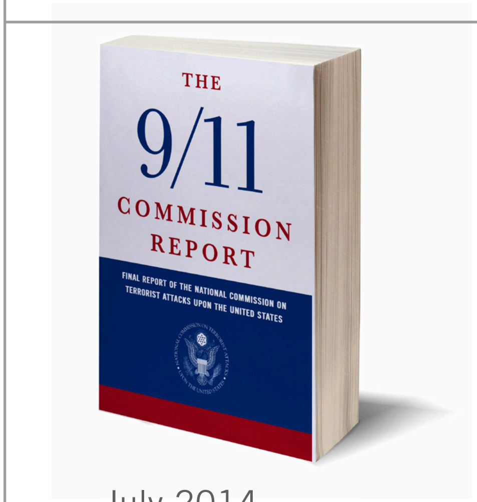
National Security Program
Homeland Security Project


THE
9/11
COMMISSION
REPORT
FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

July 2014

Today's Rising Terrorist Threat and the Danger to the United States:

Reflections on the Tenth Anniversary of *The 9/11 Commission Report*

Ten years ago, as members of the National Commission on Terrorist Attacks Upon the United States, we issued The 9/11 Commission Report, the official account of the horrific attacks of September 11, 2001. A decade later, we have reconvened, as private citizens, to reflect on the changes of the past decade and the emerging threats we face as a country. In recent months, we have spoken with some of the country's most senior current and recently retired national security leaders.

Here, in brief, is what we have learned:

- The struggle against terrorism is far from over—rather, it has entered a new and dangerous phase. Al Qaeda–affiliated groups are now active in more countries than before 9/11. The world has become more dangerous over the past few years.
- The American people remain largely unaware of the daily onslaught of cyberattacks against our nation's most sensitive and economically important electronic networks. Unfortunately, cyber readiness lags far behind this rapidly growing threat.
- Data collection and analysis are vital tools for preventing terrorist attacks, but must be tempered by appropriate measures to protect civil liberties. To date, the Government has done a poor job explaining to the public—with specificity, not generalities—what is being done and why. Government leaders must verify, and persuade a skeptical public, that data collection is no broader than necessary to keep the country safe.
- Congress has proved resistant to needed reforms in its oversight of homeland security and intelligence.
- Counterterrorism fatigue and a waning sense of urgency among the public threaten U.S. security.

BIPARTISAN POLICY CENTER
WWW.BIPARTISANPOLICY.ORG

THE ANNENBERG
PUBLIC POLICY CENTER
OF THE UNIVERSITY OF PENNSYLVANIA
WWW.ANNENBERGPUBLICPOLICYCENTER.ORG

The terrorist threat, while altered, remains very dangerous, and we still need vigorous and proactive counterterrorism efforts to protect the United States. In that spirit, we offer the following recommendations.

Sustaining Counterterrorism Authorities and Budgets

- National security leaders must communicate to the public—in specific terms—what the state of the threat is, how the threat is evolving, and what measures are being taken to address it.
- Congress and the President should update the September 2001 Authorization for the Use of Military Force. Continuing to rely indefinitely on that authorization without further congressional action threatens to erode the constitutionally mandated separation of powers.

Congressional Oversight

- Congress should oversee and legislate for DHS through one primary authorizing committee in each house.

National Intelligence Program Budget

- Congress should fund the entire National Intelligence Program (NIP) through a unitary appropriations bill. Routing all NIP appropriations through ODNI will improve the DNI's ability to manage the Intelligence Community as a cohesive entity.

Office of the Director of National Intelligence

- Future DNIs should replicate the current DNI's focus on: (1) coordinating the work of the various intelligence agencies, rather than replicating that work or turning ODNI itself into an operational entity; (2) advancing interagency information-sharing, unified IT capabilities, joint duty, and other Community-wide initiatives; and (3) providing centralized budgetary planning.
- The DNI should continue his efforts to instill counterterrorism information-sharing throughout the Intelligence Community.

Defending the Cyber Domain

- Government officials should explain to the public—in clear, specific terms—the severity of the cyber threat and what the stakes are for the country. Public- and private-sector leaders should also explain what private citizens and businesses can do to protect their systems and data.
- Congress should enact cybersecurity legislation to enable private companies to collaborate with the government in countering cyber threats. Companies should be able to share cyber threat information with the government without fear of liability. Congress should also consider granting private companies legal authority to take direct action in response to attacks on their networks.
- The administration should determine and communicate through appropriate channels what the consequences of cyber attacks against the United States will be, and then act on the basis of those statements. And we should work with our allies to establish norms of cyberspace, clearly defining what is considered an attack by one country on another.
- The administration and Congress need to clearly delineate the respective responsibilities of the various agencies in the cyber realm. DHS and other domestic agencies need to complement, rather than attempt to replicate, the technical capabilities of the NSA.

Transparency

- The National Archives and the administration should work expeditiously to make all remaining 9/11 Commission records available to the public.

Bipartisanship in National Security

- The 9/11 Commission's recommendations would not have been taken up with such urgency had its report been less than unanimous or perceived as partisan.
- Bipartisanship in national security is no less important today. America remains under terrorist threat, and it will take bipartisan trust and cooperation to develop counterterrorism policies that can be sustained until the struggle is won.

Former 9/11 Commission Members

Thomas H. Kean
Chair

Lee H. Hamilton
Vice Chair

Richard Ben-Veniste
Fred F. Fielding
Jamie S. Gorelick
Slade Gorton

Bob Kerrey
John F. Lehman
Timothy J. Roemer
James R. Thompson