Welcoming Remarks by Paul Schott Stevens

Paul Schott Stevens, Chair of the ABA Standing Committee on Law and National Security, opened the conference with the observation that the proper relationship of law enforcement and intelligence is one of the most difficult and important issues facing the national security community. "Our security and freedom as Americans," Stevens noted, "have long depended on the ability of government to adapt to changed circumstances and to respond to new threats through new institutional arrangements." The National Security Act of 1947 is a powerful example of this principle in operation. It was in—

Continued on page 2

Panel I

An Overview of a Changing World

Philip B. Heymann, James Barr Ames Professor and Director of the Center for Criminal Justice at Harvard Law School, and former Deputy Attorney General of the United States, provided a broad overview of the issues surrounding the integration of law enforcement and intelligence capabilities. He then introduced the first panel, comprised of David Bickford and Standing Committee members Elizabeth R. Rindskopf and Zöe Baird.

Elizabeth Rindskopf

Elizabeth Rindskopf, who served as General Counsel of the Central Intelligence Agency, Princi-
Stevens—Welcoming Remarks...
Continued from page 1

Stevens maintained that the expedients arrived at through the National Security Act, including the establishment of the Central Intelligence Agency (CIA) and Office of the Director of Central Intelligence (DCI), served the nation well throughout the period of the Cold War. At the same time, the idea of a powerful, secret, foreign intelligence organization has generated considerable controversy. For this reason, one “bedrock” feature of the CIA, made explicit in the National Security Act from the outset, was that it should address enemies foreign, and not domestic, and thus should have “no police, subpoena, law enforcement powers or internal security functions.”

Although the Cold War has ended, national security threats continue to exist, and to evolve rapidly, in the form of international terrorism, and global trafficking in narcotics and in technologies relating to weapons of mass destruction. These threats, Stevens cautioned, are thriving in the “partial vacuum created by the demise, powerlessness and corruption of nation states,” and are “potentiated by the ready availability of highly sophisticated information, communication and other technologies, which until recently were only accessible to the government.”

To combat the threats posed by this “global lawlessness”, the Clinton administration has dramatically increased the role of law enforcement agencies, in particular, the Justice Department and the Federal Bureau of Investigation, and has placed greater reliance on criminal prosecution as a tool of foreign policy. In the process, Stevens suggested, the administration appears to be establishing a broad new mission for the CIA in support of law enforcement. The implications of this new relationship between “American cops” and “American spies” was explored in greater detail throughout the conference. 

Panel I—Overview...
Continued from page 1

Notwithstanding any other provision of law, elements of the intelligence community may, upon the request of U.S. law enforcement agencies, collect information outside the U.S. about individuals who are not U.S. persons. Such elements may collect such information notwithstanding that the law enforcement agency intends to use the information collected for purposes of a law enforcement investigation or counter-intelligence investigation.

The question in issue concerning this legislation, Rindskopf suggested, is aptly captured in the title of a recent article by Stewart Baker, “Shall cops be spies? Shall spies be cops?” Placing the issue in historical context, Rindskopf observed that during the post World War II period, the consensus has been that we should have an intelligence capability, with a central mission and focus, even during peacetime. That consensus resulted in the enactment of

Continued on page 4
Panel II
Political Challenges in the World Environment

The second panel, moderated by Paul Schott Stevens, focused on the political challenges posed by the break up of the U.S.S.R., the loss of national sovereignty and control by nation states, the erosion of national legal systems and the existence of military threats at the subnational level.

Peter W. Rodman

Peter W. Rodman, Director of National Security Programs at the Nixon Center for Peace and Freedom, former Deputy Assistant to the President for National Security Affairs, and author of the recent monograph “America Adrift: A Strategic Assessment,” defended the continued vitality of the “traditionalist” approach to international politics. In Rodman’s view, it is premature to dispense with traditional modes of geopolitical analysis because even though new alignments are forming, many of the same tensions among states continue to exist. By way of example, Rodman cited East-West relations, which are still in a state of turbulence, and which are further complicated by the emergence of China as a major power and the developing alliance between China and Russia, and the resulting transformation of Nixon’s “strategic triangle.” Second, Rodman pointed to West-West relations, including the emergence of Germany and Japan as major players on the world scene, and the development of a common foreign security policy among the members of the European Union. Third, Rodman noted that the Third World is still an area of turbulence, as evidenced by the continued problems posed by Saddam Hussein, Islamic nationalism, and the proliferation of weapons of mass destruction. In responding to these issues, Rodman suggested, there is a need to focus on traditional structures, balance of power, and security as traditionally conceived.

Rodman observed that relationships among the major powers are more precarious than they were five years ago. As a result, if relations turn sour, there may be a recurrence of international conflict, and a decreased ability to collaborate on “new age” issues such as proliferation, global crime, environmental problems and law enforcement challenges. To minimize the threat of such conflict, Rodman suggested we need a better way to deal with China and Russia. In Rodman’s view, we also need to contain trade struggles in the G7 and pursue a common strategic partnership so that economic issues will not lead to the disintegration of political union. In closing, Rodman advocated the “primacy of the political relationship among nation states.” The operational lesson, Rodman suggested, is that there are important areas for international cooperation on trade, law enforcement, international crime and terrorism, but such cooperation is dependent upon a sense of parallel interests. These “new age” interests cannot be pursued in a vacuum. These divergent issues must be integrated into the fabric of broad national security policymaking, and both the diplomats and the geo-politicians have key roles.

Jessica E. Stern

Jessica E. Stern, a Consultant for the Lawrence Livermore National Laboratory, and Former Director of Russian, Ukrainian and Eurasian Affairs at the National Security Council, observed that, ironically, the weakness of the Russian state poses the greatest threat to U.S. national security, most notably in the area of nuclear smuggling.

The good news, Stern suggested, is that the U.S. and Russia have made great strides in their joint programs to upgrade nuclear security systems at Russian nuclear facilities. These programs are known as Material Protection Control and Accounting (MPCA) programs. Second, the evidence suggests that the problem of nuclear smuggling is not so bad. There have only been seven confirmed cases of nuclear smuggling incidents that involve nuclear weapons usable material. This figure is smaller than the number reported in the press due, in large part, to confusion about what is required to make a bomb. Another indication is that, according to U.S. and Russian officials, the sellers appear to be amateurs. Of course, this estimate must be adjusted to account for the fact that amateurs are more

Continued on page 23
Panel I—Overview...
Continued from page 1

the National Security Act of 1947. The Act, as amended in 1949, has a "law enforcement proviso" that prohibits intelligence agents from conducting law enforcement activities. The remarkable thing about the Act, Rindskopf suggested, was that it put into black and white the establishment of a secret intelligence gathering system. The "extraordinary wisdom" of the legislation, Rindskopf remarked, is reflected in the adoption of parallel provisions throughout the world.

During the next period, in the mid-1950s and 1960s, additional structures were created and organized, including the National Security Agency and the National Reconnaissance Organization. Although these structures were created through an appropriate, though relatively unknown, set of legal authorities, problems arose. The reason for this, Rindskopf suggested, was that, historically, intelligence was viewed as a foreign activity, distinct from law enforcement activity, which was considered domestic. These two activities responded, constitutionally and legally, to separate and distinct authorities designated to the President under the Constitution, to execute the laws (domestically), to serve as Commander-in-chief, and to be the principal representative for foreign affairs purposes overseas. Accordingly, the activities of intelligence and law enforcement derived their authority from two different structures. By the late 1960s and early 1970s, a question arose concerning which structure governed activities involving national security and foreign intelligence on domestic soil. This question was answered by the U.S. Supreme Court in the Keith and Truong cases, which established that when intelligence activities occur in the confines of the U.S. domestic structure, intelligence agencies must follow structures established for law enforcement activities.

Following these decisions, the Rockefeller Commission and the Church and Pike Committees conducted "probes" of the relationship between law enforcement and intelligence. By the 1980's, the response to these probes was that the intelligence community: (i) would not do law enforcement; and (ii) would not collect intelligence on U.S. persons on U.S. soil. During this second period, it was thus established that foreign intelligence activities would be confined outside the United States.

In the third period, beginning in the early 1980's, a parallel development occurred overseas as law enforcement became interested in criminal activities outside the jurisdictional boundaries of the U.S.

By way of example, Rindskopf pointed to terrorist activities which our domestic criminal laws could not reach because of extraterritorial limitations. This new development, Rindskopf suggested, legitimized the activities of law enforcement overseas. However, the parameters of the relationship between law enforcement and intelligence were not clearly defined. To be sure, the scandals that developed concerning BNL and BCCI were about two separate and parallel organizations bumping into one another and confusing one another because there were different standards in each organization. To remedy these problems, a number of initiatives were launched to review the interaction between law enforcement and intelligence.

There were three possible solutions: (i) to blend the two services and place them under rules governing the law enforcement community; (ii) to blend the two services and place them under intelligence rules; and (iii) to coordinate the activities of the two services. Ultimately, the decision was made to go forward with great caution. In so doing, the question that remains to be answered is, in the face of new threats, how will the two structures work together, and under which set of authorities?

Zoe Baird

The subject of new threats was addressed by Zoe Baird, Senior Vice President and General Counsel of Atena Life & Casualty Company, current member of the President's Foreign Intelligence Advisory Board, and former member of the President's Commission on the Roles and Capabilities of the Intelligence Community. Baird raised the issue of whether the integration of the law enforcement and intelligence community represents a new field of law,
and a new area of policy concerns, or the same concerns in a different context. What is not new, Baird observed, is the existence of terrorism, chemical and biological weapons, and organized crime. What is new is the fact that the very technology that has allowed the U.S. and others to globalize has allowed terrorists and organized criminals to create global networks for their activities.

With this change in the global nature and scale of national security threats, Baird cautioned, there have been efforts to take advantage of certain civil liberties in the U.S. For example, money for terrorist groups is raised in mosques located in the U.S., funding for terrorist training comes from the U.S., and journals are published in the U.S. that provide instructions about break-ins to computer databases. These types of activities, which were previously considered criminal activities, are now considered national security threats. This raises the question of how to deploy the full resources of the federal government to protect national security without trampling on constitutional protections.

It also requires government to face issues that have been turf issues in the past. Baird encouraged the conference attendees to listen to representatives of the various government agencies, and where appropriate, to challenge proposed solutions to these turf issues. In constructing the framework that will govern the relationship between the law enforcement and intelligence communities, Baird urged all participants to join in the debate, through writing, through dialogue, and through other means.

David Bickford

David Bickford, former Legal Adviser to British Intelligence Services, has been a frequent participant in Standing Committee programs.

"is international, multi-jurisdictional, and executed through high speed communications and encryption." Thus, the response must be tailored accordingly. In Bickford's view, it is essential to deal with this new threat through international cooperation. Hindrances to such cooperation, including political and economic tensions, must be ameliorated by the realization that the greater threat is from the outside. Bickford stated that it is a mistake to think that because the cold war is over, there are no threats. The threat of global crime, he suggested, is as great as the threat of communism during the cold war. This must be taken into account when we balance what we perceive as the threat.

For instance, in the European Community, the concept of Europol (the European Policing organization) to police Europe has been subject to lukewarm attitudes. These attitudes arise from a political self-interest, rather than focusing on the balance against the need for the police force in view of the greater security risks in Europe and the larger concept of the European Union. Any international cooperation is focused on removing the weaknesses of multi-jurisdictional laws and procedures. The international community can no longer afford to defend one legal system as more effective or fair than another. Bickford proposed that extra-territorial jurisdiction over serious crime should become the norm. Although this is an anathema to the U.K., the U.K. is beginning to understand that extra-territorial jurisdiction may be necessary to defeat global crime, including terrorism and money laundering.

"Mutual legal cooperation," Bickford suggested, "must be hastened to harmonize the legal and procedural approach to defeat present threats." Such cooperation should concentrate on abandoning the national law approach and devising a new international law approach, in order to defeat global crime. For example, Bickford proposed the definition of concepts such as "illegal international organization," the introduction of sanctions regimes, the adoption by the G7 of measures permitting the seizure of assets of cartels within their jurisdiction, the examination by the G7 of access to financial markets, and the interdiction of illegal goods and persons conducting criminal activities. In addition,
Panel III
Technical and Practical Changes in the Relevant World Environment

Stewart Baker of Steptoe & Johnson, former General Counsel to the National Security Agency, moderated the third panel, which focused on the emergence of global technologies, the issue of "equal access" to advanced technology by state and private actors, and the challenges for law enforcement and intelligence posed by changes in the size, type and location of national security threats.

Admiral William O. Studeman

Admiral William O. Studeman, USN (Ret.) and former Acting Director of Central Intelligence, asserted that changes in the nature of conflict demand a re-socialization or re-engineering of the security components to address the threats that are transnational, trans sovereign and transjurisdictional. These threats require transnational responses that are multi-sovereign, multi-jurisdictional, multi-capable and multi-coordinated. All of the future forms of conflict will require coordinated action by law enforcement and the traditional national security elements of diplomacy.

Regarding the nature and character of conflict, Studeman observed that traditional kinds of political/military conflict, where a failure in the political area results in the development of a battlefield, may take the form of low-intensity conflict, urban warfare, or even more traditional forms of conflict such as conventional or nuclear war. In Studeman's view, we must have a capability to fight the new spectrum of such wars, and the traditional cold war strategy of forward deployment and fighting these wars on someone else's territory is still a governing strategic component.

Looking forward, however, Studeman noted that one of the major features of large-scale future warfare is going to be the information component of warfare. The future battlefield, Studeman predicted, will be fought not only by military personnel, but also by information warfare resources which will attack and defend critical information components related to "the total society," including finance, banking, revenue control systems, oil, gas, water distribution, power grids, air traffic control, public safety components, electronic commerce, and information networks such as entertainment and media. Advanced states, Studeman stated, are most vulnerable to this type of information warfare.

The second category of conflict identified by Studeman is economic conflict, including industrial espionage, different global ethics, and discordant global norms governing competition. This type of conflict, Studeman maintained, has an information warfare component that impacts economic competitiveness, economic security and economic stability.

The third category of conflict identified by Studeman concerns transnational issues, otherwise known as "global crime" or "global lawlessness." This category includes proliferation, narcotics, terrorism, international organized crime, environmental crime, and illegal immigration.

Studeman observed that the U.S. plays a dominant role in the resolution of such conflicts. Thus, whenever a security issue or conflict occurs, whether it be traditional, economic or transnational, it will be viewed by law enforcement as a "crime" and by the Intelligence Community as a "national security" problem. To respond as a unified nation, Studeman maintained, there must be a re-socialization of law enforcement and intelligence. This re-socialization, Studeman contended, requires a strategy, leadership, discipline, competition, coordination, and compromise on all sides.

As law enforcement expands into new areas, Studeman proposed a number of specific adjustments to facilitate coordination between the law enforcement and intelligence communities. He also advocated the resolution of outstanding law enforcement/intelligence issues, the designation of additional resources for crime prevention, and

Continued on page 10
Luncheon Address by Philip Heymann

"Two Important Mysteries About Terrorism and Their Implication for Law Enforcement and Intelligence"

Philip Heymann presented a provocative luncheon address titled, "Two Important Mysteries about Terrorism and their Implications on Law Enforcement and Intelligence." The first mystery concerned the question of why there has been an increase in the incidence of unexplained or attributed terrorist attacks. Examples include Pan Am 103, the World Trade Center and Oklahoma City, where the perpetrators did not identify themselves, their cause or their motive. The second mystery identified by Heymann is the question of why there have been so few attempts to engage in novel forms of terrorism, such as catastrophic destruction by nuclear, biological and chemical weapons, or through major attacks on infrastructure?

Turning to the first mystery, Heymann proposed two reasons terrorists might engage in terrorism without explanation: (i) the symbolism of the target may define the cause, as with the Unabomber's attacks on modern technology; or (ii) the attack may generate, and thereby demonstrate, chaos or repressive conduct by the target government. The bombing of the marine barracks in Beirut, Heymann suggested, may be an example of the former. Such instances of unexplained terrorism, in Heymann's view, are likely to be government sponsored and retaliatory, or alternatively, non-instrumental expressions of sheer anger. The implication for law enforcement and intelligence is that, when there is no known or acknowledged perpetrator of a terrorist act, we should look to hostile governments, fervent superracial religious groups, and groups that share a common cause with other groups, such as Muslim fundamentalists.

Addressing the second mystery, Heymann observed that, in a real sense, the repertoire of terrorists has not changed in recent years. The three predominant forms of terrorism continue to be assassination, hostage taking (including hijacking), and bombing with conventional explosives. The reasons for this include the lack of capability to use a more sophisticated device, or susceptibility to detection due to fear of retaliation or massive reprisal. Heymann suggested that the implication for anti-terrorism policy is that we must determine how much to spend on protection against, and prevention of, catastrophic terrorism.
Panel IV
Protection Against New High Tech Dangers: Problems of Encryption, Information Warfare, and Computer Theft

Standing Committee member Elizabeth Rindskopf opened part two of the conference and moderated the first panel on information warfare, encryption, national security threats from cyberspace, and related issues.

Stewart Baker

Standing Committee member Stewart Baker set the stage for the discussion to follow with a hypothetical, yet plausible attack on U.S. technical systems in the next decade. He then proposed two reasonable initiatives to defend against such an attack. The first step, Baker suggested, is the development of an ability to monitor and better protect government information systems. This includes the development of an ability to launch our own attacks against our own systems, to respond to those attacks, and to engage agency heads to evaluate those responses.

The second step, Baker suggested, is to work directly with commercial technology providers to improve security for equipment users. This step is predicated on the assumption that the greatest danger of information warfare is not an attack on government systems, but rather an attack on private systems, such as the financial systems, the power grid, and the natural gas system. Although these systems have almost no connection to the defense system, the defense system rests almost entirely on them. Consequently, attacks on those private systems will have a severe impact on the ability of the U.S. to mobilize.

One potential obstacle is the wariness of private systems owners about government interference with the ability of the private sector to do their jobs. In spite of this skepticism by the computer industry, Baker contended that there is a reasonable role for government activity in the private sector in three areas: (i) providing protection against denial of service attacks; (ii) reporting of incidents of attacks on computer systems; and (iii) ensuring there is some minimum recovery capability in the event of an attack, to avoid shutdown of the civilian infrastructure system in the event of a catastrophe.

Standing Committee member and Former National Security Agency General Counsel Stewart Baker warns of the need to protect government information systems from hostile attack.

Ambassador Thomas Graham, Jr.

Continuing the theme of "new dangers," Ambassador Thomas Graham, Jr., Special Representative of the President for Arms Control, Proliferation and Disarmament, observed that in the wake of the bombing of the World Trade Center, there was a new recognition of vulnerability of the U.S. to terrorist attacks on U.S. soil. That vulnerability is exacerbated by the prospect of what would have occurred had the bomb been constructed of plutonium instead of fertilizer. The heightened awareness of this threat has led to renewed focus on the dangers of nuclear, biological and chemical weapons of mass destruction.

Graham suggested that the threat posed by weapons of mass destruction has increased in recent years due to three developments: (i) the collapse of the former Soviet Union; (ii) an increase in efforts by rogue states to acquire weapons of mass destruction; and (iii) a change in the nature of terrorism itself. An example is the so-called "loose nukes" scenario, meaning the danger that poor security over Russia's stockpile will increase the threat of theft and diversion to terrorists and organized crim-
inals. To be sure, the prevention of theft of uranium and plutonium from Russian facilities is one of the most important problems facing the world today. Related concerns identified by Graham include continued efforts by rogue states to acquire weapons of mass destruction, such as Iran's published attempts to acquire fissile materials in the black market and to develop nuclear technology; Saddam Hussein's continued efforts to hide Iraq's chemical, biological and nuclear weapon programs from United Nations inspectors; and uncertainty regarding Libya's commitment to cease production of a chemical weapons plant. In the face of these threats, Graham asserted, it is imperative to prevent these states who support terrorism from acquiring weapons of mass destruction at all costs.

The urgency of this need, Graham contended, is underscored by the trend toward more "indiscriminate killing" without an attempt to claim responsibility for the killing. For example, the cult responsible for the subway bombing in Japan last year, Aum Shinri Kyo, sought to kill thousands of innocent civilians, and made no attempt to claim responsibility or publicity for their actions. Likewise, the perpetrators of the Oklahoma City bombing had no compunction about killing hundreds of innocents merely because they happened to work in a federal building. The modern breed of terrorist, Graham stated, seeks only to kill. If such terrorists gain access to a nuclear device, or chemical or biological weapons, Graham warned, they are likely to use them.

Unlike nuclear devices, which are beyond the capability of all but the most advanced terrorist groups, chemical and biological weapons are surprisingly easy to manufacture or buy. Law enforcement officials investigating the Aum Shinri Kyo compound after the subway attack, for example, discovered that the previously unknown group had a stockpile of chemical weapon agents, had previously staged several small scale attacks that went unnoticed, and were attempting to develop biological weapons. Furthermore, Graham warned, access to such weapons is not limited to large, well-funded groups. In March 1995, a man with ties to the white supremacist group Aryan Nation purchased an organism that produces bubonic plague from a medical supply company in Maryland. Due to domestic implementing laws, which require reporting of such purchases, the vials were ultimately recovered and returned unopened. A similar incident in August 1995 resulted in the apprehension and conviction of two members of a Minnesota militia group for the possession of Ricin, a poisonous protein they produced themselves. The two latter incidents, and the lesson of Oklahoma, is that terrorist attacks are as likely to come from our own citizens as from a foreign band of religious extremists or political radicals.

Ambassador Graham proposed that we take steps to make terrorism less likely, through international agreements that seek to eliminate weapons of mass destruction and to prevent rogue states from acquiring them. Steps to accomplish this objective include the Cooperative Threat Reduction Program to improve the safety of Russian nuclear materials, the ratification of the Nuclear Non-Proliferation Treaty by 182 states; the provisions of the Comprehensive Test Ban Treaty designed to prevent the development of additional weapons and the sale of weapons to rogue states; the commitment of the parties to the Biological Weapons Convention not to produce, acquire or obtain microbiological agents except for prophylactic or peaceful purposes; and the efforts of the Australia Group to impede chemical and biological proliferation by harmonizing production controls and seeking to curb the use of chemical and biological weapons. In addition to the involvement of the U.S. in the foregoing initiatives, the success of the Unabomber and World Trade Center prosecutions demonstrates that the U.S. is ready, willing and able to fight terrorism. In Graham's view, it is imperative that law enforcement and intelligence resources remain committed to this effort.

Continued on page 10
Panel IV—New Hi Tech Dangers...
Continued from page 9

Lee Bollinger

Explaining the constitutional law dimensions of these national security issues, Lee Bollinger, Provost of Dartmouth College, juxtaposed the export control regime for cryptography and the First Amendment. First, he framed the "encryption issue" as follows: If you have cryptography, you must obtain a license from the government as required by export control laws, which creates a prior restraint and arguably violates the Constitution. However, because encryption involves matters of foreign affairs and national security, and because encryption involves technical data, not historical analysis and ideas at the core of the First Amendment, it is beyond the competence of the courts. Furthermore, laws governing encryption are based upon conduct which may be inimical to the interests of the U.S., and therefore falls outside the domain of free speech. These arguments, in Bollinger's view, raise difficult constitutional questions.

The argument that judicial competence is low, Bollinger asserted, is a difficult proposition to sustain because all constitutional questions are difficult to evaluate, and the court has in the past considered matters that involve national security issues. Regarding technical data, Bollinger indicated that the Wigmore vs. Holmes debate has been rejected over the past decade, and the court has rejected any effort to limit the concept of technical data. Professor Bollinger suggested that it is inappropriate to use "intent to do bad things" as a standard for denying First Amendment rights, or to dismiss offensive publication as unprotected "conduct."

In Bollinger's view, it is critical to think about these issues in the interests of building a medium—a system of communication. In the United States, he said, we have a system of free speech. Thus with cryptography, there is an expectation that speech will be protected. In building a medium, therefore, Bollinger concluded that we need to be aware of the bias against new technology and determine how to embrace it within the First Amendment.

Panel III—Technical Changes...
Continued from page 6

better coordination of domestic and overseas resources. In addition, Studeman indicated there is a need to work out an appropriate role for the military, for these conflicts are forms of warfare.

In closing, Studeman maintained that in addressing each of these new areas of conflict, as with traditional conflict, there must be clear chains of command; unified strategies and policies; doctrines, tactics, and technologies; research and development; communications; rules of engagement; special operations capabilities; integrated team work; common and coordinated public affairs and media related policies; and gaming and simulation analysis exercising. Neither the Justice Department nor the law enforcement community is organized to address these "military" issues.

Thus, there is a need for a reorganization of the Justice Department and the law enforcement community to adequately respond to new conflicts. This will require leadership and coordinated intergovernmental action.

Anthony G. Oettinger

Anthony G. Oettinger, Chairman, Program on Information Resources Policy at Harvard University, acknowledged the increased sophistication of information technology, but questioned its relevance. In Oettinger's view, the import of developments in modern technology is that it increases the range of choices. To defend our infrastructure against technological attacks, Oettinger maintained that we need to make choices about priorities, and develop an appropriate strategy. Oettinger contended the development of such a strategy requires an ongoing and painstaking dialogue between the public and private sectors.

Walter H. Pincus

Walter H. Pincus, National Security Affairs Reporter for the Washington Post, agreed with Oettinger about the need to consult the private sector concerning information technology, with the cave-
Panel V
Protection Against the Erosion of Civil Liberties

Richard E. Friedman, Chair of the Advisory Committee to the Standing Committee, moderated a lively panel on the sometimes contentious relationship between intelligence gathering and civil liberties. "The First Amendment," Friedman observed, "is deeply embedded in the U.S. cultural ethos." Although it has withstood attack over the years, First Amendment rights may be threatened by the increased potential for violent acts of terrorism on U.S. soil. The issue before us then, is, whether the response to this threat will jeopardize the First Amendment and free speech. While no clear answer emerged, the divergent views of the panelists set the framework for the debate.

Anthony Lewis

Anthony Lewis, the well known Columnist for The New York Times, and two-time winner of the Pulitzer Prize, criticized certain provisions of the recently enacted Omnibus Counter-Terrorism Act, using historical reference to highlight "disturbing developments" purportedly justified in the name of anti-terrorism. One such example included Fauziya Kasina's flight from Togo with a fake passport to the U.S. in search of political asylum, 9-month imprisonment in an INS jail, and eventual grant of asylum by the U.S. This type of case, Lewis contended, would not result in a hearing today because under the Omnibus Counter-Terrorism Act, the use of a fake passport would require Kasina's deportation to Togo, with no hearing, no appeal, no right of representation, and judicial review barred. This, Lewis lamented, is what has been done this year in our country in the name of fighting terrorism.

The Act has many provisions, Lewis maintained, that "clash" with notions of what is appropriate under the Constitution. For example, the designation by the government of a group outside the U.S. as "terrorist" is not reviewable by any court. Yet, when the designation has occurred, it becomes a crime for Americans or foreigners in this country to support that organization even in lawful, charitable activities. The trouble with this is that the designation may be ambiguous. The African National Congress, for example, was regarded by the U.S. for many years as a terrorist organization. Under the Omnibus Act, Americans would have been prohibited from contributing to this cause. For similar reasons, American church groups would have been prohibited from funneling relief money to El Salvador in 1981.

The new law also prohibits anyone who is a member of such a "blacklisted" organization from obtaining a visa to visit the U.S., based upon mere membership, with no showing of participation in terrorist activity. In Lewis' view, that type of prohibition takes us back to the days of the recently repealed McCarran-Walter Act, which made mere membership in certain organizations a ground for exclusion from the U.S. Further, the Act has "draconian" provisions for deportation of those suspected of connection with terrorist activity or with an organization that has been designated as terrorist. Lewis challenged these provisions as offensive to established principles of due process.

Lewis also criticized provisions of the Omnibus Act relating to federal habeas corpus proceedings, the device by which federal courts may review the constitutionality of the process by which state prisoners are convicted and sentenced. Under existing law, Lewis noted, quite a number of death sentences have been set aside in habeas corpus proceedings because the prisoner had been "railroaded" to his conviction without proper representation or phony evidence, and later proved to be innocent. As recently as May 1995, President Clinton said he would insist that "there be no change in the historic right to meaningful federal review under habeas corpus." Yet, one month later, on the Larry King Show, the President said he agreed that the habeas question "should be tackled in the context of this counter-terrorism legislation."

Two days later, the Senate added a provision to the Omnibus Counter-Terrorism bill that "guts" habeas corpus. This, Lewis stated, is another very disturbing example of what has been done in the name of fighting terrorism.

Continued on page 12
Panel V—Civil Liberties...
Continued from page 11

Yet another provision of the Omnibus Act allows the Attorney General of the United States to certify that a crime such as assault with a dangerous weapon is "terrorism." Assault with a dangerous weapon, Lewis noted, is one of the most common state crimes, and the Omnibus Act permits the Attorney General to convert this crime from a state crime to a federal crime punishable by up to 35 years in a federal prison "merely by asserting that there is some transnational element, e.g. involving drugs transported from Mexico. Lewis maintained that this provision represents the greatest "federalization of state criminal law" in our history.

Lewis acknowledged that there continue to be serious terrorist threats today, but cautioned that "the worse thing we could do in response is to panic into measures that would injure our society, making it less free and less fair." That, Lewis contended, would be to give terrorism a victory. In closing, Lewis reminded us that after Oklahoma City, then Senator Bob Dole remarked, "This is America. This not a police state. So, we want to go very slowly and make sure we do it right." The problem, Lewis opined, is that with the adoption of the Omnibus Counter-Terrorism Act, we didn't do it right.

Kate Martin

Kate Martin, Director of the Center for National Security Studies, took issue with certain provisions of the proposed Intelligence Authorization bill. Although she termed the bill a less direct "assault" on constitutional protections than the Counter-Terrorism Act, Martin maintained that the proposed legislation will "similarly threaten constitutional protections at home" and will be "significantly harmful to the efforts of the U.S. and others to develop some kind of international rule of law throughout the world."

Specifically, Martin criticized the provision of the Intelligence Authorization bill which authorizes the law enforcement community to seek the assistance of the intelligence community in collecting information abroad concerning non-U.S. citizens in criminal investigations. This provision, in Martin's words, would allow the FBI, in its efforts prosecute, imprison and perhaps execute persons who violate U.S. law, to "ask the CIA to conduct the type of illegal wiretapping and burglaries that the CIA conducts overseas and to then use that evidence against that individual in the U.S. court."

Martin asserted that one of the dangers of the bill is that it has been viewed as a classification of the law, instead of a "fundamental shift in the constitutional legal landscape" that may threaten the rights of people at home. In Martin's view, there is a need to recognize that (i) there will be an effect on the rights of people in the U.S. because the fruits of "illegal searches and seizures abroad" may be used against US citizens as long as the US citizens were not targets of the search and seizure abroad; and (ii) it will create pressure on the courts to receive "secret evidence" in criminal trials, e.g. by allowing CIA agents to testify without revealing their identity in court, which will lead to an "erosion of First and Sixth Amendment rights to a public trial in the U.S." and a "gradual enlargement at the behest of the Department of Justice in whether or not secret evidence may be presented in a public criminal trial."

In addition to threats against U.S. citizens at home, Martin contended "it is fundamentally wrong for the U.S. to take the position that foreigners are subject to U.S. criminal laws, that they may be brought here to stand trial and spend the rest of their lives in jail or be executed, but that constitutional protections don't apply to such individuals facing U.S. criminal prosecutions." In spite of established U.S. Supreme Court precedent, Martin thinks that this is a "serious and fundamental policy question that hasn't been adequately looked at by this Department of Justice." She went on to say that in her opinion, it is fundamentally wrong for the Department of Justice to view the Fourth Amendment protections as "some kind of legal inconvenience to effective law enforcement to be avoided when there is a legal argument that could succeed."

Calling the Fourth Amendment and the bill of rights the "wisest tool" to regulate the relationship between the state and individuals, Martin argued that it is appropriate for the U.S. to take that position worldwide, "regardless of what the Supreme

Anthony Lewis addresses the civil liberties panel while Kate Martin looks on.
Court says about the extra-territorial application of
the Fourth Amendment.“ To do otherwise, Martin
argued, would be detrimental for U.S. efforts to
establish the rule of law in emerging democracies.
In her view, the FBI’s “blank check to ask the CIA to
commit illegal acts in furtherance of law enforce-
ment” undermines those efforts.

In closing, Martin remarked that the dangerous
mistrust of government that exists today is fueled
by government secrecy. Although secrecy may be
required to protect sources and methods, Martin
believes that “to the extent law enforcement be-
comes entangled with intelligence, the secrecy in-
voked to protect sources and methods will further
erode public confidence in the fairness and justice
of our criminal law at home and in the government
itself.”

Howard Shapiro

Howard Shapiro, General Counsel of the Federal
Bureau of Investigation, responded to his co-panel-
lists’ concerns about the Omnibus Counter-Terror-
ism Act and the Intelligence Authorization bill.
Shapiro acknowledged that there are indeed genu-
ine constitutional questions raised by the legisla-
tion. The question, however, is whether there is an
appropriate balance, i.e., whether the procedures
put in place to protect against abuses are appro-
siate and sufficient in relation to the need for the
legislation. Shapiro noted that the legislation at
issue was enacted by publicly elected representa-
tives to address the atrocities of the Pan Am 103 and
Oklahoma City bombings. There is a widespread
belief that such measures are necessary. This does
not mean that we should disregard constitutional
liberties, but neither should we throw up our hands
and be paralyzed by our fear of infringing on consti-
tutionally protected rights.

The issue, Shapiro suggested, is far more complica-
ted than what was alluded to by his co-panelists.
Alien terrorist removal, for example, is a difficult,
complicated question. Contrary to the implication,
Shapiro stated that the proceedings under the
Omnibus Counter-Terrorism Act are not “secret,
star chamber proceedings held in the dark of the
night, as in the McCarthy era, by executive branch
officials answerable to no one other than the same
people who are bringing the charges”. On the
contrary, the procedures are the result of a com-
promise that requires in all cases—even when the
greatest threat to national security exists, and even
when information is provided by sources whose
lives undoubtedly will be in danger by providing the
information—that a deportee be provided, at a min-
imum, a summary of all the evidence provided to
the court in a form sufficient (as determined by an
Article III judge) for him to prepare his defense. In
addition, the deportation hearing will be held in
open court and the determination of whether suffi-
cient evidence exists to warrant deportation will be
made by an Article III judge. Admittedly, this is not
the same level of due process protection offered to
criminal defendants, but it is a measure of due
process.

Shapiro conceded that there is a need to find a
middle ground that offers procedural protection. If
Congress and the Executive represent all of us, and
determine that someone is a member of a terrorist
group, we need to consider whether it is unreason-
able to prohibit funding those activities. Arguably,
it is difficult to challenge that prohibition on consti-
tutional grounds, because there is no First Amend-
ment right to conduct terrorist activities. The im-
portant point is that the means must be carefully
 tailored to accomplish the objective.

Responding to Martin’s criticism of Section 17 of
the Intelligence Authorization bill, Shapiro stated
in no uncertain terms that “the FBI is absolutely
committed to the rule of law, both domestically and
overseas.” As crime has become increasingly inter-
national, Shapiro noted, so too has law enforce-
ment. Contrary to Martin’s assertion, the changes
in the new law do not represent a drastic turn-

Continued on page 21
Dinner Remarks

Professor Ernest May

Ernest May, the Charles Warren Professor of History at the John F. Kennedy School of Government, at Harvard University, addressed the question of how to maintain the accountability of the Intelligence Community. Ever since Watergate, May observed, there have been active Congressional oversight committees that have made the Intelligence Community strictly accountable, but only with respect to covert operations and related activities. May estimated that these activities represent only a small fraction of the activities of the Intelligence Community. The principal business of the Intelligence Community, May suggested, “is to acquire and analyze information.” Yet, in this area, there has been very little accounting of what the Intelligence Community has done. May discussed the reasons for this situation, and offered suggestions to improve accountability.

May suggested it is necessary to first define the critical terms used in the Intelligence Community. The two most critical terms in this analysis are “Intelligence Community” and “sources and methods.” He added a touch of humor by noting that the 1864 Webster’s Dictionary defined “intelligence agency” as “an office or place where information may be obtained, particularly regarding servants.”

The core concept of intelligence, as defined in

Encyclopedia Britannica, is information regarding an adversary of a covert nature, to aid in decision-making. In defining the phrase, the Intelligence Community, the key question identified by Professor May is, who is a part of it and who is not?

Intelligence, May observed, has become part of the occupational description of tens of thousands of people, only a few of whom wear uniforms or act in any kind of staff capacity. In our country, there are many organizations in which people essentially do nothing but collect and process information. Implicit in that premise, May suggested, is that intelligence has become something more than a staff service. Yet, it remains difficult to define. Unlike the private sector, which has developed standards for gauging progress, progress in the Intelligence Community is gauged by other criteria. Although the word “community” suggests that people share a common bottom line, intelligence “service” includes only a small part of the Intelligence Community—clandestine service.

This, of course, begs the question. The puzzle is, what makes the Intelligence Community a community? May responded that the answer has to do with the protection of intelligence sources and methods. May noted that the DCI is charged with the protec-

Continued on page 24
Friday’s Introduction: Philip B. Heymann

Philip B. Heymann opened day two of the conference with a recap of the themes that emerged on day one, namely, the political and technological developments that have affected law enforcement and intelligence and related threats to U.S. national security. First, he noted that politically, the changes that led to the dissolution of the former Soviet Union also created a power vacuum which has been exploited by organized crime groups. Second, Heymann remarked that the rapid development of information technology and electronic communication has made money laundering, fraud and other transnational crimes more difficult to detect. Third, computer advances in private industry have made the information infrastructure vulnerable to attacks by computer hackers and hostile information warfare specialists.

With these changes, Heymann observed, there has emerged some disagreement about how to value these “new threats” in relation to the “old threats”, i.e. the dangers posed by other nations on the traditional political, military and economic fronts, versus international organized crime, terrorism and the proliferation of weapons of mass destruction. This disagreement is further complicated by the overlap of old and new threats, and the difficult question of whether the response to such threats infringes upon civil liberties. The balance of the conference centered on the role of the law enforcement and intelligence communities in responding to new and old threats.

Presentation VI—James Woolsey

New Uses for Intelligence as a Necessary Arm of U.S. Foreign Policy

Departing from the panel discussion format, Friday morning’s first session was devoted to a masterful presentation by former Director of Central Intelligence R. James Woolsey, whose association with the Standing Committee dates back to the 1970s.

Currently a partner at the Washington, D.C. law firm of Shea & Gardner, Mr. Woolsey began with a tribute to the Standing Committee, and its efforts, through the conference, to help understand how to balance respect for the Constitution and the Rule of Law with the need for strength against our adversaries. In achieving this balance, Woolsey underscored the need to have a clear understanding of the nature of the threat to U.S. national security, and to avoid the historical tendency to exhibit complacency during times of peace.

In Woolsey’s considered opinion, the greatest threat to U.S. national security today is international terrorism. There are two aspects to this threat. The first, and perhaps the greatest danger, is the development and proliferation of biological weapons. The second is the government of Iran, which

Continued on page 16

Former Director of Central Intelligence R. James Woolsey, whose association with the Standing Committee dates back to the 1970s, discusses new uses for intelligence in the post-Cold War era.
Program VI—Woolsey on New Uses . . .  
Continued from page 15

Woolsey described as "the mother church of international terrorism." Woolsey contended that if we, as a nation, could find a way to address these problems, terrorism through the use of biological weapons and terrorism sponsored by the government of Iran, the threat would be diminished.

Biological weapons, Woolsey cautioned, are easier to manufacture, transport and disseminate than any other type of weapon of mass destruction. Anthrax, for example, could be made by one or two biology students in a lab the size of a microbrewery. The basic culture does not need to be smuggled out of the former Soviet Union; it grows in American cow pastures. The knowledge and the technology to produce it are widely available. Small amounts of the substance yield extraordinary lethality; a large backpack or small suitcase could contain enough Anthrax to kill hundreds of thousands of people. Dissemination is easy: Anthrax could be sprayed from a van or a crop duster. Additionally, because Anthrax is colorless, odorless, has ninety percent lethality and a delayed reaction of several days, it may be used in "false flag" operations, namely, by Iran or Iraq in an attempt to attribute blame to one another.

Turning to Iran, Woolsey described it alternatively as a country that has undergone a "real revolution" in fundamental thinking as well as "the world's leading rogue state." Our problem with Iran, he said, is not one of Islam, fundamentalist Islam, Shiite Islam or even Twelver Shiism. Throughout Iran's history, that set of beliefs has not produced terrorists. The problem, Woolsey asserted, lies instead with a small subset of Iranian clerics, together with the Iranian government, who are very clearly cooperating in the world-wide sponsorship of and commitment to terrorism.

Woolsey described the Iranian regime as one in which assassination orders are issued by senior leaders such as Ayatollah Khomeini and Hashemi Rafsanjani, and he termed "credible" reports that Iran was attempting to arrange for the assassination of Yasir Arafat. Iran, he noted, has major programs in all of the weapons of mass destruction fields, including biology. And, the Iranian government acts abroad through sponsorship of such groups as Hezbollah, Islamic Jihad and Hamas. For example, much of the problem in Northern Iraq may be attributed to Iranian support of BKK, the Kurdish terrorist group. In Woolsey's experience, there is a substantial body of information today suggesting that the support, enthusiasm, doctrinal underpinnings and encouragement of a substantial degree of international terrorism stemming from the mideast may be traced to Iran. It has become increasingly difficult to identify the source of terrorist acts, however. Unlike terrorist groups who seek to cause specific political events to occur, such as the IRA, ETA and Basque terrorists, modern terrorist groups, including the large number inspired by religious extremism, do not claim responsibility. As a result, many of the traditional investigative techniques and deterrence objectives do not work. On a more positive note, Woolsey described Iranian society as far from monolithic, and suggested that public discontent with Iranian clerics may impel the clergy to return to its traditional role.

In fashioning an appropriate response to the problem of international terrorism, Woolsey asserted that the United States must learn from history and take an active role. In the 1950's and 1960's, he recalled, the United States—in a sense of despair that nuclear war would inevitably follow a Soviet attack—failed to take steps to bolster conventional defenses in Europe. By contrast, in the 1970's and 1980's, the peace and stability that existed in Europe was substantially enhanced when the United States abandoned that view and began to effectively and thoroughly modernize its conventional forces in Europe. A similarly active initiative is required, in Woolsey's view, to address the problem of biological weapons.

On the international front, Woolsey advised that the United States must convince Germany and France that their so-called "critical dialogue" with Iran is not in the world's best interest. The United States must take a firm stand on this issue, and push hard to weaken the Iranian government, to make possible the transition of the Iranian government into something consonant with the splendid traditions, history, culture and religion of the Iranian people. This, Woolsey concluded, is not only in our

Continued on page 22
Panel VII

Law Enforcement and Intelligence

The final panel of the conference convened experts from the Department of Justice, the Central Intelligence Agency and the State Department. It was moderated by John H. Shenefield, former Chair of the Standing Committee and partner in the Washington, D.C. offices of Morgan, Lewis & Bockius.

Mark Richard

Mark Richard, Deputy Assistant Attorney General of the Criminal Division at the U.S. Department of Justice, described the history and evolution of the relationship between law enforcement and intelligence. Richard recalled when he began his career at Justice decades ago, there was a "high, impenetrable wall" between the law enforcement community and the intelligence community. At the time, intelligence agencies determined whether to make criminal referrals to law enforcement, law enforcement had little extra-territorial jurisdiction and few agents abroad, and there was no mechanism for handling classified intelligence information in the courtroom. Today, there is a procedure for the intelligence community to refer cases to law enforcement where there is criminal complicity, there are many law enforcement agents working abroad, and the Classified Information Procedures Act provides a statutory framework for the activities of law enforcement and intelligence. This latter development, Richard remarked, was a tremendous advancement in clarifying a variety of ambiguities.

Those ambiguities came to light in the late 1980's, as law enforcement expanded its territorial jurisdiction and intelligence agencies became involved in terrorism and drug trafficking, which were once solely the domain of law enforcement. The BNL and BCCI scandals publicly exposed the coordination and logistical problems presented by the existence of CIA intelligence on criminal activity by management of international financial institutions. Other problems included the question of who had responsibility going forward, and the determination of what material had to be disseminated under the Brady rule. To address these problems, a joint CIA/DOJ task force was created. The task force resulted in a report authored by Richard and then-CIA General Counsel Elizabeth Rindskopf which catalogued key communication problems to be resolved, and presented options for the Administration to consider. From Richard's perspective, the problems between the CIA and the Justice Department no longer exist.

According to Richard, the relationship that needs to be addressed going forward is not the relationship between law enforcement and intelligence, but rather, the relationship between law enforcement and the State Department. Specific issues that need to be addressed relate to leadership, operational rules and the sharing of information. Today, Richard observed, there are three players—the State Department, the intelligence community, and law enforcement—all

Continued on page 18
Panel VII—Law Enforcement . . .
Continued from page 10

focusing on different aspects of the same issues: international crime, international narcotics trafficking, proliferation and terrorism. At times, there are competing equities and competing interests. There are also issues of process, legal restrictions on dissemination, and ultimately, the question of who has the final authority to make decisions on critical issues. Resolving these issues is the challenge for the future.

Jeffrey Smith

Jeffrey Smith, then General Counsel of the Central Intelligence Agency and now partner in the Washington, D.C. law firm of Arnold & Porter, addressed the extent to which intelligence capabilities should be available to law enforcement. Generally, Smith expressed support for an interactive relationship between the intelligence and law enforcement communities, within established guidelines. Those guidelines must be respected to ensure that the CIA does not become, and is not perceived as, a law enforcement agency. The creation of JICCLE, Joint Intelligence Cooperation and Coordination with Law Enforcement, represents one measure intended to accomplish this purpose. Other measures include personnel exchanges of veteran CIA and FBI representatives, training of CIA station chiefs and FBI attaches, sharing of technology research and development including surveillance technology and analytical skills, biweekly meetings at the deputy level concerning coordination issues, and regular "Gang of Eight" meetings concerning operational issues.

Notwithstanding the successful implementation of the foregoing programs, Smith cautioned that there are lingering concerns over the appropriate role of intelligence in the law enforcement business. One concern is centered on the debate over whether prosecution of criminal matters should take precedence over intelligence and foreign policy objectives, or vice-versa. While the two objectives are not mutually exclusive, Smith called for a balancing approach based on the "true national interest." Another concern has to do with activities directed against American citizens. To avoid the abuses documented in other countries where domestic intelligence services functioned as secret police, Smith warned that any activities against Americans must be properly authorized and controlled through established channels. Finally, Smith noted that the two agencies will continue to have fundamentally different missions. Consequently, there are good reasons to keep the activities of the two agencies separate. From the perspective of the intelligence community, the concern about discovery requests by defense counsel compromising sources and methods, and the concern that CIA participation in law enforcement proceedings may lessen judicial deference to the agency in other matters, provide strong incentives for the intelligence community to proceed with caution in law enforcement matters.

In closing, Smith paid a tribute to the men and women of both the intelligence and law enforcement communities who take great risks, quietly and heroically. These individuals, Smith lamented, are subject to tremendous pressure and criticism. By necessity, i.e., because of the need for secrecy, their successes are ignored. Due to circumstance, i.e., an operation gone awry, their failures are overblown. For the record, Smith certified that in his personal experience, the good deeds performed by these individuals clearly outweigh the few, albeit public, mistakes that have been made over the years.

At the time of the conference, Standing Committee member Jeffrey Smith was General Counsel to the Central Intelligence Agency. He returned to private law practice shortly thereafter.
Michael A. Vatis

Michael A. Vatis, Associate Deputy Attorney General, addressed the coordination between law enforcement and intelligence, focusing on actions taken by the Justice Department in response to the Richards-Rindskopf report and JICCLE process. First, Vatis explained, the Justice Department has created "focal points" within the organization to interface with the CIA. Second, new procedures have been implemented to govern requests for U.S. intelligence community file searches that incorporate Brady obligations and alignment theories. Third, a rule has been adopted requiring law enforcement agencies to provide notice to prosecutors when there is an intelligence interest. Fourth, measures have been implemented concerning the treatment of the identity of intelligence officers whose names are classified as any other classified information under CIPA. Fifth, new procedures have been implemented to protect classified information in instances where CIPA would not apply, in immigration cases, for example. Sixth, a new Memorandum of Understanding between the Attorney General and the intelligence agencies outlines the circumstances under which the agencies must report criminal activity to the Justice Department. Finally, an intercommunity training plan has been developed to facilitate coordination. The foregoing measures, Vatis asserted, has enabled the law enforcement and intelligence communities to function more effectively together.

There are, however, two outstanding issues that need to be resolved. One concerns the so-called "tasking" issue, which Vatis termed a misnomer to the extent it implies law enforcement may "task," or require, intelligence agencies to obtain certain information for law enforcement. In fact, Vatis explained, the proposal seeks only to "authorize" the intelligence agencies to collect information for law enforcement, should they deem it appropriate and of sufficiently high priority. The other issue concerns the circumstances under which law enforcement agencies should provide information obtained in criminal investigations to the intelligence community. If, for example, the FBI conducts a terrorism investigation abroad, it may obtain information of interest to the intelligence community. However, the FBI may be reluctant to share such information due to concerns about relinquishing control of its investigation, or providing information that may lead to a parallel intelligence investigation which may prompt Brady requests or discovery obligations once a prosecution is brought. While this is more of a policy issue than a legal issue, Vatis emphasized the need to find a way to provide the necessary coordination, and sharing of information, without having a negative impact on a law enforcement investigation or prosecution.

Vatis concluded that there has been a great deal of progress over the past two years in resolving a number of these difficult and sensitive issues. However, there is still a long way to go in implementing these policies, and in ensuring that the policies "trickle down to the field" and result in a change of attitude.

Jonathan Winer

Jonathan Winer, Deputy Assistant Secretary of State for International Narcotics and Law Enforcement Affairs, discussed the unique but com-

Continued on page 22
Luncheon Address

Deputy Attorney General Jamie Gorelick

The conference concluded with an address by Jamie Gorelick, Deputy Attorney General of the United States. Gorelick observed that since the end of the Cold War, there has been some overlap in the function of the law enforcement and intelligence communities, most notably in matters involving terrorism and narcotics. This development has raised a number of new issues relating to tasking, information sharing, and coordination. The next new frontier, Gorelick predicted, will be law enforcement and intelligence coordination to defend the United States against information warfare.

As the economy has become more efficient, Gorelick observed, so too has information technology. While this sophistication brings many benefits, it also makes the United States vulnerable to computer attacks by hackers and narco-terrorists. Presently, NASA and the airforce have the greatest expertise in cyberspace, and the Justice Department has recently created a computer crimes/intellectual property section to emphasize the importance of this new issue. However, the U.S. security apparatus is ill equipped to deal with this new threat, and from a law enforcement perspective, the difficulty of identifying the source of the attack or the identity of the hacker raises difficult jurisdictional problems.

By way of example, Gorelick recounted the recent break-in to a sophisticated Defense Department computer system by an Argentine national. Using a “sniffer” program, Navy investigators first traced the hacker to the faculty of the Department of Arts and Sciences at Harvard University, only to learn that the computer there was only used as a transmitter center, to disguise the identity of the attacker. After obtaining the first-ever court order permitting a wiretap into the computer system to survey incoming communications, investigators set up a monitor and produced an electronic profile which included the sites invaded by the hacker. Investigators then traced the hacker to Buenos Aires, where he was apprehended with the assistance of the Argentine police.

The question that arises in the type of scenario outlined above is, whose jurisdiction does this incident fall within, law enforcement or intelligence? Our legal construct does not answer this question because it was written for a different age. The answer is contingent upon specific facts. However, the facts are not clear until the operation is well underway. Gorelick suggested that the key is to remember why the law enforcement and intelligence institutions have separate missions, and to avoid the abuses of the 1960’s and 1970’s that gave rise to the Church and Rockefeller Commissions. Legal attaches and CIA officers serve different functions abroad, and in Gorelick’s view, it is unreasonable to expect CIA officers, who are not trained to collect evidence admissible in U.S. courts, to conduct law enforcement investigations. The ability of intelligence officers to collect information concerning criminal investigations is further restricted when such investigations involve U.S. citizens abroad or activity on U.S. soil.

More generally, Gorelick objected to the transfer of funding for the National Drug Intelligence Center from the Defense Department to the intelligence community, on the ground that it violates the law enforcement proviso of the National Security Act. She also questioned the debate concerning the provision of the Intelligence Authorization bill permitting the intelligence agencies to investigate non-US persons abroad even if the purpose is to assist law enforcement. In Gorelick’s view, the provision does not raise Fourth Amendment issues and does not violate the law enforcement proviso. In coordinating the activities of law enforcement and intelligence, Gorelick concluded, we must be vigilant to ensure that we do not bring intelligence into areas where it does not belong.
Panel V—Civil Liberties . . .
Continued from page 13

around. Previously, as long as there was an independent intelligence purpose, intelligence could gather information on terrorism and narcotics and share that information with law enforcement and other appropriate agencies. There is a change in the language of the law, but this remedy has been available for four years, and Martin's "parade of horribles" has not occurred. With rare exceptions, secret CIA witnesses have not testified in proceedings brought by law enforcement agencies. Shapiro observed that the reasons for that continue to exist. The intelligence community has the same sources and methods concerns about gathering information, the rules of evidence have not been changed, and any evidence that "shocks the conscience" is not admissible.

The more relevant hypothetical presented by Shapiro is, if a foreign national commits a heinous crime in the US and then retreats abroad, and the FBI is unable to locate that person, should the FBI be permitted to ask the intelligence community for assistance in locating the person, so the FBI can then go to their liaison partners and through the normal process of law, apprehend the person and bring them to trial in the U.S. with the same constitutional protections that exist for all criminal defendants in U.S. criminal courts? Or, should "imagined dangers" prevent one arm of the U.S. government from obtaining the assistance of another arm of U.S. government? In the end, Shapiro concluded, it is the joint efforts of the law enforcement and intelligence apparatus that will lead to the apprehension of fugitives.

Harvard Professor Anthony Oettinger (right) addresses the third panel as Washington Post reporter Walter Pincus looks on. Both discussed national security implications of modern technology.

Panel III—Technical Changes . . .
Continued from page 10

at that the private sector is only partially informed about intelligence issues. Regarding the nature of the threat, Pincus disagreed with other panelists in his view that new threats are somehow less dangerous than the threats that existed during the Cold War, most notably, the fear that the future of the world lies in the nuclear balance. Even so, he acknowledged that the threats are more complex, and therefore, the new mission of law enforcement and intelligence requires adjustments, particularly in personnel and priorities. In conclusion, Pincus remarked that "peace is hell" because we are having a difficult time determining who our enemies are, and identifying issues that are important, but not devastating.

Standing Committee on Law and National Security

Chairman: Paul Schott Stevens
Advisory Committee Chair: Richard E. Friedman

Staff Director: Holly Stewart McMahon
740 15th St., NW
Washington, D.C. 20005-1009
(202) 662-1035
fax: (202) 662-1032
e-mail: natsecurity@abanet.org.
PANEL I—Overview . . .

Continued from page 5

Bickford suggested that the resources of NSA and GCHQ should become part of the legal process when necessary.

In Bickford's view, there is a need for intelligence and law enforcement to join forces in the fight against organized crime. This has been accomplished in the U.K. through legislation which permits MI5 and the police to join forces in efforts to combat organized crime. This legislation, borrowing heavily on the Classified Information Procedures Act, includes procedures designed to allow intelligence to be brought into the criminal process, while at the same time protecting sensitive information that is not relevant to the process at hand.

In closing, Bickford cautioned that we must not let the new threats cloud our judgment about how they may be recoured. The evil men in the international community have taken an early lead in realizing the advantages to them in the new age. These same advantages are available to the international community. "If these advantages are appropriately exploited," Bickford suggested, "there is no reason that the twenty-first century should not be as peaceful as the last." 

Panel VII—Law Enforcement . . .

Continued from page 19

plementary roles of law enforcement agents, intelligence officers and diplomats in combatting international crime. While each entity has its own critical mission, Winer argued that due to practical and jurisdictional constraints, law enforcement requires the resources of the intelligence community and the State Department.

Winer suggested that the containment policies of the Cold War, which sought to promote democracy and stability, provide useful models for developing programs to combat transnational crime. Just as the Communists infiltrated political systems, Winer suggested, organized criminals groups recruit and corrupt individuals in countries in transition, which results in dysfunctional or corrupt institutions. One focus of the State Department is to counter this trend through cross-border programs to strengthen indigenous institutions and create regulatory and enforcement structures to go along with the economic changes taking place in foreign countries.

The nature of the threats identified by Winer include organized alien smuggling, drug trafficking, stolen car activity, money laundering, massive international fraud, theft of natural resources in countries undergoing privatization, bribery and corruption, theft of intellectual property, and environmental dumping of toxics and pollutants. These issues, Winer pointed out, are transnational, and require the law enforcement, intelligence, and diplomatic communities to work closely together.

Turning to one of the key themes of the panel, Winer opined that the technical capabilities of the intelligence community can better support law enforcement objectives. However, the benefit to be derived from that support is dependent upon the resources devoted to the effort. The unique strength of the intelligence community, in Winer's view, is its understanding of the institutions and people of other countries, and its appreciation for the vulnerabilities exploited by criminal organizations. Winer suggested that the intelligence function should create a topographic map of international criminality to assist law enforcement efforts. Winer cautioned against the practice of "stovepiping" where agencies contain information in their own pipe instead of sharing with other agencies. To effectively penetrate cross-border networks operating throughout the world, Winer asserted that cooperation and coordination among the various agencies is essential.

Program VI—Woolsey on New Uses . . .

Continued from page 16

interest, but in the world's interest as well.

Domestically, Woolsey suggested there are a number of steps we can take to substantially reduce the threat of terrorism. He expressed concern about Congressional opposition to anti-terrorism proposals such as requiring tracing agents, known as taggants, in explosives, and cautioned that inaction now could lead to over-reaction in the wake of a terrorist incident. To avoid this, initiatives must be implemented before a crisis erupts. Woolsey also cautioned against overburdensome human rights screening criteria for human asset recruits, and challenged the view that it is somehow improper for intelligence case officers to recruit informants abroad who are not "nice" people. Such prohibitions, Woolsey argued, are akin to telling the FBI to penetrate the mafia through the PTA, without the assistance of crooks. Just as the mafia consists almost entirely of crooks, Woolsey observed, Hezbollah consists almost entirely of human rights violators. Finally, Woolsey endorsed efforts by the Department of Justice to secure lawful access to digital telephony and related communications, and he called for a partnership between pharmaceutical companies and the federal government to address the threat of a biological or chemical attack against
likely to be caught than professionals. U.S. and Russian officials also agree that there is little evidence of consumers, a contention Stern was skeptical of. The final bit of good news in this area, Stern suggested, is that there is little evidence of organized criminal involvement.

The bad news relayed by Stern is that there are hundreds of cases of radiological theft. This issue is extremely serious, given the capabilities of these materials in committing terrorist incidents. Moreover, there is very clear evidence that despite the progress of U.S. and Russian programs to improve nuclear security, security is still abominably weak at Russian facilities. There is also some evidence of involvement by Iran and Iraq in the nuclear weapons black market, and there is some evidence of involvement by organized crime. Other dangers identified by Stern include high level corruption in the former Soviet Union, smuggling of nuclear related weapons in contradiction of international law, porous borders, the rise of powerful international criminal groups with connections to the highest levels of former Soviet government, and the apparent willingness of buyers to pay high prices for controlled nuclear related materials.

Stern noted that the nuclear non-proliferation regime is based on the assumption that the difficulty of producing nuclear weapons and acquiring fissile materials will constrain nuclear proliferation. This assumption, Stern suggested, is undermined by the availability of rudimentary nuclear weapons design, in books and on the Internet. Thus, the single remaining reliable barrier to proliferation is the difficulty of acquiring nuclear fissile material. The implication is that there is a very real danger that terrorists will gain access to chemical, radiological or nuclear weapons and direct those weapons at U.S. targets.

Regarding the reasons for these developments, Stern focused on the supply side, attributing cause to chaos, crime, corruption and collapse in Russia. Russia, Stern observed, is undergoing a crisis of statehood in its transition to a law-based federal state, and thus resembles a collapsed state in several respects, including the devolution of power from the central authority to the regions, the devolution of power from the ruler to his Cabinet, and splits in the military. In the face of such “lawlessness,” it is important to develop carefully considered rules and regulations governing nuclear weapons. Second, it is important to produce a credible inventory of Russian nuclear materials. Third, it is essential to develop the rule of law. Given the dangers posed by the threat of proliferation, Stern concluded that the imposition of law and order in Russia may be more important than the establishment of democracy and civil rights.

natsecurity@abanet.org

Standing Committee on the World Wide Web

In an effort to provide quality and timely information to our members and friends, the ABA Standing Committee on Law and National Security has ventured onto the World Wide Web. The web page will house the most updated information about the Committee’s activities.

Current and past editions of the National Security Law Report can now be read online. Each issue will be indexed for easier reading.

Want to find out who is speaking at our next breakfast program, on what subject, when, and where? Don’t want to wait to receive the mailing? Then go to our web site and find out—and mark those dates on your calendar.

Keep abreast of upcoming conferences, learn the latest changes in speakers, or get a report on past programs—just by accessing the Standing Committee’s web page. For example, if you missed the presidential showcase program on Law Enforcement and Intelligence at the 1995 ABA Annual Meeting, a detailed report is available on the web.

Do you have suggestions about our web page or recommendations for future breakfast speakers or conferences programs? Send us e-mail at natsecurity@abanet.org. But first, check out our web page at: http://www.abanet.org/natsecurity.
Notwithstanding efforts to enhance accountability, the prevalent view is still that there is no accountability at the CIA. May suggested that there is a way to improve public perceptions without jeopardizing intelligence sources and methods. One solution proposed by May is for the DCI to be charged by statute to produce a fully documented Annual Report describing: (a) what the community has done, and providing information on the analysis and use of intelligence; (b) what investments are being made in the collection and analysis of intelligence by the community in the future; and (c) what investments are not being made, and why.

May acknowledged that some information contained in the Annual Report, including supporting documentation, would be highly classified. Thus, May proposed that the Annual Report be subject to review and comment by those agencies presumed or alleged to be served by the Intelligence Community. Third, May also recommended that the Annual Report be crafted so that it could be in the hands of the public as soon as possible, which means that certain parts of the report would need to be put up right away for declassification. Some parts, of course, would remain classified to protect sources and methods. Other parts would be declassified. In time, it would be available to everyone, so historians could determine if explanations are consistent with what was done at the time.

Objections anticipated by May include risk, opportunity cost, and high transaction costs. Such objections, however, must be weighed against the importance of the end. May expressed the view that in a democracy, every element of the government should be accountable to the public. At present, however, except for activity relating to covert action, our Intelligence Community is accountable in principle but exempt in practice from accountability. May concluded that the ABA should push to ensure that the Intelligence Community is fully accountable.

---

Special Words of Thanks

The Standing Committee is deeply grateful to three of its members—Philip Heymann (who first conceptualized the program), Zoë Baird, and Elizabeth Rindskopf—who planned, organized, and made important presentations during this conference. Because of the high esteem in which each of them is held by the law enforcement and intelligence communities, they were able to attract the leading figures in the nation to help make it such a success.

We are also in debt to Advisory Committee member Pamela Jimenez, who volunteered to prepare this issue of the Report.

— Paul Schott Stevens
Chairman