WEARING SUNGLASSES IN A DARK ROOM: HOW OUR OBSESSION WITH SECRECY AND SECURITY UNDERMINES COUNTERTERRORISM EFFORTS

Christopher Preble
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.

On September 10, 2001, the National Security Agency (NSA) intercepted some disturbing messages. "Tomorrow is zero hour," read one. Another cryptically declared "The match is about to begin." [1] Taken out of context, such messages did not constitute actionable intelligence. In the hands of a national security official they would not have provided a roadmap for stopping the devastating attacks of the next day. Furthermore, it would have been nearly impossible to pick out these one or two crucial pieces of information from the sheer volume of material received on any given day by America's sprawling intelligence community. Perhaps the message of an impending "match" was from someone trying to connect with friends at a soccer tournament?

There is still one other reason, beyond the noise and the problem of contextualizing ambiguous or contradictory pieces of information, why these messages had no impact: no one read them. They were in Arabic, and the NSA suffered from such an acute shortage of Arabic-speaking analysts that the messages were not translated until a few days *after* the 9/11 attacks. The information was inaccessible to policy makers, counterterrorism officials, and law enforcement personnel, and was therefore completely useless.

While many have noted the personnel shortages in this crucial area, some government agencies have been particularly resistant to change. For example, the *Washington Post* reported in October 2006 that just 33 of the FBI's 12,000 agents have "any familiarity with the [Arabic] language."[2] There is government-wide need for individuals proficient in Arabic and many other languages vital to national security policy, such as Farsi, Pashto, Korean, and Mandarin, as well as a number of languages and dialects prevalent in Africa.

The dearth of necessary linguistic and cultural skills within the government has effects that reach far beyond the intelligence community. For example, the General Accounting Office

(now the Government Accountability Office) reported in February 2004 "that insufficient foreign language skills also posed a problem for the State Department's diplomacy in the Muslim world."[3] The problem even extends to the war in Iraq. Joan Ryan, a columnist for the *San Francisco Chronicle*, noted in May 2005 that the shortage of military personnel who can speak Arabic and Farsi was "hampering efforts to translate radio transmissions and interview Iraqi citizens who might possess useful information."[4]

Plugging this skills gap has proved extremely difficult. This is because languages such as Arabic and Mandarin are not based on the Latin alphabet, and have not traditionally been taught in American schools. Rather, the individuals most likely to be proficient in such distinctive languages are those who have learned them from foreign-born parents, or who have spent considerable time overseas in places where such languages are spoken on a regular basis.

But herein lays the paradox: individuals who apply for work in the intelligence community, or indeed anyone wishing to work in a job that requires a security clearance, are flagged as potential security risks if they have foreign contacts, defined as a "foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country."

It is entirely appropriate that the U.S. government would wish to minimize the risk of foreign influence. As worded, the guidelines make reasonable accommodations for individuals with extensive foreign contacts, and further stipulate the types of contacts that are most likely to pose a security risk. The guidelines also dictate that a number of important mitigating factors must be taken into account during the adjudication process. "The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with

the interests of national security must be an overall common sense judgment," and adjudicators are directed to consider the guidelines "in the context of the whole person."[5]

In practice, however, the guidelines have the effect of discouraging the very people who possess the cultural and linguistic skills most desperately needed for waging effective counterterrorism operations. Notwithstanding reasonable accommodations for the aforementioned mitigating factors, the security clearance adjudication process often privileges people who do not possess the requisite skills to excel in such positions. As Daniel Byman, director of Georgetown University's Security Studies Program, notes "It is easier to get a security clearance if you don't have any interaction with foreigners, which is not what you want if you want better interaction with foreigners."[6]

In the current environment, we exclude a number of otherwise qualified persons on the chance that they might be a security risk. It is reasonable to be concerned about the penetration of our security services by double-agents, but we must also be concerned about the shortage of personnel with the requisite cultural and linguistic skills. If hiring officials adopted a greater degree of risk tolerance on the front end, the government could circumvent some of the skills shortage on the back end. We must change the whole approach to information, both in terms of what gets classified, and in terms of who gets to read it. Our unique strengths as a nation – our openness, tolerance, educational freedom and cultural diversity – are not being utilized to the fullest extent.

The Hiring Binge

The problem of too few analysts sifting through too much information is hardly unique to our current counterterrorism efforts; indeed it is endemic to intelligence analysis.[7] The initial response after the 9/11 attacks was a focus on reorganizing the sprawling intelligence

community. Various study groups and blue-ribbon panels had urged such reforms prior to 9/11, but the attacks served to rally political support and break down the bureaucratic inertia that had blocked such efforts in the past. There was a renewed emphasis on sharing information within and among government agencies, and a heightened awareness of just how much the enemy had changed. The institutions of our intelligence community were constructed to fight the Cold War; they were ill-suited for fighting non-state actors such as al-Qaeda.

But these changes– the most elaborate being the establishment of the Department of Homeland Security (DHS) in late 2003 – ultimately boil down to moving boxes on organizational charts. Such reforms do not fundamentally address the critical shortage. In fact, the changes that *were* implemented may even make the problem worse, by creating additional layers of bureaucracy -- or even entire agencies -- that also must be staffed.[8]

Aside from the creation of the DHS, another knee-jerk response to resolving the personnel shortage has been a government-wide hiring binge. For example, in accordance with a presidential order calling for a 50 percent increase in the number of analysts and overseas operatives, the CIA has hired an estimated 2,000 new people each year.[9] However, this push to dramatically increase the pool of *intelligence* analysts does not necessarily translate into a greater number of *qualified* analysts. One former CIA official, responding to President Bush's directive to increase the number of CIA analysts, argued that this spike will require "even more aggressive recruiting, or lowering the quality of people."[10] Another former spy told the *Los Angeles Times*, "hiring 50% more agents without fundamentally changing how they do business just makes you stupid."[11]

These criticisms have merit. Few individuals come to the job (*any* job) with all of the skills that they need to succeed. For example, analytical competency must be taught, and then

developed and perfected over time. Likewise, the government has taken responsibility for increasing foreign language proficiency by offering financial incentives to encourage current employees to learn new languages. If new hires lack the requisite foreign language, then the agency is often on the hook for filling that training gap. But the benefits are slow to materialize. According to Douglas Hart, president of the software firm Cyberneutics, and Steven Simon, Senior Fellow for Middle East Studies at the Council on Foreign Relations, "It takes 33 months of full-time instruction in a language not written in the Latin alphabet to bring the average student to a so-called 3.3 level, which reflects competence but not fluency. Part-time instruction drags this period out to 55 months."[12] The findings of the Foreign Service Institute are equally sobering. The institute estimates it would take about 2,200 hours of study for the average person to attain proficiency in Arabic.[13] Furthermore, such training is expensive. The Department of Defense estimated in 2002 that it spent up to $250 million annually on foreign language instruction, a figure that has certainly gone up since the GAO released its study of foreign language deficiencies within the government.[14]

While we can—at great cost and over considerable periods of time—teach people foreign languages, the problem is much deeper. As Hart and Simon argue:

> "The intelligence community requires analysts who are extremely culturally and psychologically aware, and self-aware, have a command of one or more foreign languages, have experienced life overseas, and possess the methodological skills to structure logical arguments based on transparent premises, while making legitimate use of the available facts, and accounting for their personal biases."[15]

In short, it is not simply a lack of linguistic proficiency that inhibits our counterterrorism efforts; it is also a lack of cultural awareness that can rarely be taught in a classroom setting. But while Hart and Simon correctly point to this pervasive problem, they do not advocate a reform of the hiring procedures that discriminate against individuals with friends and family in foreign

countries, the very people who are likely to be already proficient in a non-English language. They are also likely to have learned that language at an early age, a process that stimulates critical and analytic thinking, the very qualities that are in such great demand within the intelligence community.[16]

Expanding the Pool of Qualified Analysts

As noted above, while current regulations discourage, first generation American citizens, and anyone with one or more family members who is not a U.S. citizen, they do not categorically bar such persons from obtaining a security clearance. In practical terms, however, the persons responsible for adjudicating security clearance applications have a powerful incentive to focus solely on the concern about foreign influence (conflict of interest), and less on the mitigating factors.

This tendency flows from an understandable human impulse: risk aversion. More accurately, the entire approach to government security regulations is focused on avoiding or minimizing the risk that sensitive information will wind up in the hands of our nation's enemies. By overcompensating for this particular risk, however, they (and we) increase the chances that qualified persons whose loyalties to the United States are unassailable will be erroneously barred from government service, and therefore unable to translate, read or otherwise analyze information that might prove instrumental in preventing another terrorist attack.

Taking account of the trade-offs inherent in the current approach, which substitutes one kind of risk for another, policymakers should adopt a reasonably permissive attitude toward the sons and daughters of foreign-born persons. They should consider extensive foreign travel and interaction with persons not from the United States to be of potential benefit to the individual's

ability to make a measurable contribution to counterterrorism efforts. In this context, the mitigating factors should not be merely an affirmation of the applicant's commitment to advancing U.S. security and avowed loyalty to this country, but also a consideration of his or her unique qualifications, such as a keen intellect, knowledge of crucial foreign languages, and deep cultural understanding.

Limiting the Government's Penchant for Secrecy

Our intelligence problem is two-fold. On the one hand, security clearances are difficult to obtain, particularly for applicants who have foreign-born contacts. On the other hand, the need for security clearances continues to rise because the volume of classified material is growing dramatically; this overclassification renders more and more information off-limits to individuals who lack the requisite security clearances.

In the waning years of his long and distinguished career, the late Senator Daniel Patrick Moynihan (D-NY) weighed in on the issue of government secrecy and the problem of overclassification. In testimony before the Senate Committee on Governmental Affairs in July 2000, Moynhihan charged that "excessive secrecy has significant consequences for the national interest," invoking Jefferson's argument from two centuries earlier that "an informed citizenry is vital to the functioning of a democratic society."[17] In his 1998 book *Secrecy*, Moynihan concluded, with characteristic flair, that "secrecy is for losers," contending that Cold War-era regulations had outlived their usefulness and that "openness is now a singular, and singularly American, advantage."[18]

Moynihan's views were consistent with those of President Bill Clinton. Clinton's Executive Order 12958, issued in April 1995, automatically declassified documents more than 25 years old, that is "unless the Government took discrete, affirmative steps to continue

classification." Before this executive order, the onus had been on researchers and citizens to make the case for declassification of a particular document through a Freedom of Information Act (FOIA) request. But Clinton's directive turned this on its head. In the wake of EO 12958, the governing presumption was that information, particularly historical documents relating to wars long past, was already in the public domain. Thus, the Government could only withhold such information if it made a compelling case for secrecy. Agencies were urged to release information unless there was "foreseeable harm" in doing so.[19] The Federation of American Scientists estimates that more than a billion pages were declassified under Clinton's executive order.[20]

The push for both declassifying Cold War era documents and limiting the classification of new documents was largely derailed by the Bush administration. Following the 9/11 attacks, President Bush directed White House Chief of Staff Andrew Card to draft new guidelines governing what information would be shielded from public view. The answer: essentially everything. Under the pretense of limiting terrorists' access to sensitive information, the White House issued the so-called "Card memo" in March 2002. This document directed government agencies to treat all of their information holdings with great care; to withhold access to sensitive material either through the formal classification process, or through the liberal use of the "sensitive but unclassified" designation; and to entertain formal requests for public access to information under FOIA only when "there was a sound legal basis to do so."[21] In short, the logic of openness embraced in the late-1990s has been almost entirely repudiated.

The practical effects of these regulations have been enormous. Documents that have always been unclassified have been classified. Documents that were declassified in whole or in part have been reclassified. William Leonard, Director of the Information Security Overnight Office operating within the Department of National Archives, explained to National Public

Radio that there were 15½ million classification decisions in 2004, double the number in 2001. The costs of classifying documents are high, topping $7.2 billion in 2004.[22]

Meanwhile, all new information has been subjected to a standard that elevates secrecy above openness at virtually every step of the way. The problem goes well beyond those documents marked as "classified." As Steven Aftergood of the Federation of American Scientists explained to NPR's Jackie Northam: "Many federal employees now have the ability to withhold information by using newly created designations, such as 'For Official Use Only,' 'Sensitive But Unclassified,' 'Limited Official Use,' all markings or designations that can be used to block the release of unclassified information, and they are used very aggressively."[23] But the mindset embodied in these regulations may actually undermine U.S. counterterrorism efforts, because it inhibits information sharing between agencies. According to Scott Armstrong, Executive Director of Information Trust, an organization which tracks government secrecy, "the way the systems works is more energy goes into protecting [documents] from other officials, from people that have control of tax-payer dollars, from people that are politically interested, than actually goes into" preventing our enemies from accessing this same information.[24]

Why Do These Counterproductive Policies Persist?

It might be difficult to increase the number of persons with the necessary skills for analyzing information that may prove crucial to U.S. counterterrorism efforts, and/or reducing the volume of material shielded from public view. The resistance to change begins within the bureaucracy, specifically from those individuals responsible for rendering judgments as to the suitability of individuals and the sensitivity of information. Risk aversion is endemic within the public sector, in part because there are few of the incentives that encourage and reward risk-

taking in private firms (for example, profit). Researchers have speculated that bureaucrats exhibit not so much "an unwillingness to take risks but a lack of knowledge and tools to determine what are 'reasonable' risks."[25]

In practical terms, how do government regulations reward or punish a person who grants a security clearance to the first-generation American whose parents emigrated from Vietnam in the waning days of the Vietnam War? If the person is subsequently found to be a security risk, the adjudicating official can be held accountable. There is no comparable standard of accountability for an individual who, following the letter of the regulations, renders a negative finding against the very same person who, as it happens, posed little or no security risk.

In a similar vein, it is also easier to deny a FOIA request, or to over-classify an entire document, rather than to make the case, sometimes on a paragraph-by-paragraph basis, that the release of information poses no threat to national security. The architectural drawings of the World Trade Center weren't state secrets – and yet the value of this type of information was made clear on 9/11. Does this mean that everything, or nearly everything, falls under the "sensitive, but unclassified" standard laid out by the Card memo? A reasonable case can be made that the answer is yes. And if an employee within the Department of Agriculture blacks out information pertaining to crop yields in western Colorado, on the grounds that this information *might* be useful to terrorists, can we really blame him?

The National Archives' William Leonard explains the dilemma thusly. A federal employee will err on the side of caution because "it is a very human reaction [to say], when in doubt, 'I never get in trouble for withholding. I may get in trouble for sharing something, but I never get in trouble for withholding.' That's the thing that we have to change"[26] The very same principle should be applied to security clearances for individuals.

There is no purely objective standard. Even an advocate of far greater openness in government, Senator Moynihan, freely admitted that "Some secrecy is vital to save lives, protect national security, and engage in effective diplomacy." Disclosure of sensitive secrets, he warned in 2000, would cause "exceptionally grave damage to the national security."[27] That is objectively true, and such concerns have become more urgent in the wake of 9/11. "When the nation is at war, and the administration adopts a wartime footing," explains former White House counterterrorism official Roger Cressey, "then there is a natural inclination to further classify things."[28]

The Open Source Center: Junior Varsity, or Intellectual Ghetto?

Natural, yes, but such inclinations often have counterproductive effects. The focus should be on expanding the pool of qualified persons, and on placing more emphasis on expanding access to information that might be useful in counterterrorism operations. These two reforms would be the most efficient way to address the pervasive problem of too few people reviewing too much information. It might be impractical however to overcome the deep-seated fears that first-generation Americans, or individuals who have emigrated to the United States, or who maintain close contact with persons abroad, might harbor dual loyalties and therefore will always pose an unacceptable security risk.

These are, after all, not trivial concerns. If an individual lives in the United States, but has family or close friends living in another country, there is always the potential that the interests of those persons could come in conflict with the interests of the United States. It is also true, however, that some of the most notorious spies from the Cold War era were motivated by simple greed, not dual loyalties. John Walker, Jr., had no family or friends in the Soviet Union, but the

passing of sensitive documents to his Soviet handlers for over a nearly 20 year period proved so lucrative that he ultimately convinced his son, brother and best friend – all native-born Americans with no foreign contacts – to join in. Similarly, Aldrich Ames had no personal connections to the Soviet Union, nor any particular ideological affinity for communism. He, like Walker, betrayed his country for money.

Nonetheless, it is appropriate that the possibility of a conflict of interest be factored into the decision making process with respect to who does, or does not, obtain a security clearance. Some persons with extensive foreign contacts -- either through family or friends, or by virtue of extensive foreign travel -- might ultimately and legitimately be deemed a security risk.

There may still be a way, however, to harness the unique skills and cultural awareness of these persons in a way that advances U.S. security. Vast quantities of information processed by U.S. intelligence agencies are derived from open sources such as newspapers, magazines, television and radio broadcasts. Hart and Simon note that "the bulk of [a junior analyst's] time is consumed by 'current reporting'" whereby analysts summarize recent "intelligence gathered on a particular issue…with very little emphasis upon plausible future extrapolations concerning threat behaviour, strengths and weaknesses." Such work does not necessarily require deep analytical skills. Indeed, Hart and Simon liken the whole process to that of "monks in the Middle Ages extracting and copying…portions of manuscripts written earlier by scholars in antiquity."[29]

Most of the material is not written or broadcast in English, and it must therefore be read and translated by the very limited number of analysts with the necessary linguistic skills. While there is an inherent bias, when weighing the value of open source intelligence (OSINT) versus material acquired through special means, to privilege the latter over the former, these attitudes are changing. Expressing concern for "the Intelligence Community's surprisingly poor 'feel' for

cultural and political issues in the countries that concern policymakers most," the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (a.k.a. The Robb-Silberman Commission) explicitly directed the DNI to create an Open Source Directorate in the CIA in order to "make open source information available across the Community."[30]

The government has used information derived from OSINT materials for some time --the Foreign Broadcast Information Service (FBIS) has been around since the Cold War era -- but the government has made a concerted effort to exploit these resources in a more systematic way. As Stephen C. Mercado, a CIA analyst in the agency's Directorate of Science and Technology, explained "Open sources often equal or surpass classified information in monitoring and analyzing such pressing problems as terrorism, proliferation, and counterintelligence." Writing in the agency journal *Studies in Intelligence*, Mercado touted the value of OSINT "for following and analyzing intelligence issues," noting its real-time availability (for example, television and radio broadcasts).[31]

In accordance with the recommendations set forth by the Robb-Silberman Commission, Director of National Intelligence John D. Negroponte created the Open Source Center (OSC) in November 2005. The goal of the center is to exploit "openly available information to include the Internet, databases, press, radio, television, video, geospatial data, photos and commercial imagery."[32] But while the creation of OSC represented an important step, its hiring rules are no different than from any other agency within the intelligence community. In other words, while the center deals primarily with open and unclassified information, it still restricts access only to those individuals already cleared for intelligence work. The creation of the office by itself,

therefore, does not address the problem of the exclusion of skilled persons who lack the requisite security clearances.

This is not to suggest that classified information is irrelevant. Information derived from sensitive sources will always be an important piece of the intelligence puzzle, and it is logical to require that the recipients of the information possess both the requisite security clearance and the need to know. There is no, and there should be no, similar prohibition on the reading, translating and evaluation of open source information. Open source materials could be analyzed by individuals who might not otherwise be allowed to contribute to U.S. counterterrorism efforts.

This is not the optimal solution. Rather than adding yet another box on an already over-crowded intelligence organizational chart, leaders in the intelligence community should seek more creative way to integrate open source material, even material processed by persons who do not possess the security clearances required in other agencies. For obvious reasons, oversight responsibility, procedures for information sharing, and the rules governing recruitment and hiring must be worked out. Individuals employed in the center might be subjected to additional scrutiny given their limited access to classified information, but the risk of unauthorized disclosure can be minimized by reasonable application of "need to know" guidelines. If the OSC were restructured in that way it could also serve as a useful way-station for those individuals awaiting a final judgment on their application for a security clearance, a process that has been known to take more than a year in some instances.

There is a risk that this center could become an intellectual ghetto, a sort of perpetual purgatory for the "not-quite qualified"; policymakers and the designated leaders of the enterprise must guard against this. The optimal solution is for the center to operate as a junior varsity team, a place where individuals can hone their analytical skills, while also producing timely

information that would be of use to the wider intelligence community, and ultimately to policymakers.

A New Approach

It is appropriate to ensure that restrictions are placed on the distribution of sensitive information. It is reasonable to check the background of aspiring analysts and their families. It is wise to protect against unauthorized disclosures through current regulations that limit the flow of information between persons with a need to know. Sensitive information does not flow like water into the hands of anyone who happens to possess a security clearance, nor should it. Indeed, the holders of sensitive information have an obligation to protect such information, and must attest "that a prospective recipient requires access to perform or assist in a lawful and authorized governmental function."[33]

There are still other mechanisms for limiting the flow of information, including the application of tiered access, and separating highly classified information from data that is merely sensitive. In a similar vein, individual agencies may wish to retain standards of suitability for individual employees that might not apply across the board. Such restrictions limit the portability of security clearances, a key mandate contained within the Intelligence Reform Act of 2004, but individual agencies should retain the capacity for subjecting their employees to additional screening according to their own requirements. The CIA's Directorate of Operations, for example, is likely to want standards different from, say, the FBI, or even CIA's Directorate of Intelligence. Nothing here should be taken to imply that standards must be applied, uniformly, across all government agencies.

The crux of the problem, however, is our often counterproductive security and secrecy policies. We must reframe the risk-reward calculus. The policymakers and the public at large

must understand that these policies affect more than just a small number of aspiring journalists or intelligence analysts. There will always be some risk that sensitive information will fall into the wrong hands. As it is today, however, there is an even greater risk that actionable intelligence will *not* fall into the *right* hands, as happened in the days and weeks before September 11, 2001. The importance of various signals and messages that were ignored, or missed as noise, is often only understood after the fact, hindsight being what it is. Nonetheless, intelligence reform should include reasonable procedures for increasing the flow of information from knowledgeable analysts to empowered decision makers.

To date, the reorganizations of the intelligence community have dealt only on the surface. The 9/11 commission lamented that the "limited pool of critical experts—for example, skilled counterterrorism analysts and linguists—is being depleted," and they freely acknowledged "Expanding these capabilities will require not just money, but time."[34] But money and time are finite; and the existing bias, both the tendency to overclassify information, and the bias against individuals with the linguistic and cultural attributes that are in such great demand, must be surmounted.

Intelligence gathering has always been akin to searching for dark objects in a dimly-lit room. Today, we are wearing sunglasses in that dimly-lit room, and it surely doesn't help when the government keeps turning off more lights. In our search for a new brand of enemy waging a completely different kind of war, we must expand the volume of material that can be analyzed, even by those persons who do not possess a high-level security clearance. In other words, we must turn on more lights in the dark room. But we must also remove the sunglasses, expanding the pool of skilled analysts by loosening regulations that discourage citizens with deep cultural and linguistic expertise from contributing to the government's efforts to prevent future terrorist

attacks. Neither policy change will be easy, but the alternative – missing crucial signals because the personnel who might have been able to intercept, translate and interpret them were kept out of the fight – is worse.

---

[1] Jill Wagner, "Intelligence Community's Arabic Challenge: Lack of Language Skills Seen as a Major Pitfall of U.S. War on Terror," MSNBC, 19 October 2004, http://www.msnbc.msn.com/id/6275410/.
[2] Dan Eggen, "FBI Agents Still Lacking Arabic Skills: 33 of 12,000 Have Some Proficiency," *Washington Post*, 11 October 2006.
[3] Wagner, "Intelligence community's Arabic Challenge."
[4] Joan Ryan, "Military's Gay Policy is Absurd," *San Francisco Chronicle*, 19 May 2005.
[5] "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, Guideline B: Foreign Influence," available online at U.S. Department of State, http://www.state.gov/m/ds/clearances/60321.htm#b.
[6] Dan Eggen, "FBI Agents Still Lacking Arabic Skills: 33 of 12,000 Have Some Proficiency," *Washington Post*, 11 October 2006.
[7] Roberta Wohlstetter characterized the problem as one of "signal-to-noise" ratio. See *Pearl Harbor: Warning and Deception* (Palo Alto, CA: Stanford University Press, 1962); For a discussion of this problem in the post-9/11 environment, see Bruce Berkowitz, "Spying the Post-September 11 World," *Hoover Digest*, Fall 2003, available online at http://www.hooverdigest.org/034/berkowitz.html.
[8] The Intelligence Reform and Terrorism Prevention Act of 2004 established the position of Director of Intelligence (DNI), who is responsible for developing the annual budget for the National Intelligence Program (NIP). The act also establishes a Civil Liberties Protection Officer and a Privacy and Civil Liberties Oversight Board, both of which are responsible for the protection of civil liberties ostensibly for domestic counterterrorism efforts and *not* for internal (intelligence community employment) civil liberties protection.
[9] According to Steven Aftergood, Director of the Project on Government Secrecy at the Federation of American Scientists, "Agency hiring data are classified, but…analysis of public statements by agency officials and other information shows that CIA hiring may exceed 2,000 people a year." Quoted in John Diamond, "It's No Secret: CIA Scouting for Recruits," *USA Today*, 22 November 2005.
[10] Walter Pincus and Dana Priest, "Bush Orders the CIA to Hire More Spies: Goss Told to Build Up Other Staffs, Too," *Washington Post*, 24 November 2004.
[11] Amy Zegart, "American Intelligence—Still Stupid," *Los Angeles Times*, 17 September 2006.
[12] Douglas Hart and Steven Simon, "Thinking Straight and Talking Straight: Problems of Intelligence Analysis," *Survival*, vol. 48 no. 1, Spring 2006, p. 38.
[13] By way of comparison, individuals can acquire proficiency in languages like Hebrew and Turkish in less than half as much time. Languages such as French and Spanish, which are based on Latin alphabets taught widely in U.S. secondary and post-secondary schools, can be learned in one quarter the time. Wagner, "Intelligence Community's Arabic Challenge."
[14] GAO Report 02-514T, "Foreign Languages: Workforce Planning Could Help Address Staffing and Proficiency Shortfalls," 12 March 2002, p. 2.
[15] Hart and Simon, "Thinking Straight and Talking Straight," p. 37.
[16] Researchers have discovered that "students who speak more than one language perform higher than their monolingual counterparts on tests of academic achievement, cognitive flexibility, and creativity." See, for example, Carroll E. Moran, and Kenjii Hakuta, "Bilingual Education: Broadening Research Perspectives," in J.A. Banks, ed., *Handbook of Multicultural Education* (New York: Macmillan, 1995), pp. 445-462; and Ellen Bialystok and Kenjii Hakuta, *In Other Words: The Science and Psychology of Second-Language Acquisition* (New York: Basic Books, 1994);
[17] Statement of Senator Daniel Patrick Moynihan Before the Committee on Governmental Affairs, United States Senate, 26 July 2000, http://hsgac.senate.gov/072600_moynihan.html.
[18] Daniel Patrick Moynihan, *Secrecy* (New Haven: Yale University Press, 1998), p. 227.

[19] Genevieve J. Knezo, "'Sensitive But Unclassified' Information and Other Controls: Policy and Options for Scientific and Technical Information," CRS Report for Congress, Congressional Research Service, 15 February 2006, p. CRS-11.
[20] "White House Conference Call Background Briefing: Executive Order 12958," to Senior Administration Official, Federation of American Scientists, Project on Government Secrecy, 25 March 2003.
[21] Knezo, "'Sensitive But Unclassified' Information and Other Controls," p. CRS-11. The Card memo and supporting documents can be found via the Office of Information and Privacy, U.S. Department of Justice, and is available online at http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm.
[22] Jackie Northam, "Government Documents Increasingly Classified," Morning Edition, National Public Radio, 8 September 2005, http://www.npr.org/templates/story/story.php?storyId=4837061&sc=emaf.
[23] Ibid.
[24] Ibid.
[25] "Innovation in the Federal Government: The Risk Not Taken," Public Policy Forum, Summary of Discussion, Ottawa, Ontario, 6 October 1998, http://www.oag-bvg.gc.ca/domino/other.nsf/html/98sdis_e.html. Canadian researchers found that individuals within a bureaucracy interpret the power to make subjective decisions as a right to break the rules, which are not exactly the types of behavior that we wish to inculcate among our public sector employees. See the ADM Working Group Report on Risk Management, "Innovation in the Federal Government: The Risk Not Taken," 23 May 1999, http://www.innovation.cc/discussion-papers/risk4.htm.
[26] Northam, "Government Documents Increasingly Classified."
[27] Moynihan, Statement before the Committee on Governmental Affairs.
[28] Northam, "Government Documents Increasingly Classified."
[29] Hart and Simon, "Thinking Straight and Talking Straight," p. 44.
[30] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President, 31 March 2005, pp. 22-23, 377-380.
[31] Stephen C. Mercado, "Reexamining the Distinction between Open Information and Secrets," *Studies in Intelligence*, vol. 49, no. 2 (22 May 2006), available online at https://www.cia.gov/csi/studies/Vol49no2/reexamining_the_distinction_3.htm.
[32] "ODNI Announces Establishment of Open Source Center," ODNI News Release No. 6-05, 8 November 2005, http://www.dni.gov/press_releases/20051108_release.htm.
[33] Knezo, "'Sensitive But Unclassified' Information and Other Controls, p. CRS-75.
[34] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 22 July 2004, p. 400.