



Testimony of Prof. Amos N. Guiora

**Professor of Law, S.J. Quinney College of Law
University of Utah**

guioraa@law.utah.edu

**“The Resilient Homeland: How DHS Intelligence Should Empower America to Prepare
for, Prevent, and Withstand Terrorist Attacks”**

**U.S. House of Representatives, Committee on Homeland Security
Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment**

May 15, 2008

TABLE OF CONTENTS

I. INTRODUCTION.....3

II. UNDERSTANDING THE THREAT.....3

III. EFFECTIVELY COUNTERING THE THREAT WHILE PRESERVING AMERICAN VALUES.....4

IV. ACCOUNTABILITY.....7

V. RESILIENCY.....7

VI. CONCLUSION.....13

APPENDIX-A MATRIX FOR DETERMINING EFFECTIVENESS.....14

APPENDIX-B MATRIX FOR IMPLEMENTING ACCOUNTABILITY.....20

**THE RESILIENT HOMELAND: HOW DHS INTELLIGENCE SHOULD EMPOWER AMERICA TO
PREPARE FOR, PREVENT, AND WITHSTAND TERRORIST ATTACKS**

I. INTRODUCTION

To ensure a resilient homeland in a post-9/11 society, the United States must have a homeland security strategy that (1) understands the threat, (2) effectively counters the threat while preserving American values, (3) establishes a system of accountability, and (4) creates public-private and federal-state partnerships facilitating intelligence sharing and the continuity of society in the aftermath of an attack.

It is necessary to work with clear definitions of the terms and concepts that frame this strategy. As I have previously articulated, “one of the greatest hindrances to a cogent discussion of terrorism and counterterrorism has been that the terms lack clear, universal definitions.”¹ For this reason, I will provide clear, concrete definitions of all key terms relevant to articulating strategy necessary for a resilient homeland.

II. UNDERSTANDING THE THREAT

A. TERRORISM: RECOMMENDED DEFINITION²

I define **terrorism** as:

Terrorism: Acts of politically based violence aimed at innocent civilians³ with the intent to cause physical harm, including death, and/or conducting psychological warfare against a population aimed at intimidating it from conducting its daily life in a normal fashion.

I have chosen the definition above because it captures the core elements of terrorism in clear and concise language. In reviewing scholarship and terrorists’ writings, the overwhelming impression is that causing harm (physical or psychological) to the innocent civilian population is

* Professor of Law, S.J.Quinney College of Law, University of Utah. Publications include *Global Perspectives on Counter-terrorism*, casebook (Aspen); *Constitutional Limits on Coercive Interrogation* (OUP); *Understanding Counterterrorism* (Aspen, Fall 2008); and, general editor, *Annual Review—Top Ten Global Security Law Review Articles, Vol. I* (Oxford University Press, 2008). I would like to thank Tara Harrison, Pete Lattin, Rachel Otto, Rich Roberts, Evan Tea, Artemis Vamianakis, and Tasha Williams.

¹ AMOS N. GUIORA, *GLOBAL PERSPECTIVES ON COUNTERTERRORISM* (Aspen Publishers 2007) [hereinafter GUIORA, *GLOBAL PERSPECTIVES*].

² *Id.* at 5.

the central characteristic of terrorist action. The available literature articulates that harming civilians is the most effective manner—from the terrorist mindset—to effectuate their goals.

While causing death or injury to the innocent civilian population is the “means to the end,” I also suggest that intimidation of the population is of equal importance from the terrorist perspective. The emphasis—whether resulting in death, injury, property damage, or intimidation—is the attack, in whichever form, on the innocent civilian population. Accordingly, government must develop counterterrorism policies that protect the innocent civilian population.

In addition, the importance of impacting “daily life” cannot—and should not—be underestimated. Terrorism is a daily grind; it must be understood in the context of daily attacks rather than one-time, dramatic-effect attacks (such as 9/11). Smaller, more frequent attacks, while perhaps less “dramatic,” have a much greater long-term effect on an innocent civilian population than does a one-time major event whose undeniable short-term effect may not linger.

III. EFFECTIVELY COUNTERING THE THREAT WHILE PRESERVING AMERICAN VALUES

A. COUNTERTERRORISM: RECOMMENDED DEFINITION

I define **counterterrorism** as:

Counterterrorism: The term must be viewed with two prongs (separate, yet of equal importance): the actions of a state, proactive or reactive, intended to kill or injure terrorists and/or to cause serious significant damage to the terrorist’s infrastructure⁴ and re-financing (financing) of socio-economic depressed regions of the world and educating communities regarding democracy and its values

Counterterrorism “is a never-ending war of attrition conducted in baby steps comprised of some victories [and] some defeats.” Defining counterterrorism is inextricably linked to the definitions and limits of terrorism. Counterterrorism must also be considered in the context of domestic balancing, international law, judicial activism, intelligence gathering, and interrogation of detainees.

Furthermore, any useful definition of counterterrorism requires a recognition of critical attributes of operational counterterrorism—“actionable intelligence, operational capability, and an understanding that swift victory is, at best, a fiction.”⁵ Counterterrorism in civil democratic societies must also be “conducted according to the rule of law and morality in armed conflict.”⁶

I propose that “operational counterterrorism is *effective* if the terrorist infrastructure suffers serious damage, thereby preventing a particular, planned attack from going forth and postponing or impacting plans for future attacks.”⁷ It is important to note, that “the damage is not permanent; terrorism cannot be defeated. However, the tactical impact of the measures above

⁴ GUIORA, GLOBAL PERSPECTIVES, *supra* note 1, at 139.

⁵ *Id.*

⁶ *Id.* at 140.

⁷ *Id.*

should not be minimized [B]y attacking the terrorist—rather than the state sponsor—the effectiveness model described above is not strategic and therefore inherently limited.”⁸

B. HOMELAND SECURITY: RECOMMENDED DEFINITION

I define **Homeland Security** as:

Homeland Security: A group of preventative measures undertaken by a state in an attempt to reduce the probability that a terrorist attack will occur. This strategy will be fluid, constantly reassessing the balance between rights of the individual and rights of the state. A realistic strategy must prioritize threats according to their probability and imminence.

Priorities must be established according to the limits, both ideologically and fiscally, that the American people will support. In examining government policy in the aftermath of 9/11 the lack of a concentrated and realistic focus is dramatically apparent. In seeking to address “all” possible threats, the policy was, in actuality, not a policy.

Numerous state, federal and municipal agencies must work together to ensure public safety in the United States. These include law enforcement agencies, the military and intelligence gathering and analysis realms, public health, and emergency response sectors, which coordinate activities with the community’s utilities, infrastructure, transportation, police and fire personnel. Job security, education, and community values in the aftermath of an attack are critical components of homeland security.

Executive branch documents name two particular areas the United States must be protected against in the context of homeland security: first, al-Qaeda, its affiliates (international and domestic), and those inspired by them; and catastrophic events, including natural disasters and man-made accidents.⁹ Scholars have suggested three priorities with respect to homeland security: border security, critical infrastructure protection, and intelligence analysis.¹⁰

C. EFFECTIVENESS: RECOMMENDED DEFINITION

I define **effectiveness** as:

Effectiveness: Effective counterterrorism causes the terrorist infrastructure to suffer serious damage—including damage to finances, intelligence, resources, or personnel—thereby preventing a particular, planned attack from going forth and/or postponing or impacting plans for future attacks while minimizing collateral damage, exercising fiscal responsibility, and preserving civil liberties.

⁸ *Id.*

⁹ *Id.* at 21.

¹⁰ Paul Light & James Lindsay, Council on Foreign Relations, Views of Homeland Security (2002); http://www.cfr.org/publication/6395/views_of_homeland_security.html.

This definition incorporates the following premises: (1) terrorism is not “100% preventable”; (2) counterterrorism must have a short-term (tactical) as well as a long-term (strategic) component; and (3) counterterrorism must be conducted while balancing competing interests of human life, financial cost, and civil liberty.

1. *Terrorism is not 100% preventable.*

Security analysts are wont to frame recommended counterterrorism measures in an effectiveness paradigm that demands “fool proof” safeguards. However, it must be clearly stated that terrorism is not 100% preventable. A successful terrorist attack does not mean existing counterterrorism measures are ineffective. The inverse is also true: the absence of terrorist attacks does not necessarily indicate existing counterterrorism measures are effective.

2. *Counterterrorism must have a short-term as well as a long-term perspective.*

If a counterterrorism strategy only targets short-term threats, it will likely overlook other (long-term) real threats. It is important to note that terrorist organizations define effectiveness through the prism of “long-term” strategic considerations.¹¹ “To understand the terrorist mindset, it is necessary to appreciate the determination, resilience, and single-mindedness with which terrorists work. Terrorists are willing to engage in a ‘war of attrition’ with enormous personal hardship for the individual and his immediate family to achieve specific goals. Counterterrorism, both strategically and tactically, must be premised on this reality. Engaging in a never-ending cycle of violence is one means by which terrorist organizations signal to various audiences (the general public, followers, and the relevant government) their commitment to the cause.

3. *Counterterrorism must be conducted in balance with competing interests of human life, financial cost, and civil liberty.*

“Finding a balance between national security and the rights of individuals is the most significant issue faced by liberal democratic nations developing a counterterrorism strategy. Without a balance between these two tensions, democratic societies lose the very ethos for which they fight. As Benjamin Franklin once said, ‘those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety.’¹² Indeed, it is imperative for democracies to avoid infringing on political freedoms and civil liberties. Yet, a government’s ultimate responsibility is protecting its citizens. This struggle to balance competing interests may be the most fundamental dilemma confronting democracies today.”¹³

¹¹ GUIORA, GLOBAL PERSPECTIVES, *supra* note 1, at 14.

¹² Benjamin Franklin, Pennsylvania Assembly: Reply to the Governor, Nov. 11, 1755. The Papers of Benjamin Franklin, Leonard W. Labaree ed., vol. 6, p. 242 (1963).

¹³ GUIORA, GLOBAL PERSPECTIVES *supra* note 1, at 19.

IV. ACCOUNTABILITY

A. RECOMMENDED DEFINITION

I define **accountability** as:

Accountability: Articulating in a transparent manner the effectiveness or ineffectiveness of a particular counterterrorism measure or strategy to one's superiors who have the power to rectify or discontinue measures.

The 9/11 Commission Report emphasizes in detail the need for standards of accountability in developing and implementing counterterrorism measures. The 9/11 Commission correctly stated that “effective public policies . . . need concrete objectives.”¹⁴ That is, in the struggle against terrorism, “agencies need to be able to measure success.”¹⁵

Without standards for accountability, Congress unwittingly creates an unfettered executive. “An unfettered executive, unrestrained by courts and legislatures, is detrimental to liberal democracies attempting to balance national security and individual rights.”¹⁶ Furthermore, when neither the legislature nor the judiciary rein the executive in, the former is bound to make mistakes whereby more-effective alternative means are often overlooked. Particularly in the murkiness and uncertainty of drawn-out amorphous operational counterterrorism, the executive must know there are clear guidelines determining accountability. Counterterrorism requires both strict separation of powers and checks and balances.

V. RESILIENCY

A. RECOMMENDED DEFINITION

I define **resiliency** as:

Resiliency: the capacity to prepare for, withstand, and endure terrorist attacks in order to assure continuity.

B. ESTABLISHING PARTNERSHIPS

Post-9/11 and in the wake of Hurricane Katrina, one of the most important lessons learned by the United States was the dire consequences of the break-down in communications between governmental agencies amongst themselves and with the private sector. Ineffective communication directly led to hesitation, confusion, lost time, and ultimately lost property and lives. Effective cooperation and coordination between governmental agencies within, and among, the federal, state, and local governments is essential to achieving a successful homeland

¹⁴ “What to Do? A Global Strategy?”, The 9/11 Commission Report (364).

¹⁵ *Id.*

¹⁶ GUIORA, GLOBAL PERSPECTIVES *supra* note 1, at 75.

security strategy. However, in order to realize resiliency, it is paramount that there is clear cooperation and coordination between the public sector and the private sector.

The importance of the public-private initiative is outlined in the Department of Homeland Security's recent *National Response Framework* ("NRF"), which defines the roles and responsibilities of the government (federal, state, local, and tribal) and the private sector (private business and/or NGO). As articulated in the NRF, "Government agencies are responsible for protecting the lives and property of their citizens and promoting their well-being. However, the government does not, and cannot, work alone. In many facets of an incident, the government works with the private-sector groups as partners in emergency management."¹⁷

The NRF outlines five critical roles played by the private sector during both disasters and terror attacks. *First*, privately owned critical infrastructures such as transportation, private utilities, financial institutions, and hospitals play a significant role in economic recovery from disaster and terror incidents.¹⁸ *Second*, "owners and operators of certain regulated facilities or hazardous operation may be legally responsible for preparing for and preventing incidents from occurring and responding to an incident once it occurs."¹⁹ *Third*, private business "provide response resources during an incident—including specialized teams, essential service providers, equipment, and advanced technologies."²⁰ *Fourth*, private entities "may serve as *partners* in local and State emergency preparedness and response organizations and activities."²¹ *Fifth*, private entities play an important role "as the key element of the national economy, private-sector resilience and continuity of operations planning, as well as recovery and restoration from an actual incident, represent essential homeland security activities."²²

A necessary component to establishing a resilient homeland, therefore, is a viable public-private sector partnership that is based on (1) *defined roles and responsibilities*, (2) articulating a coordinated *prevention-response plan*, and (3) repeated *training or simulation exercises* using the prevention-response plan against realistic disaster/terror scenarios.

1. *Defined Roles and Responsibilities*

In forging lasting partnerships between the public and private sectors, the private sector (private business and/or NGO) must define its role and responsibilities relative to the public sector on all government levels (local, state, and federal). Agencies such as the New York Red Cross must work alongside FEMA and the NYPD in an effort to respond to a disaster or another terrorist attack. These partnerships must be created using individual liaisons to private and public

¹⁷ National Response Framework (hereinafter "NRF"), Department of Homeland Security, (January 2008) at 18, available at <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.

¹⁸ *Id.*

¹⁹ *Id.* at 19 (this legal responsibility is exemplified by the owners and operators of nuclear power plants obligated under federal regulations to maintain emergency plans and conduct training for a response to such an incident).

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

entities predicated on clearly defined roles and responsibilities and open and frequent communication.

2. Articulating a Plan

The private sector must work closely with the public sector to articulate, develop and implement a disaster/terror prevention prevention/response plan. Such a plan must implement the clearly defined roles and responsibilities outlined above. Additionally, a proposed plan need take into account multiple scenarios addressing prevention and response thereby ensuring that different entities are seeking to achieve similar goals. The plan will ensure that different organizations see the “big picture” and know their particular responsibilities within the larger framework.

3. Training and Simulation

Fundamental to creating and maintaining the public-private sector initiative is consistent training and simulation exercises. Members of the private and public sector should conduct scenario based, simulation exercises (together and separately) with respect to the proposed plan. These exercises must include realistic disaster scenarios subject to real-life time constraints testing the effectiveness with which both the private and public sectors respond to complicated and complex attacks and disasters. Such training and simulation will ensure that the public and private sectors understand—both theoretically and practically—the vital necessity of cooperation and coordination. Such scenario based simulation exercises—in highlighting existing institutionalized and systemic weaknesses—most effectively facilitate the development of an effective homeland security strategy.

C. GOALS FOR PARTNERSHIPS

Public-private partnerships, if properly developed and implemented, are the key to economic recovery. Such a partnership—in the aftermath of a disaster or attack—facilitates the resilience of critical infrastructure including transportation, utilities, financial institutions, and hospital care. By strategically strengthening security, sharing intelligence, and creating plans for post-attack procedures (including evacuation plans, transportation plans, identifying places of refuge, and providing basic supplies to aid first-responders) such partnerships become the key to a secure and resilient homeland.

1. Prevention & Resiliency Through Intelligence Sharing

The Department of Homeland Security (DHS) has provided excellent guidance regarding how to frame intelligence sharing between the public and private sectors. The importance of information before, during and after a disaster or attack is vital to resilience. Information sharing is, perhaps, the single most important aspect of successful resilience. Information sharing requires government agencies (federal, state and local) to share information both amongst themselves and with the private sector. Furthermore, it requires that the private sector—subject to existing legal and constitutional limits—share information with the public sector. Successful information sharing requires cooperation and coordination both internally (within sectors) and cross sectors (between public-private entities).

The process must be institutionalized, requiring a fundamental re-articulation of homeland security strategy. While various public sector agencies are historically hesitant (predicated on policy, culture and legal restraints) to share information with other agencies—much less the private sector—the lessons of 9/11 and Katrina speak for themselves. Resilience in the aftermath of either disaster or attack requires federal, state and local government agencies to understand that information sharing is vital to the nation’s homeland security. That information sharing process must include the private sector. Otherwise, the mistakes of yesterday will inevitably re-occur.

To that end, DHS recommends that public and private agencies:²³

1. Prepare memorandums of understanding and formal coordination agreements describing mechanisms for exchanging information regarding vulnerabilities and risks;
2. Use community policing initiatives, strategies, and tactics to identify suspicious activities related to terrorism;
3. Establish a regional prevention information command center; and
4. Coordinate the flow of information regarding infrastructure.

In addition, the National Infrastructure Advisory Council published a report on private and public sector intelligence coordination and made the following recommendations:²⁴

²³ *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships: New Realities Law Enforcement in the Post-9/11 Era*, U.S. Department of Justice Bureau of Justice Assistance, September 2005, at vi, *available at* <http://www.ncjrs.gov/pdffiles1/bja/210678.pdf>.

²⁴ National Infrastructure Advisory Council Public Private Sector Intelligence Coordination Final Report and Recommendations by the Council, July 11, 2006, *available at* http://www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf

1. **Senior Executive Information Sharing:** Develop a voluntary executive-level information sharing process between critical infrastructure CEOs and senior intelligence officers. Begin with a pilot program of volunteer chief executives of one sector, with the goal of expanding to all sectors.
2. **Best Practices for the Private Sector:** The U.S. Attorney General should publish a best practices guide for private sector employers to avoid being in conflict with the law. This guide should clarify legal issues surrounding the apparent conflict between privacy laws and counter terrorism laws involving employees. Moreover, it should clarify the limits of private sector cooperation with the IC
3. **Existing Mechanisms:** Leverage existing information-sharing mechanisms as clearinghouses for information to and from critical infrastructure owners and operators. This takes advantage of the realities that exist sector by sector.
4. **National-Level Fusion Capability:** Establish or modify existing government entities to enable national- and state-level intelligence and information fusion capability focused on Critical Infrastructure Protection (CIP).
5. **Staffing:** Create additional —Sector Specialist positions at the executive and operational levels as applicable in the IC. These specialists should be civil servants who have the ability to develop a deep understanding of their private sector partners.
6. **Training:** Develop an ongoing training and career development program for sector specialists within intelligence agencies.
7. **RFI Process:** Develop a formal, and objectively manageable, homeland security intelligence and information requirements process, including requests for information (RFIs). This should include specific, bi-directional processes tailored sector by sector.
8. **Standardize SBU Markings and Restrictions:** The Federal government should rationalize and standardize the use of SBU markings, especially “For Official Use Only.”

2. *Providing Critical Infrastructure—Continuity Planning*

In order to play their essential role of re-establishing critical infrastructure after an attack, private entities must have continuity plans. These plans must take into account the known threats,²⁵ which are only “known” through intelligence sharing between the public and private sectors, as discussed above. These plans must also take into account the components essential to re-establishing the service that the particular entity provides. These plans must provide details regarding how the particular entity will promptly resume service, which may differ depending on the form of attack. In addition, the plan must articulate how the entity will communicate with the

²⁵ See Appendix A for a classification of “known” risks. For this discussion, all risks, including the imminent, foreseeable, long-range, and uncertain are considered “known” threats.

public sector after an attack and what, if any, assistance the entity will surely or likely need from the public sector in order to promptly re-establish service.

The United Kingdom has enacted legislation requiring contingency plans. That legislation, the Civil Contingencies Act, requires certain private entities to “maintain plans to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable.”²⁶ Specifically, entities are required to make arrangements to warn and inform the public, handle emergencies, and make provisions to ensure that the entity’s ordinary functions can be continued to the extent necessary.²⁷ To ensure effectiveness, the legislation also requires entities enact training programs for those directly involved in the execution of the continuity plan.²⁸ To assist the entities, the legislation requires local authorities to provide advice and assistance to businesses and voluntary organizations in relation to business continuity.²⁹

New York City has taken a first step at creating similar legislation. New York City’s Local Law 26 (2004) amended the existing administrative code in relation to building safety in the city.³⁰ In particular, this new law requires owners of big buildings, in coordination with the FDNY, to prepare detailed plans, train staff members and conduct full evacuation drills of the entire building every three years.³¹ While evacuation plans are an essential first component of a contingency plan, they are not enough to establish even the hope for a resilient homeland.

The following is a list of suggested measures that would most effectively facilitate resilience in the aftermath of a disaster or attack:

²⁶ UK Resilience: Business Continuity, May 7, 2008, *available at* <http://www.ukresilience.info/preparedness/businesscontinuity.aspx> (last visited May 10, 2008).

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.*

³⁰ See Jim Dwyer, Evacuation Plans Due for High Rises in New York City, *NEW YORK TIMES* (August 5, 2004), *available at* <http://query.nytimes.com/gst/fullpage.html?res=9B03E2DA153CF936A3575BC0A9629C8B63> (last visited April 11, 2008).

³¹ *Id.*

- Educate the private sector regarding the importance of continuity plans
- Educate the public about the importance of continuity plans for the private sector
- Offer expertise in the form of training to enable private entities to create continuity plans
 - Require oversight in exchange for the expertise
- Pass legislation that puts the private sector on notice regarding the importance of continuity plans
- Encourage states to pass legislation mandating continuity plans, to the extent a state has such power
- Offer financial incentives, possibly tax incentives, to entities that establish continuity plans and continue updating those plans.

VI. CONCLUSION

Not only the public sector, but also the private must contemplate resiliency must before a terrorist attack occurs. Sophisticated planning—based on scenario based simulation exercises-- will significantly contribute to creating a resilient homeland. The first step to making the homeland resilient to a terrorist attack requires defining terrorism, counterterrorism, effective counterterrorism and accountability.

Terrorism poses a threat that cannot be eliminated. Nor can the government truthfully claim that it will prevent all terrorist attacks. While measures can be implemented to prevent attacks civil, democratic societies must recognize that at some terrorist attacks will succeed. In an effort to minimize *both* the chances of a particular attack and the consequences of a successful attack it is necessary to create public-private sector partnerships.. Such partnerships must be based upon communication, mutual (subject to legal and constitutional limits) information sharing and defined roles. Such partnerships will facilitate the development of continuity plans seeking to ensure the restoration of infrastructure vital to the nation. Resilience depends on such cooperation; information sharing between and among the public and private sectors is the essence of that relationship.

APPENDIX-A

MATRIX FOR DETERMINING EFFECTIVENESS

The first step in creating an effective counterterrorism measure is analyzing the threat. To that end, the following questions must be answered:

Analyzing the Threat

1. What is the threat the State faces?
2. Who is responsible for planning the threat?
3. Who is responsible for financing the threat?
4. Who is responsible for carrying out the threat?
5. When will the threat likely be carried out?

Once these questions are answered, the threat can be placed on an imminent continuum with the understanding that one large threat may be comprised of smaller, more manageable, threats. The imminent continuum has four major benchmarks: Imminent, Foreseeable, Long-range, and Uncertain.

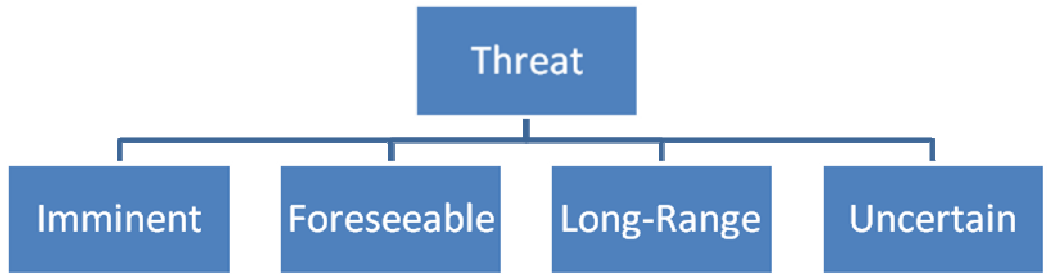
Imminent threats are those that are to be shortly conducted; as an example a “hot” intelligence report suggests that a bomb will be detonated *tomorrow* at 9:11 a.m. at a domestic terminal at JFK airport.

Foreseeable threats are those that will be carried out *within a year* and are therefore more distant than an imminent threat. For example, a foreseeable threat includes valid intelligence that indicates that terrorists will shortly begin bringing explosives onto airplanes in liquid substances.

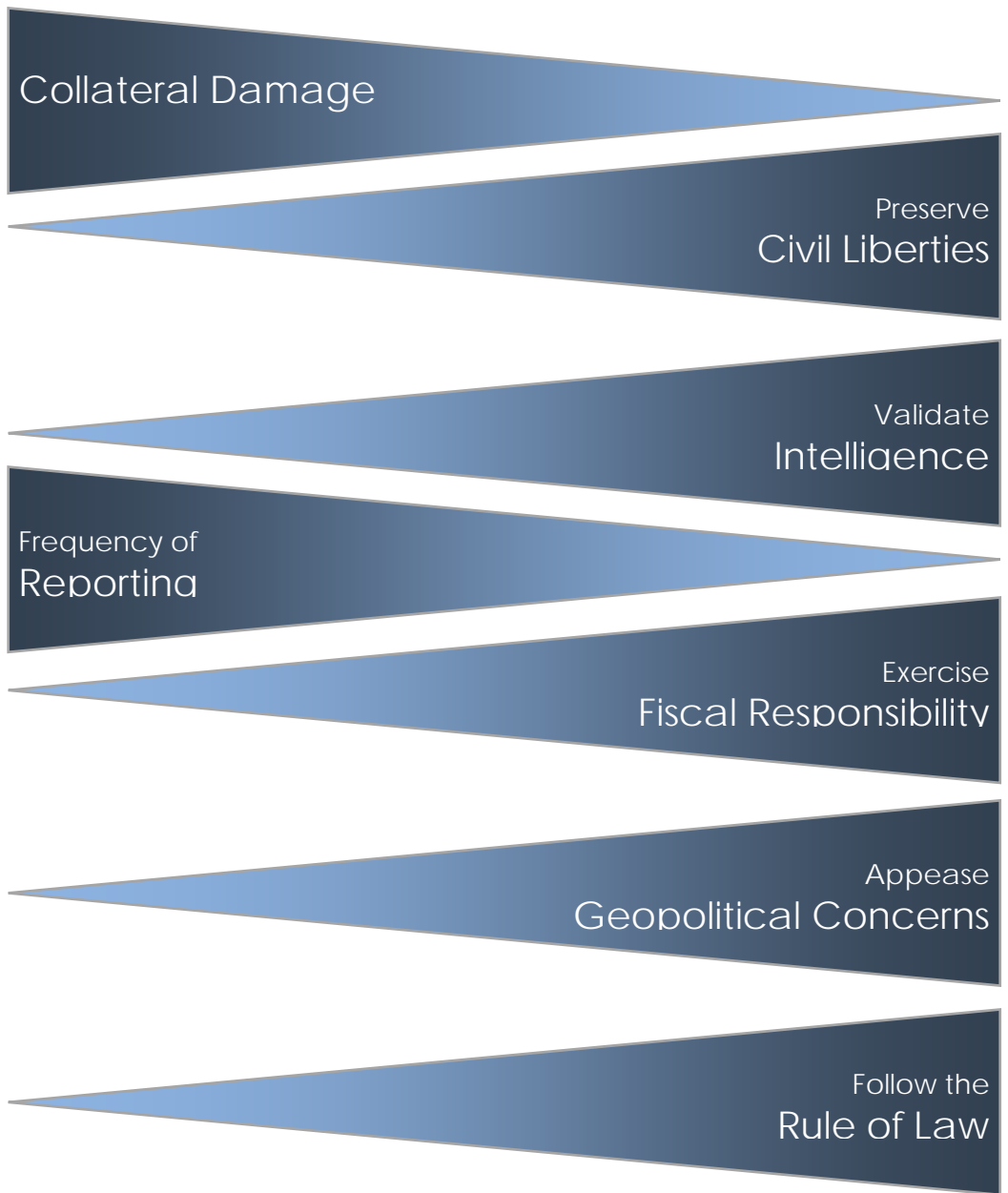
Long-range threats are specific threats that may reach fruition at an unknown time; for example, terrorist’s training with no operational measure specifically planned would fit in this category.

Uncertain threats constitute those that invoke general fears of insecurity. As a result of train bombings in England and Spain travelers in the United States might potentially or conceivably feel insecure riding trains without bolstered security. This would be true regardless of whether there is valid intelligence indicating terrorists intend to start targeting trains in the United States.

Where a particular threat fits on the continuum of imminence necessarily relates to the balance that must be struck between national security and competing interests related to that threat. The following chart depicts the imminence spectrum graphically. The threat of a terrorist attack is listed from left to right, progressing from imminent to uncertain. The vertical column on the left lists seven factors that counterterrorism measures must balance in considering these threats. The balancing factors include collateral damage, civil liberties, valid intelligence, frequency of reporting, fiscal responsibility, geopolitical concerns, and the rule of law. Understanding these factors is crucial and detailed explanations are outlined below the chart. The triangular bars in the body of the graph represent the relative priority placed on each of these factors in the event of an imminent, foreseeable, long-range, or uncertain threat of a terrorist attack. The thicker the triangular bar, the greater the importance of the corresponding factor. For example, the triangular bar representing the first factor, collateral damage, is thicker for an imminent threat and thinner as it reaches an uncertain threat. This bar indicates that collateral damage is more permissible for imminent counterterrorism measures than for foreseeable, long-range, or uncertain measures.



- Balancing Factors**
- Collateral Damage
 - Civil Liberties
 - Valid Intelligence
 - Frequency of Reporting
 - Fiscal Responsibility
 - Geopolitical Concerns
 - Rule of Law



1. Collateral Damage

“Collateral damage requires a minimizing of loss of civilian life in a military operation; proportionality requires that civilian losses be proportional to the military advantage, which will be assessed as follows: what were the factors in target selection and what were the means and methods of attack?”³² Ultimately, the public is willing to stomach greater collateral damage the more imminent a threat is.³³ However, alternative effective measures that would lessen collateral damage must also be considered. In doing so, collateral damage becomes only one of many factors to be weighed when selecting one measure over others.

2. Civil Liberties

“Liberal democratic societies that unilaterally decide on ‘self-imposed restraints’ inherently limit their responses to terrorism.”³⁴ However, “[b]alancing legitimate national security needs against the rights of those individuals living in the nation is a true test of a nation’s adherence to democratic values.”³⁵ Any suspension of constitutionally guaranteed liberty must be weighed against legitimate national security considerations. That is a balancing dilemma that decision makers must address.

3. Validating Intelligence

To be valid, intelligence must be reliable, viable, and corroborated.³⁶ Needless to say, reliable, viable, and corroborated intelligence may be difficult to obtain. In all circumstances, reasonable effort should be made to obtain valid intelligence before action is taken.³⁷ However, the level of imminence dictates the definition of reasonable (both with respect to the credulity of the information and how much time is allotted to its corroboration).

4. Frequency of Reporting

This factor encompasses the forthcoming accountability discussion. Congress has mandated annual reports on terrorist threats.³⁸ These reports, however, are too infrequent for imminent and foreseeable threats and possibly inapplicable to uncertain threats. Counterterrorism measures taken to address imminent threats should be reported to Congress

³² GUIORA, GLOBAL PERSPECTIVES, *supra* note 1, at 63.

³³ The Geneva Convention states that minimizing collateral damage is a requirement of International Law and nations must limit collateral damage in times of war. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1) art. 57 (2).

³⁴ GUIORA, GLOBAL PERSPECTIVES *supra* note 1, at 19.

³⁵ *Id.*

³⁶ *Id.* at 242.

³⁷ *Id.*

³⁸ Sec. 216, H.R. 1, “Implementing the 9/11 Commission Recommendations Act of 2007,” *available at* <http://www.cfr.org/content/publications/attachments/911.pdf> (The Assistant Secretary for Infrastructure Protection must compile an annual report notifying Congress of the following: 1. Changes in the infrastructure vulnerability from the year before 2. Explanation of the greatest risks facing the country 3. Recommendations to mitigate those risks.).

after the threat has passed. Only in this way can Congress have meaningful review of significant Executive actions.

Foreseeable threats should be reported to Congress when the threat is identified. This reporting enables Congress to coordinate efforts, emphasize to the Executive the need for balancing, and better understand how various agencies are detecting and countering various threats. Congress has appropriately addressed the need for annual reporting regarding long-range threats.

Conversely, many uncertain threats will not fall within the scope of the federal government.³⁹ Threats that do, may appropriately be addressed when agencies address long-range threats. State legislatures should implement reporting procedures for uncertain threats that exist on a state-level.

5. *Fiscal Responsibility*

Financial costs necessarily limit the quantity of counterterrorism measures a nation may conduct. With limited resources, government must pick and choose which measures will most effectively counter short-term and long-term threats. Although the need for fiscal responsibility lessens as a threat becomes more imminent, careful planning for potential attacks will allow careful use of financial resources even in the face of imminent threats. This would, thereby, free resources for countering long-range and uncertain threats. Thus, financial responsibility needs to be considered not only in light of the threat level of a particular threat, but in light of an overarching counterterrorism strategy.

6. *Geopolitical Concerns*

Counterterrorism necessarily raises international concerns because the threat does not reside exclusively within a nation's borders. Opinions of other states are not the only factors, but the court of international opinion must be considered when selecting a particular counterterrorism measure. Wrong choices cause the United States to lose global influence or be an impetus that turns swayables into terrorists. If measures are chosen under the consideration of geopolitical concerns, then weight must be given to those that have the potential to impact geopolitical considerations.. Of course, in the light of an imminent threat, geopolitical concerns do not weigh when creating deterrence strategies for uncertain threats or strategies to counter long-range threats.

7. *Rule of Law*

³⁹ “One example might be dissemination of preparedness information about potential threats and emergency plans. The state of California currently has a law pending that would ‘require the State Department of Education to electronically distribute disaster preparedness educational materials and lesson plans that are currently available to local education agencies.’” Amos Guiora & Kyle McKenzie, *A Framework for Evaluating Counterterrorism Regulations*, Mercatus Policy Series, Policy Resource No. 3, 25–26 (2006) (quoting Assembly Bill No. 103, California Legislature 2005–06 Regular sessions, *Legislative Counsel's Digest*, last amended May 22, 2006, <http://www.homeland.ca.gov/legislative.html>).

The rule of law protects free democracies and sets a basis for trust between nations. In order to best adhere to the rule of law counter terrorism measures should be drafted in advance of such an actual threat. Such measures should dictate which laws may be relaxed and to what extent when facing an imminent threat. To wait until a threat is present denies government the opportunity to make careful and conscious choices that will provide security to the public while balancing their rights.

APPENDIX-B

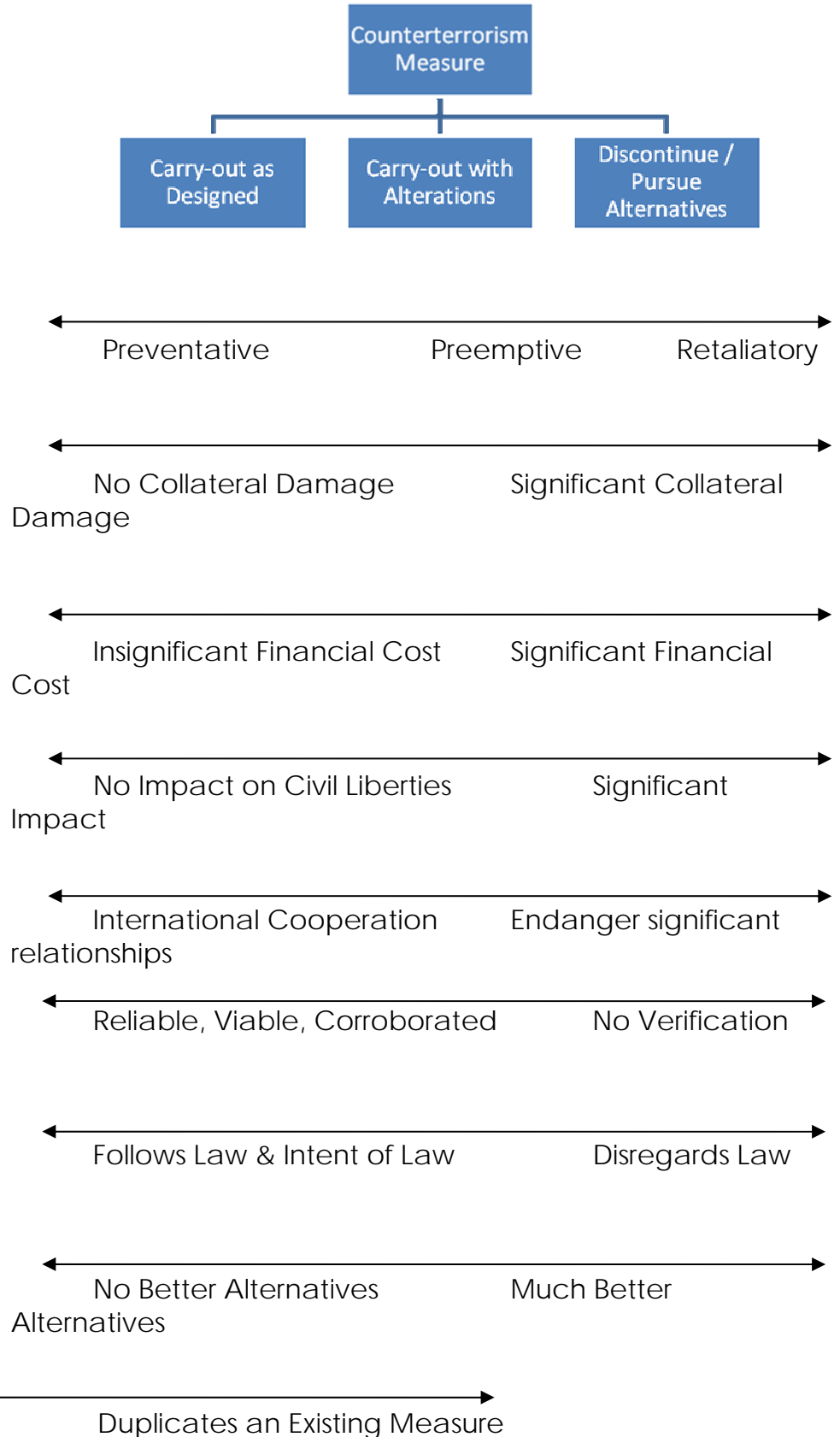
MATRIX FOR IMPLEMENTING ACCOUNTABILITY

On a practical level, Congress must ask questions that enable it to determine whether a particular counterterrorism measure should proceed as defined, should be altered, or should be discontinued. The ultimate conclusion (whether to continue, alter, or discontinue a measure) cannot be reached by the answer to only one question, such as “what is the financial cost?”. Rather, the conclusion will be reached by recognizing a balance between numerous factors. For example, the nation may be willing to pay a higher financial price tag if the measure preserves civil liberties to a greater extent than less-expensive alternatives.

The matrix below lists the questions that must be answered before Congress should decide whether a measure should be continued, altered, or discontinued. The matrix represents these three options graphically at the top of the chart, from left to right. On the left, are the questions that Congress must ask to determine whether a measure is effective: (1) is the measure preventative, preemptive, or retaliatory; (2) what is acceptable collateral damage; (3) what are the financial costs; (4) what are the costs to civil liberties; (5) what are the geopolitical costs; (6) how valid is the intelligence; (7) to what extent does the measure follow the rule of law; (8) what alternatives exist; (9) to what extent does the measure overlap with existing measures? The body of the matrix includes horizontal spectrums that allow for real-world answers to the accountability questions. Only after answer all of the accountability questions can Congress determine whether the particular measure should be continued, altered, or discontinued. For complicated measures that elicit mixed results, Congress can view the matrix and determine if the measure strikes a good balance between answers that encourage implementation and answers that encourage discontinuance or non-implementation. The questions in the matrix, if asked in a timely manner, will lead to effective Congressional oversight

The Counterterrorism Measure Must Define . . .

1. Whether the measure is preventative, preemptive, or retaliatory
2. What is acceptable collateral damage
3. What are the financial costs?
4. What the measure costs in civil liberties
5. What are the geopolitical costs
6. How valid is the intelligence
7. To what extent does the measure follows the rule of law
8. What alternatives exist
9. To what extent does



1. Is the Measure Preventative, Preemptive, or Retaliatory?

Preventative measures counter terrorism before terrorists are prepared to strike. These measures work to prevent swayables from becoming terrorists, destroy training camps and other terrorist infrastructure, and strengthen nations that are vulnerable to terrorists. Preemptive measures prevent particular terrorist acts from being carried out. Retaliatory measures are emotional responses to terrorist attacks. Preventative and preemptive measures can be considered self-defense. However, retaliatory measures are unlawful.

2. What Potential Collateral Damage does the Measure Cause?

While the goal is to minimize collateral damage, this factor is weighed in light of the other factors. It is appropriate to balance collateral damage with financial cost, cost to civil liberties, and risk to personnel.

3. What is the Financial Cost of Conducting the Measure?

Operational counterterrorism can be a costly endeavor. However, cost must be balanced with the effectiveness of the measure (including the measure's cost on civil liberties, collateral damage, the nature of the target, and more).

4. What is the Cost to Civil Liberties of Conducting the Measure?

Civil liberties define our democracy. When a measure proposes to suspend civil liberties, Congress must decide whether there are alternative measures that have a smaller impact in the context of legislative oversight.

5. How Valid is the Intelligence that Led to Implementing the Measure?

To be valid, intelligence must be reliable (to what degree is the source reliable?), viable (to what degree can the threat actually be carried out?), and corroborated (who or what else provides similar intelligence). Unless circumstances such as an imminent threat warrant otherwise, counterterrorism measures that infringe on the civil liberties must be valid.

6. What Geopolitical Concerns Arise Due to the Measure?

Ideally, the United States would work in concert with the other nations of the world when conducting global operational counterterrorism. However, achieving global consensus and support can be timely, costly, and at times impossible. Yet, the United States must understand the risks it takes when it conducts a particular measure unilaterally. Decision makers must determine if they are willing to accept the geopolitical consequences.

7. Does the Measure Follow the Rule of Law

To be valid, counterterrorism measures must be rationally based on Constitutional and legal foundations. Congress has a duty to create laws that empower agencies but also to enact clear guidelines that limit the agencies' power. Clear guidelines will enable the judiciary to hold agencies accountable for their counterterrorism efforts. Further, clear guidelines will instill with Congress greater control over counterterrorism efforts.

8. What Alternatives Exist?

Alternatives must always be identified and viable alternatives explored. Without recognizing the alternatives, Congress cannot know whether a particular measure is actually cost-effective.

9. To What Extent does the Measure Overlap with Existing Measures?

Although a measure may pass the other nine explorations without pause, this question is still significant. If a particular measure overlaps with another existing measure, then one of the two measures should be scaled back to the extent the two overlap to avoid unnecessary social and financial costs.