LESSONS LEARNED AND UNLEARNED:

THE TENTH ANNIVERSARY OF SEPTEMBER 11, 2001

THE RICHARD A. CLARKE 2011 NATIONAL

SCHOLARLY MONOGRAPH CONTEST

Sara Bjerg Moller

Ph.D. Candidate, Department of Political Science

Columbia University

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

INTRODUCTION 5

On the "Lessons" of History 5

THE PRE-9/11 PICTURE 10

PROTECTING THE HOMELAND 13

Our Cities and States 13

Disaster Response and Management 13

Safeguarding Critical Infrastructure 17

Electricity Grid 18

Oil and Gas Refineries and Pipelines 20

Transportation: Ports, Rail, and Aviation 21

Chemical, Biological, Radiological, and Nuclear (CBRN) Threats 23

Borders and Immigration 24

Homegrown Radicalization 25

Civil Liberties 26

Government and Intelligence Overhaul 28

AMERICA ABROAD 30

Afghanistan/Pakistan 31

Iraq 32

Public Diplomacy 33

Al Qaeda After Bin Laden 33

POLICY RECOMMENDATIONS 34

NOTES 37

EXECUTIVE SUMMARY

This monograph addresses both the lessons learned from the September 11, 2001 terrorist attacks and the challenges remaining in providing for America's security at home and abroad. Progress in securing the American homeland to date has been uneven. Alongside the well-publicized successes are numerous failures highlighting the incomplete implementation of many of the 9/11 Commission Report's recommendations. To borrow a phrase from U.S. officials, although we are safer, we are still not safe. A number of recent plots perpetrated by individuals should have been detected by U.S. immigration and intelligence agencies but were not. The threat from homegrown radicalization is growing, posing a new and different challenge to our national security infrastructure.

One of the principle lessons of 9/11 is the importance of crisis planning. Periodic reviews, updates, and field exercises - while costly to perform - are vital in federal, state, and local government's ongoing efforts to protect Americans. The first – and perhaps most important - lesson, in other words, is that preparedness works. Other lessons learned from 9/11 have been unlearned or not learned well enough, such as the importance of interagency communication and collaboration among government and intelligence agencies. Ten years after 9/11, communication failures are habitual and interagency cooperation remains a challenge.

On the foreign policy front, much work still needs to be done to restore America's image abroad in the aftermath of the Iraq War. The upcoming withdrawal of combat forces from Iraq and Afghanistan pose numerous diplomatic and counterterrorism challenges. Our relations toward Yemen and Pakistan also require careful review.

The *2010 Quadrennial Homeland Security Review Report (QHSR)*, the first of its kind, warned of a danger of complacency as major crises recede.[1] Our understanding of national

security must continue to evolve and adapt to new threats while remembering the lessons already learned at such a high price. Although we now stand ten years removed from the events of that fall day, the importance of getting the lessons right remains as critical as ever.

INTRODUCTION

The terrorist attacks on September 11, 2001 claimed 2,750 lives and represent the deadliest single day attack on American soil.[2] Aside from the magnitude of the loss of life, the terrorist attacks were qualitatively different from other bloody episodes in American history. The attacks of September 11 took place on the homeland, via a unique mechanism of destruction, during a period of supposed peace (although war had been declared on us by Osama Bin Laden in 1996, we did not yet fully realize the full significance of his declaration,) by an enemy many had never heard of. An entire country and people awoke on that September morning to find itself under attack, its sense of invincibility and optimism seemingly shaken forever. Ten years on, the time is now right to re-examine the lessons from all that has followed since.

ON THE "LESSONS" OF HISTORY

The twentieth century has borne witness to a number of historical turning points whose memories and lessons are recalled with ease by reference to a specific place or date: September 1938, December 7, 1941, 13 days in October 1962, August 1964, or November 9, 1989. September 11, 2001 (hereafter 9/11) joins this august list in the chronicles of American history. As with those earlier watershed moments, 9/11 has become the subject of much intense debate by policymakers and scholars as to the appropriate lessons to be drawn from the tragic events of that day. Occurring as it did so soon after the millennium, the attacks and the era it ushered in have become a natural demarcation in American history. Almost overnight, the media and public began referring to events in terms of "before" and "after" September 11. The date has become a starting point, or end point, depending on how one looks at it.[3] Among the images invoked by the attacks were those of an earthquake or lightning bolt, geological phenomena with scars visible

long afterwards. Common to many declarations in the aftermath of the attacks was the sense that everything had changed. Congressman Adam Schiff (D-CA) summed up the prevailing mood when he stated, "on September 10, the danger from terrorists was imminent, and we took no action. On September 11 we were devastated. Now it will forever be September 12."[4] Amidst this attempt to come to terms with what had happened there was a rush to define the new era and give it a name. Some suggested the coming conflict be called "al-Qaeda's war," others the "long war." One Washington commentator dubbed it "World War IV."[5] No tagline perhaps better encapsulates the changes that have occurred in the years since than the simplicity and power of the phrase the 'post-9/11 world'. After the events of that morning, the world did indeed look different.

In divining lessons from 9/11 we would do well to borrow a page from earlier attempts to derive lessons from other equally momentous and era-defining episodes in American history. Although the lessons to be drawn are different for each, these historical watersheds remain similar in one major respect: what comes after and how it is interpreted by future generations of policymakers and scholars is sometimes as important as the initial historical event itself. Witness Munich. More than any other name or place, Munich illustrates the power of historical lessons. No other historical event of the twentieth century has been invoked as often - and with as much fervor - by policymakers as that of the Munich Conference of September 1938. Historians and political scientists have long debated the use (and misuse) of the Munich analogy. The "lesson of Munich," as one commentator put it, has become "the defining lesson" of modern history. For some, like historian A.J.P. Taylor, Munich was a triumph in British diplomacy; the best a declining and unprepared power that lacked the cards for a difficult game could do.[6] For others, Munich represents the "fatal delusion" of "the idea that safety can be purchased by throwing a

small state to the wolves."[7] Under this view, Munich is proof extraordinaire that appeasement does not work. Ever since that September more than seventy years ago, American leaders have recalled the lessons of that fateful fall during times of key foreign policy decisions. Successive presidents including Truman, Kennedy, and Johnson all evoked the "lesson of Munich" during their administrations. The latter with force when defending his decision to carry on the war in Vietnam declaring, "We learned from Hitler at Munich that success only feeds the appetite of aggression."[8] Ronald Reagan similarly explained his decision to bomb Libya in 1986 by saying, "Europeans who remember their history understand better than most that there is no security, no safety, in the appeasement of evil."[9] Precisely what the lesson (or lessons) of Munich should be however is still widely contested today.

Immediately prior to the terrorist attacks of 2001, the American government's attention was focused on a number of other lessons. Before 9/11, then Director of the Policy Planning Staff Richard Haass said, the United States "still lived the messy 'lessons' of Vietnam, Somalia and Bosnia…That changed on the morning of September 11."[10] As we know now, Al Qaeda derived its own lessons from many of these same events, viewing our rapid departures from Lebanon and Somalia as proof the U.S. was a paper tiger.

True to precedent, the always-popular Munich analogy resurfaced with fervency in the months and years immediately following the attacks. Nor were America's leaders the only ones to draw parallels to the 1930s. Only a few days after the attacks British Foreign Secretary Jack Straw urged Parliament "to draw lessons from the experience of the 1930s." "We all know," Straw continued, "the consequences of what followed." Prime Minister Tony Blair similarly insisted, "All our history, especially British history, points to the lesson that if international demands are not backed up with force, the result is greater insecurity."[11] The analogy became

increasingly popular in the run-up to the Iraq War in 2003. Testifying before Congress Defense Secretary Donald Rumsfeld summed up the lessons of the 1930s as one of mounting evidence of the capabilities and intentions of Hitler that went ignored. "The historical record of appeasement," Rumsfeld stated, "is a sorry one. And in an age when terrorists and dictators are seeking nuclear, chemical, and biological weapons of mass murder, we need to consider the lessons of history."[12] Across the Atlantic, meanwhile, British historians were busy debating whether the coming war more closely resembled the events of 1939 or the Suez Crisis of 1956.[13]

Other historical lessons were also invoked in the aftermath of September 11. The analogy of an earlier strategic surprise, the Japanese attack on Pearl Harbor in December 1941, occupies a similar pride of place alongside that of Munich in the lexicon of policymakers. September 11th's association with Pearl Harbor began almost immediately. Within hours of the attacks, Senator Chuck Hagel (R-NEB) announced, "This is the second Pearl Harbor."[14] Evoking as it did memories of another surprise attack on the country half a century earlier, Pearl Harbor seemed the perfect precedent for what American had just experienced with the terrorist attacks. "The events of September 11," President George W. Bush reminded the world in 2003 while on a visit to Poland, "were as decisive as the attack on Pearl Harbor and the treachery of another September in 1939."[15]

As the shock of the terrorist attacks faded and the country turned its attention to the possibility of war with Iraq, yet another historical analogy emerged. In debates leading up to the war several members of Congress cited the lessons learned by an earlier generation of American foreign policy experts in Vietnam. The ghosts of Vietnam featured prominently in debates over the Resolution for Authorization for the Use of Military Force Against Iraq in the House and Senate in October 2002.[16] With members of Congress from both parties drawing on the lessons

of both Munich and Vietnam to buttress their arguments, the debate over what form America's post-9/11 foreign policy should take descended into a "battle of the history lessons." The exchange led Senator James Inhofe (R-OK) to exclaim, "Are they more concerned about a war that took place over 30 years ago, or the tragic events that took place on September 11?"[17]

Just as contemporary policymakers have viewed the lessons of Munich and Vietnam through the lenses of the present, so too we risk future generations viewing the lessons of 9/11 through the prism of the events of their day. But if Munich teaches us anything it is that the analogies derived from it are often inapplicable to other situations. The same is true of 9/11. Lessons can become history in themselves and quickly overshadow the events they harken back to.[18] The lessons we draw from this tragic day in American history and the subsequent events that have followed must not fail prey to the fate shared by the Munichs or Vietnams of earlier generations, to be dusted off anew during every new major foreign policy debate and unveiled as talking points. Nor should the lessons contained in this monograph be overlooked. Instead, they should be seen in their proper light, as a nation's response to an unprecedented attack in an era of relative peace.

For over 60 years, the Munich analogy served as the basis of American security policy. Ten years removed, we run the risk of the memory of 9/11 becoming similarly abused. Our charge, in other words, is not to be consumed by our history; to know when the lessons of 9/11 bear remembering and when a new threat requires a new outlook. Alongside this warning of the danger of misperception or misapplication of the lessons of 9/11 follows another cautionary note to pay attention to what others hold to be the lessons of that day. Our failure to heed Osama Bin Laden's numerous declarations of war against America is partly what brought us to that day ten years ago. It would be equally dangerous now to disregard the lessons that America's enemies

have taken from the events since. The same is true of America's allies, many of whom have derived their own lessons from their participation in the American-led War on Terror.

Similarly, we would do well to remember that the terrorist attacks proved to be such a decisive turning point in American history not only because of the nearly 3,000 people who lost their lives that day but also because of what followed: bloody and costly wars in Afghanistan and Iraq, the collapse of America's standing abroad, and a national debt out of control. The challenge before us now is not only to derive the right lessons from 9/11 but also to derive lessons from these lessons.

A mere three days removed from the attacks on New York City, Washington, D.C., and Shanksville, Pennsylvania, President George W. Bush spoke of our responsibility to history at a remembrance ceremony held at Washington's National Cathedral. Back then he said our responsibility was clear: "to answer these attacks and rid the world of evil."[19] Ten years on our responsibilities to history have grown. To the lessons of September 11 we must now add the lessons of Afghanistan and Iraq.

THE PRE-9/11 PICTURE

The purpose of this section is to provide a brief overview of the information leading up 9/11. As has been well documented elsewhere, several government agencies had pieces of information pertaining to the hijackers' plot but failed to put them together or share them with others in the federal government, the result of a longstanding culture of secrecy and institutional turf battles. Multiple investigations have singled out the nation's intelligence services, in particular the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI), for failing to work together to protect America from the looming terrorist threat. The 9/11

Commission Report noted that the CIA and FBI both had opportunities to unravel the plot on at least four separate occasions in 2001.[20] Although mistakes were clearly made, one of the many tragedies of September 11 is how close the hardworking men and women of our intelligence services came to discovering the real purpose of the 19 hijackers' presence in our country.

As early as 1999, the National Security Agency (NSA) intercepted communications indicating an Al Qaeda operational cadre was on route to Kuala Lumpur and planning something big. Although the trail of three of the hijackers was eventually lost in Thailand, the CIA learned in early 2000 that at least one of the men was now living in the Los Angeles area. The CIA failed to place the names of his traveling companions on the State Department's TIPPOFF watch list or notify the FBI of these developments.[21]

The increased volume of threat reporting in the intelligence community in the summer of 2001 indicated something was afoot. Although the number and severity of threat reports was unprecedented at the time, the still transitioning Bush administration was slow to take in the seriousness of the threat despite efforts by several outgoing Clinton administration officials to make them do so. The Federal Aviation Authority (FAA) and other relevant government agencies were briefed on some of this intelligence but were not given additional directions or told what plans should be instituted and their resources never mobilized as a result.

In mid-August, the Minneapolis FBI Field Office launched an investigation of Zacarias Moussaoui, a French national who had overstayed his visa and had begun flying lessons at Airman Flight School in Norman, Oklahoma the previous February. In the days that followed, FBI agents in Washington and Minneapolis debated whether there was enough evidence to seek a Foreign Intelligence Surveillance Act (FISA) warrant to search Moussaoui's computer. Such a search could have yielded evidence of connections to Al Qaeda and the wider hijacking plot.[22]

Among the more troublesome findings from investigations into the 9/11 attacks was the discovery that several hijackers entered the country under suspicious circumstances and overstayed their visas, living amongst us in the weeks and months before they struck.[23] According to the 9/11 Commission, at least two of the hijackers' passports were manipulated in ways known to be associated with Al Qaeda. More troublesome, the Commission stated that visa applications submitted by three hijackers contained false statements that could have been proved false at the time of application.[24] Two of the hijackers, Mohammed Atta and Marwan Al-Shehhi, were able to persuade agents from the Immigration and Naturalization Services (INS) to grant them admittance after returning from a trip overseas in January 2001 so that they could continue their flight training even though they lacked student visas.[25] In March 2002, six months after the attacks, the INS sent the flight school that Atta and Al-Shehhi attended in Venice, Florida notices of approval of the student visas for the two hijackers.[26]

Despite these and other failures, there were also instances in which the system worked. An FBI agent working out of the Phoenix field office sent a memo to FBI headquarters and the New York Field Office, warning of the "possibility of a coordinated effort by Usama Bin Ladin to send students to the United States to attend civil aviation schools."[27] Investigative work connected to the 2000 USS Cole bombing by two other FBI agents led to the names of two of the hijackers being added to the TIPPOFF watch list on August 24.[28] That same month, Border Agent Jose Melendez-Perez turned away Mohamed al-Kahtani, one of the alleged twentieth hijackers, from Orlando airport after having a gut feeling that al-Kahtani "was up to no good."[29] Still, as CIA Director George Tenet acknowledged after the attacks, "the system was blinking red."[30]

PROTECTING THE HOMELAND

Our Cities and States

On September 11 we learned that homeland security requires a national effort. All levels of government, as well as the private and non-profit sectors, must work together to fulfill the goals outlined by the *2007 National Strategy for Homeland Security* to "prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[31] Although the Federal Government is a full partner in these tasks, America's cities and states represent our first line of defense against a terrorist attack. Intelligence efforts at the community level by local police and state authorities have paid off, disrupting several plots. In the event of an attack, city and state first responders will be the first on the scene. However, burden-sharing within the homeland security "enterprise," the term coined by the Obama administration to refer to collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners, remains uneven.[32]

Disaster Response and Management

Many lessons for disaster management were learned (or re-learned) and implemented within minutes of the attacks on the World Trade Center in New York. Veterans of the 1993 World Trade Center (WTC) truck bombing downtown on September 11, 2001 reported using their experience from that earlier attack as the basis for their decision to evacuate right away. In 1993, Dharam Pal, working from the 74th floor of the North Tower, and many others had stayed behind because they didn't realize the severity of the situation or know what to do. On 9/11, Pal

and other WTC veterans reacted differently: "I might have stayed this time, too, if I hadn't gone through 1993."[33] The 1993 attacks instilled in many an acute sense of awareness of any changes in the building's environment. This, along with the evacuation training carried out in response to the confusion that followed the 1993 bombing and improvements such as the addition of battery-powered lights and glow-in-the-dark paint in the stairwells undoubtedly saved lives on 9/11.[34] Still, survivors of the 1993 bombing in the World Trade Center on the morning of September 11, 2001 faced a difficult decision. Many recalled the loss of power that had trapped people in elevators for hours in 1993 and decided to try their luck with the stairs instead. Nor were all the elevators fully operational. At most five of the 10 express elevators running from the 78th-floor sky lobby to the 44th-floor sky lobby were running that morning, with the remaining elevators due to begin operation after the 9 o'clock start of the business day or out of service altogether for repairs.[35]

Lessons from the first WTC bombing were also evident nearby at St. Vincent's Hospital, the 550-bed hospital located in downtown Manhattan that served as one of the primary recipients of patients on September 11. After the 1993 bombing, St. Vincent's received approximately 200 victims, of whom more than half were later admitted.[36] In 1993, the hospital's handling of the crisis had been slow to begin and the chain of command unclear. It took hospital staff five hours to open the first satellite patient care area, during which communications were erratic. In the aftermath of the 1993 attack, the hospital instituted a thorough review, which resulted in a formal disaster plan detailing a comprehensive response to future terrorist attacks. It was this plan that was in place on the morning of September 11 and that, within minutes of American Airlines Flight 11 striking One World Trade Center at 8:46 am, went into effect. Long before the first patient from Ground Zero arrived, the facilities and staff at St. Vincent's were ready. Elective

surgeries were cancelled, extra beds opened with physicians and nurses standing by, and communication established and collaboration begun with the New York City Police Department (NYPD) – all products of an incident command system that had been established as part of the emergency management external disaster plan set up in the wake of 1993.[37]

Although St. Vincent's experience demonstrates that preparedness works, the emergency management disaster plan did not adequately prepare staff to deal with all of the developments that day. Electricity and phone services were lost in lower Manhattan as a result of the collapse of the Twin Towers and the hospital's computer communication lines, which were routed through the WTC, were knocked out of commission. Water tanks had to be brought in when St. Vincent's water pressure – the hospital was on the same water line as the WTC – dropped from 130 to 10 pounds per square inch.[38] The use of two-way radios however, instituted as part of the post-1993 disaster planning, mitigated several logistical and communication problems that day.

After-action reports examining the response of the New York Police Department and the Fire Department of New York (FDNY) on 9/11 praised the heroic actions of first responders but identified several areas of weakness in the city's emergency response. Although the FDNY was able to establish an Incident Command Post at the site within minutes of the first aircraft striking Tower 1, the initial site chosen was vulnerable to falling debris and had to be moved outside the WTC site perimeter.[39] Several Fire units responding to dispatchers failed to check-in at the staging areas set up around the site to coordinate the rescue and instead proceeded directly into the tower lobbies without first receiving instructions. As a result, Fire chiefs that day were unable to accurately track the whereabouts of all units. (A 'significant number' of NYPD personnel also bypassed mobilization points and went directly to the site.[40]) The main limitation encountered by the FDNY that morning however concerned the inability to maintain

communications. Portable radios used by the FDNY depended on a repeater system located in 5 WTC to amplify and rebroadcast their signals but upon testing that morning was found to be malfunctioning.[41] While the NYPD were able to maintain radio communications with their personnel throughout the day[42], interagency communication with the FDNY was minimal. Command and control information between the two services was limited. Despite protocols that called for them to be placed in NYPD helicopters in incidents involving high-rise buildings, no FDNY personnel were on board the NYPD helicopters circling the site that morning. This prevented 911 operators and FDNY dispatchers from informing callers stuck in the buildings that no rooftop rescues were being attempted and instructing them not to climb to the roof.[43]

The NYPD response was hampered by a number of other problems. The post-collapse search for survivors proved to be particularly difficult for the NYPD who struggled to alleviate the severe congestion caused by emergency vehicles around the incident site.[44] Although an investigation later found that the emergency plans that morning called for coverage of an "unrealistic number of sensitive locations (2600+)," the NYPD was able to protect and evacuate the most sensitive locations around the city.[45] Both services suffered as the result of the absence of clear command structure and direction on 9/11 and the days after. Investigations cited clearer delineation of roles and responsibilities of leaders and better clarity in the chain of command, as well as new protocols for radio communications and procedures to optimize information flow and interagency communication as areas for improvement.

In Washington, where there was no comparable previous experience with a large-scale terrorist attack and the number of casualties far lower, the initial disaster response was also mixed. As in New York, local, regional, state, and federal agencies quickly mobilized and responded to the Pentagon attack. An after-action report of Arlington County's first responders

noted similar problems as those experienced at the WTC site with units "proceeding on their own initiative directly to an incident site, without the knowledge and permission…of the incident commander." These self-dispatching units hindered the ability of commanders to gain control of the available resources on site. Communication problems also proved cumbersome, with both cellular communication networks and radio channels oversaturated, as well as reports of interoperability problems among different jurisdictions and agencies.[46]

At Virginia Hospital Center-Arlington (VHC-Arlington), which served as the primary recipient of Pentagon patients on 9/11, many important phone numbers to local fire and police services and other hospitals were discovered to be out-of-date or not available. The command center set up to deal with the crisis lacked a fax, computer, printer, and copier.[47] Such shortfalls are, and indeed were, easily corrected. Harder to fix are the logistical and communication problems that hindered both rescue operations in Washington and New York on 9/11. Although on the surface the medical and emergency response system worked on 9/11, the attacks left few wounded and did not stress the medical response system preventing an accurate assessment of its weaknesses. (Medical staff reported having few patients to treat.) Medical preparedness will be crucial in any future attack, particularly those involving chemical, biological, or radiological weapons.[48]

Safeguarding Our Critical Infrastructure

In the wake of 9/11 safeguarding our critical infrastructure has become of paramount importance. America's critical infrastructure is vulnerable not only to physical attacks by terrorists but also cyber attacks. Executive Order 13010, signed by President William J. Clinton in 1996, defined critical infrastructure as "infrastructures so vital that their incapacity or

destruction would have a debilitating impact on defense or economic security."[49] Such infrastructure includes telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services and continuity of government. While tremendous progress has been made since 9/11 in securing some areas of critical infrastructure, including nuclear and chemical plants, security improvements in other areas – most notably pipeline, maritime, and rail security - have been much slower. An attack on any of these critical infrastructures could cause irreparable damage to America's industry and economy. In a time of limited government resources, however, the number one priority for the Department of Homeland Security in coming years will be to do more with less.

Electricity Grid

Comprised of more than 200,000 miles of transmission lines, the nation's commercial electric grid represents a critical national security problem. Alongside natural disasters and operator error, the nation's bulk power system is vulnerable to terrorist attacks. The Department of Defense (DOD) relies on the grid for nearly 99 percent of its power needs at military installations around the country.[50] Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs Paul Stockton recently told Congress that the on-site back-up diesel generators intended to provide continuity of operations in the event of an attack or short-term outage would be unable to sustain basic functions beyond 3 to 7 days.[51] A June 2010 report from the North American Electric Reliability Corporation (NERC) conducted in conjunction with the Department of Energy (DOE) stated that the system "remains an attractive target for acts of both physical and cyber terrorism" and concluded that such an attack "could result in long-term

(irreparable) damage."[52] In May of this year the president and CEO of NERC informed Congress that of all the challenges facing the bulk power system he remained "most concerned" about terrorist attacks upon the power grid.[53]

Elements of the country's electrical control network such as Supervisory Control and Data Acquisition, or SCADA systems, are especially vulnerable to cyber attacks. SCADA software systems monitor and control everything from oil and gas pipelines to power generation, transmission, and water management, and have been labeled the "Achilles heel of critical infrastructure."[54] A successful attack by a terrorist group or enemy state could cripple the nation. Documents seized from Al Qaeda training camps contained manuals full of SCADA information, indicating the organization's members are well aware of the opportunities these targets pose. Hackers have already carried out numerous cyber-security attacks on American SCADA systems. In January 2003 the "Slammer Worm" brought down the safety monitoring system of a nuclear power plant in Ohio for five hours.[55] In 2009, President Obama publicly acknowledged that, "cyber intruders had probed our electrical grid." Hackers no longer require physical access to penetrate SCADA systems, as evidenced by the frequent Chinese attacks on American industry and infrastructure.[56] Despite these and other well known and reported incidents, the Obama administration's *Plan for a 21st Century Electric Grid* lists security last on the four pillars of the "Smart Grid Strategy," behind cost-effectiveness, innovation, and consumer empowerment.[57]

As with most critical infrastructure, the mix of public and private sector interests in the electricity industry complicates efforts aimed at security. Enhanced public-private partnerships are vital to effective cyber-security protection. Greater government authority is needed to deal

with cyber emergencies as well as enhanced information and intelligence sharing to ensure that those charged with protecting the grid against threats are able to perform their jobs.

Oil and Gas Refineries and Pipelines

Pipeline and refinery security are another area that has received inadequate attention by federal authorities since 9/11. With nearly half a million miles of oil and natural gas pipelines crisscrossing the United States[58], protecting these systems from terrorist attacks represents a major challenge. Al Qaeda has sought to target pipelines in this country since as far back as at least 2006. In recent years, Al Qaeda-affiliated websites have identified the Trans Alaska Pipeline System (TAPS), responsible for 17% of the United States domestic oil production, as a target of interest.[59]

Although the nature of the threat is clear, the infrastructure set in place by the Pipeline Safety Improvement Act of 2006 to improve pipeline safety and security is hobbled by insufficient resources and oversight problems. While the Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA) is responsible for pipeline safety, the security of these systems falls under the purview of the Transportation Security Administration (TSA) – the lead federal agency for security in all transportation areas.[60] The TSA's Pipeline Security Division (PSD) is responsible for developing, implementing, and monitoring security standards as well as maintaining relations with industry. The formidable charge of conducting security inspections on the nation's pipelines, maintaining TSA's asset database, and developing new security standards and regulations, falls to a staff of just 13.[61] With no separate line item for TSA's pipeline security activities, it is impossible to know for certain how many funds are allocated to this task. However, DHS's total FY 2012 budget request for

"Surface Transportation Security" (which includes all non-aviation transportation systems like pipelines,) was $134.748 million, far less than what is needed.[62]

Transportation[63]: Ports, Rail, and Aviation

In addition to pipeline security, the TSA is responsible for all aspects of the U.S. transportation system. Ensuring the lawful travel of people and trade of goods is vital to America's economy and security but remains an ongoing challenge. The TSA's continued focus on threats in the aviation sector risks overlooking dangers from other transportation areas. Although aviation security already receives the vast majority of TSA resources (a 2004 report by the Congressional Research Service stated that as much as 90% of annual federal funding for transportation security goes towards this one mission,[64]) additional resources continue to be allocated toward it. By the DHS's own admission, "a significant portion" of the new initiatives outlined in the FY 2012 budget request are for aviation and passenger security. Alongside funding for additional passenger screening technology and an expansion of watch list vetting, DHS requested $236.9 million to fund 3,336 Behavior Detection Officers (BDOs).[65] The October 28, 2010 terrorist plot to detonate explosives hidden in printer ink cartridges in commercial aircraft cargo along with recent reports that terrorists are attempting to surgically implant explosives in operatives indicate not only that airliners remain an attractive target for terrorists but also that Al Qaeda is adjusting to the security improvements in aviation.

Unlike aviation, maritime (port and cargo) and rail security is an often overlooked and neglected part of our strategy for homeland security. Funding for maritime and rail security remains less than a fraction of that allocated toward aviation security. Less than $40 million in federal grants were allocated to port security at Los Angeles and Long Beach in the four years

immediately following 9/11; an amount equivalent to what was spent on airport security in a single day during this period.[66] The concern first identified by the 9/11 Commission that continued security improvements in commercial air traffic could "shift the threat to ports, railroads, and mass transit system" remains a very real danger.[67] Documents recovered from Osama Bin Laden's compound in Pakistan revealed that U.S. rail systems were an ongoing target of interest by Al Qaeda as recently as February 2010.[68] Currently, the TSA employs just 175 inspectors as part of its Surface Transportation Security Inspections Program to conduct inspections of the nation's 140,000 miles of railroad track.[69]

The TSA has been slow to carry out risk assessments and training of personnel in the area of passenger and freight rail security. As of early 2011, the TSA had still not issued regulations for public transportation and railroad security programs as mandated by the *Implementing Recommendations of the 9/11 Commission Act of 2007*. The agency lags behind schedule on security training for rail employees and rail stakeholders have voiced repeated dissatisfaction with the quality of information the TSA shares.[70]

Ongoing efforts to ensure that all cargo bound for the U.S. is screened have also met with a number of challenges. Foreign governments and terminal operators have understandably been reticent to sign off on the costs and delays required by 100 percent scanning of U.S.-bound cargo. The Secure Freight Initiative (SFI) program has experienced heavy funding cuts in recent years: DHS' FY 2011 Congressional Budget Justification sought to decrease the program's $19.9 million budget by $16.6 million in connection with the discontinuation of operations at three foreign SFI ports. Senior officials from Customs and Border Protection (CBP) now acknowledge that the majority of foreign ports will be unable to meet the July 2012 target date for scanning all U.S.-bound cargo.[71]

Chemical, Biological, Radiological and Nuclear (CBRN) Threats

The federal government's efforts to prevent a chemical, biological, radiological or nuclear (CBRN) incident on the American homeland are woefully inadequate. Risk assessment is one area of major weakness. Collaboration between the Departments of Homeland Security and Health and Human Services (HHS) to provide CBRN risk assessments is hindered by the absence of written procedures. A 2011 report from the Government Accountability Office (GAO) found that although the two departments had coordinated with each other to develop these assessments, neither had fully institutionalized them in writing.[72] More alarming, the interagency agreement by which officials from the two departments collaborate on these matters expired in June 2011 with HHS officials unsure whether it would be renewed.[73]

Efforts to protect the country's chemical plants, initially slow to get started, have continued to lag behind other programs. DHS continues to struggle to enact and enforce security regulations at chemical facilities around the country. The Chemical industry has been reticent to allow oversight by DHS, successfully procuring facility exemptions for public water systems and water-treatment plants, as well as maritime facilities from the Chemical Facility Anti-Terrorism Standard (CFATS).[74] The industry also opposed the Inherently Safer Technology (IST) provision in a recent bill before Congress (HR 2868), citing costs.[75]

Finally, while DHS has made significant progress in deploying radiation detection equipment, scanning close to 100% of the cargo that enters the U.S. through land borders and major seaports, progress in scanning railcars entering the U.S. from Canada and Mexico as well as international air cargo has been slow.[76]

Borders and Immigration

The 20,000 Border Patrol agents and 21,000 CBP personnel in charge of protecting America's 327 air, land, and sea ports of entry face a daunting task.[77] Their charge is to provide for the continued lawful movement of people and goods into the United States on a daily basis while insuring terrorists do not gain admittance. This mission requires striking a fine balance between security and other goals. Too stringent regulations risk provoking resentment amongst the thousands of talented individuals who seek to come to America each year to study or pursue entrepreneurial plans. Too lax enforcement risks more cases like that of Hosam Smadi who plotted to blow up a Dallas office building in 2009 after overstaying his visa. During his time in America Smadi, who entered in 2007 on a six-month tourist visa, was able to enroll in high school, obtain a California identification card, purchase two used cars, and procure a handgun and ammunition. Two weeks prior to his arrest on terrorism charges by the FBI, a sheriff's deputy in Texas pulled over Smadi for a broken taillight. Although Smadi's name appeared on a FBI watch list when the deputy checked his identity, the background check did not turn up any immigration information.[78]

Despite visa reform like US-VISIT, a biometric screening program used by federal, state, and local authorities, DHS still has trouble tracking the entry and exit of individuals into this country. As of January 2011, US-VISIT computers had a backlog of 1.6 million potential overstay records.[79] Knowing who has entered the country provides only half the picture. Ten years after 9/11, however, the U.S. still lacks a universal and reliable electronic exit monitoring

system. The current system which relies on departing visitors to turn in paper stubs when they leave is outdated and in urgent need of updating.

Intergovernmental cooperation and division of responsibilities over visa issuance also continues to pose difficulties. Umar Farouk Abdulmutallab, the Christmas bomber, was able to board Northwest Flight 253 after purchasing his ticket in cash and checking in with no luggage although he had already been placed on the government's terrorism watch list. More troubling still, Abdulmutallab – who had a two-year visa to enter the U.S from London – had been denied a British visa in May 2009, a fact communicated by British officials to U.S. authorities.[80] Even with all of this information in the system, a breakdown in communication occurred between the State Department and the National Counterterrorism Center (NCTC) and Abdulmutallab was allowed to board his flight.

Homegrown Radicalization

In the years since 9/11, the threat from the radicalization of homegrown terrorists has grown. Of the 175 cases of Al Qaeda-related homegrown terrorism since 2001, nearly half occurred in 2009 and 2010.[81] A 2011 report from the Bipartisan Policy Center's National Security Preparedness Group, a successor organization to the 9/11 Commission, however voiced concerns that "it remains unclear who is leading the effort to share information."[82] The November 5, 2009 killing of 13 Department of Defense employees at Fort Hood, the worst terrorist attack on U.S. soil since September 11, 2001, illustrates many of the ongoing challenges in domestic counterterrorism. A report by the Senate Committee on Homeland Security and Governmental Affairs into the attack found that both the DOD and the FBI possessed information related to the radicalization of Army Major Nidal Malik Hasan, including

knowledge of his communications with a suspected terrorist.[83] Officials at the DOD and FBI failed to coordinate their intelligence efforts and Hasan's immediate superiors remained unaware of his extremist activities until it was too late.

The Americans inspired by Al Qaeda and radicalized on the Internet who seek to harm us represent a tiny minority of the law-abiding Muslim-Americans living in this country. The Muslim community in America is an active participant in securing our homeland: American Muslims helped foil seven of the last ten Al Qaeda plots within America.[84] Because successful counter-radicalization begins at the local level, efforts by state and local authorities are vital in safeguarding the homeland from this new threat. Community policing and outreach efforts represent our best chance at preventing future homegrown attacks.

Civil Liberties

In the climate of fear and vulnerability following the attacks of 9/11 it was understandable that initial policy changes would emphasize security above civil liberties. However, the swift passage of a four-year extension of the PATRIOT Act in May 2011 without a national debate is deeply troubling. As a result, Congress and the courts may have missed their best opportunity to date to re-examine controversial provisions of the Act in order to ensure that the right balance between security and privacy is struck.

Critics, including the American Civil Liberties Union (ACLU), charge that the PATRIOT Act's passage in October 2001 and subsequent renewal in March 2006 and May 2011 violates American's Fourth Amendment rights against unreasonable searches and seizures as well as First Amendment protections of free speech and association.[85] Although the majority of the Act's provisions are uncontroversial, three key law enforcement provisions have drawn heavy

criticism, including the FBI's right to continue "roving wiretaps"; a provision which allows surveillance of foreigners without known links to terrorist groups, known as the "lone wolf" provision; and a provision that allows authorities to investigate "tangible items," including library records, of suspected terrorists.[86]

Following the act's first renewal in 2006, a number of abuses were subsequently uncovered. A 2007 report by the Inspector General of the Department of Justice (DOJ) found that the FBI had carried out a number of intelligence-gathering abuses involving "national security letters," documents approved only by FBI officials without knowledge or approval by judicial authorities, issued for U.S. citizens. An analysis of a small sample of the letters by the Office of the Inspector General (OIG) found that the letters had been used improperly 16 percent of the time. The same investigation revealed that the FBI had, through an arrangement with major telephone companies, gained access to more than 3,000 phone numbers, often without a subpoena.[87]

Changes in aviation security since 9/11 have also raised privacy concerns. Both the public and the ACLU have been critical of the TSA's deployment of advanced imaging technology (AIT) systems for whole body scanning of passengers at airports. Although the 9th Circuit Court of Appeals ruled that airport searches are reasonable, a recent government report recommended additional policy and legal analysis to address "whether the new procedures are no more intrusive or intensive than necessary."[88] To further allay public concerns over privacy, the TSA announced in July 2011 it will begin installing new software designed to produce a more "generic" body image by the end of the year. According to TSA Administrator John Pistole, the new software will "enhance privacy by eliminating passenger-specific images." Passengers will also be allowed to view the images on a video monitor.[89]

Government and Intelligence Overhaul

In the wake of the 2001 terrorist attacks the U.S. government underwent the largest reorganization of its kind since the *National Security Act of 1947*. The creation of the Department of Homeland Security from 22 different Federal department and agencies continues to be controversial and the department has encountered many challenges since its standing up. A mere three years after the passage of the *Homeland Security Act* by Congress in November 2002, Secretary for Homeland Security Michael Chertoff initiated a *Second Stage Review (2SR)*, a wide-ranging formal review which led to a major reorganization of the department. Along with ongoing management and information technology (IT) challenges, DHS is weakened by cumbersome obligations to repeatedly appear before Congress. Congressional oversight, while vital, taxes the limited man-hours and resources of the department. In 2009, DHS officials answered 11,680 letters, provided 2,058 briefings and sent 232 witnesses to 166 hearings; the equivalent of about 66 work years spent in responding to questions from Congress.[90] A way must be found to better allocate the resources of the staff of the DHS who currently spend a majority of their time testifying on the Hill rather than responding to the challenges facing our nation.

The department's broken multibillion acquisition system also requires urgent fixing to prevent the additional waste of hundreds millions of dollars in faulty technologies and programs.[91] Among the many failings of DHS in this area identified by the GAO are "implementing technologies that did not meet intended requirements and were not appropriately tested and evaluated," and repeated failures to conduct adequate cost-benefit analyses.[92] One such example from 2007 involved a $1.2 billion program to deploy new radiation monitors to screen vehicles and cargo for signs of nuclear materials. Despite promising Congress that the

machines had a 95 percent success rate in detecting uranium, a GAO audit revealed the detection rates were as low as 17 percent.[93]

In addition to the creation of the Department of Homeland Security, Congress enacted wide-ranging intelligence reform in the wake of the September 11 attacks. Some of the same stovepipes (along with new ones,) that prevented members of the intelligence community from "connecting the dots" prior to 9/11 still exist today, however. Despite efforts to improve relations between the FBI and CIA, interagency collaboration is hampered by confusion about the rules governing the sharing and use of information gained from the intelligence community. The FBI, historically a law-enforcement agency, continues to struggle with the new emphasis placed on its intelligence-gathering role. FBI headquarters lack effective strategic control of field offices, which continue to "prize and protect their autonomy from headquarters," often resulting in poor communication of the kind that was evidenced in the Fort Hood case.[94] State and local stakeholders complain that the FBI's Joint Terrorism Task Forces (JTTFs) "serve up" to the federal bureaucracy, rather than working "down" to the local level.[95] The CIA, for its part, continues to struggle to recruit people proficient in key foreign languages.

The creation of the Office of the Director of National Intelligence (ODNI) under the *Intelligence Reform and Terrorist Prevention Act (IRTPA)* of 2004 added another layer in an attempt to integrate the activities of the country's sixteen intelligence agencies. Since then, there have been four Directors of National Intelligence (DNI), suggesting the office lacks the stability of leadership that is vital to its mission. Six years after it's creation, the ODNI has ballooned to a staff of 1,600, many of them contractors; far more than what Congress initially envisioned when it established the office. Critics charge that the creation of the ODNI has only complicated the intelligence community's ability to communicate and share information. Former Congressman

and Co-Chairman of the 9/11 Commission Lee Hamilton recently told Congress that it was still not clear that the DNI was the "driving force" for intelligence community integration that the Commission envisioned.[96] According to at least one former DNI, despite the gaps in legislation filled in by Executive Order 12333, IRTPA remains unfinished business.[97] The CIA in particular has not adjusted to the new realities of intelligence reform and has challenged the ODNI's authority on more than one occasion.[98]

AMERICA ABROAD

The September 11, 2001 terrorist attacks brought about not only changes in our government and society but also ushered in a new global outlook for many in Washington. When asked what lesson he learned from the attacks on 9/11, President Bush declared, "Here's what I took away from September the 11th, 2001 – that any time a president sees a gathering threat to the United States, we must deal with it…In the old days oceans protected us from harm's way, and a president could stand back and say, well, maybe this gathering threat is an issue, maybe it's not. After September 11 that complacency…is no longer relevant."[99] Senior administration officials spoke in similarly stark terms of changes. "What's happened, what's different?" Secretary of Defense Donald Rumsfeld told the Senate Armed Services Committee in September 2002 when asked what had prompted the new policy response toward Saddam Hussein's longstanding obfuscation, "What's different is 3,000 people were killed…I think that in answer to the question, What's different? What's happened? What's changed? That I would say that's changed."[100] National Security Advisor Condoleezza Rice took a similar lesson away from the attacks: "Take care of threats early."[101] In short, the Bush administration responded to the attacks of September 11, 2001 not only with a new national security infrastructure but also with a

different worldview, one in which prevention (or preemption) replaced the containment of threats.

AFGHANISTAN/PAKISTAN

No off-the-shelf military contingency plan for Afghanistan existed on September 11, 2001, causing the Pentagon to scramble to complete one in the days immediately following the attacks.[102] Although the CIA had been active in Afghanistan for several years, cultivating a number of sources in the process, the agency initially oversold President Bush. At a meeting of the National Security Council (NSC) on September 13, 2001, a senior CIA official told the Commander-in-Chief that victory there could take as little as a few weeks.[103] As the enormity of the task before us became apparent, the mission transformed from one initially focused on covert action and special forces to a full-fledged military operation involving 150,000 foreign troops.[104]

After years of experimenting with different strategies there are no good options left in Afghanistan. Coming up on the ten-year anniversary of our mission there, the country remains marked by the absence of a monopoly of governance and rampant corruption and violence. A number of high-profile attacks in recent months, including the assassinations of President Ahmed Karzai's half-brother and the mayor of Kandahar, testify to the ongoing strength of the insurgency. NATO governments, which have struggled to sustain their deployment from the start, will only hasten to withdraw their troops in the wake of President Obama's recent announcement that the 30,000 American surge forces deployed in December 2009 would be pulled out by the end of 2012.

In the aftermath of the killing of Osama Bin Laden, our relations with the Pakistani government are at the lowest in recent memory. Yet Pakistan remains the linchpin for our

strategy in Afghanistan. Without a coherent plan to tackle the border region, home to the Pakistani Taliban, Al Qaeda, and terrorist groups like Lashkar-e-Taiba, nothing approaching success can be achieved next door. There are some grounds for hope however. A recent poll from the Pew Research Center's Global Attitudes Project found that while disapproval of U.S. foreign policy in the region and opposition to drone strikes remains high, most Pakistanis "support the U.S. providing financial and humanitarian aid to areas where extremist groups operate, and many want the U.S. to provide intelligence and logistical support for Pakistani troops fighting extremists." Only 12 percent of Pakistanis have a positive view of Al Qaeda, down from 18 percent in 2010.[105] Still, in a number of areas, our counterterrorism relationship with Pakistan is deeply unsatisfying. A successful global counterterrorism strategy requires partnerships built on trust between nations.

IRAQ

In Iraq, the situation is now less dire but still fragile. The war diverted our attention from the mission in Afghanistan at a critical juncture and has cost America dearly. The well-documented failures of intelligence and the rush to war without adequate planning or consideration of the aftermath has now cost more than 4,400 American lives and $3 trillion in treasure.[106] In the wake of congressional authorization for the use of force in Iraq it is refreshing to see the legislative branch reassert itself in discussions over who takes America to war as it has done in challenging the White House's handling of the NATO operation in Libya.

In the short term, the U.S. must focus on securing a stable and orderly withdrawal of coalitional combat forces from the country by December 31, 2011, while ensuring the continued cooperation of the Iraqi government and Iraqi Security Forces (ISF). The removal and

destruction of millions of tonnes of military equipment and material from nearly a decade of war will continue to occupy the DOD in the months ahead. The long-term challenges caused by this war, however, will be with us for years to come.

PUBLIC DIPLOMACY

Although the 9/11 attacks represented an opportunity for America to reshape relationships around the world, many of the relations damaged due to America's "go-it-alone" attitude after 9/11 are only now being repaired. Abu-Ghraib, Guantanamo, and controversial CIA rendition programs have greatly damaged America's standing in the world, as did the Bush Doctrine's heavy reliance on military – over legal, financial, and diplomatic – tools. Still, despite stumbles from time to time, the U.S. appears to be winning the battle of ideas. While the recent Arab Spring offers cautious grounds for optimism, the U.S. should avoid any major policy pronouncements voicing support for one opposition group over another, so as to avoid the long held impression in the region that Washington is pulling the strings.

AL QAEDA AFTER BIN LADEN

U.S. officials and terrorism experts alike have long acknowledged that there would be no surrender on the deck of the USS Missouri to mark the end of this global struggle. The recent claims by senior Obama administration officials that Al Qaeda as an organization is nearing 'strategic defeat' are not only premature but also dangerously misleading.[107] True, much of the Al Qaeda senior leadership, including Osama Bin Laden, has been hunted down and killed in the tribal areas of Afghanistan-Pakistan, but the Al Qaeda of yesteryear ceased to exist long ago. Almost immediately after 9/11, the organization began to morph into an unwieldy group of

regional affiliates. Operating out of Yemen, Al Qaeda in the Arabian Peninsula (AQAP) now represents the point of the spear of this hydra-headed threat. The defeat of the leadership in Pakistan and Afghanistan does not mean an end to terrorist targeting the United States. U.S. counterterrorism efforts should be directed toward ensuring that no safe haven is established in Somalia or Yemen.

POLICY RECOMMENDATIONS

In the coming weeks and months, Americans must engage in a national discussion over what constitutes success in the War on Terror and what the proper tradeoffs between security and liberty should be. Such a public debate is necessary to ensure the continued security of the United States in a manner keeping with its values and ideals. In addition to beginning this long-term conversation with the American people, there are a number of specific changes that Congress and the White House can take now to make America more secure.

Domestic Affairs and Homeland Security

- In keeping with the recommendations of the 9/11 Commission Report, **the federal government should allocate an additional 10 megahertz of radio spectrum to public safety to facilitate interoperable communications for first responders.** Along with a clear chain of command, the ability to communicate effectively was one of the main lessons learned by first responders on September 11.
- **Overhaul the DHS system of grant making for state and local homeland security agencies.** States and local governments have become overly reliant on DHS's State, Local and Tribal Grant Programs to fund their homeland security efforts. Currently, the

homepage for the DHS's grant programs reads "Open for Business."[108] In an era of growing fiscal crisis, this sends the wrong message. Ten years after 9/11, more responsibility for homeland security must shift to state and local governments. Funding programs like the Driver's License Security Grant Program (DLSGP), which provided State Driver's License Agencies and Departments of Motor Vehicles with $44,910,000 in federal funding in FY 2011 should be the responsible of state governments not Washington.[109]

- **Congress should move quickly to enact the "Grid Reliability and Infrastructure Defense Act" (GRID),** which strives to overcome a number of current limitations and vulnerabilities pertaining to the electricity grid. Currently, the Federal Energy Regulatory Commission (FERC) does not have authority or jurisdiction over the bulk power system in Alaska and Hawaii as well as all local distribution facilities in large cities such as New York.[110]
- **The intertwined pipeline safety and security missions of DOE's PHMSA and the TSA's PSD should be consolidated under one lead federal agency.**
- **Congress should support DHS's plan to phase in a per-ticket airline passenger security fee of $1.50 to help offset expenses associated with aviation security.** Additional resources should be devoted to securing the nation's ports, rail and mass transit systems.
- More resources should be allocated for overstay enforcement to U.S. Immigration and Customs Enforcement (ICE)**. ICE's Counterterrorism and Criminal Exploitation Unit (CTCEU), which currently devotes only 3% of its total field office investigative hours to visa overstays, should be mandated to devote more time to investigations.**[111]

DHS also needs to step up its identification and sharing of information on overstays with federal, state, and local agencies.

- **Efforts to establish a universal and reliable electronic monitoring exit system for visitors should be redoubled in order to close a dangerous security loophole.**
- **The White House should move quickly to nominate, and the Senate confirm, the remaining members of the Privacy and Civil Liberties Oversight Board, created at the recommendation of the 9/11 Commission.** Once fully staffed, the board should lead a national discussion about the tradeoff between liberty and security in future national security reform.
- **The FBI should establish basic training and record-keeping procedures to ensure that civil liberties are protected**, in keeping with the *2010 Quadrennial Homeland Security Review Report's* call for the liberties of all Americans to be ensured and privacy protected.[112] Additional congressional oversight of the PATRIOT Act and internal FBI audits may also be warranted to prevent additional abuses.

Foreign Policy

- In Afghanistan, where there is no good endgame, we should continue to **drawdown our forces while shifting to a more limited counterinsurgency (COIN) operation with renewed emphasis on counterterrorism operations.** The 305,000 members of the Afghan National Security Forces (ANSF) should take the lead in future COIN operations.[113]
- As unpalatable as it may be to many, **the U.S. should engage in peace talks with the Taliban**. In doing so, we should work with the Saudis – the only other government

besides Pakistan to formally recognize the Taliban before 9/11 – to facilitate negotiations with the group's Afghan leadership.

- **Cultural exchanges between Pakistan and America should be stepped up** to facilitate the understanding of American values and strategic interests. America can, and must do better, in explaining itself to the people of Pakistan, where currently only 12% express a positive view of us.[114]
- The nearly 50,000 American soldiers wounded in Iraq and Afghanistan deserve the very best this nation has to offer. **Although the cost of caring for veterans will continue long after the fighting ends, Congress and the executive branch should make sure that America's soldiers receive the necessary medical, financial, legal and employment assistance in the months and years ahead.**

[1] Department of Homeland Security, "Quadrennial Homeland Security Review Report," (2010): 9.

[2] The official death toll from the terrorist attacks of September 11, 2001 stands at 2,753. Three of those whose names are listed on the official list of victims died in the years after from diseases related to their exposure from the collapse of the World Trade Center. The New York City's medical examiner subsequently ruled their deaths a result of the terrorist attacks. By comparison, 2,400 Americans lost their lives during the Japanese attack on Pearl Harbor in 1941. The deadliest day in American history remains September 17, 1862, when 3,600 soldiers from the Union and Confederate armies lost their lives at the battle of Antietam. David B. Caruso, "Official 9/11 death toll grows by 1" *Associated Press*, June 17, 2011.

[3] Authors Derek Chollet and James Goldgeier deliberately gave their book, *America between the Wars*, the subtitle "From 11/9 to 9/11," to highlight that the terrorist attacks represented not just the beginning of a new era but also marked the end of a decade of post-Cold War diplomacy. Derek Chollet and James Goldgeier, *America Between the Wars: From 11/9 to 9/11,* (New York: Perseus Books Group, 2008).

[4] Christopher Hemmer, "The Lessons of September 11, Iraq, and the American Pendulum," *Political Science Quarterly* 122:2 (2007): 228.

[5] Eliot A. Cohen, "World War IV – Let's call this conflict what it is," *Wall Street Journal*, November 20, 2001.

[6] Robert J. Beck, "Munich's Lessons Reconsidered," *International Security* 14:2 (1989): 165-7.

[7] The words are those of Winston Churchill. Beck, "Munich's Lessons Reconsidered," 185.

[8] Statement by President Lyndon Johnson, "White House News Conference on July 28, 1965: We Will Stand in Viet-Nam," *Department of State Bulletin*, August 16, 1965, accessed July 26, 2011, http://www.myholyoke.edu/acad/intrel/pentagon4/ps2.htm.

[9] Beck, "Munich's Lessons Reconsidered," 161.

[10] Hemmer, "The Lessons of September 11, Iraq, and the American Pendulum," 217.

[11] Sidney Aster, "A Shaky Grasp of History," *The Globe and Mail*, February 25, 2003, A19.

[12] Although the lessons of that September long ago remain contested, the charge of Munich, and the association with appeasement it carries, remains the quintessential knockout argument. As historian Sidney Aster has argued, it allows for the easy rationalization of decisions that have already been taken and allows public opinion to be quickly mobilized. "Its brilliance," he notes, "is that that the familiarity of the analogy replaces its questionable validity." Hemmer, "The Lessons of September 11, Iraq, and the American Pendulum," 216; Aster, "A Shaky Grasp of History," A19.

[13] In one of those oddities of history, British Prime Minister Anthony Eden is known to have viewed the crisis over the nationalization of the Suez Canal by Nasser in analogous terms with Hitler's rise. Matt Seaton, "Blast from the past: Politicians on both sides of the argument over Iraq have been busy rummaging through the history books," *The Guardian,* February 19, 2003, 2.

[14] Charles Babington, "Bush to Address Nation; Explosions Reported in Afghanistan," *Washingtonpost.com*, September 11, 2001, accessed July 23, 2011, http://media.washingtonpost.com/wp-svv/natoin/article/trade091101.htm.

[15] Bush has invoked the Pearl Harbor analogy on numerous occasions. According to Bob Woodward, Bush first employed the analogy on the evening of September 11, 2001 when he

dictated to his diary: "The Pearl Harbor of the 21st century took place today." Bob Woodward, *Bush at War* (New York: Simon & Schuster, 2002), 37; George W. Bush, "Remarks by the President to the People of Poland," Krakow, May 31, 2003, accessed July 23, 2011, http://georgewbushwhitehouse.archives.gov/news/releases/2003/05/20030531-3.html. Accessed on 19 July 2011.

[16] For a selection of instances in which members of Congress drew comparisons between Vietnam and Iraq before the war, see S10236, S10296, H7183, H7202, H7227, H7245, H7744, E1927, Congressional Record, 107th Congress, 2nd Session.

[17] Hemmer, "The Lessons of September 11, Iraq, and the American Pendulum," 229.

[18] Mikkel Vedby Rasmussen, "The history of a lesson: Versailles, Munich and the social construction of the past," *Review of International Studies* 29(2003): 500.

[19] George W. Bush, "Remarks by the President," September 14, 2001, accessed July 24, 2011, http://www.nationalcathedral.org/worship/sermonTexts/gwb20010914.html.

[20] *The 9/11 Commission Report*, (Washington: Government Printing Office, 2004), 266, accessed July 24, 2011, http://www.9-11commission.gov/report/911Report.pdf.

[21] *The 9/11 Commission Report*, 181-2.

[22] On the Zacarias Moussaoui case, see *The 9/11 Commission Report*, 273-6.

[23] Five of the 19 hijackers overstayed their visas. Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate, "Overstay Enforcement: Additional Mechanisms for Collecting, Assessing and Sharing Data Could Strengthen DHS's Efforts but Would Have Costs," GAO-11-411 (2011): 1.

[24] Kevin Johnson and Mimi Hall, "Inspector's instincts win praise, gratitude," *USA Today*, January 27, 2004, 3A.

[25] *The 9/11 Commission Report*, 227, 229.

[26] Lenny Savino, "President condemns INS over hijackers' visa paperwork," *The Philadelphia Inquirer*, March 14, 2002.

[27] *The 9/11 Commission Report,* 272.

[28] *Ibid,* 269-270.

[29] Johnson and Hall, "Inspector's instincts," 3A.

[30] *The 9/11 Commission Report,* 259.

[31] Department of Homeland Security, "National Strategy for Homeland Security," (2007), 3.

[32] "Quadrennial Homeland Security Review Report," 12.

[33] Stephen Murphy, "The Human Factor: World Trade Center Evacuees Share Lessons Learned as NFPA Starts New Behavior Study," *NFPA Journal* (2002): 54.

[34] Thomas Virgona. "September 11, 2001: Lessons Learned for Planning Disaster Recovery," (White Plains, New York: Pace University, 2009): E2.2.

[35] Murphy, "The Human Factor," 59.

[36] The 1993 bombing killed six people and wounded 1,000 more.

[37] Linda Kirschenbaum et. al., "The experience at St. Vincent's Hospital, Manhattan, on September 11, 2001: Preparedness, response, and lessons learned." *Crit Care Med* 33.1 (2005): S48-S52.

[38] *Ibid,* S50-51.

[39] The second command post location was later destroyed by the collapse of WTC2, further weakening the command and control structure.

[40] "Improving NYPD Emergency Preparedness and Response," McKinsey & Company, August 19, 2002, 26.

[41] "McKinsey Report: Increasing FDNY's Preparedness," (2002), 7 and 283 of report.

[42] Though there were reports of radio clutter in the initial phase of the response, fewer than 15% of NYPD personnel experienced radio communications failure on 9/11. 25.

[43] *The 9/11 Commission Report,* 292.

[44] "Improving NYPD Emergency Preparedness and Response," 16.

[45] *Ibid,* 19.

[46] "Arlington County After-Action Review on the Response to the September 11 Terrorist Attack on the Pentagon," last modified December 2, 2010, accessed July 23, 2011, http://www.arlingtonva.us/departmetns/fire/edu/about/fireeduaboutafterreport.aspx.

[47] Kimberly A. Cyganik, "Disaster Preparedness in Virginia Hospital Center-Arlington after Sept 11, 2001," *Disaster Management & Response* 1 (2003): 80-86.

[48] Richard A. Clarke and Rand Beers, *The Forgotten Homeland: A Century Task Force Report,* (New York: The Century Foundation Press, 2006): 43.

[49] Congressional Research Service Report, "Critical Infrastructures: What Makes an Infrastructure Critical?" Updated January 29, 2003, 5.

[50] George V. Hulme, "Despite years of talk, utilities remain comprised, vulnerable," CSO, June 14, 2011, accessed July 22, 2011, http://www.csoonline.com/article/684287/despite-years-of-talk-utilities-remain-comprised-vulnerable.

[51] Testimony of the Honorable Paul Stockton before the Subcommittee on Energy and Power, The Committee on Energy and Commerce, U.S. House of Representatives, May 31, 2001.

[52] The NERC report, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," is no longer available on line. The quotes are taken from the Kramer testimony. Statement of Franklin D. Kramer before the House Energy and Commerce Committee

Subcommittee on Energy and Power, May 31, 2011, accessed on July 25, 2011, http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=8639.

[53] Summary of Testimony of Gerry Cauley, President and Chief Executive Officer, North American Electric Reliability Corporation, May 31, 2011, accessed on July 25, 2011, http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=8639.

[54] Tony Bradley, "SCADA Systems: Achilles Heel of Critical Infrastructure," PC World Online, June 20, 2011, accessible July 25, 2011, http://www.pcworld.com/businesscenter/article/230675/scada_systems_achilles_heel_of_critical_infrastructure.html.

[55] Rachel Ross, "Hackers threaten power grid: Expert," *Toronto Star,* September 12, 2003, E06.

[56] Richard Clarke. "China's Cyber Assault on America," *Wall Street Journal*, June 15, 2011.

[57] The White House, "Fact Sheet: The President's Plan for a 21st Century Electric Grid," June 13, 2011, accessed July 23, 2011, www.whitehouse.gov.

[58] Paul W. Parfomak, "Pipeline Safety and Security: Federal Programs," Congressional Research Service Report for Congress, Updated February 29, 2008, 2.

[59] Parfomak, "Pipeline Safety," 3.

[60] *Ibid,* 2.

[61] *Ibid,* 9.

[62] "FY 2012 Budget in Brief – Department of Homeland Security," accessed July 23, 2011, http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf.

[63] For lessons learned on mass transit, see Brian Michael Jenkins and Frances Edwards-Winslow, "Saving City Lifelines: Lessons Learned in the 9-11 Terrorist Attacks," MTI Report 02-06, September 2003.

[64] John Moteff, "Critical Infrastructure Protections: The 9/11 Commission Report," Congressional Research Service, August 16, 2004.

[65] "FY 2012 Budget in Brief – Department of Homeland Security," 89-90.

[66] Clarke and Beers, "Forgotten Homeland," 190.

[67] Moteff, "Critical Infrastructure Protections," 2.

[68] Steve Lord, Testimony Before the Committee on Commerce, Science, and Transportation, U.S. Senate, "Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing," GAO-11-688T, June 14, 2011, 1.

[69] Transportation Security Agency, "Programs and Initiatives: Freight Rail," accessed July 23, 2011, http://www.tsa.gov/what_we_do/tsnm/freight_rail/programs.shtm.

[70] Lord, "Rail Security," 2.

[71] Stephen Caldwell, Testimony Before the Committee on Commerce, Science, and Transportation, U.S. Senate, "Maritime Security: DHS Progress and Challenges in Key Areas of Port Security," GAO-10-940T, July 21, 2010, 14-15.

[72] "National Preparedness: DHS and HHS Can Further Strengthen Coordination for Chemical, Biological, Radiological, and Nuclear Risk Assessments," GAO-11-606, June 2011, 1.

[73] *Ibid.*

[74] Dan Eggen, "DHS panel on at-risk chemical plants is stacked with insiders," *Washington Post*, November 25, 2010; Department of Homeland Security, "Identifying Facilities Covered by the Chemical Security Regulation," accessed July 23, 2011, http://www.dhs.gov/files/prgorams/gc_1181765846511.shtm.

[75] R. Loughin, "Chemical Facility Anti-Terrorism Standard turns four: What's next?" *Hydrocarbon Processing*, March 2011.

[76] Testimony of David C. Mauerer before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, U.S. House of Representatives, GAO-11-869T, July 26, 2011, 6.

[77] Department of Homeland Security, "Bottom-UP Review Report," July 2010, 41.

[78] James McKinley Jr. and Julia Preston, "U.S. Can't Trace Foreign Visitors on Expired Visas," *New York Times*, October 12, 2009.

[79] Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate, "Overstay Enforcement: Additional Mechanisms for Collecting, Assessing and Sharing Data Could Strengthen DHS's Efforts but Would Have Costs," GAO-11-411, April 2011, 41.

[80] Editorial, "A failure to communicate; Lapses in information-sharing allowed a would-be bomber on Flight 253," *Washington Post*, December 30, 2009.

[81] "The Homegrown Threat: Post-9/11 Jihadist Terrorism Cases Involving U.S. Citizens and Residents," New America Foundation, accessed July 27, 2011, http://homegrown.newamerica.net/overview.

[82] Peter Neumann, "Preventing Violent Radicalization in America," *National Security Preparedness Group*, Bipartisan Policy Center, June 2011, 8.

[83] "A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack," U.S. Senate Committee on Homeland and Governmental Affairs, February 3, 2011, 7-8

[84] Testimony by Sheriff Lee Baca, Los Angeles County before the House Committee on Homeland Security on "The Extent of Radicalization in the American Muslim Community and the Community's Response," March 10, 2011.

[85] Written Statement of Michael German before the Subcommittee on Crime, Terrorism and Homeland Security House Committee on the Judiciary on "The Permanent Provisions of the PATRIOT Act," March 30, 2011, 6.

[86] Patrick Jonsson, "Why is Patriot Act under fire if homegrown terror threat is rising?" *The Christian Science Monitor*, February 20, 2011; Lisa Mascaro, "Congress to Vote on Patriot Act; Members on both sides remain wary of surveillance aspects of the anti-terrorism law," *Los Angeles Times*, May 21, 2011; Aliyah Shahid, "Patriot Act gets renewed for 4 yrs.," *Daily News*, May 28, 2011.

[87] Dan Eggen and John Solomon, "FBI Audit Prompts Calls for Reform; Some Lawmakers Suggest Limits On Patriot Act," *Washington Post*, March 10, 2007; Dan Eggen, "FBI Found to Misuse Security Letters; 2003-2006 Audit Cites Probes of Citizens," *Washington Post*, March 14, 2008.

[88] Bart Elias, "Changes in Airport Passenger Screening Technologies and Procedures: Frequently Asked Questions," Congressional Research Service, January 26, 2011, 6.

[89] Keith Herbert, "Full-body scans revised; New Software to make images less revealing; Passengers will view same video as TSA screener," *Newsday*, July 21, 2011.

[90] Testimony by Lee Hamilton before the U.S. House Committee on Homeland Security, Hearing on "Threats to the American Homeland after Killing Bin Laden: An Assessment," May 25, 2011, 5.

[91] Robert O'Harrow Jr., "Radiation Detector Program Delayed; DHS May Have Misled Congress, GAO Audit Finds," *Washington Post*, July 20, 2007.

[92] Testimony of David C. Mauerer, 8.

[93] O'Harrow Jr. "Radiation Detector Program Delayed," July 20, 2007.

[94] "A Ticking Time Bomb," 9-10.

[95] Clarke and Beers, *Forgotten Homeland,* 148.

[96] Hamilton, "Threats to the American Homeland," 5.

[97] Prepared Statement of Dennis C. Blair for the U.S. Senate Committee on Homeland Security and Governmental Affairs Hearing, "Ten Years After 9/11: Is Intelligence Reform Working? Part II," May 19, 2001.

[98] Blair, "Ten Years After 9/11," 12.

[99] Hemmer, "The Lessons of September 11, Iraq, and the American Pendulum,"212.

[100] Testimony of U.S. Secretary of Defense Donald H. Rumsfeld before the Senate Armed Services Committee Regarding Iraq, September 19, 2002, accessed July 21, 2011, http://www.defense.gov/speeches/speech.aspx?speechid=287.

[101] Woodward, *Bush at War*, 350.

[102] Woodward, *Bush at War*, 24.

[103] Woodward, *Bush at War,* 40, 53.

[104] Phil Steward, "U.S. to send 1,400 Marines to Afghanistan," *Reuters*, January 6, 2011.

[105] "Support for Campaign Against Extremists Wanes," Pew Global Attitudes Project, June 21, 2011, accessed July 26, 2011, htpp://pewglobal.org/2011/06/21/u-s-image-in-pakistan-falls-no-further-following-bin-laden-klling/.

[106] U.S. Department of Defense, "Casualty Status: July 27, 2011," accessed July 27, 2011, http: http://www.defense.gov/releases/; Joseph Stiglitz and Linda Blimes, "The true cost of the Iraq War: $3 trillion and beyond," *Washington Post*, September 5, 2010.

[107] Greg Miller, "U.S. officials believe al-Qaeda on brink of collapse," *Washington Post*, July 27, 2011.

[108] Department of Homeland Security, "Open for Business-Grants," accessed July 24, 2011, http://wwww.dhs.gov/xopnbiz/grants/.

[109] FEMA, "FY 2011 Driver's License Security Grant Program (DLSGP)," accessed July 27, 2011, http://www.fema.gov/government/grant/dlsgp/.

[110] Testimony of Joseph McClelland before the Committee on Energy and Commerce Subcommittee on Energy and Power, U.S. House of Representatives, May 31, 2011, accessed July 22, 2011, http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=8639.

[111] "Overstay Enforcement," 21.

[112] "Quadrennial Homeland Security Review Report," vii.

[113] The ANSF estimate is taken from Michael O'Hanlon and Bruce Riedel, "Plan A-Minus for Afghanistan," *The Washington Quarterly* 34:1 (2011): 127.

[114] "Support for Campaign Against Extremists Wanes," Pew Global Attitudes Project.