Preface

The Director of National Intelligence's Intelligence Science Board (ISB) was chartered in 2002 to provide "expert advice, unconventional thinking, and early notice of advances in science" (where "science" is defined to include "science, technology, research, engineering, business, organization, social sciences, the humanities, and other matters of interest"). From its origins as the Advanced Technology Panel, the ISB has grown steadily in both size and diversity of member expertise as the Intelligence Community adjusts to identify and confront the challenges of the 21st century.

Many of the Intelligence Community's strategic needs intersect, and many of the scientific community's interests and approaches inter-relate. Exploration of the commonalities across these topic areas may help identify more fundamental issues and more common solutions across disciplines, agencies, stovepipes, and intelligence missions.

Having now held some seventeen quarterly meetings, conducted twenty formal studies, hosted several targeted executive forums, and engaged in numerous informal discussions, the ISB has extracted and highlighted common themes (challenges or solution strategies) that it has addressed explicitly or implicitly in its various deliberations. This unclassified paper represents an attempt to identify and capture these common themes by looking across the National Intelligence Strategy (NIS) and the various ISB studies and initiatives, characterizing the intelligence and technology issues each has addressed and summarizing their recommendations.

This paper, as currently drafted, stems from the Board's deliberations to date and does not yet fully capture emerging science themes or the subject matter interests of its most recently added members. The Board plans to devote more discussion to current trends and additional topic areas during its quarterly meeting in March 2007.
Recurring Strategic Themes for the Intelligence Science Board

Many of the key challenges confronting the nation, the Director of National Intelligence (DNI), and the U.S. Intelligence Community (IC) will likely persist for years to come as our national security threat environment continues to evolve in a multi-polar world. In the National Intelligence Strategy of the United States (NIS), the DNI emphasizes “transformation through integration and innovation” and establishes the following Enterprise Objectives for the IC:

- Build an integrated intelligence capability to address threats to the homeland, consistent with U.S. laws and the protection of privacy and civil liberties.
- Strengthen analytic expertise, methods, and practices; tap expertise wherever it resides; and explore alternative analytic views.
- Rebalance, integrate, and optimize collection capabilities to meet current and future customer and analytic priorities.
- Attract, engage, and unify an innovative and results-focused IC workforce.

- Ensure that IC members and customers can access the intelligence they need when they need it.
- Establish new foreign intelligence relationships and strengthen existing ones to help the United States meet global security challenges.
- Create clear, uniform security practices and rules that allow IC agencies to work together, protect our nation’s secrets, and enable aggressive counterintelligence activities.
- Exploit path-breaking scientific and research advances that will enable the IC to maintain and extend intelligence advantages against emerging threats.
- Learn from both successes and mistakes to anticipate and prepare for new challenges.
- Eliminate redundancy and programs that add little or no value and redirect savings to existing and emerging national security priorities.

Recently the DDNI/A asked the ISB for help in improving the analytic process. In particular, the DDNI/A suggested topic areas where the ISB might provide its expertise, research capabilities, and access to external resources on how to:

- Make virtual teams more productive across the Community;
- Improve the process of analysis and enhance the analytic methodology;
- Effectively improve collaboration among diverse groups (analysts and scientists);
- Use analytic and communications tools better (within the IC and with its customers);
- Improve the overall process of S&T intelligence;
- More effectively convey findings by S&T analysts to non-scientific consumers;
- Effectively engage across the public-private divide and across international boundaries; and
- Apply industry best practices in risk management to the business of intelligence.

The ISB has addressed most of these topics at formal quarterly meetings, in
subsequent and ongoing discussions, and, in some cases, through in-depth studies and assessments. As a result, the ISB has recognized that many of the themes and issues intersect: solutions and strategies in one area depend on or can assist approaches in other areas. By exploring these and future topics from a variety of perspectives, embodied in an integrated heterogeneous board of specialists, the ISB is better able to advise the DNI and the IC on comprehensive strategies to address the complexities inherent in many of these challenge-issues. Recurring ISB themes include:

- Transforming Intelligence Analysis
- Leveraging Human Intelligence
- Intelligence Operations in Cyberspace
- Trusted Information Sharing
- Countering the Proliferation of Weapons of Mass Destruction
- Sustaining Our Science and Technology Advantage
- Managing Risk in Intelligence
- Leveraging the Private Sector
- Understanding Non-Western Thought.

Integrating across this set of themes or issues, the ISB notes the following trends:

- The relentless global spread of science and technology (S&T) and the increasing ability to corrupt S&T or use it against the United States or its interests worldwide;
- A significant decline in IC S&T pre-eminence and the concomitant ability of others to rapidly close the S&T strategic gap with the United States;
- A dramatic increase in the need for intelligence against a globally diversified target base and for support of an expanding set of complex customer missions;
- The re-emergence of interest in social and behavioral science research as it contributes to deeper understanding of some of the nation’s hardest targets;
- The rapid advancement of biological science and the ability to synthesize and deliver pathogens cheaply; and
- A continuing need to balance national security and civil liberties in the face of global terrorism and constrained budgets.

In light of these and related trends, the ISB encourages the DNI and the IC to mount a rigorous program to:

- Enhance the IC’s internal expertise in S&T to outpace our potential adversaries’ ability to exploit S&T;
- Establish a process of continuous learning and program enhancement to maintain internal S&T knowledge and practices at the state of the art;
- Leverage the knowledge, expertise, and access now prevalent in the private sector (domestic and global); and
- Share resources and knowledge across intelligence disciplines and domains to improve intelligence effectiveness and reduce cost.

In addressing these challenge-issues, the ISB deliberately pursues a longer and more ecumenical view that cuts across intelligence agencies and programs to identify viable strategic investment directions for the IC as a whole. The ISB welcomes opportunities to explore these topics further and to offer its assistance to the nation in these and other emerging areas.

This report briefly summarizes the challenges inherent in each of these themes and the ISB’s initiatives and recommendations. It also provides pointers to relevant
(typically classified) ISB publications, executive forums, or quarterly meetings where each issue was substantively discussed, and identifies cognizant ISB members for each study or topic area.

For its recommendations to remain useful to the IC, the Board must continue to be exposed to current and anticipated intelligence issues and programs. The lines of communication must remain open between the Board and Community scientists, analysts, operators, program managers, and executive leaders. The ISB must also continue to leverage its connections with the larger scientific community and the private sector, to integrate the diverse expertise represented by the Board members, and to more thoroughly understand the objectives and constraints of the IC.

**ISB Membership**


Robert M. Chesney, Esq. (associate)  
Rita R. Colwell, PhD  
Alan S. Counter, PhD  
Jack Downing (ret.)  
James J. Duderstadt, PhD  
Gerald M. Edelman, MD/PhD *(emeritus)*  
Robert A. Fein, PhD  
Randall M. Fort (ret.)  
John D. E. Gabrieli, PhD  
Michael Goldblatt, PhD  
Paul E. Gray, PhD  
J. Richard Hackman, PhD  
Margaret A. Hamburg, MD  
Philip B. Heymann, Esq.  
W. Daniel Hillis, PhD *(emeritus)*  
Timothy G. Hochst  
Stephen T. Kent, PhD  
Robert P. Liscouski  
N. John MacGaffin, III  
Ernest R. May, PhD  
C. Lawrence Meador  
Marshall Monroe  
Sally F. Moore, PhD  
Anthony G. Oettinger, PhD, Chair  
Ervin J. Rokke, PhD  
Alton D. Romig, Jr., PhD  
Harold Rosenbaum, PhD, Vice Chair  
John R. Schott, PhD  
Charles V. Shank, PhD (ret.)  
Charles W. Shanley, PhD  
Thomas E. Shenk, PhD (ret.)  
James M. Simon, Jr.  
George A. Spix *(emeritus)*  
Stephen L. Squires, PhD (ret.)  
Michael J. Sulick, PhD  
George M. Whitesides, PhD  
Joan B. Woodard, PhD (ret.)

**For Further Information**

For access to the referenced documentation or for contact information for ISB members, please contact Mr. Roy Pettis, ISB Executive Secretary, at 202.201.1079 or Dr. Lisa Allen, MITRE ISB Program Manager, at 703.983.7880.
Transforming Intelligence Analysis

NIS Enterprise Objective #2 is to strengthen analytic expertise, methods, and practices; tap expertise wherever it resides; and explore alternative analytic views. To achieve this objective, the Deputy Director of National Intelligence for Analysis will develop a plan to identify expertise inside and outside government, establish virtual teams of experts and interested analysts from across the Intelligence Community and U.S. government, improve cooperation between analysis and collection, improve analytic methods and practices, and ensure analytic integrity.

Enhancing the Effectiveness of Analytic Teams

In a recent study the ISB explored the conditions that, when in place, would allow the Community to enhance analytic team effectiveness while optimizing the value of intelligence for the consumer. The study examined 64 teams of analysts involving over 450 individuals from 6 different intelligence agencies and provided specific feedback to each analytic team lead.

Research has identified five conditions that increase the likelihood (but do not guarantee) that a work group will perform effectively:

1. The unit is a real team (bound, stable, with members interdependent);
2. It has compelling direction/purpose (challenging, clear, consequential);
3. Its structure facilitates team work (task design, team composition, and norms about behavior);
4. Its organizational context is supportive (rewards/recognition, information, education/consultation, and material resources); and
5. It has access to competent team coaching (available, expert, and focused on task processes).

The ISB’s research did not identify coaching by the designated leaders of analytic groups as being among the strongest influences on team effectiveness. This finding may reflect that those leaders were, in the main, so preoccupied with other duties that they did not actually perform much hands-on team coaching.

Because the primary determinants of team behavior and performance are how well the team is structured and supported, intelligence analytic leaders would be well advised to give first priority to setting their teams up correctly. Only then should they turn to coaching activities intended to help team members fully exploit the resources available to them.

Cognizant ISB Members
Dr. J. Richard Hackman, Study Chair

For more information, see:

ISB Meeting Minutes – June 2006 [S//NF]
ISB Meeting Minutes – October 2003 [S//NF]
ISB Meeting Minutes – September 2002 [S//NF]
Leveraging Human Intelligence

NIS Enterprise Objective #3 is to rebalance, integrate, and optimize collection capabilities to meet current and future customer and analytic priorities. In support of this objective, the IC will establish a national clandestine service to integrate all the elements of human source collection in accord with the highest traditions of professionalism and intellectual prowess. Therefore, the Deputy Director of National Intelligence for Collection will develop a comprehensive plan for achieving a new balance among our various collection methods – open source, human, and technical sources – while taking account of the differing legal and policy framework for collection with the United States.

Educing Information from Custodial Sources

The “art” of educing (drawing out) information from uncooperative sources has not changed substantially over the past 40 years. During this same period, however, considerable progress has been made in neuroscience, psychology, and behavioral science (including negotiation theory) that has potential applicability to information eduction. But much of this new knowledge has yet to find its way into the practice of interrogation or other forms of intelligence gathering from human sources. The United States must fundamentally rethink its national approaches to educing information (EI). This includes identifying different techniques for different purposes (intelligence, law enforcement, source validation), devising more reliable methods, and developing a systematic approach to applying such methods for information collection.

The ISB recommends that the DNI establish a centralized IC capability for EI. This capability should rest upon U.S. traditions, values, history, laws, scientific discoveries, successful experience, and research. It should draw upon a cadre of experts with backgrounds in intelligence, military, and law enforcement organizations, and serve as a “center of excellence” for EI operations, teaching/training, and research.

Cognizant ISB Members:
Dr. Robert A. Fein, Study Chair

For more information, see:
ISB Book – Educing Information, JMIC Press, January 2007 [U]
ISB Report – Educing Information, December 2006 [U//FOUO]
ISB Meeting Minutes – September 2004 [TS//SI//NF]
Detecting Unexploited Signatures and Emissions

Emission detection has typically focused almost entirely on the electromagnetic spectrum. Scientific and technological advances now allow contemplation of a broadly expanded definition of detection to include not only the electromagnetic spectrum but also the exploitation of other phenomenology such as acoustic emissions, odors, environmental changes, DNA shedding, and others.

At the behest of the Under Secretary of Defense (Acquisition, Technology and Logistics), the Under Secretary of Defense (Intelligence), and the Associate Director of National Intelligence for Science and Technology the ISB is embarking on a joint study with the Defense Science Board (DSB) of both passive and active non-conventional emissions and signatures.

In evaluating the exploitation of the different phenomenology, the Task Force will assess what level of information such detections provide. Will the information merely provide indication of presence, or can it provide higher levels of information such as location, identification, or even intention?

The Joint Task Force will also assess the systems engineering required to integrate across the entire spectrum of possible phenomenology to be exploited and address the required platforms, sensors, communications requirements, collection techniques and analytical tools when assessing the utility of exploited emissions. In addition, the needs of the entire range of users, from tactical, strategic and autonomous and/or human aided, will be considered as a part of any new exploitation techniques.

Since significant investments have been made in legacy systems, the Task Force will assess the possibility of exploiting new phenomenology with current assets which enhance sensor capabilities. In addition, an evaluation will be made as to whether legacy systems should be incorporated in any new systems or maintained as a stand alone capability. Finally the Task Force will assess whether the new capabilities will allow old systems to atrophy as new systems reach operational capability.

The Task Force will also examine techniques to protect any capabilities the United States develops in new areas and to minimize the effects of disclosure.

Cognizant ISB Members
Dr. George M. Whitesides, Co-Chair

Cognizant DSB Members
Dr. Matthew Ganz, Co-Chair

For more information, see:
ISB-DSB Joint Study Terms of Reference – January 2007
Exploiting Open Source Information

TBD – Do we intend to do anything more with this topic area?

Cognizant ISB Members
Dr. Harold Rosenbaum

For more information, see:
ISB Meeting Minutes – June 2006 [S//NF]
Intelligence Operations in Cyberspace

NIS Enterprise Objective #7 is to create clear, uniform security practices and rules that allow us to work together, protect our nation's secrets, and enable aggressive counterintelligence activities. The IC must dramatically change the basis of its security and counterintelligence policies in order to remain effective. Toward this end, the Deputy Director of National Intelligence for Management will develop a plan for changing physical, information, and personnel security policies impeding the IC's ability to achieve its mission and enterprise objectives.

Impact of Globalization on Foreign Information Operations

Recent trends in the globalization of information technology development and production, coupled with the growing global dispersion of knowledge and skills in information operations among both state and non-state actors, substantially increase the risk of an effective information attack against our national security and our critical infrastructure. While use of information technology pervades U.S. society, effective responses to the resulting vulnerability to information attack, disruption of operations, information espionage, or identity theft remain less widely understood. The need for a coherent national strategy that clearly defines responsibilities across the public and private sectors grows more apparent every day, yet multiple authorities, separate control systems, and contradictory policies and practices contribute to our continuing vulnerability.

The ISB recommends that the IC formulate a more coherent and comprehensive Community-wide approach to confronting the challenges of information operations as they continue to be exacerbated by relentless globalization. Such a strategic approach would include:

- Encouraging the installation of sound security business practices,
- Taking other specific preventive measures and engage the private sector,
- Finding and fooling adversaries in their information operations pursuits,
- Developing effective contingency plans for when information operations attacks succeed, and
- Developing a risk assessment approach to information security.

Cognizant ISB Members:

Dr. Charles W. Shanley, Study Chair
Dr. Stephen T. Kent
Mr. Robert P. Liscouski
Mr. C. Lawrence Meador
Dr. Harold Rosenbaum
Mr. James M. Simon
Mr. George Spix
Dr. Stephen L. Squires

For more information, see:

ISB Meeting Minutes – December 2006 [U//FOUO]
ISB Meeting Minutes – September 2004 [TS//SI//NF]
ISB Meeting Minutes – June 2004 [TS//SI/TK//NF]
ISB Meeting Minutes – December 2003 [TS//SI/G//ORCON//NF]
ISB Meeting Minutes – June 2003 [TS//SI/TK//NF]
Trusted Information Sharing

NIS Enterprise Objective #5 is to ensure that IC members and customers can access the intelligence they need when they need it. Toward this end, the Deputy Director of National Intelligence for Requirements will oversee the development of plans to provide maximum access to intelligence information among IC customers, consistent with applicable laws and the protection of civil liberties and privacy.

Trusted Information Sharing

Throughout its history much of the intelligence business has focused on controlling the dissemination of information (e.g., to avoid revealing U.S. strategies and tactics or to avoid disclosing — and thereby risk losing — sources and methods of future intelligence information). The press, multiple commission reports, and Executive Orders and legislation have often expressed the need to improve collaboration and the sharing of information across the IC and between the IC and its customers in Defense, Homeland Security, law enforcement, diplomacy, and other federal, state, local, and tribal organizations.

Multiple initiatives are underway to improve information integration and information sharing while preserving the security of sensitive information and the privacy of U.S. persons. Yet there remains a lack of fundamental understanding of the basic principles of information sharing and the barriers to such sharing across technical, legal, organizational, personal, and cultural domains.

The ISB recommends that the DNI join with the Secretary of Homeland Security, the Director of the Federal Bureau of Investigation, the Secretary of Defense, and other interested parties to establish an “institute” for the study of trusted information sharing. Such an institute would provide longer-term exploration of the broad field of trusted information sharing from a variety of interrelated perspectives (technical, social, organizational, political, public, and private). This will lead to the definition of fundamental information sharing principles, the establishment of rules and best practices governing trusted information sharing, and the identification of research and experimentation programs focused on ensuring that any and all information that can support our national security mission is readily and securely available to those who need it.

Cognizant ISB Members:
Mr. Timothy G. Hoechst, Study Chair
Mr. Robert P. Liscouski

For more information, see:
ISB Meeting Minutes – December 2005 [S//TK//NF]
ISB Meeting Minutes – March 2005 [S//NF]
ISB Concept Paper – Trusted Information Sharing, November 2004 [U]
ISB Meeting Minutes – September 2004 [TS//SI//NF]
ISB Meeting Minutes – March 2004 [S//NF]
Balancing Privacy, Security, and Technology

The U.S. Constitution and legal statutes staunchly protect our citizens' rights against unreasonable intrusion by their government. Adversaries have learned how to use this protection to their own advantage: they hide their activities "in plain sight" by using U.S. communication systems where our foreign intelligence capabilities are directed "not to look." Recent attempts to close this gap have encountered considerable public indignation.

In the modern age of rapid and multi-modal telecommunications, the hand-off from foreign intelligence to domestic law enforcement must occur at electronic speeds. Upgrades to the transition process are needed to enable "hot pursuit" of agile targets operating throughout the global communications network.

A national dialogue is needed to reach an understanding about ways to balance our citizens' right to privacy with their need to be protected from threats to their safety, well-being, and way of life. To further this national dialogue, the ISB recommends that the IC conduct specific experiments targeted at elucidating and evaluating the expected intelligence value of various mechanisms and the role technology can play in pursuing targets of interest and protecting civil liberties.

Cognizant ISB Members:
Mr. Philip B. Heymann, Esq.
Dr. Anthony G. Oettinger
Dr. Harold Rosenbaum

For more information, see:
ISB Letter to DGC/ODNI – February 2006 [TS/SL/NF]
ISB Letter to DDCI/CM – December 2004 [S/NF]
ISB Meeting Minutes – September 2004 [TS/SL/NF]
ISB Meeting Minutes – December 2002 [TS/NF]
ISB Meeting Minutes – September 2002 [S/NF]
Countering the Proliferation of Weapons of Mass Destruction

NIS Mission Objective #2 is to prevent and counter the spread of weapons of mass destruction. As the WMD Commission stated in its March 2005 report, there is no single strategy the IC can pursue to counter the proliferation menace. Rather each destructive capability – biological, nuclear, chemical, radiological, or otherwise – will require unique and focused approaches to combating their use. Therefore, the Director of the National Counter-Proliferation Center will develop a comprehensive national intelligence plan for supporting the nation’s efforts to prevent and counter the development and proliferation of weapons of mass destruction.

Biosecurity Intelligence

The United States is unprepared for a substantial attack involving biological agents. For example, our public health care system lacks surge capacity and stockpiles of antidotes and vaccines are inadequate to respond to biological threats.

Multiple initiatives are underway to develop and deploy proximal biological agent sensors to alert authorities once an agent has been released. However, the nation has not invested sufficiently in developing the tools, techniques, sources, and methods for determining, in advance of release, the production of and intent to disperse biological agents against the United States or its allies and interests around the globe.

Much of the expertise in biological science resides in the private sector: in universities, pharmaceutical companies, and biotechnology research and development firms. The IC needs to develop meaningful approaches for properly leveraging this external expertise while enhancing its own internal expertise to interact credibly with external scientists.

The ISB recommends that the IC elevate the effective priority of biosecurity intelligence collection and analysis and remove biosecurity intelligence from under the umbrella of weapons of mass destruction, where it will always be overshadowed by the nuclear threat. Further, the IC should establish better relationships with the private sector, including creating an intelligence business board to engage the biotechnology industry and anticipating future attacks to avert over-reaction.

To accomplish this, the IC will need to substantially increase the level of funding for biosecurity research and development and threat analysis to project 5-10 years into the future to anticipate the role of synthetic biology in creating novel threats.

Cognizant ISB Members:
Dr. Rita R. Colwell
Dr. Michael Goldblatt
Dr. Margaret A. Hamburg
Dr. George M. Whitesides

For more information, see:
ISB Letter to DNI – in process 2007
ISB Meeting Minutes – June 2006 [S//NF]
ISB Forum – "Biological Threats, Intelligence, and Relationships," October 2005 [U]
ISB Letter to DNI – July 2005 [S//NF]
ISB Meeting Minutes – March 2005 [S//NF]
ISB Meeting Minutes – September 2002 [S//NF]
Counter-Proliferation of Fissile Materials

The proliferation of knowledge about nuclear technology cannot be stemmed. Information on how to build a nuclear or radiological explosive device is freely available on the Internet. Educated and skillful nuclear engineers abound worldwide and can help developing nations pursue the economic advantages of nuclear energy.

At present, the most controllable aspect of nuclear proliferation seems to be the actual acquisition of sufficient fissile material to constitute a nuclear device. The United States needs persistent and effective mechanisms to identify, monitor, track, and warn about fissile material transfer from existing sources to potentially threatening actors.

For more information, see:
ISB Meeting Minutes – December 2005 [S/TK//NF]
Sustaining Our Science and Technology Advantage

NIS Enterprise Objective #8 is to exploit path-breaking scientific and research advances that will enable the IC to maintain and extend intelligence advantages against emerging threats, and Enterprise Objective #4 is to attract, engage, and unify an innovative and results-focused IC workforce. To this end, the IC must deepen technical expertise and strengthen advanced research and development programs within the agencies while providing opportunities for professional growth and leadership development. The Associate Director of National Intelligence for Science and Technology will develop a plan for leading the IC’s S&T resources and activities.

Managing Science and Technology Programs and Talent in the IC

The U.S. intelligence advantage depends strongly on scientific innovation and the deployment of technology. Understanding the need for, and the implications of, prudent and sustained investment in S&T is critical to making informed budget and program decisions.

The advancement and application of S&T require substantial and continuing education, as well as persistent experimentation and patience – as does the analysis of foreign S&T capabilities. Recruiting, developing, and retaining a highly talented S&T workforce in the IC are fundamental to sustaining our intelligence advantage in a world where scientific knowledge and access to technology are globally available to our nation’s current and potential adversaries.

The ISB recommends that the IC give its S&T analysts more direct reporting responsibility that empowers a fundamental understanding of the subjects for which they are responsible. The Board also recommends that the IC modulate its personnel and hiring practices to encourage prudent risk taking and to provide meaningful employment for new hires pending the completion of their clearance process.

In addition, the ISB encourages the DNI to proceed with plans for establishing an intelligence-Advanced Research Projects Agency (iARPA), but to do so only in a manner that produces an integrated, well-funded, and innovative organization capable of succeeding.

Cognizant ISB Members:
Dr. Harold Rosenbaum, Study Chair
Dr. J. Richard Hackman
Mr. N. John MacGaffin
Mr. C. Lawrence Meador
Dr. Ervin J. Rokke

For more information, see:
ISB Report – The Challenge of the New S&T Landscape, November 2006 [FOUO]
ISB Meeting Minutes – September 2006 [TS/SI/TK/NF]
ISB Meeting Minutes – June 2006 [S//NF]
ISB Meeting Minutes – December 2005 [S//TK//NF]
ISB Whitepaper – “Big Ideas for Intelligence R&D,” October 2005
ISB Meeting Minutes – September 2005 [TS/SI/TK-RSEI//IOC/NF]
ISB Meeting Minutes – March 2005 [S//NF]
ISB Meeting Minutes – September 2004 [TS/SI//NF]
ISB Meeting Minutes – June 2004 [TS/SI/TK//NF]
ISB Report – The State of Science and Technology Analysis in the Intelligence Community, April 2004 [S//NF]
ISB Meeting Minutes – March 2003 [TS/SI/TK//NF]
ISB Meeting Minutes – December 2002 [TS/SI/TK//NF]
Managing Risk in Intelligence

In the NIS the Director of National Intelligence openly encourages prudent risk taking across the IC. Highlighted in the NIS description of the mission of national intelligence is the need to transform our capabilities in order to stay ahead of evolving threats to the United States, exploiting risk while recognizing the impossibility of eliminating it.

Risk Management for Intelligence

Over the years, the U.S. IC has grown increasingly risk averse. Recent highly publicized world events have been labeled “intelligence failures,” leading to further reluctance among intelligence personnel to take risks outside the norm of pre-published guidance. Yet the business of intelligence is the pursuit of the unknown, and such pursuit must entail taking risks – certainly prudent risks – not only in the collection of intelligence but also in the choice of what intelligence to pursue.

Lack of a fungible bottom-line measure (such as revenue stream or profitability) complicates the challenge of assessing risk and comparing alternatives. Choosing a viable alternative can yield benefits essential to our national security.

At the request of the Deputy Director of National Intelligence for Analysis and the Assistant Secretary of State for Intelligence and Research, the ISB will explore how risk management-based decision processes may assist senior management in planning and conducting the business of intelligence. The ISB will examine risk management models and define prototype tools and processes that can assist the IC in managing this new environment.

There are many categories of risk to consider in making intelligence-based decisions and prioritizations, including: international relations and policy implications, protection of our national security and that of our allies, preservation of intelligence sources and methods, protection of intelligence assets, preservation of our citizens’ civil liberties, the inadequacy of available information to support decision-making, possible errors in analytic judgment, and the potential for misinterpretations of intelligence reports. In today’s highly dynamic world, the demand for timely and accurate intelligence stresses our intelligence system, and the IC cannot always afford the luxury of time while it gathers more information, performs an alternative analysis, or rewrites its intelligence product.

In addition, there are also risks associated with leadership decisions to implement management programs to transform the business of intelligence as well as lost opportunity costs associated with failure to act. The IC lacks many tools and processes that can effectively map into traditional risk management models as these threats and risks may not lend themselves to the traditional business methods of quantification, actuarial analysis and predictive modeling.

Cognizant ISB Members:
Mr. Robert P. Liscouski, Study Chair
Dr. Harold Rosenbaum

For more information, see:
ISB Study Terms of Reference – February 2007
ISB Meeting Minutes – March 2006 [U/FOUO]
Leveraging the Private Sector

NIS Mission Objective #2 is to prevent and counter the spread of weapons of mass destruction while NIS Enterprise Objective #2 is to strengthen analytic expertise, methods, and practices, tap expertise wherever it resides; and explore alternative analytic views. In pursuit of these objectives, the IC is encouraged to reach outside the IC for relevant information and expertise to inform judgments and to bolster areas where knowledge is lacking in the IC.

Public-Private Relationships for Intelligence

As world circumstances continue to change, the information needed by intelligence customers and the knowledge needed to produce intelligence also evolve. In areas involving new technology and its application, such as Internet usage and protection, telecommunications, or public health, the relevant operational data resides primarily within the private sector.

The U.S. IC can no longer afford to uniquely collect, process, and exploit all the information it needs to produce cogent intelligence reporting. The IC needs new ways to engage the private sector that will allow government to make effective use of existing information and to properly interpret its meaning – without jeopardizing the private sector's economic viability or the public's trust.

With today's trends toward globalization, more and more U.S. firms are gaining unprecedented access to foreign populations. New opportunities are growing for greater collaboration between the public and private sectors for the collection and interpretation of information of potential intelligence value.

Cognizant ISB Members:
Dr. Anthony G. Oettinger
Mr. Robert P. Liscouski
Dr. Michael J. Sulick

For more information, see:
ISB Meeting Minutes – December 2005 [S//TK//NF]
ISB Meeting Minutes – June 2005 [S//NF]
ISB Executive Forum – “Self-Organizing Information Networks,” August 2002 [U]
ISB Meeting Minutes – September 2002 [S//NF]
Understanding Non-Western Thought

NIS Mission Objective #5 is to anticipate developments of strategic concern and identify opportunities as well as vulnerabilities for decision-makers. To support policymakers, the IC should promote deeper cultural understanding, better language proficiency, and scientific and technological knowledge among personnel at all levels. The Deputy Director of National Intelligence for Analysis will develop a plan to improve the language skills, scientific and technological skills, and cultural insight of analysts.

Behavioral and Social Science and Cultural Anthropology

TBD – What do we intend to do with this topic?

Cognizant ISB Members

Dr. Sally Falk Moore
Dr. Robert A. Fein
Dr. J. Richard Hackman
Mr. Philip B. Heymann, Esq.
Dr. Ervin J. Rokke

For more information, see:

ISB Seminar Series – “Understanding Non-Western Thought,” planning in process 2007 [U]
ISB Meeting Minutes – June 2006 [S//NF]
Communications Excellence

Communication is a topic as old as recorded history; in fact, recorded history is a form of communication. Communication not only empowers the accumulation of knowledge, but it enables the process of sharing, disseminating, and collectively acting upon that knowledge. The topic is core to shared understanding, belief systems, social orders, coordinated action, team and organizational performance, learning, power structures, personal realization, insurrection, war-fighting, and in social species, communication is core to survival itself.

In the modern age, we have technologies and modalities that are changing communication. We are living in the information age, and while much has been written and projected regarding the implications of these technologies, we continue to be surprised by new application developments. Not only are the new forms of communication changing how messages are transmitted, but they are changing the very nature of the messages, and the filtering of which messages become transmitted.

Recent initiatives by Islamic terrorist groups to capitalize upon modern Internet technology for conveying video-based propaganda to sway public opinion and to recruit new insurgents show the power and agility of social network video communications in the modern age.

In the intelligence sector, communication has many levels of application, ranging from the acquisition/collection of information, to the articulation of the nature of national security threats, to the cross-correlation of intelligence, to the dissemination and application of findings and recommendations, to the conduct of information operations. Yet, despite the pervasive significance of communication to the intelligence sector, research and synthesis within the topic has not kept pace with the emerging and accelerating evolution of the phenomenology.

The ISB will explore the hard and soft sciences of communication as they relate to the role and value proposition of contemporary intelligence practice. By gathering and integrating empirical knowledge from a range of fields (public and private), this study will establish a clear delineation between two primary aspects of communication: “deciding what to say” and “saying it well and with insight into the audience.”

For more information, see:

ISB Meeting Minutes – planned for March 2007
Processing Human Language

TBD – Do we intend to pursue this topic?

Cognizant ISB Members

Mr. James M. Simon

For more information, see:
ISB Meeting Minutes – June 2006 [S//NF]
Other ISB Studies and Initiatives

Countering Denial and Deception
Mr. Randall M. Fort

Hyperspectral Intelligence
Mr. C. Lawrence Meador

Integrated Space-Air Architectures
Dr. Harold Rosenbaum

Quantum Cryptography Research Assessment
Dr. Charles V. Shank

Radar Applications for Intelligence
Dr. Paul E. Gray

TBD – These studies are each more highly classified. Do we want to discuss them in this FOUO document?

For more information, see:

ISB Report – Countering Denial and Deception, December 2005 [TS//SI//TK// NF/ORCON]