5

The Role of Science and Technology in Transforming American Intelligence

Kevin M. O'Connell

I. OVERVIEW

Among the most important legacies of modern-day American intelligence is its emphasis on science and technology. Technical programs such as the U2 reconnaissance aircraft and the CORONA photo reconnaissance satellite provided independent perspectives for corroborating, modifying, or adding to the information provided by spies operating against the Soviet Union and its allies. The early success of these and other programs in signals intelligence (SIGINT), imagery intelligence (IMINT), and measurement and signature intelligence (MASINT) created an impetus for technical intelligence that was unmatched by any other kind of intelligence capabilities during the Cold War.[1] Beyond an improved understanding of the Soviet Union as a political and ideological enemy, technical intelli-

1. See Loch Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (New Haven, CT: Yale University Press, 1996), 14–26.

gence collection capabilities and the use of technology to support analysis, counterintelligence, and covert action provided a unique intelligence advantage over our adversaries.

Yet if science and technology represent a major component of the American intelligence enterprise, they have thus far received little attention within major reviews and legislative initiatives. Neither the Intelligence Reform and Terrorism Prevention Act of 2004 (hereafter, the Intelligence Reform Act) nor *The 9/11 Commission Report* devoted much time and attention to science and technology and their roles in U.S. intelligence. This is somewhat surprising. To be sure, recent headlines have dampened appreciation of the value of technical intelligence programs and, in part, focused attention in other areas, particularly the perceived failures in the cases of the 9/11 terrorist attacks on the homeland and Iraqi weapons of mass destruction (WMD) programs. At the same time, the increasing complexity and high costs of technical programs, as well as the continuing concerns about the ability to manage science and technology programs, have raised legitimate questions about whether they can and how they should remain a key element of American intelligence. Yet today's intelligence struggles in the global war on terrorism (GWOT) against proliferators of WMD and other illicit goods, and even in regard to advanced conventional threats demand technical intelligence insights. And there are high expectations for science and technology in helping to solve some of the more modern aspects of intelligence, like the analyst's challenge of information overload and the visualization of complex phenomena like radar and biological data.[2]

2. As of this writing, but too late for full inclusion in this chapter, the final report of the Commission on Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction was released. It is sharply and deeply critical of U.S. intelligence performance on Iraq's WMD programs, indcluding numerous challenges to U.S. technical collection in the chemical, biological, and nuclear arenas. The report discusses many of the primary and underlying issues raised in this chapter and strongly recommends an emphasis on creating a more inte-

Aside from what technical intelligence programs can do is the issue of how to undertake them. Historically, what made them successful were an unwavering focus on the conceptualization and development of new capabilities, an emphasis on risk-taking, dedicated and flexible investment, and the nurturing of human capital or people with critical technical talent. Well beyond today's headlines lie these critical management challenges.

This chapter begins with a discussion of technology's impact on intelligence in the early part of the twenty-first century. It then turns to a discussion of how technology contributes to various intelligence disciplines and identifies some of the key technologies that may be useful to intelligence functions during the coming years. It contains a lengthy discussion about how to stimulate, nurture, and manage the development of technical capabilities for intelligence, which require a reorientation both on internal management processes and on external linkages. Development raises basic questions of focus, risk, investment, and people, as well as some higher level issues related to the link between requirements and capabilities, internal management processes, and challenges to the industrial base. The chapter then concludes with observations on how science and technology can contribute to the transformation of U.S. intelligence.

---

grated collection enterprise—including target development, investment, and system development—and the strong need to reinvigorate innovation across the intelligence community. The panel also envisioned roles for science and technology as key enablers for better analysis, collaboration, information sharing, and other essential intelligence functions. Any reader interested in this topic will also make use of the commissions report at www.wmd.gov.

II. THE CHANGING TECHNOLOGY ENVIRONMENT FOR INTELLIGENCE

Technology and the Era of Transparency

Today, various technologies create the means for governments, intelligence services, and even individuals to gather and interpret information about others that was historically held only in the coffers of intelligence services in Washington and Moscow. Because of the information and communications revolution, access to this information is often exceptionally fast and relatively inexpensive. The era of transparency is upon us.

At the same time, the world of terrorist cells and the illicit trade in, among other items, weapons of mass destruction that intelligence targets remains murky. Accordingly, transparency does not mean that everything is completely open, nor that it should be. It means rather that there are increasingly unprecedented types and amounts of information available to any one interested party about almost any other.[3]

More precisely, while American intelligence has a wealth of both classified and unclassified information sources from which to draw, so to do our adversaries.[4] Much of the electronic data that al Qaeda acquired prior to the 9/11 attacks, for example, came from Web sites, later verified by individuals performing their own surveillance. Beyond Internet-based sources of analysis about foreign military and security developments, new technical sources of information—such as global positioning system (GPS) navigational data, commercial space imagery, and biometrics—are also available to

3. For a generalized discussion about transparency, see David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Reading, MA: Addison Wesley, 1998). For a more specific reference to intelligence, see John Baker, et al., *Commercial Observation Satellites: At the Leading Edge of Global Transparency* (Bethesda, MD: RAND-ASPRS, 2001).

4. See Kevin O'Connell and Robert Tomes, "Keeping the Information Edge," *Policy Review* 122 (2004): 19–39.

anyone who has an interest and a modest budget. Coupled with instantaneous communication through cell phones, instant messaging, e-mail, and other sources, foreign governments and nongovernmental actors can be part of a "virtual" surveillance team, military action group, or terrorist cell.

While some might believe that intelligence is immune to such developments, it is actually in many ways driven by transparency. The first aspect of the issue, driven as much by spy novels, media leaks, and counterintelligence disasters as it is by technology, is that the traditional tools of espionage are now well known in detail, thereby diminishing some of their value. Even the simplest-minded adversary knows that intelligence services use both human and technical means to conduct intelligence, including the collection of telephone calls and other signals, the taking of pictures and other images from space, and the use of sophisticated technical sensors to look for specialized signs of harm. They also know, of course, that the embassy cocktail circuit no longer serves as a purely innocent venue within which to share information, unless one is looking to be recruited. For an even more sophisticated adversary, additional information is known, such as the methods of agent debriefing, the susceptibility of technical intelligence to deception, and the predictability of satellite orbits.[5]

But transparency's implications for intelligence range much farther, creating, in essence, a "loss of exclusivity" for most intelligence tools and techniques. Beyond the realm of sophisticated technical intelligence systems, an entire slate of commercial technologies has both explicit and implicit utility as a tool of surveillance and intelligence. Modern cities are replete with video surveillance, for example, and the prevalence of GPS embedded in navigational and other technologies is designed to help one find out where he

5. See Dennis Gormely, "The Limits of Intelligence: Iraq's Lessons," *Survival: The IISS Quarterly* 46, no. 3 (2004): 7–29.

or she is (thereby potentially helping others as well): The salesman pitching a father purchasing a cell phone for his daughter assures the father how good he will feel knowing that the phone's location can be determined, whether after curfew or under more serious conditions. Other modern conveniences, such as credit cards, Internet portal access, electronic toll paying, electronic car safety, and security systems not only help pinpoint people's location but also identify many of their habits.

Although strong concerns certainly exist within the American public about the intelligence community's access to and use of these data, they are clearly of potential value as intelligence sources. The Defense Advanced Research Projects Agency's Total Information Awareness (later Terrorism Information Awareness) program, for example, was envisioned as arraying these and other data sets in the hopes of identifying anomalies and improving efficiency in the use of existing intelligence information about suspected terrorists. But if American intelligence might tap these sources, so might others, and almost certainly under fewer restrictions. Aside from the broader social and economic implications of this data-gathering by others—witness, for example, the rapid rise in identity theft—technologies like biometrics and tracking tools represent challenges to human intelligence (HUMINT) and covert action.

In other words, the information age may have spawned a new intelligence age, an age that might be characterized as a footrace between intelligence services, including a constant race for U.S. intelligence to provide information to national security decision makers better than our adversaries can. In these circumstances, the United States is running a series of footraces against multiple adversaries simultaneously, including nation-states as well as terrorists, all focused on defeating American intelligence activities in the context of their own strategies and security activities.[6]

6. O'Connell and Tomes, "Keeping the Information Edge."

Clearly, transparency holds both promise and threat for U.S. intelligence, with important implications for the roles of science and technology. If transparency is the norm, sanctuaries and hiding places will become highly valued by our adversaries. Intelligence will be operating in a much less structured framework and against a much more organizationally and technically complex target set, which will limit the ability of agencies to organize around a predictable set of security issues that have specific collection targets. Flexibility and adaptation are key. The pursuit of an "information edge" will have to take place within a context of a more diffuse and dynamic global information technology environment and an increased ability by adversaries to collect information, protect information, and deceive U.S. intelligence agencies about their information and ours. This will place a premium on applying science and technology to developing unique intelligence capabilities across all intelligence functions and disciplines. If done correctly, the combination of persistent and exquisite technical intelligence capabilities and the reality of transparency will mean that sanctuary for our adversaries will come only at a premium, if not unaffordable, cost. Science and technology must be a key element of intelligence transformation.

III. THE CONTRIBUTIONS OF SCIENCE AND TECHNOLOGY TO U.S. INTELLIGENCE

From the early U2 spy plane and CORONA satellite to today's unmanned aerial vehicle (UAV) and SIGINT developments to tomorrow's future imagery architecture and space-based radar, U.S. intelligence draws, and will continue to draw, considerable insight from an extraordinary array of technical collection, processing, and exploitation capabilities. Science and technology make vital contributions to the classic areas of intelligence: collection, analysis, counterintelligence, and covert action. At the same time, the pace

at which new technologies are emerging, their variety, and the threat they pose are creating additional challenges for U.S. intelligence.

When assessing the roles of science and technology, it is important to note that U.S. intelligence has drawn predominantly on technology and left the pure science to others. But as the overall and technical complexity of intelligence problems increases, basic scientific research, development, and expertise are playing increasingly important roles in sensing and exploiting complex technical intelligence data, such as those related to biological and chemical weapons or the penetrability of underground facilities.

Areas of Technological Focus

While technology supports all aspects of intelligence, it dominates the collection function through its role in SIGINT, IMINT, MASINT, and even the more recent construct of geospatial intelligence, or GEOINT,[7] which is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict geographically referenced physical features and activities on Earth in support of national security information needs.[8] These capabilities are sometimes described collectively as technical intelligence sources, or TECHINT. From the exploitation of the electromagnetic spectrum to sensing and identifying unique elements (such as radionucleides), phenomena (such as terrain data), and signatures (such as temperatures or reflectants of certain metals or gases), technical collection helps create important raw inputs to U.S. intelligence. Beyond the pure sensing function, the combination of sensor technology and platform development—satellites, aircraft, and

7. See National Geospatial-Intelligence Agency (NGA). *National System for Geospatial Intelligence Statement of Strategic Intent: The Functional Manager's Perspective* (April 2004).

8. Ibid., 3.

UAV—allows creative combinations for effective collection about our adversaries.

But technology's reach extends beyond collection. Technology also assists in conducting intelligence analysis by helping analysts sort, manage, highlight, and share data. Modern computing and communications capabilities allow for the use of complex models—such as exploratory modeling[9] and social network analysis—to understand multilayered relationships among people, events, and technologies. Within the realm of intelligence sharing, technology provides the foundation for expanded collaboration among analysts from diverse disciplines, agencies, and geographic locations, usually focused on a specific problem, like the activities of a terrorist cell or the status of the North Korean nuclear program. Data storage, communications, collaboration tools, and data mining technologies are of particular importance.

Although we might think of the gathering of all relevant information—usually in the head of a CIA or DIA all-source analyst—as fusion, technology today creates an opportunity for an even deeper horizontal integration of all available information. Sometimes referred to as a "multi-INT" analytic approach, horizontal integration is based on a set of capabilities designed to acquire, synchronize, correlate, and disseminate intelligence across sources and missions.[10] Some of the most operationally relevant intelligence during Operations Enduring Freedom and Iraqi Freedom was created in this fashion.

But there are substantial challenges as well. While technology's contributions to collection and analysis are evident, its contribution to the overall effectiveness of U.S. intelligence is less certain: Ques-

9. For one discussion about the use of models in intelligence, see Robert Clark, *Intelligence Analysis: A Target-Centric Approach* (Washington, DC: CQ Press, 2003), ch. 3–7.

10. National Geospatial-Intelligence Agency, *Horizontal Integration: Connecting the Unconnected* (2004).

tions range from the severe imbalance in using technology to collect data rather than to make use of it[11] to a debate that centers on whether technology can be a true source of sophisticated analysis or only an enabler—and perhaps a very good one—of human judgment. Although computers can generate, at lightning speed, many more hypotheses or potential outcomes from a data set than an analyst can—as in a game of computer chess—there remains no substitute for human judgment when trying to assess human behavior. Technology's real value today lies in increasing efficiency in both intelligence collection and analysis.

Technology also supports the counterintelligence and covert action functions, although in different ways. In the former case, technology's utility largely contributes to those same functions it provides to analysis, although new technologies are emerging to supplant the polygraph as the main tool by which to detect deception, whether by employee or by foreign agent.[12] In the case of covert action, technology potentially supports a set of capabilities that range from disguise and counterbiometric capabilities to tools for conducting influence operations, whether of a traditional nature or in cyberspace.

Emerging Technologies of Potential Importance

A diverse slate of technologies, if properly nurtured and managed with a view toward intelligence, has great potential to sustain the intelligence edge that America needs to stay ahead of its adversaries. Emerging space and sensor technologies will help intelligence move beyond the realm of black-and-white photography from

11. See Margaret MacDonald and Anthony Oettinger, "Information Overload: Managing Intelligence Technologies," *Harvard International Review*, Fall 2002: 44–48.

12. Various articles discuss new pathways in the neurosciences to detect political preferences, shopping preferences, and deception.

space. Other technologies will facilitate the collection of more advanced adversary telephone calls and radio and Web communications, while defending against similar threats that arise from them. Yet others will help spot a terrorist covertly at a long distance, while determining that the package he holds contains either food or fissile material. And yet others will mean less need for the risky, indeed potentially fatal, physical meetings that take place between case officer and agent. Elsewhere, computing and collaboration technologies will greatly expand the intellectual reach of the analyst to collector, colleague analyst, or even an outsider, in order to improve understanding of the content or context of a particular piece of information. And analysts' considerations of alternatives and complex situations will be enhanced by modeling, simulation, and visualization tools.

The new technologies are many and varied. Among them, advanced remote sensing, long-range photography, nanotechnology, quantum computing, biometrics, data mining, collaboration tools and devices, visualization, multilevel security, deception detection, and stealth merit attention for the collection and analysis of information about an adversary. And collection technologies will clearly benefit from increasingly adaptive platforms upon which to base them, whether under water, in the air, on the ground, or in the deep reaches of space. Analytic technologies will help with the organization and interpretation of data, the creation and testing of alternate hypotheses, and collaboration and visualization, both among analysts and between analysts and the policy makers they serve. And, as will be discussed, the quantum leaps taking place in the commercial world can only improve the chances of being faster, if not more sophisticated, in what intelligence is trying to understand and convey.

Technology Challenges

The unique role of technology in American intelligence carries its own imbalances and weaknesses, creating a potential vulnerability in the overall intelligence architecture, and therefore in our ability to understand our adversary's motives and intentions. Our use of technology to enhance our own intelligence performance carries a number of important challenges, each of which demands prompt attention.

The first challenge is that U.S. intelligence has been and remains overwhelmingly collection-centric, with insufficient attention paid to the creation of end-to-end (or sensor-to-analyst) architectures that will be needed to create useful and actionable intelligence. While technology can help make greater use of collected data, it must do so with relevant operational concepts and what might be called "metadata." For example, though constructing a massive database with current and archival data of all types may provide a powerful tool for an intelligence analyst, it will be useless without some regard for the education level, experience, and technical skill of the analyst who is using that database. Further, if horizontal integration is the wave of the future, it must accommodate more than a massive accumulation of data in the hope that "smoke, light, and heat"—one analyst's description of a fully comprehensive intelligence picture—will emerge. If data are not thought about more holistically—including how it can be processed, evaluated, and understood by both analysts and decision makers—utter confusion may just as likely be the outcome. Among other issues, consideration must be given to the relative values of specific pieces of information, their real or potential error values, and their overall potential utility in providing an intelligence assessment to someone with little or no experience in the exotica of intelligence.

The second challenge is that, as intelligence problems are becoming more complex, so are the means to understanding them.

In other words, current intelligence problems are not only organizationally more complex—increasingly transnational—but technically more complex as well. Technology's contribution here will be to develop both sophisticated algorithms and the visualization tools necessary to support the intelligence analyst and the decision makers that analysts are supporting. For example, we are moving well beyond the notion of satellite imagery intelligence as the analysis of mere pictures, as the science of remote sensing already extends into subpixel and molecular-level detail. At a minimum, the technical and economic trade-offs associated with turning these data back into pictures for intelligence are likely to be extraordinary. Further, the data collected by advanced remote sensing capabilities—such as multi- or hyperspectral data—are so rich and complex that they will require analysts to have or call upon those who possess technical skills in biology, chemistry, physics, and other disciplines that are uncommon within the ranks of U.S. intelligence yet vitally important to understanding phenomena related to weapons of mass destruction or other technical targets. And these data clearly force choices and trade-offs in collection, processing, and storage. Rather than a pure technology solution, some combination of organizational, technology, and other solutions will be necessary to ensure good analysis and actionable intelligence.

In other words, the complexity that the analyst faces must also be dealt with in presenting the intelligence analysis to decision makers. If a picture is worth a thousand words—especially for presidents, diplomats, and others who might try to persuade or compel others with pictures—then the direction of advanced remote sensing and the way it is used by decision makers run in opposite directions. Data will have to be turned back into pictures for such policy purposes. Similarly, for the decision maker who wishes to use an intercept for the same purposes—such as former Secretary of State Colin Powell at the United Nations in the run-up to the war with Iraq—the best and most sophisticated SIGINT will have little to do

with the sound of a hushed voice whispering about his weapons program or operational plan. It will be much more the product of a technical signature, stripped out of a crush of signal noise and decrypted and processed through some of the most complex algorithms in the world. Although technology depends on an extremely complex set of processes, ultimately, its contribution is to simplify how the world is portrayed.

The third challenge, as the case of Iraq shows, is that technical intelligence often provides information that, in the face of an overall poor understanding of an issue or problem, has high potential to be misunderstood or misinterpreted.[13] Although most of the technical data released by the Bush administration, while sketchy, did point to elements of Iraqi WMD programs, these were misinterpreted in the context of an Iraqi regime that was either patently deceptive or whose servants found good cause to convince its leadership of these programs where there were little or none. Moreover, the success of U.S. technical intelligence over time has placed a premium on the denial and disguise of those capabilities by our adversaries, with everything from traditional camouflage to the rapid development of underground facilities in places like North Korea. As technical intelligence capabilities become more sophisticated, the vulnerability of both the collection and the analytic algorithms to deception will rise dramatically. Intelligence managers, technologists, and analysts must work hard to understand the technical phenomena related to proliferation, WMD, terrorism, and other technical problems.

The fourth challenge is that as new intelligence technologies are developed, managers must deal with intelligence and operational realities that will force them to innovate much faster than in the past. While American technical successes historically remained secret, at least to most of the world, tomorrow's intelligence tech-

13. See Gormely, "The Limits of Intelligence."

nologies will be drawn from a scientific and technical milieu that is accessible to the entire world.[14] Although countries or groups may not have the financial wherewithal to invest in these technologies for intelligence purposes, they may very well have the ability to understand and counter them, if not pursue limited capabilities that meet their own needs and purposes. In other words, while American intelligence can take advantage of advanced technologies, it will be difficult to keep sufficiently far ahead, given the pace at which the rest of the world is adopting new technology.[15] Aside from the natural proliferation of scientific knowledge in many areas, the commercialization of many technologies is advancing the spread of information relevant to both new threats and intelligence countermeasures.

An example might help. While America's SIGINT function took great advantage of the architectural stability and predictability of global communications in the 1970s, it has, for the past decade, struggled to keep up with the explosive rate of change in communications technologies and methods. There is not only an exponentially greater volume in communications, but also a much greater diversity in the types and methods used to secure them. Similar conditions are emerging in the GEOINT arena, as commercial sources of imagery and mapping data proliferate in the context of a rapidly changing environment for geographic information systems (such as maps and georectified data bases). Post-9/11 imperatives to share data will exacerbate this problem. Yet there is no going back. No classification system can stop the advance of science, nor should it. This places a premium on innovation in intelligence technologies.

14. This will vary across technical disciplines, of course. Numerous countries have advanced SIGINT capabilities, based on its traditional use in foreign intelligence systems. Even in the more modern case of imagery, countries are developing and accessing capabilities, combined with commercial geographic information system and other processes.

15. Taken from O'Connell and Tomes, "Keeping the Information Edge."

In this regard, the set of issues related to intelligence sharing and collaboration that, while by no means new for intelligence, has moved to the forefront since 9/11, especially in the homeland security arena, presents distinct challenges. Historically, access to technically sophisticated sources of intelligence was tightly controlled and handled on a need-to-know basis. A premium was placed on protecting intelligence sources and methods. Yet, as the 9/11 Commission and other reports indicate, the need-to-know principle is today turned on its head: In a world of terrorist threats, one may not know who needs to know, so it is imperative for U.S. intelligence to share with, say, coalition partners, law enforcement officers, or Coast Guard captains. While there are important counterintelligence dimensions of this new reality, its most important impact may be in the extreme pressures that it will create for the rapid development of new intelligence sources and methods.

In sum, technology has been, and remains, the darling of American intelligence, yet it presents both tremendous opportunity and risk. We will have to be both sophisticated and flexible in how we use technology and recognize that intelligence technology for its own sake is useless; only technology that gets unique information to the eyes, ears, and brains of America's intelligence analysts, both individually and collectively, has the promise of keeping us steps ahead of our adversaries. Understanding and selecting the technologies that will provide an intelligence advantage is hard enough. Providing the right context for developing them, knowing how to acquire them, and engineering their interaction with the intelligence community's most valuable resource—people—are equally difficult and certainly pose a very tough management task. We turn to this in the next section.

IV. MANAGING SCIENCE AND TECHNOLOGY RESOURCES FOR INTELLIGENCE

As mentioned, neither the Intelligence Reform Act nor the 9/11 Commission devoted much attention to science and technology matters. In fact, right beneath today's broad discussions about U.S. intelligence is an urgent, vitriolic, and sometimes melancholy debate about how to manage technical intelligence resources. A variety of management issues arises in connection to the creation of technical intelligence capabilities and the organizational foundations upon which they rely.

While the creation of a Director of National Intelligence and other initiatives has clear implications for the management of technical intelligence discussions and decisions, in places like the National Geospatial Intelligence Agency (NGA), National Security Agency (NSA), and National Reconnaisance Office (NRO) other discussions are much more focused on how to manage and advance these capabilities. These discussions must take into account the high cost and complexity of technical systems, a highly diverse set of intelligence requirements set forth by various U.S. national security constituencies (such as the Department of Defense, the CIA, and the Department of Homeland Security), and common government budgetary and acquisition practices. For example, officials conducted a relatively public comparison between the ability of former and current officials of the National Reconnaissance Office to acquire innovative satellite systems within cost, performance, and organizational constraints.[16] Other reports focus on the lack of management data with which intelligence community leaders can make effective trade-offs between intelligence capabilities, such as

16. See Robert Kohler, "One Officer's Perspective: The Decline of the National Reconnaissance Office," *Studies in Intelligence*. Followed by Dennis Fitzgerald, "Commentary on 'The Decline of the National Reconnaissance Office,'" *Studies in Intelligence* (2003).

space platforms and UAVs.[17] The failure to effectively set requirements or leverage the industrial base is the subject of yet other critiques and reports.[18] Technical intelligence capabilities can help maintain a comparative advantage over our adversaries only when they are effectively conceived, created, and managed.

The challenge is daunting, not only because of the difficulty of planning individual technical systems, but also because of the volume and diversity of requirements that have to be satisfied. Speed, collaboration, and creative analysis will be the key defining elements of the war on terror, while precision and persistence will dominate strategic and military intelligence requirements. Important trade-offs will have to be made between precise capability and the need for overall flexibility in a rapidly changing world. Similarly, decisions makers will have to weigh the use of new commercial capabilities—especially information technology—against government-designed systems, and consider trade-offs between near-term capabilities and experimentation for the future.

Today's U.S. intelligence community already has a wide range of centers and organizational subelements, such as the Intelligence Technology Innovation Center (ITIC) and Advanced Research and Development Agency (ARDA), CIA's Directorate of Science and Technology, the NRO's Advanced Systems and Technology Office, NGA's Innovision, and other organizations that emphasize technical solutions and forward-looking innovation. Other U.S. government agencies have broader departmental responsibilities, such as the Defense Advanced Research and Development Agency (DARPA) and the Science and Technology Directorate of the Department of Homeland Security (DHS). Although these offices have opportunities for considerable experimentation and outreach, they are also

17. See Richard Best, *Intelligence, Surveillance, and Reconnaissance Programs: Issues for Congress*, CRS Report for Congress, August 2004 (updated).

18. See Baker et al., *Commercial Observation Satellites*.

plagued with many challenges that inhibit initiative and innovation. Nevertheless, the U.S. intelligence enterprise is likely to benefit considerably from the work going on in all of these centers, even though dialogue historically has been impeded by compartmentalization and bureaucratic politics in a declining resource environment.

Creating technical intelligence capabilities poses some unique challenges: Technical collection systems, such as imaging satellites and SIGINT platforms, typically have billion-dollar costs, including the costs of covert development, acquisition, and operation. Estimates of the investment in technical intelligence capabilities have ranged from 60 to 80 percent of a typical $30 billion dollar budget[19] for U.S. intelligence, now closer to $40 billion.[20] Technical system planning and development are especially difficult given the rapid pace of technological change, risking the waste and irrelevance of these intelligence systems as the targets they are designed to pursue evolve.

In this regard, an important intelligence collection and analysis problem involves the need to understand how adversaries undertake their own research programs. Their programs might be highly deceptive in nature, scientifically different in approach, and with fewer concerns about safety or engineering precision.[21] Finely tuned intelligence collection systems risk missing key technical clues if overly focused, or inflexible in how they collect and process information against adversaries who adopt different research models. An adversary concerned about revealing a known thermal sig-

19. See Stephen Orgett, The U.S. Intelligence Budget: A Basic Overview, CNS report for Congress, September 2004.

20. Ibid.

21. This was very much the way in which Iraq began to build WMD precursors in the early 1990s, through development paths that "violated" Western technical and economic constructs for building them.

nature associated with a known scientific process, for example, only needs to heat or chill its product to avoid intelligence collection. In other words, today's intelligence problem is no longer as simple as determining the numbers and types of Soviet aircraft. Knowing how to ferret out a chemical weapons program in a world rife with legitimate but crucial ingredients is truly a scientific challenge. And there remains a need for people who have unique technical skills, security clearances, and expertise, only a few of whom will continue to reside within the organizations of U.S. intelligence.

Basic Elements

To reiterate, while intelligence is often viewed as a walled-off enterprise, it does not and cannot operate in a vacuum: Science and technology development requires focus, investment, people, and a culture of innovation. Few of these ingredients have been richly present in U.S. intelligence over the past decade, in the period between the Cold War and the global war on terrorism. Each of these is worth examining.

Focus

Past program reviews cite "heroic leadership," the use of small teams with authority and responsibility, and an intense focus of effort as key sources of historical success in America's technical intelligence programs.[22] In recent years, however, the development of technical programs has been plagued by extensive and conflicting oversight from within both the executive and legislative branches, an overemphasis on cost control, and an exaggerated need to accumulate customer requirements as part of the process by which to

22. See Kevin Ruffimer, ed., CORONA: America's First Satellite Program, Center for the Study of Intelligence, CIA, Washington, DC, 1995, part I.

gain political and budgetary support for individual programs. Marketing, management, and political consultations have taken place at the expense of attention to the technical aspects of intelligence systems and a focus on accomplishing the specific intelligence mission. Increasing demands by intelligence consumers have also put a premium on creating near-term capabilities, vice long-term ones.[23]

Investment

As mentioned, technical intelligence systems are among the most costly aspects of the entire intelligence enterprise. Recent headlines proclaim the cost and necessity of planned technical systems.[24] The broad reduction in funding for new intelligence systems during the 1990s gave rise to a crisis of trust: The case of a new NRO facility and the "forward funding" associated with that agency ushered in a decade of detailed oversight that represented the most extensive levels of micromanagement in the history of U.S. intelligence, at least in the technical domain.[25] While the American way of planning, programming, and budgeting has its strengths, it substantially limits the flexibility of intelligence program managers in their oversight of technical programs that need to remain financially flexible and aptly funded in the face of technical, engineering, and mission challenges throughout the life cycle of their programs.

23. See Michael Wertheimer, "Crippling Innovation—And Intelligence," *Washington Post*, July 21, 2004, A19.

24. "New Spy Satellite Debated on Hill," *Washington Post*, December 11, 2004, A1.

25. The mid-1970s investigations into U.S. intelligence abuses of civil liberties might be a parallel basis for micromanagement, but it was less focused on technical capabilities.

People

For a variety of reasons, including mandatory personnel reductions and an expansion of lucrative opportunities in the private sector, the U.S. government experienced an overall downsizing in the early 1990s. U.S. intelligence experienced a mandatory 17 percent reduction in personnel, including a number of highly qualified technical personnel who took advantage of jobs in the communications, computing, and related industries. The end of the Cold War saw a reduced interest in American intelligence as a long-term career, because the intelligence community's importance seemed to decline and more lucrative opportunities in the private sector arose. Yet the successful exploitation of science and technology for intelligence purposes requires a highly qualified workforce with access to state-of-the-art research. Further, qualified people are not only essential to the business of building collection and analysis technical systems; in a more complex world, they are also central to the analysis of developments within it.

Culture of Innovation

Just as important as the resources associated with technical intelligence programs is the context within which they are provided and nurtured. CORONA aficionados cite the thirteen failed launches before success as emblematic of the risk that must be encouraged and accepted in order to develop truly innovative technical intelligence systems. Failure must be recognized as a legitimate part of the scientific process. While this is helpful in theory, it must also be considered in the bureaucratic and operational context of the cost of failure. Ironically, the intense oversight, limited resources, and focus on efficiency have forced intelligence program managers to a point where they avoid risk and have fewer resources—in areas like

testing and systems engineering—available to optimize the chances for success for truly innovative systems.[26]

Time is of the essence. Science and technology, in general, and their specialized application to intelligence take time, but the rate of change in the world that intelligence is designed to understand is rapid. Former DCI George Tenet testified in 2001 that the "accelerating rate of change" in the world, as viewed through the eyes, ears, and brains of intelligence, was unprecedented.[27] As we now know, this rate of change has created structural weaknesses in American intelligence, such as the concentration of analysts on more tactical, day-to-day reporting. In addition, collection demands often exceed capacity, especially in global hot spots. But beyond the competition for today's collection, demands for new kinds of collection based on adversary behavior have clearly outstripped U.S. government planning, budgeting, and acquisition cycles. Even today, while the war on terror continues and new threats emerge, American intelligence is in the process of modernizing its SIGINT, IMINT, and MASINT architectures[28] for the current threat environment. Every one of the elements mentioned here—focus, investment, people, and philosophy—are keys to success in that endeavor.

Higher Level Issues and Challenges

Beyond the basic issues lie a number of other challenges to the development of technical intelligence capabilities. These include the role of priorities, needs, and requirements; internal management; external relations; research frameworks for highly risky or controversial topics; and trade-offs within the technical program.

26. Wertheimer, "Crippling Innovation."

27. See www.odci.gov/cia/public_affairs/speeches/2001/UNCLASWWT_0207 2001.html.

28. Various

Priorities, Needs, and Requirements

The cost of technical system planning, development, acquisition, and operations is so prohibitive that some logical link to consumer intelligence should be required. Debates have emerged in the recent past on the respective roles of functional managers for GEOINT and SIGINT (NGA and NSA) and the NRO on which overhead sensors and platforms should be built, with NGA and NSA representing intelligence consumers and NRO representing state-of-the-art knowledge of satellite platforms and technologies. Yet the effort to understand what type of information intelligence consumers say they need—in volume, type, depth, and precision—has given rise to a "tyranny of requirements" that technology developers and their managers need to deal with.

During any given data call for requirements, intelligence consumers, with no incentives to control their needs, pile on every conceivable information requirement they can imagine (and perhaps in some sense need). Rather than focusing on what intelligence can uniquely provide, consumers add thousands of information needs, stated as requirements, in the face of uncertainty about their targets and missions. The problem is compounded by the lack of a coherent system for aggregating and merging the military, intelligence, and homeland security requirements. Indeed, the problem is even worse. Today, intelligence system planning and development must be reviewed by dozens of panels and boards, the most important being the Department of Defense's Joint Requirements and Operations Council (JROC) and the CIA's Mission Requirements Board (MRB). Although these reviews serve as an important vetting process, they also have the effect of driving program managers to intense marketing of their program within the U.S. national security community. More important, these boards can impel managers to create programs that are far too complex. One consequence is that

programs are canceled or scaled back—mostly on cost and technical risk concerns—to a point where they serve a "least common denominator" requirements set, often at the expense of innovation and experimentation. Among the ways to deal with these problems are to place more of the burden of proof on the consumer and to create incentives for appetite suppression among them. At the broad architectural level, efforts must be made to create a portfolio of investments, some of which provide important must-have capabilities while maintaining some innovative high-risk experiments. But experimentation must be recognized and evaluated as such, as opposed to requiring buy-in from every potential user. Real innovation is unlikely to happen without some educated risks.

Internal Management

U.S. intelligence agencies have a can-do culture that emphasizes operations and flexibility over in-depth management and planning.[29] Unlike the sets of organizations used for the Department of Defense—the Office of the Secretary of Defense and the Combatant Commands—focused on operations, and another set—the Joint Staff and the Armed Services—focused on preparing for the future, U.S. intelligence agencies maintain both functions at the agency (e.g., NSA, NGA) level. While external organizations like Congress, the Community Management Staff, and the Undersecretary of Defense for Intelligence play important roles in encouraging, scrutinizing, and overseeing these functions, in fact they are executed at the agency level. This structure has led to an unhealthy competition between operations and modernization,[30] a competition that was exacerbated by successive world crises during the 1990s. As

29. Michael Turner, *Why Secret Intelligence Fails* (Potomoc Books, 2005).

30. William Odom, *Fixing Intelligence for a More Secure America* (New Haven, CT: Yale University Press, 2004), 31–34.

intelligence demands rose, the satisfaction of them came largely at the expense of modernization across the intelligence enterprise.

While an emphasis on satisfying day-to-day intelligence needs represents one challenge to the development of technical intelligence capabilities, the culture of secrecy, a largely inadequate level of investment over the past five decades, and relative political insularity created few incentives for the development of rigorous internal management structures within the agencies. The historical lack of management data and systems and the pervasive secrecy meant that there was almost no way to determine which programs were more effective from an intelligence perspective or more cost-effective from a budget and management perspective.[31] Outside organizations, like Congress, ultimately demanded this rigor and, absent it, stepped in, perhaps dealing a blow to innovation from micromanagement.

Over time, increased oversight, the large costs associated with science and technology intelligence capabilities, the rapid pace of information technology, and other factors have created demands for better overall enterprise management. This was central to the argument for a DNI and other features of the Intelligence Reform Act. Elsewhere, normally quiet congressional concerns about how well the agencies are being managed have spilled into the public debate in the cases of the NRO[32] in the early 1990s and the NSA[33] in the more recent past; they were also a small focus of the 9/11 Commission.[34] Among the recommended elements of more rigorous management are the need to develop a strong enterprise architecture, perform better financial management, undertake more

31. David Kaplan, "Mission Impossible: The Inside Story of How a Band of Reformers Tried—and Failed—to Change America's Spy Agencies," *U.S. News and World Report*, August 2, 2004: 32–42.

32. Robert Wall and Craig Covault, "Trouble at the NRO," *U.S. News and World Report*, August 18, 2003: 24–26.

33. Wertheimer, "Crippling Innovation."

34. *The 9/11 Commission Report*.

rigorous strategic and technical planning, and develop an improved understanding of the links among requirements, investments, and outputs. Although improved internal management is an important and legitimate goal, some worry that an overemphasis on management structures removes attention from the intelligence mission and limits the potential for innovation at exactly the time when it is needed.[35] Whatever the case, intelligence managers must have a better understanding of what they are investing in, and why, especially at a time when attention to developing new capabilities is needed.

External Relations

The planning, development, acquisition, maintenance, and operations of technical systems require a strong and creative interaction with U.S. industry. This relationship historically has been an intimate one—as reflected, for example, in histories of the CIA and the NRO[36]—in part because of the nature of the work and the importance of secrecy and compartmentalization. But these old models are no longer realistic or even helpful. Changes in both government and industry have created the need for a much more open "cast of the net" to find the most potentially useful technologies. Historically, the U.S. intelligence community had access to state-of-the-art technology, by virtue of developing it (e.g., satellites and satellite processing), cultivating it as a potential source of intelligence information (e.g., telecommunications), or establishing proximity to the industry groups that were fostering innovations (e.g., computer networks). Traditional activities, like satellite programs, were large and lucrative and based on a decisive technology advantage in

35. Wertheimer, "Crippling Innovation."

36. This issue is keenly revisited in the *Studies in Intelligence* debate cited above.

space platforms, communications, satellite navigation and control, and state-of-the art exploitation systems for SIGINT and imagery.

The information age and its splintering of hardware, software, and application developers, both nationally and internationally, altered technology as well as the pace at which it changes. Today, commercial developments quickly outstrip government frameworks for understanding and acquiring capabilities in traditional ways. And as commercial opportunities expand, and the U.S. defense industry downsizes and consolidates, the challenge of knowing who to work with becomes much harder. The reduced investment levels for traditional intelligence programs during the 1990s slowed the technology investment and left almost an entire generation of industrial partners with little hands-on experience in technology or systems engineering. From a technological footrace perspective, the pressures on American intelligence were twofold, with our advantage slipping at the same time our adversaries' knowledge of them—for both their own offensive and defensive purposes—was growing.[37] Increased oversight and a demand for more accountable financial and procurement practices have exacerbated relations with U.S. industry.[38] To the extent that oversight has become more detailed, both in dollar terms as well as in technical and programmatic intent, intelligence agencies have imposed those details on the agency contractors. This constrains innovation. Rather than defining the capabilities required in broad terms and allowing the contractors to propose various technical approaches to obtain them, U.S. government agencies are tending to overspecify how the contractors should proceed.

Even if new intelligence technologies can be identified, technology insertion and systems engineering remain key gaps. Traditional acquisition approaches in government create incentives for

37. See Aris Pappas and James Simon, "The Intelligence Community, 2001–2015," in *Studies in Intelligence* (2003).

38. Wertheimer, "Crippling Innovation."

stability and longer-term architectural strategy rather than the rapid architectural changes and their attendant financial implications that today's technology and intelligence environments demand. Even if new technologies can be identified, it takes on average about ten years from the time a major technical intelligence idea is developed to the time it is used operationally, the equivalent of an ice age in the current environment. Successful transitions have involved direct user involvement in the development, the running of parallel and redundant capabilities, and the determination tolerance for failure. Many of these are very difficult to achieve in intelligence, given technical system complexity, the cost of redundancy, and the need to deliver must-have capability to the intelligence mission. These realities are forcing decisions that may create near-term capabilities, but ones that may come at the expense of longer-term intelligence advantages.

To summarize, the state of relations between the intelligence community and U.S. industry today involves too many structural barriers and intellectual boundaries, including ingrained expectations about procedures and oversight mechanisms. Technical systems are no longer conceived and built in an environment structured to sustain an innovative spirit. Rather, they emerge from a consensus-based process designed to satisfy as many standardized engineering and financial requirements as possible. Planning occurs from the top down, rather than from the bottom up. Systems integration, which should derive from technological best practices, has become a political and actuarial process that values integration *within* agencies at the expense of integration *across* agencies. This runs contrary to the direction in which American intelligence should be headed.[39]

Ineffective use of the commercial sector is a particularly serious problem. Intelligence technologies for collection and analysis range

39. Taken from O'Connell and Tomes, "Keeping the Information Edge."

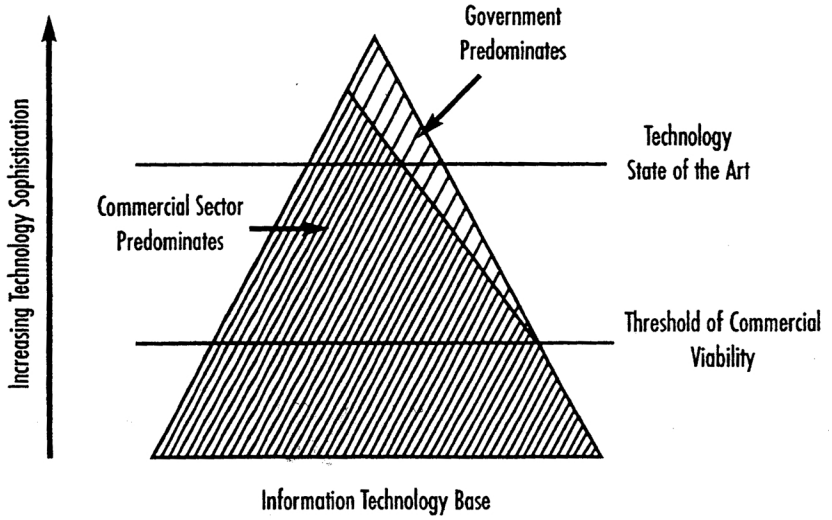
from the one-of-a-kind, exotic systems—such as satellites or SIGINT collectors—to the kinds of collaborative networked environments that both professionals and even students have grown accustomed to in their work. While intelligence technologies have been historically developed and built within the government or its first-tier vetted industry partners, there are increasing opportunities, even in the systems realm, to make use of emerging technologies from the commercial sector. But how and when to use commercial technologies and practices remain hotly contested questions. Although government acquisition usually ensures a capability tailored to specific requirements—using known providers and under known security conditions—costs are generally higher in government procurement. Using commercial technologies usually requires less funding, but also less control of the process and the overall market.

Of course, the private sector today is often more effective at providing information technology and services than is the government. This was reflected in the highly successful establishment by the CIA of In-Q-Tel, a nonprofit venture capital fund designed to connect with entrepreneurs, established companies, universities, researchers, and venture capitalists in order to develop technologies—mostly information technologies—that provide superior intelligence capabilities.[40] The In-Q-Tel model has been so successful—more than sixty investments in companies whose technologies help improve intelligence processing and analysis—that U.S. intelligence and even other government managers have tried to expand and export the model, which relies heavily on the DCI's special acquisition authorities.[41]

But what about the areas of technical intelligence beyond information technology, such as those required to gather exotic signals or the development of WMD? Clearly, the government-industry mix

40. See In-Q-tel website at www.in-q-it.com.

41. Interview with Gilman Louie, "Defense Firms Look to Mimic CIA Strategic Venture Firm," *Federal News*, July 12, 2004: 8.



Relationship and Comparative Advantages of Government and Commercial Technology Sectors

will be different, based on current investment levels and market demands. One approach is to have the government take maximal advantage of the commercial sector while continuing to emphasize its own investments in areas where no market is desirable or expected to emerge. The chart, from Bruce Berkowitz, depicts the comparative advantages that government and industry have in regard to technology.

The government's role is much smaller overall than that of the private sector, but it is concentrated at the more advanced levels.[42] This reflects the realities on both sides of the fence, namely, that the government has more of an ability to spend money without regard to a bottom line—in essence, taking more risk—while industry is much more sensitive to the bottom line. Industry is therefore available for capabilities that are important, but perhaps less state-

42. The argument of this section is drawn from Bruce Berkowitz and Melvin Goodman, *Best Truth: Intelligence in the Information Age* (New Haven, CT: Yale University Press, 2002), ch. 2.

of-the art, absent government guarantees and investment. Berkowitz describes a number of possible approaches to exploiting the private sector for intelligence purposes, including subsidization and partial privatization, flexible regulation, and the creation of competition within the government. While each of these approaches has been pursued, the last is typically hindered by traditional secrecy and mission specialization, as well as a culture that has tried to eliminate competition for both good and bad reasons.

There is good news. Some innovative approaches have been tried to some success. Each year, the NRO director's Innovation Initiative casts a very wide net concerning the future of the space reconnaissance enterprise and the technologies that might help transform it.[43] This initiative has been creative not only in terms of its role in advancing the NRO's mission, but also in feeding other intelligence community agencies with potentially innovative ideas. CIA's STEP program, undertaken by the Directorate of Science and Technology, fosters links to scientists, researchers, and technologists in academia and industry for purposes of providing inputs to key analytic and technical questions underpinning U.S. intelligence. And, in the past, a broad exchange between the intelligence community and environmental scientists fostered as much of a benefit for U.S. intelligence as it did for improving how we might understand key collection and analysis questions related to the environment.[44] In all cases, this broader network of collaborations with academia and industry has pointed to a key method for advancing the use of science and technology for intelligence purposes.

43. DII website at www.nro.gov.

44. See Kevin O'Connell, *Using Intelligence Data for Environmental Needs: Balancing National Objectives* (RAND, 1996).

Trade-offs

As intelligence managers exploit science and technology for the purposes of improving intelligence, they must understand the trade-offs they are making within their programs and, ultimately, within the entire architecture. As mentioned, American intelligence has devoted an inordinate amount of resources and attention to the collection of data, rather than to its processing and exploitation. Collection that remains unexploited—lacking analysis and contextual consideration—may be as useless as no collection at all. Security practices must shift toward allowing better intelligence sharing, and even the most secretive project today must be planned with a view toward the day when it is less secret or even known in a widespread fashion. In this newfound intelligence-sharing environment, managers will have to realize, like Silicon Valley did, that advantage is fleeting. Maintaining the intelligence edge will require much shorter cycles of innovation.

Understanding trade-offs is important in other ways, such as the drive for greater efficiency across the entire intelligence enterprise. Congress, for example, has strongly criticized the poor coordination of and trade-off analysis within intelligence investment in potentially redundant capabilities like UAVs and satellites.[45] While efficiency is rarely a useful goal in the collection of intelligence, it must remain an important target for resource use and allocation. Scale and scalability of new technical concepts must also be understood: Technological innovations may mean nothing without parallel adaptations in both organizations and people. While an extraordinary amount of work has gone into developing analyst tools, these are typically disregarded by analysts unless they are easy to learn, easy to use, and increase the amount of time that they have to think.[46] And while some technology-driven develop-

45. See Best, *Intelligence, Surveillance, and Reconnaissance Programs*.
46. RAND Analytic Tradecraft report (forthcoming).

ments are extremely positive, producing highly innovative intelligence under tight and operationally challenging time lines, uncertainty remains about where these activities actually fit within the overall intelligence enterprise.

V. MOVING AHEAD WITH SCIENCE AND TECHNOLOGY

The global war on terrorism, WMD proliferation, and other intelligence challenges demand a complex approach to understanding our adversaries, including their capabilities, their potential to change, and, most important, their intentions. While the post-9/11 public discussion about the future of U.S. intelligence has been fraught with gross generalizations—such as "less TECHINT, more HUMINT"[47]—the reality is that we must use each part of our intelligence enterprise to maximum effect and in as creative and synergistic a way as possible.

Long a key element in the American intelligence arsenal, science and technology will continue to play a crucial role for U.S. intelligence, whether in creating new capabilities or in improving our ability to use existing ones. But it will have to do so in a much more difficult context than in the past, to deal with the dual challenges of increased complexity in the intelligence mission and of changing balances in the use of technology. In a period of increased transparency and intelligence footraces, U.S. intelligence will have to get beyond moving faster and more efficiently; it must become qualitatively more effective in collecting, processing, disseminating, and acting upon information. In a rapidly changing information market, U.S. intelligence innovations must drive toward increasingly specific and specialized forms of information. And identifying and breaking sanctuary for our adversaries will have to become the new norm for U.S. intelligence. Moving from a target-based orien-

47. See Bruce D. Berkowitz and Alan Goodman, *Best Truth: Intelligence in the Information Age* (New Haven, CT: Yale University Press, 2000), 41.

tation to more of a search orientation will have to take place as well.

Science and technology can dramatically improve U.S. intelligence in a world of greater threat and greater transparency. They must provide new and exotic sources of information in addition to the daily information commodities—basic images, intercepts, and technical reports that help us understand the "normal" state of the world. These new sources will help us maintain an information advantage. In a world of information overload and opportunity, science and technology must also help optimize our most important intelligence resource—people—by optimizing the targets, issues, and details on which these people focus.

We can optimize the utility of technology by a renewed concentration on management of all the key elements—risk, resources, and people—that underpin the development of new technical capabilities. And by managing the elements not only inside our intelligence organizations—for better and worse, the locus of preparation for the future—but also within the U.S. industrial base and other outsiders who can bring creative new approaches, new ideas, and expertise to bear on the future of the intelligence enterprise.

The key to success in the intelligence footrace is a renewed emphasis on innovation across the intelligence spectrum.[48] Real innovations alter core tasks—an extremely difficult undertaking for centralized, insular intelligence organizations that persist more as self-protective guilds than as the complex adaptive organizations that are required to anticipate and respond to rational, strategic adversaries engaging in asymmetric attacks. These adversaries are rational in that they learn, adapt, and organize based on our defenses. And they are strategic because they have long-term objectives and engage in planning to meet them by adjusting to our actions, capabilities, and knowledge about the strategic environ-

48. Taken from O'Connell and Tomes, "Keeping the Information Edge."

ment. Sustaining America's information edge is less about infrastructure than it is about leadership, engendering cultural change, encouraging entrepreneurial analysis, and learning to accept risk, whether in operational, informational, or acquisition processes. It requires focus and innovation at every level, with an active public debate about the strategic effectiveness and future direction of U.S. intelligence.

Finally, there is a need to nurture and reinvigorate the intelligence community's innovation ethos—to reenergize and focus American ingenuity on emerging intelligence collection, analysis, counterintelligence, and other challenges. Doing so, in past eras, has advanced both our leadership in world affairs and our ability to prevent conflicts or terrorist attacks at home and abroad. The global war on terrorism and the broader U.S. national security environment provide a context that is ripe for pursuing intelligence innovations across American intelligence. Within the current storm clouds over U.S. intelligence is a consensus for change, including innovation and experimentation. To maintain our intelligence advantage, we must take advantage of it.