The Brookings Institution
POLICY BRIEF
September 2003
Policy Brief #125

Related Brookings Resources

- *Protecting the American Homeland: One Year On*
  Michael E. O'Hanlon, Peter R. Orszag, Ivo H. Daalder, I. M. Destler, David L. Gunter, James M. Lindsay, Robert E. Litan, and James B. Steinberg
  (2003)
- "Consolidating Intelligence Analysis: A Review of the President's Proposal to Create a Terrorist Threat Integration Center"
  Testimony by James Steinberg
  Senate Governmental Affairs Committee
  (February 14, 2003)
- "The New National Security Strategy: Focus on Failed States"
  Policy Brief #116
  Susan E. Rice
  (February 2003)
- "The New National Security Strategy and Preemption"
  Policy Brief #113
  Michael E. O'Hanlon, Susan E. Rice, and James B. Steinberg
  (January 2003)

To receive a weekly e-mail about Brookings news, events, and publications, sign up for the Brookings Alert at www.brookings.edu.

The Brookings Institution
1775 Massachusetts Ave., N.W.
Washington, DC 20036

Building Intelligence to Fight Terrorism

JAMES B. STEINBERG, MARY GRAHAM, ANDREW EGGERS

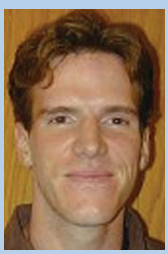
The Bush administration has begun to revise cold war rules governing national security information in order to counter terrorist threats to the United States. The president's homeland security plan calls for new intelligence efforts to protect the nation's borders, defend against threats within the United States, minimize infrastructure vulnerabilities, and improve emergency responses. Congress has given the new Department of Homeland Security responsibility for coordinating these strategies and assuring that accurate and complete information gets to those who need it.

Policymakers must go further to build a new intelligence system to support transformed national security needs. Threats involving unknown perpetrators, methods, and targets cannot be countered with strategies designed for use by federal officials to combat more predictable adversaries. Today, state and local law enforcement, public health, and emergency response personnel are on the front lines of detecting and responding to terrorist threats; corporate managers are responsible for securing key infrastructure such as energy supplies, chemical plants, and telecommunications; and workers and neighborhood residents may hold information that can help prevent attacks.

Cold war intelligence policies aimed to protect sources and methods and keep adversaries from gaining access to military secrets. To achieve these goals, defense and intelligence agencies compartmentalized acquisition, analysis, and dissemination of information, an approach that worked reasonably well as long as policymakers knew who the enemy was,

James B. Steinberg is the vice president and director of Foreign Policy Studies at the Brookings Institution. He is a member of the Markle Foundation Task Force on National Security in the Information Age, from which portions of this analysis are drawn.

Mary Graham is a visiting fellow in Governance Studies at the Brookings Institution.



Andrew Eggers is a senior research analyst in Governance Studies at the Brookings Institution.

what information to look for, where to look for it, and who needed to have it. Analysts became specialists and information was shared among carefully defined groups of federal officials and contractors who were specified in advance and who held appropriate security clearances based on lengthy, costly background investigations.

These policies are ill-suited to the challenge of counterterrorism. Their dual requirements of appropriate security clearance and "need to know" designation inhibit the free flow of information to and from today's diverse community of relevant federal, state, local, and private sector actors.

It is impossible to anticipate "need to know" in a world where enemies are little understood, means of attack are unpredictable, and potential targets are many, diverse, and changing. The need to cast a broad net—to gather information about threats and vulnerabilities from state and local governments and the private sector and return needed information to them—creates a heightened government responsibility to protect core values of openness and privacy.

Since September 11, 2001, the administration and Congress have adopted a number of incremental changes designed to improve the quality and integration of intelligence information. They have broadened government screening of airline passengers, foreign visitors, and imported goods, and added federal resources to state and local public health and emergency communication systems. Incremental changes are not enough. Policymakers must build a new intelligence system to fight terrorism. The formal, hierarchical, and compartmentalized information strategies of the past need to be replaced with a new architecture featuring flexible, decentralized networks of public and private information providers, analysts, and users. Policymakers should establish procedures to assure access to critical information needed to address national security priorities while taking into account openness and privacy concerns. Public guidelines will ensure that new information strategies are consistent with these goals.

ANTI-TERRORISM INFORMATION STRATEGIES

Policymakers recognize that the intelligence system in place before September 11 failed to get the right information to the right people at the right time. As the joint House-Senate committee that investigated the 9/11 attacks observed: "Serious problems in information sharing . . . persisted, prior to September 11, between the Intelligence Community and relevant non-Intelligence Community agencies. This included other federal agencies as well as state and local authorities. This lack of communication and collaboration deprived those other entities, as well as the Intelligence Community, of access to potentially valuable information in the 'war' against Bin Ladin."

To date, administration and congressional efforts to reorganize national security intelligence have focused mainly on reducing barriers to sharing information among federal agencies, improving federal information

technology capabilities, coordinating analysis of federal and local law enforcement and intelligence data, and supporting state and local emergency communication. At the borders, customs officials have enhanced cargo screening using radiation detectors and x-ray scanners and immigration authorities have upgraded checks on foreign visitors using improved databases. Around the country, newly expanded joint terrorism task forces bring together federal and local law enforcement officials. Terrorism investigators more easily combine law enforcement and intelligence data as permitted by the USA PATRIOT Act, which Congress passed one month after the terrorist attacks. Federal airport security officers conduct more rigorous screening of passengers under the terms of the Aviation and Transportation Security Act, enacted two months after the attacks. The new Department of Homeland Security, charged with coordinating domestic intelligence gathering and information sharing, has begun collecting data about vulnerabilities in the nation's critical infrastructure. A new Terrorist Threat Integration Center, under the supervision of the director of central intelligence, is charged with synthesizing counterterrorism intelligence from all sources.

Some of the changes have created serious concerns about potential conflicts between national security measures and principles of personal privacy and government openness. The Defense Advanced Projects Administration (DARPA), which sponsored research into data mining and pattern recognition technologies under its Terrorist Information Awareness (formally Total Information Awareness) program, was temporarily halted by Congress because the sponsors failed to address potential privacy concerns. Civil liberties advocates have challenged administration efforts to harness new information technology to screen airline

FEDERAL COUNTERTERRORISM PROGRAMS

In the wake of the September 11 terrorist attacks, federal officials worked quickly to enact policies that aimed to shore up national security by strengthening efforts to reduce potential terrorist threats and vulnerabilities. Following is a sampling of post-September 11 policy changes:

The USA PATRIOT Act, enacted in October 2001, provides federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence surveillance purposes. It also makes it easier for law enforcement and intelligence authorities to share information gathered through their respective investigations.

CAPPS II (Computer Assisted Passenger Prescreening System), under development at the Transportation Security Administration since January 2002, is a computer program that is designed to use personal information stored in government and commercial databases to identify airline passengers likely to have terrorist ties.

The Critical Infrastructure Information Act, part of the Homeland Security Act enacted in November 2002, creates a new exemption from public disclosure laws for information that the private sector provides voluntarily to the Department of Homeland Security about vulnerabilities in the nation's physical and computer infrastructure.

In his January 2003 State of the Union address, President Bush announced plans for the **Terrorist Threat Integration Center** (TTIC), a new entity under the supervision of the director of central intelligence charged with facilitating information sharing between law enforcement and intelligence agencies throughout the federal government. TTIC began operations May 1, 2003.

TIA (Terrorism Information Awareness): Formerly known as Total Information Awareness, TIA is a DARPA (Defense Advanced Research Projects Agency, an arm of the Department of Defense) program designed to develop information technologies to detect terrorist groups planning attacks against the United States.

Sources: Various federal government sources, including the Congressional Research Service, Federal Register, www.darpa.mil, and www.cia.gov; 2003 State of the Union address; press accounts.

"Policymakers recognize that the intelligence system in place before September 11 failed to get the right information to the right people at the right time."

passengers (the CAPPS II program) and proposals to share personal information about individuals gathered from a variety of sources authorized by the USA PATRIOT Act.

Similar concerns have arisen about conflicts with government openness, especially when secrecy has been expanded without public debate. Soon after September 11, federal agencies removed thousands of pages of public documents about the nation's infrastructure from their websites, including maps of pipeline and water supply locations and data about shipments of hazardous materials and security breaches at airports. In October 2001, Attorney General Ashcroft reversed a long-standing policy under the Freedom of Information Act (FOIA) that required agencies to disclose information unless disclosure would cause "foreseeable harm" and replaced it with one that allows agencies to keep government information secret if there is a "sound legal basis" for doing so. In March 2002, White House Chief of Staff Andrew Card ordered all agencies to adopt guidelines to prevent inappropriate disclosure of "sensitive but unclassified" information. Rejecting a bipartisan compromise, the administration supported a broad new exemption to FOIA in the Homeland Security Act for information voluntarily provided by businesses to the government about infrastructure vulnerabilities that might cause massive casualties or disruptions in a terrorist attack.

Many of these actions were couched as emergency measures—extraordinary steps to counter extraordinary threats. However, nearly two years after September 11, it is clear that they represent important building blocks for a new generation of intelligence policy. The president emphasized in his 2002 national homeland security strategy that "protecting the homeland from terrorist attack is a permanent mission."

More security issues that affect openness and privacy will be decided in the coming months. The administration will determine if additional rules are needed to shield "sensitive but unclassified" information from public view, which might include scientific research, law enforcement records, or infrastructure vulnerability reports. Policymakers have to define policies and procedures for the Terrorist Threat Integration Center as well as determine the future of the Terrorist Information Awareness and CAPPS II programs. Congress has promised to revisit the broad and controversial requirement in the Homeland Security Act that allows the government to withhold information about infrastructure vulnerabilities, and key components of the PATRIOT Act expire in 2005.

A NEW INTELLIGENCE ARCHITECTURE

Defending against terrorism threats will require policymakers to replace the formal, hierarchical intelligence structure with a horizontal, cooperative, and fluid architecture that gets information from those who have it to those who need it through the development of virtual communities of

information sources, analysts, and users. "Hard-wiring" intelligence relationships when actors, methods, and targets are uncertain impairs our ability to adapt to changing threats and vulnerabilities.

Advances in information technology can facilitate this transformation. Internet and teleconferencing technologies allow virtual communities to gather and share information in real time. Instead of focusing on central control, federal officials should spend more time setting priorities, coordinating communication, supplying technical assistance, and assuring data quality. Collecting more information from more sources will require more federal analytical capability to prevent information overload.

ASSESSING INFORMATION NEEDS

The first step in designing an intelligence system to fight terrorism while protecting openness and privacy is to understand what information is needed to support each homeland security challenge. For example, to protect America's borders, we need more complete information about people and goods entering the country. To detect potential terrorist threats within the United States, we need to enhance traditional investigative techniques by cross-referencing databases such as airline reservation records, phone logs, and credit histories with government law enforcement, immigration, and intelligence information. To protect critical infrastructure in areas such as agriculture, food, water, public health, emergency services, telecommunications, energy, transportation, banking, and finance, we need to map vulnerabilities against capabilities of potential terrorists, people who have access to those infrastructures, and the means available to carry out effective attacks. To respond to emergencies, we need two-way communication in real time between first responders and other officials about the extent and nature of the attack, the resources available to respond, and the risk of further terrorist action.

GUIDELINES FOR PROTECTING OPENNESS AND PRIVACY

The long-term acceptance by the American people of an enhanced intelligence effort will depend heavily on the adoption of clear, public guidelines governing the collection, retention, and dissemination of information, and the development of strong procedures for oversight and accountability. Modern information technology can play an important role in helping to implement and enforce these policies.

In principle, no one disputes that anti-terrorism measures should protect the values that anchor democratic processes and personal security in the United States. Introducing his homeland security strategy, President Bush called for protecting national security in ways that keep our fundamental values intact and cautioned that "[w]e should guard scrupulously against incursions on our freedoms, recognizing that liberty cannot exist in the absence of government restraint." He acknowledged that protecting such values might mean accepting a higher level of risk: "Because we must not

"The long-term acceptance by the American people of an enhanced intelligence effort will depend heavily on the adoption of clear, public guidelines."

permit the threat of terrorism to alter the American way of life, we have to accept some level of terrorist risk as a permanent condition."

In practice, however, policymakers must make difficult choices. Guidelines to promote security while furthering openness and privacy should be a matter of public debate and will need mid-course corrections as policymakers and analysts gain experience with new information practices and technologies. The recommendations that follow provide a framework for beginning such a deliberative process.

Emphasize information sharing. Openness can further security. Quickly identifying terrorist threats and infrastructure vulnerabilities calls for cooperative, fluid information networks. Reducing barriers to information-sharing rather than compartmentalizing secrets represents the greatest challenge in fostering such networks. State and local governments, the private sector, and the public have a central role to play in identifying suspicious activities and individuals and in finding and correcting security vulnerabilities. Sharing information about threats and infrastructure vulnerabilities enhances security by multiplying sources of information, empowering Americans to make their own choices about what risks they are prepared to accept, and creating market incentives and political pressures to reduce vulnerabilities.

On the other hand, security or commercial interests will sometimes override a presumption of openness. There may be little public benefit and considerable security risk in revealing floor plans of nuclear power plants or exact locations of military weapons or vaccine stockpiles, for example. In addition, trade secrets, which provide an underpinning for competitive enterprise, should continue to receive careful protection under federal laws.

An analogous situation occurs in the field of computer security, where software companies grapple with the question of whether to alert customers about vulnerabilities that hackers can exploit. Proponents of secrecy argue that revealing security weaknesses invites exploitation of those weaknesses. Proponents of openness argue that public knowledge helps spur solutions and provides users with information to guard against breaches. There is growing support for the idea of making programming code more accessible as a way to enhance overall security.

Maintain high hurdles for sharing personally identifiable information. Sharing personally identifiable information among commercial and government databases raises serious privacy concerns. In many cases the value of intelligence information does not depend on links to identified individuals. Sharing data about imported goods, suspected means of attack, likely targets, critical vulnerabilities, and emergency response plans raises few privacy issues. However, combining databases to screen individuals at border crossings, sharing

law enforcement and intelligence information to identify suspects, "data-mining" to determine suspicious patterns of behavior, and employing commercial databases to screen airline passengers alters the patchwork of privacy protections that has been constructed over many years by private companies, Congress, and the courts. Requests to acquire and share such information should meet threshold tests:

- Intelligence architecture should be designed to minimize privacy intrusions and construct consistent technological barriers that limit users of personally identified information, restrict time periods for information-sharing, or remove personal identifiers altogether until a specified level of evidence is reached.
- Authorizations to access personal data should be subjected to rigorous substantive standards that balance the importance of national security needs against the seriousness of privacy intrusions.
- Access to data should require third party review. Depending on the seriousness of the privacy intrusion, approval could range from a signature by a high-ranking federal official to a court order.
- Data collection, analysis, and feedback should document how authorizations are used in practice, providing a basis for periodic adjustments based on experience.

Protect important secrets. While the emphasis of the new intelligence architecture needs to be on information sharing, important secrets must still be protected. In the cold war context, classifying data as top secret, secret, or confidential protected sources and methods of obtaining information and guarded military plans and capabilities. In the homeland security context, such priorities remain important. But new areas of sensitive information—such as protecting the gene sequence of a lethal pathogen developed in a private lab—call for new approaches to limiting information access.

The traditional system of classification should be strengthened by congressional action to rationalize and update the system to reflect the new threat environment. Important as it is, the nation's protection of national security secrets remains a legal patchwork of mandates created by executive orders and presidential directives. Over time, the classification system has also suffered from overuse. More than two million individuals—mostly Defense Department officials and federal contractors—hold federal security clearances. According to the Information Security Oversight Office, an arm of the National Archives and Records Administration that oversees the classification system, federal agencies still create more than 260,000 official secrets each year and that number is increasing. It is too early to predict the character and extent of new secrets that will be created by four agencies recently granted classification authority by President Bush (the Department of Health and Human Services, the Department of Homeland Security,

"Federal agencies still create more than 260,000 official secrets each year and that number is increasing."

Recent Policy Briefs

- "Higher Education Spending: The Role of Medicaid and the Business Cycle" Thomas J. Kane and Peter R. Orszag (September 2003)
- "Making the Millennium Challenge Account Work for Africa" Lael Brainard and Allison Driscoll (September 2003)
- "Fiscal Millstones on the Cities: Revisiting the Problem of Federal Mandates" Pietro S. Nivola (August 2003)
- "Africa's Economic Morass—Will a Common Currency Help?" Paul Masson and Heather Milkiewicz (July 2003)

Editor
Elana Mintz

Production/Layout
Mary Techau

Vice President of Communications
Stephen G. Smith

The Brookings Office of Communications
202/797-6105
communications@brookings.edu

the Environmental Protection Agency, and the Department of Agriculture).

Increasingly sophisticated tools can help protect sensitive information while assuring appropriate information sharing, such as "tear sheets" (unclassified versions of classified reports) and "metadata" (which can point individuals without security clearances to potentially relevant sources of information without revealing the sensitive information itself).

CONCLUSION

Even if policymakers are careful in defining a new structure for gathering, analyzing, and disseminating national security information, they cannot avoid difficult questions about how to improve security while furthering openness and protecting personal privacy. Vigorous public debate is essential to answering these questions. Clear guidelines, formulated in a deliberative process, can assure public confidence in new policies. Information technology can provide tools to minimize these conflicts, foster collaboration, and help assure that the right information gets to the right people at the right time. Nonetheless, missteps are inevitable. Procedures that provide accountability and oversight can assure that lessons from early experiences strengthen the nation's information strategies to fight terrorism.

Tell us what you think of this Policy Brief.
E-mail your comments to yourview@brookings.edu.

The Brookings Institution
1775 Massachusetts Ave., N.W.
Washington, DC 20036

NONPROFIT ORG.
U.S. POSTAGE
PAID
FREDERICK, MD
PERMIT NO. 225