TESTIMONY OF JAMES B. STEINBERG, VICE PRESIDENT AND DIRECTOR OF FOREIGN POLICY STUDIES, THE BROOKINGS INSTITUTION

NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

"INTELLIGENCE AND NATIONAL SECURITY POLICY"

OCTOBER 14, 2003

The attacks on September 11, 2001 awakened the people of the United States and the world to a profound shift in the international landscape; a shift that was well underway long before that tragic date. At least since the end of the Cold War in the late 1980s, the principal challenge to American security no longer came from established states whose interests were adverse to those of the United States. Instead, the most immediate and serious threats were those associated with the forces of disorder, closely connected to the process that has loosely been called "globalization."

Globalization has had a deep impact on American security for two important, inter-related reasons. First, the rapidly accelerating movement of people, goods and ideas has contributed to blurring the boundaries between nations and increasing the vulnerability of the American homeland to threats from abroad. Second, the disruptive effects of change and modernization have challenged traditional beliefs, and social and political orders around the world. Globalization has brought with it many dramatic benefits, not only to people in the developed world, but also to those struggling to emerge from poverty and deprivation – as we see in China and India today. But it has also provided new opportunities for dangerous actors, such as terrorists, international criminals and drug traffickers. The technologies of globalization, especially modern communications and the Internet, have been an important factor in heightening these risks, allowing these dangerous actors to cause harm at a distance, to operate across the world in small, easily concealed cells, to communicate surreptitiously, and to spread their ideology of hate globally. And the growing availability of increasingly deadly technologies to non-state actors further exacerbates the danger.

As the 1990s unfolded, senior political leaders in the United States and abroad increasingly came to recognize both the opportunities and threats of this new world. In 1995, on the occasion of the fiftieth anniversary of the signing of the United Nations Charter, President Clinton said

> Our generation's enemies are the terrorists and their outlaw nation sponsors -- people who kill children or turn them into orphans; people who target innocent people in order to prevent peace… Their reach is increased by technology. Their communication is abetted by global media. Their actions reveal the age-old lack of conscience, scruples and morality which have characterized the

> forces of destruction throughout history. Today, the threat to our security is not in an enemy silo, but in the briefcase or the car bomb of a terrorist. [1]

The next year, in March, representatives from 29 countries and institutions (including leaders from the Middle East, Europe, United States, Japan, Russia and Canada) met in Sharm-el-Sheikh, Egypt in an anti-terrorism summit following a wave of suicide bombings in Israel. Later that summer, the G7 in Lyon decided to focus on the problems of global terrorism and crime, including through the creation of the Lyon Group to provide an on-going mechanism of international coordination.[2]

Here in the United States, under President Clinton and his National Security Advisor, Sandy Berger, we began to focus on how to organize ourselves to meet these new challenges, through actions such as the issuance, in May 1998, of Presidential Decision Directive-62 (PDD-62), which established the position of National Coordinator for Security, Infrastructure Protection and Counter-terrorism,[3] and PDD-63, which mandated the establishment and implementation of a national plan to protect critical infrastructure. This was accompanied by substantial increases in funding for counter-terrorism activities.[4] These efforts intensified following the attacks on our embassies in Kenya and Tanzania in 1998, leading to the disruption of a number of terrorist cells and organizations, and culminating in the truly extraordinary effort surrounding the thwarting of attacks associated with the Millennium celebrations.

Despite these important actions on both the national and international level, the success of the September 11th attacks has appropriately forced us to confront the question of what more we must do to meet these new challenges in the future. Of course, we cannot expect to have 100% success in preventing all acts of terrorism – there are too many inherent advantages to the "offense" to achieve that goal. But it is equally clear that the institutions, policies, procedures and mindsets that were developed to meet the threat posed by the Soviet Union or other potential state adversaries are poorly suited to meet a radically different challenge. As President Lincoln said in his message to Congress in December 1862, "As our case is new, so we must think anew, and act anew."[5]

---

[1] Clinton, William Jefferson. "Remarks at the United Nations 50th Anniversary Charter Ceremony." United Nations' 50th Anniversary Closing Ceremony. Opera House, San Francisco. 26 June 1995.

[2] "We proclaim our common resolve to unite our efforts and our determination to fight terrorism by all legal means. In keeping with the guidelines for action adopted by the Eight in Ottawa, we strongly urge all States to deny all support to terrorists. We rededicate ourselves and invite others to associate our efforts in order to thwart the activities of terrorists and their supporters, including fund-raising, the planning of terrorist acts, procurement of weapons, calling for violence, and incitements to commit terrorist acts. Special attention should be paid to the threat of utilization of nuclear, biological and chemical materials, as well as toxic substances, for terrorist purposes." G7. Declaration on Terrorism 27 June 1996. Lyon: G7, 1996.

[3] PDD-62 built on an earlier effort to strengthen interagency coordination in PDD-39, issued in 1995.

[4] Non-classified spending for counter-terrorism doubled from $5.7 billion in 1996 to $11.3 billion in 2001. See Benjamin, Daniel and Stephen Simon. The Age of Sacred Terror. New York: Random House, 2002: 248.

[5] Lincoln, Abraham. "Annual Message to Congress." Washington, DC. 1 December 1862.

To understand both why we must change, and how we must change, it is useful to reflect on some of the differences between the Cold War challenge and what we face today. The tasks involved in the fight against terrorism, in many ways, are far more difficult than the intelligence challenge we faced during the Cold War. At that time, we faced a known enemy. We knew generally what to look for, and where to look for it, although we had to deal with our adversaries' attempt to conceal crucial information from us. For the most part, the information we needed was overseas, and largely concerned military activities, limiting our need to collect information in the United States, or about US citizens. Most of the expertise and knowledge resided in the federal government, and the actions needed to be taken rarely involved the public, the private sector or state and local officials.

All of this has now changed. Today, terrorists threaten us both at home and abroad. They have no fixed address, and only occasionally are their identities – or their targets or means -- known. Technology and globalization have made it easier for would-be terrorists to bring dangerous people and weapons into the United States and to conceal their activities. Globalization has also meant that the American presence abroad is more widespread, increasing the number of possible targets. Key information that we need to detect and prevent terrorist attacks lies in the private sector – at airlines and flight schools, with operators of chemical plants and high-rise buildings, with local police and community doctors – and we must increasingly count on the private sector to take the actions necessary to prevent attacks or deal with their consequences.

As a result, we must build a new approach – at both the national and international level -- that reflects these changes. And at the heart of the new approach is how we use information. I use the word information, rather than intelligence, to suggest that we are dealing not simply with information acquired (most typically, clandestinely) by the government, but with a much broader array of data and knowledge, some of which is public, and much of which is held by the private sector.

The reason that information plays such a principal role is closely connected to the nature of the threat. In traditional state-to-state conflict, it was easier to prepare to defend against an attack – the direction and source of attack were clear, as was what we needed to defend against an attack. Even if the adversary gained the advantage of surprise as with Pearl Harbor or the 1973 Middle East War, the ability to recover, counter-attack and prevail remained. Over time, especially with the advent of weapons of mass destruction (WMD), knowing the adversary's intent as well as capabilities grew increasingly important, as our preoccupation with measures to deter or survive a pre-emptive Soviet first strike illustrate.

But the marriage of non-state actors and weapons of mass destruction have, as President Bush rightly recognized in his 2002 National Security Strategy,[6] dramatically altered the

[6] "But new deadly challenges have emerged from rogue states and terrorists…the nature and motivations of these new adversaries, their determination to obtain destructive powers hitherto available only to the world's strongest states, and the greater likelihood that they will use weapons of mass destruction against us, make today's security environment more complex and dangerous…Given the goals of rogue states and terrorists, the United States can no longer solely rely on a reactive posture as we have in the past. The

importance of preventing attacks (even though we cannot afford to neglect measures to mitigate the harm of attack and improve our ability to recover). Thus prevention in all its forms takes on a new urgency, which in turns heightens our dependence on information. And, as the controversy over the intelligence regarding WMD in Iraq has shown, the quality of that information also becomes increasingly important.

Over the past year, I have had the opportunity to serve on the Markle Foundation Task Force on National Security in the Information Age, whose first Executive Director was Philip Zelikow, now Executive Director of this Commission. The purpose of the Task Force was to examine how best to mobilize information to assist in meeting new security challenges. Although my remarks today draw heavily from the work of that Task Force, the specific conclusions and recommendations I offer today are my own.

The new approach must have the following key "design" characteristics, which reflect the character of the threat we confront.

1) The handling of information must be decentralized, modeled on a network approach (just as our adversaries have modeled their actions on a network approach).
2) Our strategy must focus on prevention. Although apprehension and conviction of wrong-doers may in some cases contribute to prevention, a prevention mind-set must dominate.
3) The line between "domestic" and "foreign" threats is increasingly difficult to sustain, and our approach must avoid rigid structures and procedures based on this distinction.
4) The range of actors necessary to this task inevitably will extend beyond what can be contained in any single department or organization.
5) The network must reflect the fact that most of the key actors are not in the federal government, but in state and local government, and in the private sector.
6) Because the problem of terrorism is transnational, our approach must integrate the need for wide-scale international cooperation.
7) Since the effort to combat terrorism is a long-term problem and is designed to protect our way of life and our values, as well as our security, the policies and actions undertaken must have the support of the American people.

What do these principles mean in practice?

First, we must continue to increase the priority we give to sharing information. In the Cold War security/intelligence architecture, we placed a premium on the security of information. We developed a system based on elaborate background investigations as a predicate to obtaining security clearances, then layered on the requirement of "need to know," tightly controlled compartments to limit the number of individuals with access,

---

inability to deter a potential attacker, the immediacy of today's threats, and the magnitude of potential harm that could be caused by our adversaries' choice of weapons, do not permit that option." The National Security Strategy of the United States of America September 2002. Washington: The White House, 2002. 13-15.

and implemented strong procedures that allowed the agency that initially acquired the intelligence to control further dissemination. This system assumed that it was possible to know a priori who "needed to know" and that the risk of inadvertent or malicious disclosure was greater than the benefit from wider information sharing.

This architecture and the underlying assumptions are ill-suited to today's challenge. The events of September 11th have starkly demonstrated the dangers associated with the failure to share information, not only within the federal government, but more broadly between the federal government, state and local governments and the private sector – a key conclusion of a Congressional Joint Inquiry.[7] Therefore, we must open up the system to state and local agencies and officials, providing not just access but technology and money as well. We must allow the two-way flow of information between government and the private sector. We must build the technology architecture and tools that facilitate sharing and interoperability, and we must take into account the needs of the users, as well as the originating agency in deciding whether to control where the information goes – all the while ensuring that both the need to protect the security of sensitive information and civil liberties are addressed.[8]

Second, we must think more radically about the way in which the federal government approaches its role in the collection, analysis and dissemination of information related to homeland security. For historical reasons, we established a sharp dividing line between foreign and domestic intelligence, and assigned responsibilities for these activities to two separate agencies (the Central Intelligence Agency and Federal Bureau of Investigation). The USA PATRIOT Act took a first step toward recognizing the costs of that separation to the effectiveness of the counter-terrorism mission, and the creation of the Terrorist Threat Integration Center (TTIC) this year is a further step toward breaking down these walls. But we have not yet gone far enough to recognize the seamlessness that must prevail across the domestic/foreign line. This has two important organizational consequences.

To begin with, we need a single individual with responsibility (and accountability) for all intelligence related to the counter-terrorism mission. There has been considerable debate in recent years about the desirability of strengthening the Director of Central Intelligence (DCI)'s authority over the entire intelligence community. For the most part, this debate has focused on the tensions between the Pentagon and the DCI over control of intelligence resources and assets. But today, an equally compelling argument can be made that a true Director of National Intelligence (DNI) is needed to integrate the full

---

[7] "Serious problems in information sharing also 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." House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. Report of the Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001. Washington: GPO, 2002.

[8] A more detailed set of principles can be found in the Markle Foundation Task Force on National Security in the Information Age. Protecting America's Freedom in the Information Age. Washington, DC: Brookings Institution Press, 2002. 17-19.

spectrum of intelligence-related functions both at home and abroad with respect to counter-terrorism. This would include not only the activities of the traditional intelligence community (Defense Intelligence Agency, the services' intelligence agencies, State Department's Bureau of Intelligence and Research, and the CIA) but also the FBI (which is active both in the United States and, increasingly, abroad), and the various intelligence activities of the Department of Homeland Security (not only in the sphere of the Under Secretary for Information Analysis and Infrastructure Protection, but also the Secret Service, Coast Guard, etc.) The DNI should be given meaningful powers beyond coordination, to include significant authority over budgets and operational priorities and practices. Through the creation of a DNI, we can assure a more integrated and interoperable system of intelligence to deal with counter-terrorism.[9]

In addition, on the policy side, we also need better integration of the domestic and international operations.

Prior to the creation of the Department of Homeland Security (DHS), there was a compelling rationale for a White House-driven coordination of homeland security efforts, given the extraordinary dispersal of functions across over some 70 or more agencies of the federal government. Today, DHS consolidates some 60% of homeland security activities, but there is clearly a need for a coordinating mechanism to address those functions -- both domestic and foreign -- that are not in DHS.

To date, there have been some valuable strides made to coordinate the efforts of the National Security Council (NSC) and the Homeland Security Council (HSC), through strengthening the role of the dual-hatted Deputy National Security Advisor for Combating Terrorism**,** particularly for sharing relevant counter-terrorism information among operational agencies. But it is less clear that this coordination translates into effective efforts to integrate the operational activities of security agencies operating both domestically and internationally, particularly the Department of Defense; and there is still no meaningful effort to coordinate funding priorities across the domestic/foreign line. The ability of the HSC to resolve conflicts among its members is much weaker in practice than that of the NSC; its functioning is comparable to other White House policy councils, such the Domestic Policy Council, which is not surprising given the relative infancy of the HSC. In the intelligence sphere in particular, the HSC voice is limited compared with the NSC, especially with respect to priority setting and policies.

Prior to the creation of DHS, I, along with a number of colleagues proposed a different model for organizing the homeland security effort.[10] Rather than creating a multi-function DHS, we suggested a much smaller consolidation, involving only the border protection agencies, while achieving the broader coordination through a strong, statutory body in the White House. Today, we have an approach that falls between two stools – a massive

---

[9] A number of thoughtful observers have proposed the creation of a Director of National Intelligence, including members of Congress through the Report of the Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001 (cited above), and former National Security Advisor, General Brent Scowcroft.

[10] See Protecting America's Freedom in the Information Age, Ch. 7.

consolidation of many agencies in DHS that has proven difficult to implement, but one which still leaves 40% or so of the homeland security effort outside its jurisdiction, and a relatively weak HSC.

There are two alternatives to remedy this deficiency. One would be to strengthen the role and authority of the HSC and the Assistant to the President for Homeland Security. The second, and I believe preferable, approach, now that DHS has been created, would be to strengthen the role of the Secretary of DHS as the principal point of coordination for internal homeland security functions, while vesting the overall responsibility for coordination between domestic and foreign aspects of homeland security in the NSC (rather than dividing that function between the HSC and NSC). Today, the Secretary of DHS is seen as simply one among many Cabinet Secretaries, rather than the individual who is accountable for the entire homeland security effort. Strengthening the Secretary's role in the inter-agency process could help alleviate this problem. Giving the NSC overall responsibility for coordination between the domestic and foreign policy agencies is appropriate since the mission of the NSC is national security; and it would be strange indeed if the principal national security threat we face today was seen as only partially within the ambit of the NSC. Of course, there are legitimate questions concerning whether this places an insupportable burden on an already heavily engaged NSC process, but I believe that the advantages of integration outweigh those costs. As a practical matter, the primary day-to-day responsibility would lie, as at present, with the Deputy National Security Advisor for Combating Terrorism, but she would be fully backed up by the well-established NSC processes.

Third, if prevention is the primary focus, there are serious reasons to doubt whether it can be effectively achieved by vesting responsibility for both domestic intelligence collection and operational activity in a law enforcement agency. The FBI and Director Mueller have made admirable efforts to overcome the legacy of a law enforcement-based organization and mindset, but all of these are second best to recognizing that this mission is distinct from law enforcement. Using law enforcement tools as the focus of the counter-terrorism effort has disadvantages both from an effectiveness and a civil liberties standpoint. Constraints on building a case that will stand up in a criminal procedure may cause delay or failure to take actions which could prevent harm but might undercut a criminal case (e.g. tainting evidence, tipping off criminals). Moreover, the law enforcement "case" orientation is ill-suited to the much more fluid world of prevention, where both the identity and the target of the terrorist may not be known. Because the criminal system is associated with consequences (such as the deprivation of liberty), the danger to civil liberties from an expanded role of the FBI is also greater.[11]

For this reason, a separate domestic security organization is needed, which can focus on prevention, and help overcome the artificial foreign/domestic divide. This is a choice made by most developed democracies, such as the British who have the MI-5, which is involved in foreign intelligence activities related to threats to the homeland. Such an

[11] For a similar view of these problems, see Center for International Security and Cooperation and Eisenhower National Security Series. Intelligence and Prediction in an Unpredictable World: Summary of Conference Proceedings, June 20-21, 2003. Alexandria, VA: ENSS, 2003: 2-3.

agency can be subject to clear rules, which can be established for the protection of civil liberties. (I discuss this in greater detail, below.)

There are three possibilities for where such an agency could be located: in the Department of Justice but separate from the FBI; in the DHS; or as an independent agency. While each could work, I believe the best solution would be for it to be located within the DHS so as to connect it better to other homeland security functions, such as border and infrastructure protection. However, if it is created as a separate agency reporting to a DNI, it would have the advantage of independence from all policy agencies.

Fourth, whatever organizational strategy is adopted, it is critical to empower the relevant government agencies to do what is necessary to protect the homeland, while maintaining the trust of the public. Recent controversies over government data mining and access to personally identifiable data, such as over the Pentagon's Total/Terrorism Information Awareness (TIA) program and JetBlue's data sharing with an Army contractor, illustrate the nature of the problem. Today we face the dangerous possibility of having the worst of two worlds: the public fears that the government has a "fishing license" to acquire sensitive personal information regardless of its value to counter-terrorism, while government agencies are afraid to do anything lest they end up on the front page of the newspapers.

To untangle this dilemma, we need a set of rules and guidelines concerning government acquisition and use of data about individuals and their activities, so that both government officials and the public clearly know what is permitted and what is not. Although the details of these guidelines may need to be classified to protect sensitive methods, the basic principles should be a matter of public debate and Congressional oversight. New technology tools can build accountability into the system, embedding agreed policies into the technology, and assuring that accurate, accessible records are maintained of information collection and use. These tools must be accompanied by on-going training of personnel, which in many ways is the most important means of assuring that rules are observed in practice.[12]

Fifth, we must deepen international cooperation as a core element of our counter-terrorism strategy. International cooperation serves two vital purposes: it leverages our ability to take on adversaries who are spread across the globe; and it broadens the political legitimacy behind our counter-terrorism efforts, which is essential to the long-term success of defeating this adversary.

Over the past decade, we have seen a significant enhancement of international cooperation, beginning with the Lyon summit in 1996, and accelerating in the wake of 9/11. Nonetheless, more can be done. At the Prague NATO summit, the NATO allies

[12] In the first Markle Foundation Task Force report, we identified some basic principles that should govern these guidelines. See Protecting America's Freedom in the Information Age, pgs. 32-34. A forthcoming report of the Task Force will offer a more detailed framework.

agreed to increase counter-terrorism cooperation, including intelligence sharing.[13] This is an important opportunity to use NATO security procedures to overcome chronic information sharing problems (particularly from the United States to other partners), and create a more effective two-way street for intelligence, which will enhance the willingness of others to cooperate with us. Similarly, recent steps by the European Union to strengthen Community-wide counter-terrorism efforts (including the establishment of a common arrest warrant) offer another valuable channel for information sharing and cooperation.[14] Another important avenue for greater intelligence cooperation is the Administration's recently launched Proliferation Security Initiative (PSI), designed to thwart transnational transfers of WMD materials and technology. Although the PSI has gotten off to a promising start, reliable information sharing policies and procedures will be essential, not only to facilitate international cooperation, but also to assure partners that any preventive measures undertaken by participants in the PSI are warranted by facts.

Congress has a critical role to play in assuring that we develop a sound information strategy for dealing with counter-terrorism, both from a policy and resource perspective. Recent Congressional reorganizations have been an important step in recognizing the central role of homeland security and the need for an integrated effort. The creation of the two homeland security appropriations subcommittees provides an opportunity for an integrated look at resources across agencies, while the House Select Committee on Homeland Security also provides a venue to examine cross-cutting policy issues. These committees also offer a forum for vitally needed oversight.

From an information/intelligence perspective, the House and Senate Intelligence Committees have a particularly vital role. The House Permanent Select Committee on Intelligence has already created a subcommittee on terrorism and homeland security, which offers a focused opportunity to address some of the issues that the Commission is addressing today. In particular, I think it is essential that both Intelligence Committees move forward to address the adequacy of our current information architecture, and the degree to which we have taken full advantage of modern information technology to support counter-terrorism. In addition, I believe as a matter of urgent priority, the two committees should address the question of what guidelines and procedures are needed to make sure that officials and agencies get the information they need to do their job, in a way that instills confidence in the American public that the information is being used for appropriate purposes. I do not suggest that such guidelines themselves need to be statutory, although I believe it would be appropriate for Congress to enact a requirement that such guidelines be developed on a government-wide basis, and certainly Congress should play an active role (through both public and closed hearings) in overseeing the implementation of executive branch guidelines.

---

[13] At the summit, NATO allies agreed to "Endorse the agreed military concept for defence against terrorism. The concept is part of a package of measures to strengthen NATO's capabilities in this area, which also includes improved intelligence sharing and crisis response arrangements." North Atlantic Treaty Organisation. Prague Summit Declaration. Brussels: NATO, 2002.

[14] For a more detailed assessment at US-EU cooperation on counter-terrorism, see Steinberg, James B. "An Elective Partnership: Salvaging Transatlantic Relations." Survival, Summer 2003 45 (2): 135-136.

Thank you for the opportunity to testify before the Commission, as you carry out this vitally important work.