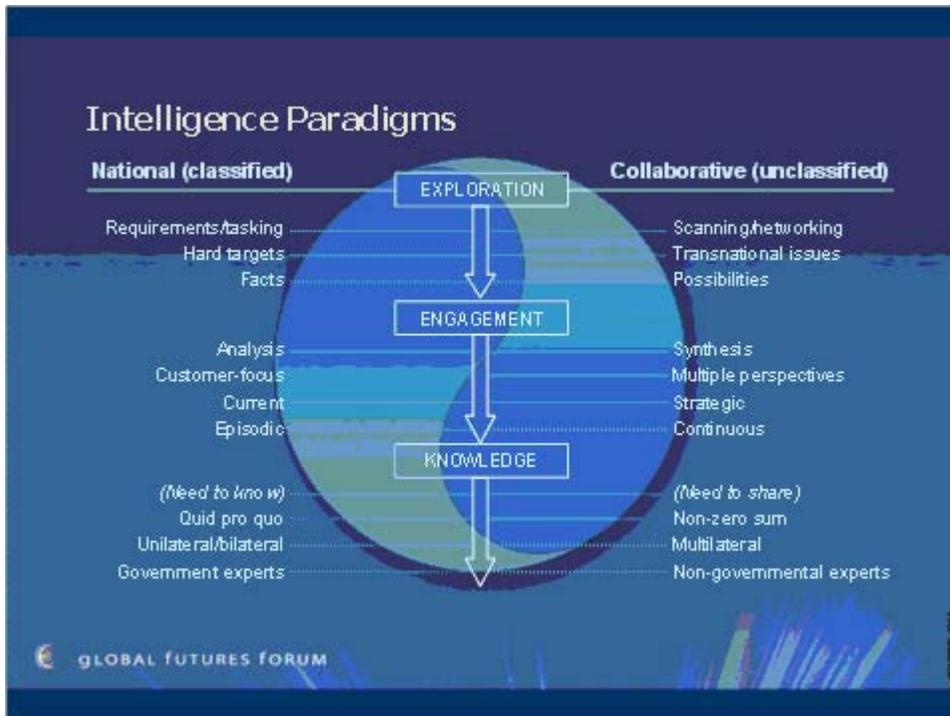
The opportunity now exists to tap into a vastly larger amount of expertise than was previously available to US intelligence. However, this will require working from a very different paradigm from that which characterized much of our Cold War history. The key features of that traditional paradigm were: secrets; classified channels of information flows; a focus on a few hard targets (e.g., the Soviet Union, other so-called “denied area” Communist Bloc countries, their military forces and technologies and other observables); very limited contact with outside experts who were almost always US citizens; and focus on key facts and finished intelligence products.

The new paradigm, in contrast, will focus on “open source” information and reach out to a wide variety of experts who are non-intelligence professionals drawn from different sectors and often non-Americans. As the 21st century is expected to be far less predictable and dynamic, the objective is to scan the horizon for emergent issues and so-called weak signals that are harbingers of futures for which few governments have begun preparing.

This more collaborative paradigm is clearly a major departure from the traditional one, as the figure below suggests. While it cannot begin to replace the old model, it surely can complement it and build knowledge that can be used by those still working largely within the traditional “secrets”-driven paradigm.

*The opportunity now exists to tap into a vastly larger amount of expertise that was previously available to US intelligence.*

This new collaborative paradigm is more than simply an open source collection model. Indeed, it is an approach that attempts to synthesize knowledge found in various academic, business, and other private sectors with government expertise. While the traditional paradigm would focus on specific “hard targets” for specific facts (also known as plans, intentions and capabilities), the collaborative model is scanning for interesting interconnections among issues, anomalies from what experts might normally expect to see, and other insights, which in the traditional paradigm would be considered irrelevant or too unconventional to be of use.



This collaborative model is based on a great deal of work done in academia and industry that suggests “knowledge management” and “innovation” require connecting people with diverse perspectives to harness collective insights and combine their expertise in novel ways. As many business innovation experts also point out, “new” ideas are generally not entirely new, but rather spring from existing ideas, which are combined in new ways or built upon by experts who bring new insights to them. So, the iPod was born from combining the notion of miniaturized data storage with online music services. From that has grown the phenomenon of broadcasting video/audio interviews to MP3 owners who can view this information a thousand times. And so on, and so forth.

[Top of page]

### ***The Global Futures Forum: The Transnational Agenda***

In recognition of the dynamic and unpredictable nature of the 21st century security environment, the CIA has begun experimenting with the collaborative intelligence paradigm. In November 2005, following a series of intensive workshops cosponsored by Harvard University, the CIA’s Global Futures Partnership invited 111 from over 20 foreign governments, intelligence and law enforcement agencies, and non-governmental organizations to participate in a conference in the Washington, DC, region aimed at creating a global intelligence network. One of those meetings was fashioned the “Global Futures Forum (GFF),” an unclassified, multilateral and cross-sectoral network of experts who would collaborate in examining global security issues. The three-day discussions led to a strong consensus for networking among intelligence experts, academics, business, private-sector groups, which could work more cooperatively in understanding highly complex and very difficult issues.

---

The  
form

of  
the  
Global  
Futures  
Forum  
(GFF)  
would  
be  
a  
multinational,  
multi  
disciplinary  
community  
focused  
on  
transnational  
security  
issues.  
It  
would  
be:

- Exclusively unclassified,

although the network would operate under the “Chatham House” Rule that would facilitate free candid exchanges.

- As diverse as possible, drawing from both government and non-government to stimulate and challenge prevailing assumptions.
- Focused on specific issues or themes around which strategic-level conversations could occur, drawing on members’ interests and knowledge.
- Operated in both a face-to-face and virtual (online) fashion by invitation only, in order to build trust and experiment with new thinking styles and IT tools.

At this initial meeting, discussions focused on the need to build subgroups of experts (communities of interest) around significant transnational themes that participants agreed to explore in an unclassified, multi-disciplinary environment.<sup>12</sup>

Since November 2005, the GFF, as it has become known, is now well established and gathering momentum, broadening its membership and its communities of interest. In just over a year, the GFF has hosted more than a dozen events on a half dozen issues, with a similarly ambitious agenda for 2007.

Moreover, the initial Web site ([www.globalfuturesforum.org](http://www.globalfuturesforum.org)) has become fully operational, hosting members from a number of countries, with diverse backgrounds, as well as discussions for nearly a dozen global security topics. At the second annual GFF meeting in December 2006, more than 250 representatives from more than 40 countries and over 90 government and non-government organizations exchanged views on major transnational security topics, developed agendas for upcoming events on important topics, and committed themselves to be even more deeply involved in this new business practice.

*The Global Futures Forum is now well established and gathering momentum in broadening its membership and its communities of interest.*

The Global Futures Forum is now well established and gathering momentum in broadening its membership and its communities of interest

The GFF is now promoting a series of face-to-face and online discussions among an international group of experts that touches on some of the most pressing global security issues like radicalization, terrorism, illicit trafficking, and pandemics.

To take one example, the forum has held three international meetings on “Radicalization,” attended by more than a dozen governments’ intelligence and security services, as well as academics, NGO experts, and other civil society leaders. At these meetings, discussions ranged from the conceptual (“what is radicalization” or “concepts of multiple identities”) to more specific topics (“the deeper roots of extremism” or “impact of immigration and social policies on radicalization”).

These meetings have also brought new experts and ideas to the attention of US analysts—for example, researchers from far-flung academic institutions in Sweden, Norway, India, and Singapore, who work with European institutions as well as the United Nations. Other knowledgeable Islam experts attending GFF events have also worked in such organizations as the International Crisis Group or direct strategic futures projects in South Asia.

This mix of perspectives has generated great interest on the part of all the participants to keep the dialogue going and to broaden it to include other diverse perspectives. One current interest is the idea of preparing a series of future scenarios looking at where “radicalization” as a global phenomenon might be by 2012.

The forum is simultaneously examining social networking tools (such as the Internet-based phenomenon Second Life) for their applicability to intelligence topics like illicit trafficking, organized crime, and sub-national power centers that might be challenging the central authority of weak governments in failing states. (See chart below).

In another community of interest on “Foresight and Warning,” the forum has already introduced the IC to new concepts for collaboration and anticipation of future trends. One such tool is a “horizon scanning” program being used in Singapore and the United Kingdom to scan for new emerging trends that might have important implications for national security policies. In Singapore, for example, this technique is being applied to develop a network coordinated approach to the fight against terror. 13

Experimenting with this new paradigm opens up a number of avenues for new learning and insight. First, as many business and knowledge management experts have noted, bringing diverse perspectives together to work on a problem is inherently worthwhile, as it exposes organizations to the hidden assumptions and prevailing mindsets that prevent new thinking or new business practices from being taken seriously. This approach is also a practical way of harnessing the so-called wisdom of crowds by gathering a large number of views, not just more of those who hold ones we already share, to see if there is some nuances which we are missing.

Second, global collaboration holds the promise of developing more common vocabularies for thinking about problems with fewer inter-cultural and international misunderstandings. This can be as simple as trust-building among experts from a variety of governments, disciplines, or philosophies; or it can be as complicated as developing accepted definitions of what radicalization or terrorism means. Enabling experts from a number of fields to exchange and debate different perspectives must often follow the establishment of a common basis of trust and understanding of the topic.

Third, collaboration in the GFF will inevitably lead to some changes in our work practices simply by virtue of a different way when meeting within the GFF paradigm. This learning does not come easily and some are themselves reluctant to permit this type of learning; however, the more we experiment with new methods to find practices and partners that can help us adapt to the 21st century challenges.



the Global Futures Partnership, recognizing the power of exploiting more open and diverse sources of

Other services have over the past 12 months identified points of contact for the GFF and asked for a dialog that can be managed in a way that provides all participants with influence in developing the activities and tasks. Moreover, many non-government experts have not only supported this activity as a useful counter-measure to traditional insularity, but also because the forum presents a novel opportunity for them to deal with issues on an equal footing and also air their ideas in front of government specialists normally not available to them.

[Top of page]

### ***Looking Ahead***

As the global environment continues to move toward more multipolar sets of relationships, there will be a need for the intelligence agencies to develop a new intelligence paradigm. The Global Futures Forum is but one of the innovations which must occur to keep the IC flexible and adaptive to a new environment.

*The forum gives non-government experts opportunities to deal with intelligence experts on an equal footing and to air their ideas in front of government specialists normally not available to them.*

Other important initiatives and experiments are underway in other parts of the IC as well. The CIA's Office of Transnational Issues has created a "CoLab" (Collaboration Laboratory) designed to test new methods of collaboration across the IC and to engage with outside business and scientific entrepreneurs to practice using new technologies in the pursuit of faster and smarter team work.

The Open Source Center (OSC) has initiated the use of online "bloggers" to encourage postings from worldwide users of its services who have comments on open source materials posted to the OSC Web site. The DNI itself is underwriting a number of IT-related experiments, including the drafting of unclassified national estimates on infectious diseases by inviting global experts to post their information, perspectives and comments on an unclassified Wiki space. This effort has so far produced more than 1,000 pages of data and insight. The DNI has also initiated a strategy for analytic outreach that seeks to harness "expertise, wherever it resides."

In April 2007, the newly appointed Director of National Intelligence, Admiral Mike McConnell, acknowledged this overall objective of global collaboration in his "100 Day Plan for Integration and Collaboration."<sup>14</sup> Many of the ideas central to the DNI effort go to the heart of creating a global intelligence paradigm.

- First, the plan aims at creating a culture of collaboration that can foster the diverse community of professionals needed to provide the best intelligence possible for decision makers.
- Second, it commits the IC to fostering transformation and removing obstacles to collaboration.
- Third, the IC must begin modernizing business practices to operate more effectively in a dynamic and interconnected global environment.
- And fourth, it sets out to accelerate information sharing to eliminate out-dated controls and streamline authorities to provide useful information to those that need it.

All these efforts will be necessary to fashion a more global intelligence network that will harness the combined insight and knowledge now available to the United States and its allies. If the DNI is able to put these broad goals into practice, we will indeed have the makings of a new intelligence paradigm for the 21st century.

[Top of page]

---

## Footnotes

1. See Director of National Intelligence, Report on the Progress of the Director of National Intelligence in Implementing the "Intelligence Reform and Terrorism Prevention Act of 2004," May 2006, 5–11. Available on line at [http://www.dni.gov/reports/CDA\\_14-25-2004\\_report.pdf](http://www.dni.gov/reports/CDA_14-25-2004_report.pdf).

2. The Intelligence Community Directive (ICD) 301, promulgated on 11 July 2006, establishes open source as an enabler and precursor to traditional intelligence disciplines. It attempts to build an infrastructure and capability to hold all open source in a single repository with the US Intelligence Community. This was mentioned in the DNI "Strategic Horizon: DNI Newsletter of the Office of Strategy, Plans and Policy," 1 August 2006, 2.

3. Thomas Friedman, *The World Is Flat: A Brief History of the Twenty-first Century* (New York: Farrar, Strauss and Giroux, 2005).

4. Moises Naim, *Illicit: How Smugglers, Traffickers, and Copycats Are Hijacking the Global Economy* (New York: Doubleday, 2005), 5.

5. Sherman Kent School, "Making Sense of Transnational Threats," *Occasional Papers*, vol. 3, No. 1, October 2004: 1–25. The principal authors were Gregory Treverton of the Rand Corporation and Warren Fishbein of the CIA's Global Futures Partnership.

6. Ernst Uhrlau, "A Post-Cold War Intelligence Service," *Transatlantic Internationale Politik*, vol. 4 (2000): 1–7. Uhrlau, then the German chancellor's coordinator of intelligence and currently the president of the German Foreign Intelligence Service (Bundesnachrichtendienst, BND), emphasizes that "in the future the BND will have to confront the dynamics of the dangers arising from today's transnational issues, besides carrying out its share of intelligence-gathering duties in Germany's international peacekeeping, peacemaking, or humanitarian missions." (7)

7. European Union, "A Secure Europe in a Better World," *European Security Strategy*, 12 December 2003, Brussels. It was approved by the European Council held in Brussels on 12 December 2003 and drafted under the responsibilities of EU High Representative Javier Solana. Available at: <http://www.consilium.eu.int/uedocs/cmsUpload/78367.pdf>

8. & German Marshall Fund, *Transatlantic Trends: Key Findings 2006* (Washington DC: German Marshall Fund, 2006), 7. Available at [wwwhttp://www.transatlantictrends.org/trends/doc/2006\\_TT\\_Key%20Findings%20FINAL.pdf](http://www.transatlantictrends.org/trends/doc/2006_TT_Key%20Findings%20FINAL.pdf).

9. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States, March 31, 2005*.

10. David Robson, "Innovation in Business – Culture and Practice," Remarks to the Global Futures Forum Conference on Strengthening Partnerships to Meet Security Challenges, 3–6 December 2006; forthcoming publication.

11. See Sherman Kent School, *Insights: Strategic Issues for Intelligence Practice in the 21st Century: Responding to Future Intelligence Consumers*, April 2005, Harvard Executive Seminar Series. This report capped a two-year study by the CIA's Global Futures Partnership, State Department INR, and the John F. Kennedy School. The report examined the changing global security environment, dramatic scientific and technical changes, and new intelligence collection and analysis needs and encouraged a rethinking of intelligence outreach, national and global collaboration, and organizational frameworks. More than 100 senior intelligence managers with a wide group of prominent academic specialists and consultants from business, academia, the sciences, and IT business and learning firms participated in the five-day event.

12. The preliminary set of topics selected included: Socio-economic disparities resulting in migration and humanitarian crises; competition for resources (especially energy and water); synergies between terror, crime and drug networks; pandemics (including Avian flu and HIV/AIDS); extremism and societal intolerance of minorities; roots of radicalization and extremism; WMD; and global environmental disruptions.

13. The Centre of Excellence for National Security (CENS) in Singapore has pioneered much of this work on "horizon scanning" and is sponsoring a series of symposiums in 2007 to examine how the technique might be applied to many of the transnational threats facing many nations. The UK Department of Trade and Industry has also been developing its own scanning approach that tries to identify emerging scientific and technical trends that would impact the global economy and the UK's economic prospects.

14. Office of the Director of National Intelligence, News Release, *DNI Announces 100 Day Plan for Integration and Collaboration*, April 11, 2007; a copy of the plan is available at [www.dni.gov](http://www.dni.gov).

[Top of page]

- Privacy
- Copyright
- Site Policies
- USA.gov
- FOIA
- DNI.gov
- NoFEAR Act