TRANSFORMING INTELLIGENCE THROUGH NEW INSTITUTIONAL ARRANGEMENTS

Dennis M. Gormley
University of Pittsburgh
2007

About the Matthew B. Ridgway Center

The Matthew B. Ridgway Center for International Security Studies at the University of Pittsburgh is dedicated to producing original and impartial analysis that informs policymakers who must confront diverse challenges to international and human security. Center programs address a range of security concerns—from the spread of terrorism and technologies of mass destruction to genocide, failed states, and the abuse of human rights in repressive regimes.

The Ridgway Center is affiliated with the Graduate School of Public and International Affairs (GSPIA) and the University Center for International Studies (UCIS), both at the University of Pittsburgh.

This working paper is a product of the Ridgway Center's working group on "Internal Security and the Rule of Law," co-chaired by Janne E. Nolan.

This paper and the working group that produced it were made possible by a generous grant from the Ford Foundation to the Ridgway Center on The Determinants of Security Policy in the 21st Century, Grant # 1050-1036.

Repeated failures on the part of American intelligence services and policy-making officials have brought into focus an array of new challenges facing the 21st century intelligence and policy-making communities. While substantial efforts are underway to reform the U.S. intelligence community to address new transnational non-state threats, the very nature of new globally networked threats demands that U.S. intelligence reforms incorporate much more novel ways of improving coordination and collaboration not only within the United States but equally among foreign intelligence and security organizations, multilateral institutions, academia, and non-governmental organizations. This paper focuses on the key challenges to improving the means of intelligence collection, analysis, and collaboration—including in the broadest global sense—in light of the new demands presented by apocalyptic terrorism.[1]

Fixing intelligence to improve its prospects of furnishing useful information to policy officials will not be accomplished through the types of reforms being implemented at present in the United States. While the creation of a Director of National Intelligence (DNI) with full budgetary authority might well increase collaboration throughout the intelligence community, it will not deal with the more prosaic but far more critical matter of intelligence effectiveness. This depends on the quality of collected information, on the nature of the analytic process, and ultimately, on the relationship between intelligence and policy-making officials.

While a host of individual, institutional, and political factors can bias analysis and threat perceptions, low-quality intelligence is more susceptible to political and analytical manipulation than high-quality intelligence. Revitalization of human and technical intelligence and improved liaison relationships between intelligence organizations of friends and allies are essential requirements in confronting non-state violence. Nevertheless, the challenge of penetrating organizations like al-Qaeda should not be underestimated, nor should the peculiar demands of

maintaining quality control of source information. More and better human intelligence collectors with appropriate skills, languages, and cultural sensitivities are necessary but not sufficient to enhance the quality of collected information. Truly agile human intelligence also requires more sophisticated methods of gathering information, particularly via human-emplaced sensors. Equally important, America's huge investment in overhead imagery sensors must dispense with its fixation on ever increasing improvements in resolution and move increasingly toward systems that are less predictable and more persistent in their orbital paths and much more capable of monitoring patterns of activity, or "movement intelligence."

The chief analytic shortcoming that invites both performance errors and political manipulation of intelligence is the decidedly unscientific nature of the intelligence community's approach to analysis. Intelligence analysis for the world of transnational non-state threats needs to be very different from the traditional approach. It has to recognize complexity and variability of outcomes by using multiple alternative competing hypotheses, while making greater use of efforts to probe and manipulate transnational actors in order to achieve a greater understanding of their structure and behavior. Moreover, it must adjust analytic priorities, now heavily biased toward producing current intelligence, to a more balanced mix of both current and strategic research products.

Organizationally, the creation of the DNI mirrors American corporate culture of the mid-1950s (General Motors comes to mind), in which additional layers of management and attendant staffs have been added, along with corresponding increases in decision and coordination nodes. Ironically, strengthening the hierarchical center comes long after American corporate culture has dramatically adapted to the introduction of information technology that has enabled a flattening of corporate headquarters and an expansion of far-flung and highly decentralized component

elements. One notion now under exploration within the U.S. intelligence community is the cultivation of a transnational intelligence community to provide more comprehensive coverage and more sophisticated analysis. Such a truly global endeavor would involve the creation of a dynamic ad hoc network that shifts from issue to issue and that includes trusted (but uncleared) individuals, including those from NGOs, universities, and think tanks. Instead of relying primarily on classified intelligence, the endeavor would develop communities of interest engaged in transnational, non-secret but controlled collaboration aimed at detecting anomalous patterns of activity based on information derived from the public domain.

Transforming the Collection Paradigm

So much depends on improving public, governmental, and international confidence in the performance of the U.S. intelligence community. Not least is the very credibility of U.S. diplomacy in building future coalitions to address mutual interests. The consequences of suffering another major terrorist attack on U.S. soil—particularly one involving nuclear or biological weapons—are incalculable.[2] Today's privacy and economic concerns about the most pernicious law enforcement and intelligence applications—including intrusive database mining and monitoring, ubiquitous surveillance schemes, and tightened border security—will disappear in the aftermath of another mass casualty attack on an American target.

There is no reason to believe that the most toxic forms of transnational terrorism, nor the means that permit their effectiveness, will fade over time. No longer dependent on state sponsorship in Afghanistan and emboldened by Iraq's insurgency, al Qaeda, for example, has achieved a form of virtual statehood, creating operational cells around the globe. Linked in network form through the exploitation of Western information technology, cells come and go,

moving and morphing so rapidly as to render detection of their activities by hierarchically bound Western intelligence organizations problematic. Western technology not only affords such anti-Western radicals the means to become nimble and malleable, but also the capacity to achieve increasingly catastrophic forms of attack, from remotely controlled means of delivery to frightening forms of biological weapons.[3] The very same explosion of knowledge and technology that enables a more comfortable existence and longer lives in the developed world could conceivably be exploited to achieve immense harm. While the stakes are abundantly clear, far less evident is the prospect that traditional intelligence collection methods, which performed so poorly prior in preventing 9/11's terrorist attacks and in assessing Iraq's weapons of mass destruction (WMD) in advance of the U.S. invasion in March 2003, are up to the task to monitoring these new security threats. Clearly, improving the quality of collected intelligence demands new thinking, including consideration of new institutional arrangements with global reach.

Particularly in the aftermath of 9/11's terrorist attacks, most attention has focused on the need for better human intelligence, the prominent domain of the CIA's Directorate of Operations (DO). Pride in gathering secrets dominates CIA culture; thus, it is not surprising that the DO is roughly three times the size of the CIA's Directorate of Intelligence, where analysis of collected intelligence occurs. Yet, the DO reportedly failed to recruit even one significant Soviet spy and instead relied on walk-ins during the Cold War.[4] The DO has also developed a penchant for quantity over quality; new recruits and raw information, no matter the quality, became the measure of effectiveness for DO performance. In studies conducted in support of the Congressionally mandated Aspin-Brown Commission, more formerly known as the Commission on Roles and Capabilities of the U.S. Intelligence Community (1996), it was found that 80 to 90

percent of the information collected by the CIA's clandestine service came from open sources.[5] This is not to denigrate the importance of open source information. Rather, the point is to question using such an expensive means of collecting it simply because performance is measured by volume instead of virtue. The challenge now, of course, is penetrating the inner sanctum of terrorist organizations like al-Qaeda, the achievement of which dictates recruiting new personnel with appropriate language skills, and developing new tradecraft to fully exploit emerging opportunities afforded by the emplacement of smaller and smaller sensor technology. None of these new demands will be readily implemented; they are likely to materialize over perhaps a decade of so.

In the meantime, and notably since 9/11, quite narrow arrangements have been instituted with the intelligence services of U.S. friends and allies to enhance liaison services, establish prisons on foreign soil, and coordinate renditions of suspected terrorists, the sum of which, notably in the case of prisons and renditions, appears to have created more problems than solutions in the so-called global war on terror. A much more fundamental transformation of the CIA's clandestine service will be needed to cope with the challenges presented by, *inter alia*, networked transnational terrorist threats, rogue states bent on acquiring nuclear and biological weapons, and the uncertain pace of China's emergence as a regional and international economic and military power—challenges vastly different and more complex than those presented by the Soviet Union. Indeed, the CIA would do well to heed the recommendations of the 1996 Aspin-Brown Commission, which argued that new post-cold war threats demanded a narrowing of the clandestine service's mission to a focus on "hard" targets (terrorist cells, rogue states, etc.) instead of broad DO representation around the globe, working primarily out of U.S. embassies.[6]

Critical to such a new focus are decisions about how the DO should operate. There have been recent calls for DO case officers to rely less on 'official cover,' under the guise of diplomatic service, and more on 'deep cover,' literally requiring the officer to blend into the local environment. Clearly, deep cover would dictate increased risks, costs, and time to achieve positive results. And many areas, the Arab world included, represent problematic penetration challenges without an extraordinary sensitivity to local circumstances. But facing the kind of opaque transnational threats that dominate today's security environment, we may have little choice but to accept fundamental changes in the way human intelligence is collected.

Truly agile human intelligence collection will not occur until there is a suitable marriage between more spies and improved ways of collecting information. Prospects for making such a marriage a reality are improving as rapid progress is achieved in manufacturing very small sensors—or tiny wireless microelectromechanical sensors (MEMS) as small as 1 cubic millimeter in size. One could readily imagine scattering hundreds of "smart dust" sensors around sensitive facilities to monitor signatures that suggest or verify not only specific activities but also fluctuations in those activities. Because of breakthroughs in silicon and fabrication techniques, the prospect exists for units the size of a grain of sand containing sensors, circuitry, bidirectional wireless communications, and a power supply. Spread around a large area, these devices could gather, compute and communicate by means of two-way band radio between individual devices each separated by as much as 300 meters.[7] Applications for products born of the current revolution in nanotechnology are virtually limitless. The major challenge will be breaking through the cultural disinclination of case officers to be seen as too heavily dependent on technology, or merely a means to a technical collection end.[8]

Overhead collection systems, which consume nearly 20 percent of the U.S. intelligence community's annual budget of over $40 billion, are generally viewed today as irrelevant to the challenges of finding and destroying terrorist groups.[9] Such a belief has merit with regard to the current generation of overhead imaging systems, which operate in fixed and readily predictable orbits that make them highly vulnerable to simple concealment and deception measures.[10] Moreover, today's satellites, few in number, capture only infrequent images of activity each day. If overhead imaging systems are to become relevant to the terrorist challenge, no less to monitoring WMD proliferation, a fundamental overhaul of America's approach to developing and procuring such imaging satellites is essential.

Fixing this critical limitation is improbable without a fundamental shake-up of the business-as-usual managerial style within the US intelligence community. Even the senior leadership of the once super-secret National Reconnaissance Office (NRO), which is responsible for building and operating overhead reconnaissance systems, has admitted that it is no longer the agile, innovative organization it once was. That said, there are positive signs that the NRO may move away from its traditional dependence on a few large, enormously expensive satellites to slightly less sophisticated but larger constellations of smaller satellites.[11] Indeed, today's cold-war-era overhead reconnaissance satellites will be are replaced are by a larger number of smaller imagery satellites. However, the program, called the Future Imagery Architecture (FIA), which was initiated in 1999, has experienced cost overruns of several billion dollars and schedule delays.

Assuming cost and schedule challenges are met, FIA points the nation generally in the right direction. A larger but smaller sized architecture of overhead reconnaissance satellites would in fact increase the amount of area and point imaging of targets, permit more rapid

revisiting of key targets, and increase changes that the most difficult targets (ones that move or are deeply buried) can be monitored. Even more so would a new Space-Based Radar (SBR) architecture, which the Pentagon envisions deploying sometime in the next decade.

Featuring 20 satellites in low-earth orbit, each capable of collecting either ground moving target indicator (GMTI) imagery or synthetic aperture radar (SAR) returns, SBR would provide regional commanders and national intelligence users with near-continuous global coverage against both stationary and moving targets. Most important of all, SBR would change the imagery paradigm from infrequent to virtually continuous coverage, regardless of weather, and not just against fixed targets but targets that move frequently. Such movement intelligence, or "moveint," would exploit the fact that entities, including small terrorist cells, must transit between geographical locations, leaving behind in the process artifacts of passage that can be collected. Rather than a traditional imagery centric approach to collection, SBR's collection of moveint would be based on detection of motion and change with an a priori precise knowledge of the terrain and the normal behavior of targets on that terrain.[12]

But what makes SBR potentially even more revolutionary beyond its inherent technical features is the prospect that the constellation could become a truly multilateral collection system through international participation. Because a larger constellation of satellites decreases the time of arrival of the next available satellite over any particular targeted area, there is a built-in incentive to seek other government participation in the program. While security reasons would likely force the U.S. to remain the exclusive system integrator, other government participation would nonetheless create opportunities to share moveint products in collaboration with participating states' intelligence organizations.[13] Working together on moveint products could

also conceivably create broader opportunities to share and analyze intelligence within other multilateral contexts.

Despite an increase in the revisit time of larger space constellations like SBR, orbital predictability would still remain a problem. Existing, and no doubt future, satellites could use on-board fuel to adjust their orbit or reduce their speed temporarily, which would inject some unpredictability into their operation. However, these satellites have a finite amount of fuel just to maintain their everyday orbits, no less ones that require even more fuel to reduce their susceptibility to cover, concealment or deception. But even greater agility would arise were the NRO to adopt a wholly new conceptual approach to future space-based reconnaissance. One such approach underway at the Pentagon's Defense Advanced Research Projects Agency (DARPA), called *Orbital Express*, is examining the feasibility of on-orbit refueling of satellites.[14] Using robotic technology, the Orbital Express programme intends to test a servicing satellite that would deliver fuel and electronic upgrade packages to on-orbit satellites. Besides extending the lifetime of satellites in orbit, refueling would permit frequent orbital maneuvers and changes in satellite arrival times over targets. Such adjustments would counter adversary cover, concealment and deception measures as well as greatly increase coverage of unsuspecting targets on the ground. On-orbit transfers of electronics would dramatically reduce the amount of time to deploy product improvements of imaging system capability. DARPA intends to work closely with the National Aeronautics and Space Administration (NASA) to enable the application of these developments to servicing the International Space Station. A similar strategy should be initiated between DARPA and the NRO.

A New Analytic Paradigm

The poor performance of American intelligence services prior to 9/11 and leading up to the invasion of Iraq brought into sharp relief palpable deficiencies in intelligence analysis. These shortcomings are nothing new. Recognizing that the end of the Cold presented new challenges for intelligence collection and analysis, several government and nongovernmental groups undertook detailed investigations of the intelligence process during the 1990s and suggested changes in practices and procedures to improve intelligence performance.[15] Remarkably, and sadly, despite these many post-mortem critiques, little if any significant progress in analytic quality seems to have occurred over the last decade.

Parts of the intelligence community have striven to understand the nature of their deficiencies and ways to make improvements.[16] Yet, two primary factors, which are interrelated and mutually reinforcing, stand in the way of significant progress. The first is a seemingly unalterable bias toward current intelligence reporting at the expense of strategic research. The second derives from a culture of secrecy, which abjures internal openness, broad collaboration, and external outreach.

Current intelligence, pejoratively referred to as CNN with secrets, now dominates analytic production throughout most of the intelligence community. Carl W. Ford, Jr., former CIA and DIA analyst and Assistant Secretary of State for Intelligence and Research, claims that 90 percent of the intelligence community's analysts are now preoccupied with current reporting.[17] Thus, with a rewards system based on quantity and short deadlines and an analytic "tradecraft" oriented towards enhancing writing and briefing skills, it comes as no surprise that few analysts have time to produce longer analytical pieces or to work in groups that might permit them to expose their assumptions to a broader array of thinking or systematic refutation of

alternative explanations of events. In fact, although the DNI has called for new methods to avoid group think, analysts today rarely expose their thinking to more rigorous forms of appraisal by employing scenario development, red teams, or structured-argumentation tools.[18] The latter are simply of little use when the demands of time dictate dependence on individual intuition rather than methodological rigor.

Paradoxically, secrecy — the defining characteristic of any intelligence organization[19] — acts as the most unalterable impediment to ameliorating the analytic process. The vicissitudes of organizational routine, emanating from the legitimate fear of compromising highly protected sources and methods of intelligence acquisition, make collaboration within the intelligence community and especially without it highly improbable, save for few exceptions. Regarding intra-community collaboration, Bruce Berkowitz's 2002 study of the use of information technology (IT) within the CIA's Directorate of Intelligence found an environment that "is largely isolated from the outside world."[20] Security processes and procedures not only affected the posting of classified CIA products on the intelligence community's classified equivalent to the World Wide Web (called Intelink), but made it difficult for analysts to move easily between accessing unclassified open sources and classified ones.[21] An overwhelming perception of risk takes its toll: both access to the outside world as well as collaborating effectively within the secret world are compromised. According to Berkowitz, "current arrangements to mitigate those risks send implicit messages to analysts: that technology is a threat, not a benefit; that the CIA does not put a high priority on analysts using IT easily or creatively; and, worst of all, that data outside the CIA's own network are secondary to the intelligence mission."[22] In sum, because a culture of secrecy will always operate using risk aversion principles rather than a truly cost-benefit approach to assessing security risks, the kind of analytical performance

improvements needed to address 21st century threats may be impossible without more revolutionary institutional arrangements than those currently envisioned by the creation of the DNI.

Incompatibility may be a more definitive characterization of the relationship between the clandestine routines of intelligence organizations and the demands of analytic improvement. In a now classic article in the formerly classified CIA journal, Studies in Intelligence, published in 1976, William R. Johnson argued that "the production of current intelligence and the conduct of espionage are incompatible."[23] This tension is reflected in the DNI's recent efforts to create an array of outreach projects with academics, think tank experts, foundations, businesses, scientists, medical doctors, and various international groups.[24]

The legacy of the CIA's past secret or less-than-transparent engagements with academic and student organizations hasn't dissuaded intelligence community officials from pursuing a huge agenda involving all of the community's intelligence agencies in numerous endeavors to reach out for help. Some of these activities are entirely unclassified but off the record; others necessitate security clearances. The objective, in part, is to foster communities of interest, where individual participants maintain a passionate interest in a particular subject (transnational organized crime groups, for example) and are willing to share ideas, impressions, and to remain engaged for lengthy and continuous periods of time, face-to-face and via computer blogging. As for concerns about potential friction between outside experts (especially academics) and insiders, Tom Fingar, the DNI's head of analysis, argues that "The new outreach effort has to be 100 percent transparent."[25] Yet, the prospective incompatibility of such outreach endeavors manifests itself both on the part of outside experts, most notably, academics, who fear any relationship with secret agencies as damaging to their careers, and intelligence agency

participants, some of whom remain most reluctant to disclose even what areas they work in. While much good can come from such efforts, their inherent limitations should not be underestimated. As one academic observed after a recent DNI outreach workshop, "It was hardly the stuff of open, honest discourse."[26]

Adequately exploiting rich sources of human knowledge together with an ever-exploding world wide web of open source information may just require even more fundamental solutions than simply reaching out from within secret organizations. As Greg Treverton, former vice chairman of the National Intelligence Council (NIC) has argued, "[I]intelligence is the business of information, not secrets."[27] To be sure, the NIC, now subsumed under the new Director of National Intelligence, John Negroponte, acts as a true integrator of secrets and open-source information, not least due to its propensity for turning to outside experts to act as national intelligence officers for particular regional or functional accounts. The NIC's mission has prominently taken on the formal responsibility for reaching out to nongovernmental experts in academia and the private sector to assure that the intelligence community's perspectives are broadened. But given the scope of open-source and specialized unclassified information available from worldwide sources, it make sense to look to new organizations outside of the intelligence community to collect and evaluate these information resources using the best analytical methodologies and data mining tools private industry can offer. One alternative would be to create an organization akin to the defunct Office of Technology Assessment, with branch offices located in key regions of the world. An existing or new Federally Funded Research and Development Center (FFRDC), like RAND, might also contribute to the objective of more effective analytic outreach. Such alternative initiatives ought not supplant the intelligence community's outreach activities; they should be pursued as complementary endeavors in

recognition of the inherent limitations facing secret organizations in truly and effectively interacting with people and information outside of their unique cultural domain.

Besides greater recourse to outside expertise, more resources and ample imagination should be devoted to experimentation. One failed attempt to experiment with open source databases and analytical tools illustrates the potential value of experiments. Six years ago, a French-German-U.K.-U.S. working group proposed a multinational program to conduct open-source analyses of emerging threats, but the proposal fell on deaf ears in Washington.[28] Most of the critical challenges facing the United States and its European allies revolve around questions of prospective behavior—what will Iran do in regard to nuclear weapons? Iran's behavior will not just be the product of its own intentions, but also actions taken by the United States and its European partners. Thus, analysis and dialogue employing abundant open-source information would be an invaluable process in support of diplomatic policy formulation.[29] Especially in light of damage done to U.S foreign policy in the aftermath of Iraq, the U.S. should open as many doors as possible, even if experimental at first, to multinational dialogue on emerging threat issues.

* * *

In essence, no matter how outreach activities are developed, they represent perhaps the initial slice of a wholesale effort to reconstitute the basic structure of the Cold War national security community: a dense hierarchical center surrounded by a sparse network at the edge.[30] The hierarchy's center is heavily populated with "doers" who analyze, assess, and take actions to thwart the goals of those groups and states that threaten basic security interests. The basic structure of the center hasn't been altered since the collapse of the Soviet Union, despite fundamental changes in the security environment. Supporting the center is a sparse set of

"finders" who collect data and turn it into information in support of the center. Consistent with its support relationship, the edge has superb communication links with the center, but there is virtually no communication among clusters operating at the edge. The center must be compressed into a much flatter hierarchy not unlike what modern corporations have done in flattening their headquarters through the use of enterprise-wide information technology. The edge must be expanded greatly into a dense network of highly connected communities of interests, where insights, perspectives, and long-lead-time indicators of anomalous behavior are analyzed, discussed, and thoroughly debated.

New institutional arrangements within and without the U.S. intelligence community can contribute to populating the edge to make the center's decisions more enlightened. Within the U.S. intelligence community, overhead intelligence systems would benefit greatly from a truly multinational approach to populating future system architectures with the means to achieve truly persistent coverage against fleeting targets. On the covert side, a narrowing of effort toward hard targets, bolstered by much greater attention to the emerging revolution in infinitesimally small collection means, would maximize prospects for success. The analytical side, by contrast, should help populate the edge through broadened outreach activities, liberal rotational assignments of analysts into policy positions, academic institutions, and NGOs in the U.S. and abroad. Complementary open-source analytical activities by FFRDCs would compensate in part for the expected constraints that persist within secret cultures that inhibit full participation in such activities.[31] Although these institutional arrangements may never tap the power of Metcalf's Law—that network information value is not just additive but increases as a function of the square of the number of participants—their transformative impact on intelligence

effectiveness and increased prospects for a truly multinational response to terrorism might well prove profound.

[1] This paper builds on Dennis M. Gormley, "The Limits of Intelligence: Iraq's Lessons," *Survival*, vol. 46, no. 3 (Fall 2004), pp. 7-28.
[2] On nuclear threats, the best treatment is Charles D. Ferguson, William C. Potter, et al., *The Four Faces of Nuclear Terrorism* (New York: Routledge, 2005). On biological developments, see Malcolm Dando, "The Bioterrorist Cookbook," *The Bulletin of the Atomic Scientists*, vol. 61, no. 6 (November/December 2005), pp. 34-39.
[3] See Dennis M. Gormley, "Unmanned Air Vehicles as Terror Weapons," Nuclear Threat Initiative Issue Brief, July 2005, at http://www.nti.org/e_research/e3_68a.html.
[4] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (Cambridge, UK: Cambridge University Press, 2003), p. 142.
[5] *Ibid*., p. 163.
[6] *Preparing for the 21st Century: An Appraisal of U.S. Intelligence,* March 1, 1996, p. 68, at http://www.gpoaccess.gov/int/report.html.
[7] Nanotechnology applications are being pursued aggressively under the sponsorship of the Pentagon's Defense Advanced Research Projects Agency (DARPA). For a popular description of such applications, see http://www.computerworld.com/mobiletopics/mobile/story/0,10801,79572,00.html. For a description of the DARPA Smart Dust program, see http://www.darpa.mil/mto/mems/summaries/Projects/University_44.html.
[8] Another critical area is a more focused approach to collecting signals intelligence, now the primary domain of very expensive satellites that collected microwave signals from space. However, fiber optic lines have increasingly replaced microwave transmissions, the implications of which dictate targeting particular communication lines. This can only be accomplished close up, via human means, not from space.
[9] Annual intelligence budgets are classified secret in the U.S., except for 1997 and 1998 when the Director of Central Intelligence publicly informed the Congress of respective spending figures for those two years of $26.6 and $26.7 billion. The figure of over $40 billion is taken from a Center for Defense Information estimate based on press reports and found at http://www.cdi.org/terrorism/intel-funding.cfm. The assumption that over 20 percent of this estimated amount goes to overhead collection is based on the budget estimate for the National Reconnaissance Office ($7.5+billion in 2003), the principal agency responsible for building and operating overhead collection systems. In fact, the *U.S. News & World Report* indicates that the budget figure for 2005 was $44.4 billion. See David E. Kaplan and Kevin Whitelaw, "Playing Defense," *U.S. News & World Report*, November 13, 2006, pp. 46-53.
[10] India and Iraq, for example, both used deception and denial effectively against U.S. overhead imaging systems. See Gormley, "The Limits of Intelligence," pp. 11-13.
[11] Robert Wall, 'National Reconnaissance Office Looks at New Satellite Architecture, Technologies', *Aviation Week & Space Technology*, 5 January 2004, p. 24. For an insider's view of the NRO, see Robert Kohler, 'One Officer's Perspective: The Decline of the National Reconnaissance Office', *Studies in Intelligence*, vol. 46, no. 2 (2002), at http://www.cia.gov/csi/studies/vol46no2/article11.html.
[12] Knowledge of the terrain would tell operators where to look; the detection and tracking of motion would tell them where and when to look; and precision geolocation of these targets would tell them where to attack.
[13] The manor in which the U.S. Joint Strike Fighter program operates with regard to multiple levels of foreign participation might offer a useful model for the SBR program.
[14] See http://www.darpa.mil/tto/programs/astro.html for a description of the *Orbital Express* program.
[15] See Jack Davis, 'Improving CIA Analytic Performance: Analysts and the Policymaking Process', *Sherman Kent Center for Intelligence Analysis Occasional Papers*, vol. 1, no. 2 (September 2002), available at http://www.cia.gov/cia/publications/Kent_Papers/index.html. For more recent critiques, see the 'Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001', at http://www.gpoaccess.gov/serialset/creports/911.html; and the 'staff statements' of the National Commission on

Terrorist Attacks Upon the United States (also known as the 9-11 Commission), at http://www.9-11commission.gov/.

[16] See, for example, Rob Johnston, *The Culture of Analytic Tradecraft: An Ethnography of the Intelligence Community* (Washington, D.C.: CIA Center for the Study of Intelligence, 2005) and Jeffrey R. Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis* (Washington, D.C.: CIA Center for the Study of Intelligence, 2005).

[17] See his remarks at the 2005 Eisenhower National Security Conference, "Panel III: The Intelligence Challenge: Understanding and Preventing Strategic Surprises," Washington, D.C., September 28, 2005, at http://www.vodium.com/MediapodLibrary/index.asp?library=pn100203_eisenhower2005&SessionArgs=0A1U0000000100000101.

[18] See http://www.ai.sri.com/software/SEAS for one example of a structured argumentation analytical tool.

[19] According to James B. Bruce, "Intelligence requires secrets. . . . The future of U.S. intelligence effectiveness depends to a very significant degree on keeping its secrets about collection sources and methods and analytical techniques. When secrecy is breached, foreign targets of U.S. intelligence—such as adversary countries and terrorists—learn about, and then often develop countermeasures to, U.S. intelligence techniques and operations. As a result, the effectiveness of intelligence declines, to the detriment of the national security policymakers and warfighters, and the citizenry that it is meant to serve." See his "The Consequences of Permissive Neglect, *Studies in Intelligence*, vol. 47, no. 1 (2003), at https://www.cia.gov/csi/studies/vol47no1/article04.html.

[20] Bruce Berkowitz, "Failing to Keep Up with the Information Revolution," *Studies in Intelligence*, vol. 47, no. 1 (2003), at https://www.cia.gov/csi/studies/vol47no1/article07.html.

[21] According to Kaplan and Whitelaw, *ibid*., the DNI has pressured the CIA to make the Pentagon's SIPRNET, an all-source operational intelligence network, open to America's closest allies (viz., the U.K., Australia, and Canada).

[22] *Ibid*. Berkowitz notes that a combination of compartmentation, rigid procurement protocols, bottlenecks in coordination and review, and inefficient resource management add to the CIA's disinclination to foster the use of IT tools to enhance analytic performance, no less interact seamlessly with other agencies of the intelligence community or the outside world.

[23] William R. Johnson, "Clandestinity and Current Intelligence," *Studies in Intelligence*, vol. 20, no. 3 (1976), in H. Bradford Westerfield, ed., *Inside the CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992* (New Haven, CT: Yale University Press, 1995), pp. 118-184. See also William R. Johnson, "The Elephants and the Gorillas," *International Journal of Intelligence and Counterintelligence*, vol. 1, no. 1 (Spring 1986), pp. 42-56.

[24] David E. Kaplan, "Hey, Let's Play Ball: The Insular World of Intelligence Reaches Out for A Few New Ideas," *U.S. News & World Report*, October 29, 2006, at http://www.usnews.com/usnews/news/articles/061029/6outreach.htm.

[25] *Ibid*.

[26] *Ibid*.

[27] Gregory F. Treverton, *Reshaping National Intelligence For An Age of Information* (Cambridge, UK: Cambridge University Press, 2003), p. 250.

[28] The study group's final report, including this recommendation, is found in *Coalition Military Operations: The Way Ahead through Cooperability*, A Report of a French-German-U.K.-U.S. Working Group (Arlington, VA: U.S.-Crest, 2000).

[29] Consider that prior to India's "surprise" 1998 nuclear test, open-source information on the BJP's intent to test was available but dismissed because it did not fit the narrow mind-set of U.S. policymakers. Subjecting such open-source information to the multiple perspectives of close allies would add value to an open, collaborative analytical process. For details on the India test, see Treverton, *Reshaping National Intelligence for an Age of Information*, pp. 4 and 11-13.

[29] Here I am indebted to a longtime colleague, Douglas M. Hart, President of Cyberneutics, Inc. The notion of center-edge paradigms emanates from social network theory.

[30] Such constraints also apply to academic and other institutions that may remain suspicious of any interaction with intelligence organizations.