UNIVERSITY OF COLORADO AT COLORADO SPRINGS
COLLEGE OF ENGINEERING AND APPLIED SCIENCE
COMPUTER SCIENCE DEPARTMENT

Ph.D Thesis Proposal

Informing Homeland Security Strategy Through Applied Game Theory

November 2011

Richard White

(This page intentionally blank.)

Respectfully submitted by:
Richard White
Ph.D. Candidate
1827 Snowflake Dr.
Colorado Springs, CO 80921
rwhite1354@peoplepc.com
rwhite2@uccs.edu
Phone 719-360-3805

Date:
November 16, 2011

Advisor:
Dr. Edward Chow

Committee Members:
Dr. Edward Chow (chair)
Dr. Terrance Boult
Dr. Xiaobo Zhou
Dr. Scott Trimboli
Dr. Stan Supinski

(This page intentionally blank.)

Abstract

The lesson of 9/11 is not the threat of Islamic extremists. The lesson of 9/11 is that nineteen young men armed with nothing more than box cutters and pepper spray inflicted as much damage and destruction on September 11, 2001, as the Imperial Japanese Navy on December 7, 1941. 9/11 opened the eyes of the nation and the world to the threat of critical infrastructure as a means for small groups or individuals to inflict catastrophic damage. Critical infrastructure joined the ranks of weapons of mass destruction as a means for achieving macroterrorism, over 500 deaths or $1B in damages. This realization prompted the largest reorganization of the US federal government since World War II, and the development of homeland security strategy to orchestrate counterterrorism efforts across all of government, including state, local, tribal, and federal. The question we address in this thesis proposal is whether or not it's a good strategy, and might it not be improved? We note that current homeland security strategy has no theoretical underpinning, and after examining several alternatives, propose gaming theory as an appropriate framework. A theoretic framework offers many advantages to strategy formulation, among them being a methodological basis for disciplined development, easier communication, and objective evaluation. Among available theoretic frameworks, game theory seems most appropriate because it mathematically captures strategic interactions between human agents who act with purpose and objective, even if their actions aren't perfectly understood. Game theoretic analysis by Sandler and others has already provided insight into broader counterterrorism policies on 1) negotiating with terrorists, 2) target substitution, 3) international cooperation, and more. Their methods are restricted, however, to the ability of framing specific problems within a small set of parameters amenable to mathematical computation. We wish to extend Sandler's work to better inform homeland security strategy, specifically with respect to the macroterrorism threat. The key is framing the problem. We suggest a method using heuristic analysis of a representative macroterrroism model. We contend that macroterrorism is a crime, and as such, may be thwarted by eliminating either *means*, *motive*, or *opportunity*. We evaluate the various weapons of mass destruction and critical infrastructure to construct a Macroterrorism Risk Model illuminating critical relationships between different components. We then evaluate the Macroterrorism Risk Model using the Denial Topoi of *means*, *motive*, and *opportunity* to identify three homeland security problems potentially amenable to game theoretic analysis. We propose solving these problems and publishing the work over the next twelve months in partial fulfillment of our Ph.D. dissertation requirements, and to strengthen and improve the nation's homeland security strategy.

(This page intentionally blank.)

Table of Contents

Table of Figures

(This page intentionally blank.)

1 Introduction

As the United States commemorates the tenth anniversary of the September 11th, 2001 terror attacks (9/11), we recognize that we are a nation profoundly changed. Our military is engaged in the longest war in the nation's history.[1] Our government has undergone the most extensive reorganization since World War II.[2] Our civil liberties are at risk as at no other time since the founding of the nation.[3] Ten years, 11,300 American lives[4] (1 p. 3), and $2.3T dollars later[5] (1 p. 7), the fundamental question remains: are we safe?

Despite killing Osama bin Laden[6] May 2, 2011, the mastermind of 9/11 (2), few would argue that the country is safe from another terrorist attack (3 p. 6). Even as Secretary of Defense Leon Panetta declares that al-Qaeda is nearing defeat (4), its legacy remains alive, with many eager to pick up the mantle (5 p. 5). Though Osama bin Laden is dead, his threat remains.

Yet, what exactly is the threat from Osama bin Laden and al-Qaeda? What is it about 9/11 that instigated this massive investment of the nation's blood and treasure? Why don't we feel secure? Why are we not safe?

The answer is not Islamic extremism. If it were, then the US might have reacted in a similar fashion following the 1993 attacks on the World Trade Center[7] (6 pp. 71-73), or even earlier,

[1] In October 2011, US military operations in Afghanistan surpassed 104 months, longer than the US involvement in Vietnam, formerly the longest conflict in US history.

[2] As a direct result of 9/11, Congress authorized establishment of the Transportation Security Administration (2002), United States Northern Command (2002), Department of Homeland Security (2003), National Counterterrorism Center (2003), and the Office of the Director of National Intelligence (2004).

[3] Denial of habeas corpus to Guantanamo prisoners, kidnapping terror suspects, warrantless wiretaps, water boarding, airport scanners, and capture/kill lists have all pressed the bounds of Constitutional authority. While past presidents have suspended US civil liberties in times of crisis or war (Adams – Alien and Sedition Acts, Lincoln – Suspension of Habeas Corpus, Roosevelt – Japanese American Internment), judicial precedent threatens to embed current measures in customary law.

[4] 3,000 killed on 9/11 + 6,000 US soldiers + 2,300 US Contractors killed in Afghanistan and Iraq.

[5] $1.3T Congressional War Appropriations + $326B Additions to Pentagon Budget + $185B Interest on War Appropriations + $33B Veteran's Medical & Disability + $74B Related International Assistance + $401B Homeland Security Spending.

[6] "Osama" or "Usama"? Both are transliterations of an Arabic name "أسامة". Standard transliteration uses a systematic convention of rendering Arabic scripts, however, it does not carry enough information to accurately write or pronounce the original Arabic word, consequently alternative transcriptions may result. A word has a primary transcription if at least 75% of all references in English use the same transcription, or if a reference shows that the individual self-identified with a particular transcription, and if that transcription does not contain any non-printable characters. The primary transcription of the leader of al-Qaeda (itself a primary transcription of standard form al-Qa`ida) is "Osama bin Laden" (Wikipedia).

[7] On February 26, 1993, a huge bomb went off beneath the two towers of the World Trade Center. Ramzi Yousef, the Sunni extremist who planted the bomb, said later that he had hoped to kill 250,000 people. He and his accomplices were successfully captured by the FBI, and later prosecuted and sent to prison. The 9/11 Commission Report cites the 1993 bombing as signaling a new terrorist challenge, one whose rage and malice had no limit. The 9/11 Commission also implicates the superb investigative and prosecutorial effort in creating a false sense that the law enforcement system was well-equipped to cope with terrorism.

after the 1983 attacks that killed 241 Marines in Beirut, Lebanon[8] (6 p. 96). Although the 1995 National Intelligence Estimate[9] warned of the threat from Islamic terrorism, many officials continued to think of terrorists as agents of states (Saudi Hezbollah acting for Iran against Khobar Towers[10]) or as domestic criminals (Timothy McVeigh in Oklahoma City[11]) (6 p. 108).

The answer is not the high number of casualties caused by 9/11. Officially, 2,997 people died as a direct result of al-Qaeda's attacks on 9/11 (7 p. 1). While tragic, these numbers fall far short of the leading causes of death in the US: more than half-a-million citizens die of heart disease each year. Heart disease, cancer, respiratory disease, and vascular disease collectively kill more than 1.5M Americans annually, occupying the top four positions in the Centers for Disease Control and Prevention National Vital Statistics Report (8 p. 5). Unintentional deaths due to accident rank fifth on the list with 117,176 fatalities. Deaths due to terrorism are classified under Assault (homicide), and rank 15th (out of 16) on the list with 16,591 deaths (2009) (8 p. 35), just above the final category of "All other causes" (471,455) (8 p. 5). Since 2001, there have been only 25 deaths attributed to terrorism in the US (7 p. 2). In fact, the death rate from terrorism has dropped in half (0.24 per terrorist attack) compared to the decade before 9/11 (.42 deaths per terrorist attack) (7 p. 2).

> *The reason for the dramatic US response following 9/11 has to do with the fact that on September 11, 2001, nineteen men inflicted as much damage on the United States as that caused by the Imperial Japanese Navy on December 7, 1941*[12].

While by no means as threatening as Japan's act of war, the 9/11 attack was in some ways more devastating. It was carried out by a tiny group of people, not enough to man a full platoon. Measured on a governmental scale, the resources behind it were trivial[13]. The group itself was dispatched by an organization based in one of the poorest, most remote, and least industrialized countries on earth (6 pp. 339-340).

The lesson of 9/11 was not the threat posed by Islamic extremists, or even the tactic of terrorism. The lesson of 9/11 was that small groups or individuals can subvert critical infrastructure (CI) to inflict damage on a scale that once required a nation's military might. 9/11 ushered in the threat of macroterrorism:

---

[8] In 1983, a Hezbollah suicide bomber drove a truck bomb into the Marine barracks in Beirut, killing 241 US Marines. The Marines had been sent to Lebanon on a peace keeping mission during the Lebanese civil war. As a result of the attack, President Reagan withdrew the Marines from Lebanon; a reversal routinely cited by jihadists as evidence of US weakness according to the 9/11 Commission.

[9] National Intelligence Estimates (NIEs) are authoritative documents produced for policymakers assessing intelligence related to a particular national security issue. While the 1995 NIE did not mention bin Laden or al-Qaeda by name, it clearly warned that civil aviation, Washington landmarks such as the White House and Capitol, and buildings on Wall Street were at the greatest risk of a domestic terror attack by Muslim extremists (Wikipedia).

[10] On June 25, 1996, 19 US servicemen were killed by Muslim extremists employing a truck bomb against Khobar Towers, an eight-story barracks housing US Air Force personnel in the city of Khobar, Saudi Arabia.

[11] On April 19, 1995, 168 were killed and 680 injured when a truck bomb destroyed the Alfred P. Murrah Federal Building in downtown Oklahoma City . Timothy McVeigh was arrested within 90 minutes for an unrelated offense of driving without a license plate. In 1997 he was convicted of murder, and executed June 11, 2001.

[12] On the morning of December 7, 1941, a strike force of the Imperial Japanese Navy struck the US naval base at Pearl Harbor Hawaii. The base was attacked by 353 Japanese fighters, bombers and torpedo planes in two waves, launched from six aircraft carriers. Four US Navy battleships were sunk, 188 aircraft destroyed, 2,402 Americans killed, and 1,282 wounded (Wikipedia).

[13] Khalid Sheikh Mohammed, the architect of 9/11, estimated the total cost of the operation at less than $400,000.

> *"Macroterrorism" is any single malicious act that inflicts more than 500 deaths or $1B in damages* (9 p. 5).

9/11 exposed the vulnerability of technological society to catastrophic loss by anybody who possesses the means, motive, and opportunity. The remainder of this paper, and the purpose of this dissertation proposal is to examine how they can be stopped.

We will begin by examining the threat of macroterrorism. We will continue by exploring the US response to macroterrorism and the development of homeland security strategy. We will assess current homeland security strategy and analyze alternative theoretic underpinnings to strengthen it. We will recommend game theoretic analysis of terrorism risk to better inform homeland security strategy against macroterrorism. We will review gaming theory contributions to broader counterterrorism strategy, and suggest a new mechanism for applying similar analysis to homeland security strategy. We will conclude by applying the Denial Topoi of means, motive, and opportunity against our Mactroterrorism Risk Model to identify three specific areas of homeland security strategy amenable to game theoretic analysis. We propose solving these problems and publishing the results in partial fulfillment of our Ph.D. dissertation requirements.

2 The Macroterrorism Threat

9/11 did not create macroterrorism. 9/11 only exposed society's vulnerability to macroterrorism through other means. Prior to 9/11, most experts considered weapons of mass destruction (WMD) the primary avenue for catastrophic attack (10). These concerns were not unfounded[14].

According to Section 2302, Title 50 United States Code (USC), War and National Defense, a "weapon of mass destruction" is:

> *(1) Any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of—*
>
> *(A) toxic or poisonous chemicals or their precursors;*
>
> *(B) a disease organism; or*
>
> *(C) radiation or radioactivity.*

Given the above definition, chemical, biological, radiological, and nuclear weapons, CBRN, have become commonly associated classes of WMD[15]. Above all other classes of weapons, these pose a significant danger in their capacity to wreak catastrophic damage merely by their employment (11 p. 1). All were developed using the vast resources of nation states, oddly

[14] On April 6, 1995, William O. Studeman, the acting Director of Central Intelligence testified before the House Judiciary Committee "Particularly disturbing is the terrorist use of a chemical weapon, possibly the nerve gas sarin, in the attack on the Tokyo subway. We hope that it does not herald the dawn of a new era long feared by counterterrorist experts: the use of weapons of mass destruction against urban populations."

[15] Use of high explosives is sometimes included in this classification, thus the acronym CBRNE. This category of weapons is not included in our consideration because the designation depends on their effects, i.e., whether they result in mass casualties or damage, not just their deployment. CBRN, on the other hand, are a particular concern because their mere deployment poses the potential for mass consequences.

enough, to deter their use on the battlefield. UN conventions ban their use[16], and major parties have worked to reduce or eliminate their number[17] (12). Despite these efforts, intelligence analysts have determined that WMD are within the capability of terrorists to manufacture or acquire (13 p. viii). Terrorists, in fact, have already employed some to their purpose.

In 1995, the Japanese cult Aum Shinrikyo manufactured Sarin gas, a chemical nerve agent, and deployed it on the Tokyo subway killing 12 people and injuring hundreds. The fact that there weren't more casualties was due to improper deployment (14 p. 5). A similar scenario considered by the 2004 National Planning Scenarios (#7, Chemical Attack – Nerve Agent) projects a probable 6,000 fatalities (15 pp. 7-1).

In September and October 2001, at least five envelopes containing anthrax bacteria were mailed to Senators Patrick Leahy and Thomas Daschle in Washington, DC, and to media organizations located in New York City and Boca Raton, Florida (16 p. 1). Again, the attack caused minimal casualties, five people killed, while the 2004 National Planning Scenarios suggests as many as 13,000 people could die in a similar attack (15 pp. 2-1).

While nuclear and radiological devices have yet to be employed by terrorists, documents and interrogations from military operations in Afghanistan have reinforced the assessment that the Taliban sought, and al-Qaeda, continues to seek to obtain radioactive material for a radiological weapon (17 p. 3). Government officials are particularly concerned with the deployment of a radiological device as the materials are readily accessible from a broad range of poorly protected sources, especially medical equipment[18] (17 p. 4). And while nuclear devices require more refined and better protected materials, analysts worry about the problem of "loose nukes," i.e., the possible leakage of nuclear weapons material and technical know-how from the former Soviet states, increase the likelihood of a terrorist group obtaining a nuclear capability (17 p. 4).

As yet, no terrorist group has successfully deployed a weapon of mass destruction to its full potential. Experts cite the difficulty of acquiring, manufacturing, and deploying WMD as the main reason for relying on conventional weapons. For example, even if a terrorist group were to get hold of an assembled nuclear weapon, the built-in safeguards and self-destruction mechanisms would pose a serious challenge to detonating the weapon. In addition, the size of most nuclear weapons makes them rather hard to transport, especially clandestinely (17 p. 4).

---

[16] In connection with the perceived increase in WMD proliferation by states and non-state actors, new international legal efforts and proposals aimed at strengthening deterrence against WMD development and use have appeared. These include: (1) Security Council action against Iraq concerning its alleged WMD programs; (2) U.S. efforts to extend the right of anticipatory self-defense to justify military action in "pre-emptive self-defense" against a hostile regime armed with or pursuing WMD; (3) criminalizing WMD terrorism in treaty law; and (4) proposals to make the development, retention, acquisition, or transfer of biological and chemical weapons a crime under international law.

[17] International cooperation and legal activity has also begun to address the increasing technological feasibility of WMD. International efforts to improve national control and regulation of access to, and transfer of, WMD materials have started, for example, within the Australia Group and through the Biological Weapons Convention. Multilateral initiatives, such as the G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction, also contribute to international activities designed to protect WMD materials from malevolent appropriation. In the same spirit, experts have proposed new treaties on improving the safety and security of biological agents.

[18] Radiological weapons use conventional high explosives to disperse any type of radioactive material, obviating the need for fissile material and the complexity of a nuclear bomb. Though unlikely to cause mass casualties, radiological weapons could still have very significant radiation contamination effects if well-targeted.

Similarly, although Aum Shinrikyo was able to produce the nerve agent Sarin and release it in a closed environment — the Tokyo subway—the attack resulted only in 12 fatalities and injury to hundreds of others, whereas there were 301 fatalities and 5,000 injured in the conventional bombing of the US embassies in Kenya and Tanzania[19] (14 p. 5).

For those wishing to inflict catastrophic damage on the US, critical infrastructure offers an attractive alternative to WMD. On September 11, 2001, terrorists exploited elements of the aviation infrastructure to attack the World Trade Center and the Pentagon representing seats of US economic and military power (18 p. 8). They killed nearly 3,000 people and caused more than $41.5B in damage[20] (19 p. 2). This immeasurable pain was inflicted by 19 young Arabs acting at the behest of Islamist extremists headquartered in distant Afghanistan. Most spoke English poorly, some hardly at all. In groups of four or five, carrying with them only small knives, box cutters, and cans of Mace or pepper spray, they hijacked four planes and turned them into deadly guided missiles (20 p. 2). The 2003 National Strategy for the Physical Protection of Critical Infrastructures and Key Assets called 9/11 a "wake-up call" (18 p. 5).

The federal government definition of critical infrastructure is found in the USA Patriot Act (Public Law 107-56, October 26, 2001):

> *"Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."*

Homeland Security Presidential Directive (HSPD) #7[21], Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003), classified critical infrastructure by sector. The original classifications were later expanded and now encapsulated within the 2009 National Infrastructure Protection Plan. The federal government recognizes 18 critical sectors:

[19] On August 7, 1998, US embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya were simultaneously attacked by truck bombs. The bombings marked the eighth anniversary of the arrival of American forces in Saudi Arabia, and brought Osama bin Laden to the attention of the American public for the first time as he was placed on the FBI's Ten Most Wanted list (Wikipedia).

[20] Direct 9/11 costs include $34B in insured losses for buildings and infrastructure, plus $576M for rebuilding the Pentagon, and $7B for official victim compensation. Indirect losses due to the downturn in world markets may place the total cost of 9/11 near $300B.

[21] HSPDs and Executive Orders(EOs) are issued by the President to establish Executive policy and otherwise interpret laws passed by Congress. Unless otherwise challenged in court, HSPDs and EOs have the force of law (73 p. 2).

1. Agriculture and Food
2. Defense Industrial Base
3. Energy
4. Healthcare and Public Health
5. National Monuments and Icons
6. Banking and Finance
7. Water
8. Chemical Plants
9. Commercial Facilities
10. Critical Manufacturing
11. Dams
12. Emergency Services
13. Nuclear Reactors, Materials, and Waste
14. Information Technology
15. Communications
16. Postal and Shipping
17. Transportations Systems
18. Government Facilities (21 p. 3)

The vast majority of the critical infrastructure and key resources (CIKR)-related assets, systems, and networks are owned and operated by the private sector. However, in sectors such as Water and Government Facilities, the majority of owners and operators are governmental or quasi-governmental entities. The great diversity and redundancy of the Nation's CIKR provide for significant physical and economic resilience in the face of terrorist attacks, natural disasters, or other emergencies, and contribute to the strength of the Nation's economy. However, this vast and diverse aggregation of highly interconnected assets, systems, and networks may also present an attractive array of targets to domestic and international terrorists and magnify greatly the potential for cascading failure in the wake of catastrophic natural or manmade disasters. (21 p. 11)

Urban society cannot function without critical infrastructure. Millions of US lives would be put at risk without it. The science historian James Burke described this predicament as a "technology trap" (22). To live and make a living, urban society is wholly dependent upon technology it doesn't understand. In the eerily prescient opening episode of his 1978 series "Connections", Mr. Burke postulated from atop the World Trade Center what would happen if all technology suddenly failed. He persuasively argued that urban society would collapse, and without the benefit of technological infrastructure, millions would die and the few lucky survivors would be reduced to struggling for subsistence (22).

> *The essential vulnerability of today's critical infrastructure is that little of it was centrally planned or designed, and virtually none of it was built to withstand deliberate attack. The result is that millions of lives depend upon a network that's not fully understood, riddled with weaknesses, and susceptible to malicious tampering.*

A key concern of the federal government since 9/11 is that terrorists will target critical infrastructures to achieve three general types of effects:

- Direct infrastructure effects: Cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function.
- Indirect infrastructure effects: Cascading disruption and financial consequences for government, society, and economy through public- and private-sector reactions to an attack.
- Exploitation of infrastructure: Exploitation of elements of a particular infrastructure to disrupt or destroy another target. (18 p. viii)

Of particular concern is the threat of cyber attack. Without a great deal of thought about security, the control of essential processes in manufacturing, utilities, banking, and

communications over the years shifted to networked computers. As a result, the cost of doing business dropped and productivity skyrocketed. However, the US economy and national security became fully dependent upon information technology and the information infrastructure. A network of networks directly supports the operation of all sectors of the US economy—energy (electric power, oil and gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, defense industrial base, food, agriculture, and postal and shipping. The reach of these computer networks exceeds the bounds of virtual cyberspace[22]. They also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars. (23 pp. 5-6)

The National Planning Scenarios depict a diverse set of high-consequence threat scenarios of both potential terrorist attacks and natural disasters. Collectively, the 15 scenarios are designed to focus contingency planning for homeland security preparedness work at all levels of government and with the private sector. The scenarios form the basis for coordinated federal planning, training, exercises, and grant investments needed to prepare for emergencies of all types (24 p. iii). Scenario 15 examines the specific targeting of financial institutions through cyber attack. Specifically, credit-card processing facilities are hacked and numbers are released to the Internet, causing 20 million cards to be cancelled; automated teller machines (ATMs) fail nearly simultaneously across the nation; major companies report payroll checks are not being received by workers; and several large pension and mutual fund companies have computer malfunctions so severe that they are unable to operate for more than a week. Individually, these attacks are not dangerous – but combined, they shatter faith in the stability of the system. Citizens no longer trust any part of the US financial system and foreign speculators make a run on the dollar. (15 pp. 15-1).

The federal government is similarly concerned about the vulnerability of the national electric grid. Electric utilities rely on supervisory control and data acquisition (SCADA) systems to manage the nation's power generation, transmission, and distribution networks. While generally protected from intrusion, SCADA systems operate over the Internet. The move to SCADA boosts efficiency at utilities because it allows workers to operate equipment remotely. But this access to the Internet exposes these once-closed systems to cyber attacks. In 2006, the Department of Energy and Department of Homeland Security jointly conducted Project Aurora to assess the potential vulnerability of the national electric grid. In a dramatic video-taped demonstration, engineers at Idaho National Labs showed how the weakness could be exploited to cause any spinning machine connected to the power grid -- such as a generator, pump or turbine -- to physically self-destruct (25). As a critical node in the infrastructure network, a cyber attack on the electric grid would produce cascading effects across other infrastructures including sewage treatment plants and waterworks as turbines and other electrical apparatuses in these facilities shut down. Cascading events within the electric utilities themselves can spread the effects across broad geographic regions affecting millions. On July 2, 1996, a cascade event left

[22] The term "cyberspace" was first used by science fiction author William Gibson. The first component of the term comes from "cybernetics", which is derived from the Greek κυβερνήτης (kybernētēs, steersman, governor, pilot, or rudder), a word introduced by Norbert Wiener for his pioneering work in electronic communication and control science. Now ubiquitous, in current usage the term "cyberspace" stands for the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems. The term has become a conventional means to describe anything associated with the Internet and the diverse Internet culture.

2 million customers in 11 states and 2 Canadian provinces without power. On August 10, 1996, a similar event caused 7.5 million customers in seven western states and parts of Canada to be without power for up to nine hours (26 p. 9). The August 2003 blackout of the northeastern United States and parts of Canada, also a cascade event, has been invoked as indicative of the potential effects of a successful terrorist cyber-attack on electrical utility control systems (26 p. 10). While widespread, these outages were not long term. The same might not be true of a targeted attack. The physical damage of certain system components (e.g. extra-high-voltage transformers) on a large scale could result in prolonged outages as procurement cycles for these components range from months to years (27 p. 11). Such an outage would be unprecedented, and the impact much greater than any weapon of mass destruction.

While possible, a cyber attack on the electric grid, or any other critical infrastructure would not be easy. Yet, the sophistication required to infiltrate and compromise such systems has been amply demonstrated by the Stuxnet worm. In September 2010, media reports emerged about a new form of cyber attack that appeared to target Iran, although the actual target, if any, is unknown. Through the use of thumb drives in computers that were not connected to the Internet, a malicious software program known as Stuxnet infected computer systems that were used to control the functioning of a nuclear power plant. Once inside the system, Stuxnet had the ability to degrade or destroy the software on which it operated. Although early reports focused on the impact on facilities in Iran, researchers discovered that the program had spread throughout multiple countries worldwide (28 p. 2).

From the perspective of many national security and technology observers, the emergence of the Stuxnet worm is the type of risk that threatens to cause harm to many activities deemed critical to the basic functioning of modern society. The Stuxnet worm covertly attempts to identify and exploit equipment that controls a nation's critical infrastructure. A successful attack by a software application such as the Stuxnet worm could result in manipulation of control system code to the point of inoperability or long-term damage. Should such an incident occur, recovery from the damage to the computer systems programmed to monitor and manage a facility and the physical equipment producing goods or services could be significantly delayed. Depending on the severity of the attack, the interconnected nature of the affected critical infrastructure facilities, and government preparation and response plans, entities and individuals relying on these facilities could be without life sustaining or comforting services for a long period of time. The resulting damage to the nation's critical infrastructure could threaten many aspects of life, including the government's ability to safeguard national security interests (28 p. 2).

The risk of such attack on US critical infrastructure is non-zero as determined by the National Infrastructure Protection Plan risk equation. According to the government plan, Risk is a product of Consequence times Vulnerability, times Threat (21 p. 33). In this equation, Risk is a relative measure of potential danger as determined by the relative Vulnerability of a targeted system, the potential Consequences measured in terms of deaths and damage if the system is successfully attacked, and the Threat probability that the system will be targeted. While the Vulnerability and Threat to critical infrastructure might be low, the potential Consequences are high, making the risk non-zero. By definition, a macroterrorism attack results in significant consequences, therefore the risk is significant. The problem cannot be ignored.

On October 8th, 2001, President George W. Bush issued Executive Order 13228 establishing the Office of Homeland Security within the Executive Office of the President to coordinate a comprehensive national strategy to secure the United States from terrorist threats and attacks.

Thomas Ridge, former Governor of Pennsylvania, was appointed Assistant to the President (29). On July 16th, 2002, Mr. Ridge released the nation's first National Strategy for Homeland Security designed to enhance the nation's protection and reduce its vulnerability to terrorist attacks (30 p. 4). Over ten years, homeland security strategy has remained virtually unchanged through two revisions[23] and two presidential administrations. We ask ourselves:

1. *How was homeland security strategy formulated?*
2. *Is it a good strategy?*
3. *Can we make it better?*

3 Homeland Security Strategy

Protecting American citizens is the responsibility of all of government, including state, local, tribal, and federal government. Domestic protection is conferred on citizens through law. International protection is negotiated through treaties. Domestic protection is enacted through legislative, judicial, and executive agencies at all levels of government. International protection is strictly enacted by the federal government through the Department of State and Department of Defense. Since the threat of terrorism crosses domestic and international boundaries, it requires the cooperation of state, local, tribal, and federal government to address it. This cooperation is formulated at the federal level by the National Security Council.

The National Security Council (NSC) was established by the National Security Act of 1947 creating an interdepartmental body to advise the President with respect to the integration of domestic, foreign, and military policies relating to national security. As specified in the 1947 statute, the NSC is comprised of the President, Vice President, the Secretary of State, the Secretary of Defense, and, since 2007, the Secretary of Energy; but, at the President's request, other senior officials participate in NSC deliberations. The Chairman of the Joint Chiefs of Staff and the Director of National Intelligence are statutory advisers (31 p. 2).

The National Security Council is supported by an NSC staff, organized and administered by a National Security Advisor appointed by the President. While the President clearly holds final decision-making authority in the executive branch, over the years the NSC staff has emerged as a major factor in the formulation (and at times in the implementation) of national security policy. Similarly, the head of the NSC staff, the National Security Adviser, has played important, and occasionally highly public, roles in policymaking (31 p. 2).

Since 1986, the National Security Advisor has assisted the president with publishing National Security Strategy (32 p. 3) formally identifying national security objectives and the means for attaining them. This congressionally-mandated document helps guide Congress in determining national funding priorities. The National Security Strategy also serves as a coordinating framework for federal agencies to prioritize resources and schedule activities to work towards common national goals (32 p. 2).

[23] In October 2007, the National Strategy for Homeland Security was revised by the Bush Administration to accommodate greater recognition of the threat of natural disasters due to Hurricane Katrina in August-September 2005. In May 2010, homeland security strategy was merged into National Security Strategy by the Obama Administration in recognition of the shared objectives of protecting America and American lives.

Before 9/11, national security strategy primarily addressed the roles and responsibilities of federal agencies to achieve national security objectives (33 p. 5). Following 9/11, seven new national strategies were developed and published to guide US efforts in combating terrorism, homeland security strategy among them. "Combating terrorism" refers to the full range of policies, programs, and activities to counter terrorism, both at home and abroad. "Homeland security" is distinguished within this broader strategy by its focus on domestic terrorism (34 p. 5). Homeland security strategy differed markedly from previous national security strategies for the significant role it cast for state, local, and tribal governments as federal partners to achieve homeland security objectives (33 p. 5).

The first homeland security strategy identified four security objectives: 1) prevent terrorist attacks within the US; 2) reduce America's vulnerability to terrorism, and 3) minimize the damage and recover from attacks that do occur (33 p. vii). The corresponding strategy was "prevent, protect, respond, and recover". The US would Prevent terrorist attack by overhauling its intelligence apparatus to thwart future attempts by external agents; tighten border security to keep terrorists and their weapons from entering the country; and strengthen law enforcement to thwart future attempts by internal agents. The US would Protect critical infrastructure and key assets, and further tighten controls on WMD and their materials to make the country less vulnerable to catastrophic terrorist attack. And the US would implement measures to more quickly and ably respond and recover from terrorist attack, including those using WMD (33 p. 60)

In 2002, the Homeland Security Act passed by Congress authorized the creation of the Department of Homeland Security to implement the domestic provisions of homeland security strategy (35 p. Sec. 101). The department was created by combining offices from across 22 existing federal agencies and grouping them under the unified direction of the new Secretary of Homeland Security (36). The Department of Homeland Security was meant to mobilize and focus the resources of the federal, state and local government, the private sector, and the American people. The creation of the Department of Homeland Security empowered a single Cabinet official with the primary responsibility of protecting the American homeland from terrorism (37 p. 8). Almost immediately, the new Department of Homeland Security was tasked with helping shape as well as implement homeland security strategy.

In 2007, homeland security strategy and the Department of Homeland Security underwent significant change as a result of Hurricane Katrina in 2005 (38 p. 1). When the Department of Homeland Security was established in 2003, it subsumed the Federal Emergency Management Agency (FEMA) within its organization. FEMA was added to DHS on the premise that many of the same methods for preparing and responding to natural disasters would be required for preparing and responding to catastrophic terrorist attacks (37 p. 2). Some thought the change went too far, and diluted both FEMA's authority and mission (39 p. 53). In August 2005, Hurricane Katrina, a category-five storm, hit Louisiana, Alabama, and Mississippi (39 p. 1). In New Orleans, the storm surge overtopped levies holding back the Mississippi River, flooding approximately 80% of the city under six to twenty feet of water, and instigating one of the largest search and rescue operations in the nation's history. More than 1,300 people were trapped and killed by the rising water, and social order collapsed as tens of thousands more were left stranded without basic necessities (39 pp. 1-2). FEMA's response was perceived as slow and inept, and blamed for much of the human suffering in New Orleans (40 pp. 1-5). As a result, Congress directed changes elevating FEMA's position within the Department of Homeland

Security, and the Homeland Security Council issued a new National Strategy for Homeland Security placing greater emphasis on natural disasters.

Homeland security strategy encompasses more than just the roles and responsibilities of DHS. The Department of Homeland Security Prevents terrorist attacks by fusing intelligence data from various sources, but has no collection authorities. It relies on intelligence information collected and forwarded by the seventeen authorized national intelligence agencies, and domestic reports collected by fusion centers working in cooperation with state and local law enforcement agencies. If intelligence data indicate a domestic threat, DHS has no authority to act, but must notify the Federal Bureau of Investigation within the Department of Justice (41 pp. A-1). Nor can DHS respond directly to overseas threats. It cooperates with the National Counterterrorism Center operated by the Central Intelligence Agency, working together with the Department of State and Department of Defense to monitor and respond to international threats (41 pp. A-2). The Department of Homeland Security operates Customs and Border Protection to secure the nation's borders, but must work with both the State Department and Department of Commerce to regulate passengers and cargo. DHS must also work with the Department of Commerce to Protect the nations' ports, airways, waterways, and highways through the Federal Protective Service, US Coast Guard, and Transportation Security Administration. DHS also works closely with the Department of Energy and Health and Human Services to safeguard the nation against radiological and biological attack (41 pp. A-3). DHS has formed cooperative ventures with private industry to Protect critical infrastructure under the aegis of the National Infrastructure Protection Program. In addition to FEMA, DHS administers block grants to states to train and equip First Responders to prepare for terrorist attack (42).

The broad scope of homeland security strategy encompassing both foreign and domestic policy, and entailing extensive interagency cooperation, prompted the Obama Administration in 2009 to re-integrate the Homeland Security Council into the National Security Council, and homeland security strategy within national security strategy (43). In 2010, President Obama released the most current National Security Strategy, subtitled "Renewing American Leadership – Building at Home, Shaping Abroad." The new strategy identifies four national security objectives: 1) security, 2) prosperity, 3) values, and 4) international order. Homeland security strategy is embedded within the new national security strategy primarily under its security objective. The current homeland security strategy is built upon 1) strengthening security and resilience at home, 2) disrupting, dismantling and defeating al-Qaeda and its affiliates, 3) reversing the spread of nuclear and biological weapons and securing nuclear materials, 4) advancing peace, security, and opportunity in the greater Middle East, and 5) securing cyberspace (44 p. 15).

Despite the different wording, the new homeland security strategy doesn't offer anything new. The "security" provision is still bound to "preventing" terrorist attack within the US. The addition of the word "resilience" only encapsulates the "protect" and "recover" provisions of the original homeland security strategy (30 p. vii). Similarly, the remaining statements, if not exactly the same, were part and parcel of the original homeland security strategy of "protect, prevent, respond, recover". That the current homeland security strategy remains essentially unchanged is borne out by the fact that federal agency budgets and organizations remain substantially the same (45 p. 83). This only means that President Obama is steering the same course first chartered by President Bush to protect the US against terrorist attack. This raises the question, is it a good strategy?

A 2004 report from the Government Accountability Office (GAO) examining national strategies for combating terrorism determined that a good strategy addresses six things: 1) purpose, scope, and methodology, 2) problem definition and risk assessment, 3) goals, subordinate objectives, activities, and performance measures, 4) resources, investments, and risk management, 5) organizational roles, responsibilities, and coordination, and 6) integration and implementation. The GAO identified these criteria after 1) gathering statutory requirements pertaining to some strategies, 2) compiling legislative and executive branch guidance for other strategies, 3) consulting the 1993 Government Performance and Results Act, 4) reviewing general literature on strategic planning and performance including guidance from the Office of Management and Budget on the President's Management Agenda, 5) studying past GAO reports, 6) researching past commission recommendations, and 7) soliciting comments from the ANSER Institute on Homeland Security, the RAND Corporation, and Brookings Institution. The GAO was asked by the House Subcommittee on Emerging Threats and International Relations to identify and define characteristics of effective national strategy and evaluate whether prevailing strategies related to terrorism address those characteristics. The purpose of the study was to provide additional guidance to responsible parties developing and implementing strategies, and enhance their usefulness as guidance for resource and policy decision-makers to better ensure accountability (34 pp. 2-3).

The GAO evaluated seven national strategies related in part or in whole to combating terrorism and homeland security, including the 2002 National Strategy for Homeland Security. The GAO study found that none of the prevailing strategies completely addressed all six desirable characteristics. However, among the published strategies, the 2002 National Strategy for Homeland Security was most complete. Within its analysis, the GAO determined that the National Strategy for Homeland Security fully addressed the first criteria, stating that it "explicitly identifies its fundamental objectives, coverage, and how it was developed." An important component of this criteria is "methodology", which the GAO describes as "the principles or theories that guided [the strategy's] development, what organizations or offices drafted the document, whether it was the result of a working group, or which parties were consulted in its development." (34 p. 4) The GAO report does not identify the specific passages supporting its analysis, but the following excerpt seems to be relevant:

> *"The National Strategy for Homeland Security is the product of more than eight months of intense consultation across the United States. My Administration has talked to literally thousands of people–governors and mayors, state legislators and Members of Congress, concerned citizens and foreign leaders, professors and soldiers, firefighters and police officers, doctors and scientists, airline pilots and farmers, business leaders and civic activists, journalists and veterans, and the victims and their families. We have listened carefully."* (33 p. 3)

The 2002 homeland security strategy further states that eight principles shaped its design: 1) that it require responsibility and accountability, 2) mobilize the entire society, 3) manage risk and allocate resources judiciously, 4) seek opportunity out of adversity, 5) foster flexibility, 6) measure preparedness, 7) sustain efforts over the long term, and 8) constrain government spending (33 p. 3).

Despite the favorable assessment by the GAO, it's clear that there's no theory or model underlying homeland security strategy development.

Why should we seek a theoretical framework for homeland security strategy?

> *The framework of theory provides a methodological basis for a disciplined thought process to assist the strategist in developing strategy, and it also serves as a guide for others to follow in comprehending, evaluating, and critiquing the merits of a particular strategy. Theory disciplines strategic thinking by explaining strategy's inherent logic; it serves to remind all involved with strategy neither to promise too much nor fail to consider any of the attributes of strategy. A coherent theory also helps leaders, planners, and others to evaluate and execute strategy. It serves as a common frame of reference for the development and evaluation of an appropriate strategy and the communication of it to those who must implement it* (46 p. 2).

At the highest level of strategy, the nation-state has interests that it pursues to the best of its abilities through the use of the instruments of power (46 p. 1). Policy articulates the reflection of these interests in the strategic environment. In pursuing its policies, the state confronts adversaries and other actors, while some factors simply remain beyond control or unforeseen. Strategy, acting within the confines of theory, is a method of creating strategic effects favorable to policy and interests by applying ends, ways, and means in the strategic environment. In doing this, strategy has an inherent logic that can be understood as a theoretical construct and applied in the development and consideration of strategy at all levels (46 p. 65).

> *As a component of national security strategy, it would seem appropriate to seek theoretical underpinnings for homeland security strategy within international relations theory.*

4 In Search of a Theoretical Framework

Four alternative schools of theory prevail in today's studies of international relations: 1) Institutionalist, 2) Liberal, 3) Epistemic, and 4) Realism. Each includes a family of theories, a "paradigm" that is based on a different set of assumptions to explain interaction among equal and sovereign states (47 pp. 10-11). The Institutionalist paradigm contains theories and explanations that stress the role of formal norms and institutions in providing information to states. The Liberal paradigm contains theories and explanations that stress the way ideas shared or manipulated by groups influence state preferences and policy (47 p. 10). The Epistemic paradigm contains theories and explanations that stress the exogenous variation in the shared beliefs that structure means-ends calculations and affect perceptions of the strategic environment (47 p. 11). The Realist paradigm treats material capability as an objective, universal, and unalienable political instrument that exercises an exogenous influence on state behavior independent of national preferences, institutions, and perceptions (47 p. 18). Enduring international relations paradigms have helped to focus attention on particular core assumptions and causal mechanisms. Debates among realists, liberals, epistemic theorists, and institutionalists have traditionally centered around the scope, power, and interrelationship of variation in material capabilities (Realism), national preferences (Liberal), beliefs (Epistemic theory), and international institutions (Institutionalism) on state behavior (47 p. 11). Today, Realism is considered the most prominent theoretical paradigm in international relations (47 p. 5).

Realists examine how states maximize their power or security as they pursue national survival (48 p. 639). Realism is based upon three core assumptions: 1) state actors are rational, unitary political units in anarchy, 2) states have fixed and uniformly conflictual goals, and 3) state relations are governed by the primacy of material capabilities (47 pp. 12-16). The first assumption addresses the nature of basic social actors. Realism assumes the existence of a set of "conflict groups," each organized as a unitary political actor that rationally pursues distinctive goals within an anarchic-setting. Within each territorial jurisdiction, each actor is a sovereign entity able to undertake unitary action. Between jurisdictions, anarchy (no sovereign power) persists (47 p. 12). The second assumption conceptualizes interstate politics as a perpetual bargaining game over the distribution and redistribution of scarce resources (47 p. 13). The third assumption stipulates that the bargaining power of a state is directly related to its ability to coerce or bribe another state. The primary means of redistributing resources, therefore, is to threaten punishment or offer a side payment. Each state employs such means up to the point where making threats and promises are less costly to them than the (uniform) benefits thereby gained (47 pp. 16-17).

Realism evolved from the study of post-Westphalian Europe and in reaction to inconsistency between the optimistic view advanced by Wilsonian idealists and reality after World War I. During the decades of the 1930s, realists observed that the Russian Revolution, naval arms races both in Europe and between European powers and Japan, and regional conflicts seemed incompatible with Liberal expectations. By the end of World War II, structural Realist approaches largely supplanted Wilsonian idealism (48 p. 639). Today, Realist ideas, in their turn, are being modified as they face practical and theoretical challenges. These challenges reflect 1) the force of history that has uncovered the insufficiency of Realist theories to anticipate or explain the implosion of the Soviet Union and the unraveling of the its East European empire, 2) the discovery that several of the propositions of structural Realist theories contain internal inconsistencies when assessed from the perspective of their micro-foundations, and 3) the growing evidence from political economy studies that causes of and solutions to international conflict can be better understood by looking within states (48 pp. 637-638).

As an underpinning for homeland security strategy, international relations theories in general, and Realism in particular, suffer from one major shortcoming: they deal with state actors. Certainly, states may sponsor terrorism, such as Libya in the 1980s. Muammar Qaddafi established a large network of training camps and invested $100M to export upwards to 8,000 terrorists to clandestinely implement Libyan foreign policy (49 p. 268). In response to Libyan provocations in the Gulf of Sidra, and the April 4, 1986 bombing of La Belle Discotheque killing four US servicemen in West Berlin, President Reagan ordered Operation El Dorado Canyon, an air strike against government targets in Tripoli and Benghazi. The raid was intended as a punishing demonstration to Libya and other potential enemies, demonstrating the reach of US military power (49 p. 269). The frequency of Libyan-sponsored attacks against US targets indeed declined after the raid (49 p. 267), proving the effectiveness of military power among the traditional instruments of national power for conducting international relations[24]. By the same token, the number of terrorist acts worldwide remained the same after El Dorado Canyon (49 p. 267), demonstrating the basic shortcoming of international relations theories with dealing with

[24] Traditional government instruments for influencing international relations are enumerated as DIMEFIL: Diplomatic, Information, Military, Economic, Financial, Intelligence, and Law Enforcement.

non-state actors. Terrorists are not recognized under the strictures of Realism as they are not sovereign entities able to undertake unitary action within a territorial jurisdiction (47 p. 12).

> *International relations theory therefore seems ill suited for informing homeland security strategy. Terrorism theory, on the other hand, might offer better insight for strengthening homeland security strategy.*

Various theories of terrorism have been advanced over the decades, mostly since 1968, and may be classified as 1) Psychological, 2) Societal, or 3) Systemic. Psychological theories examine groups and individuals and seek explanations such as why individuals join a terrorist group. Explanations on the Societal or national level primarily attempt to identify causal relationships between certain historical, cultural and socio-political characteristics of the larger society and the occurrence of terrorism. Explanations on the Systemic or international level seek to establish causal relationships between characteristics of the international state system and relations between states on the one hand, and the occurrence of international terrorism on the other hand (50 pp. 37-38).

Psychological theories of terrorism can be divided into two main traditions: 1) psycho-pathological and psycho-sociological. The first tradition treats individual terrorists in isolation and searches for deviant character traits. The simple assumption is that non-violent behavior is the accepted norm, and that those engaged in terrorist activities therefore necessarily must be abnormal. Researchers seek to identify common terrorist attributes based on behavioral studies and psychological profiles. On the other hand, psycho-sociological theories focus on individual characteristics and mechanisms as they are influenced by their surrounding environment. Psycho-social theories fall into two main traditions: 1) relative deprivation, and 2) contagion theory. Relative deprivation contends that the basic condition for participation in collective civil violence and terrorism occurs when the gap between expectations and satisfaction grows rapidly. Contagion theory contends that the occurrence of terrorism in one country often leads directly or indirectly to more terrorism in other countries (50 pp. 9-10).

Societal theories of terrorism seek explanation in the historical development and culture of a larger society or system, and in its contemporary social, economic and political characteristics and environments. Research questions often focus on whether it is possible to identify a causal relationship between certain characteristics of a society and the occurrence of terrorism. Societal theories for terrorism encompass four separate schools of thought: 1) economic, 2) political, 3) historical, and 4) ecological (50 pp. 14-26).

Economic-based societal theories of terrorism revolve around two opposing paradigms: 1) rapid modernization, and 2) liberal peace theory. Rapid modernization contends that economic change, measured in Gross Domestic Product (GDP)-growth, makes societies more exposed to ideological terrorism. Social inequality measured in income inequality tends to increase the potential for ideological terrorism. Liberal peace theory, on the other hand, contends that increased trade and economic interdependence tends to discourage both inter-state and probably also the prevalence of international terrorism. Long term economic growth and development are conducive to internal political stability and hence works against the occurrence of domestic terrorism (50 p. 37).

Political-based societal theories of terrorism focus on the political environment that give rise to terrorists. According to political observers, democracy and terrorism are correlated, but the relationship is complex. States in democratic transition are more exposed to armed conflict and

terrorism than democracies and autocracies. Because of pervasive state control, totalitarian regimes rarely experience terrorism. At the same time, states with high scores on measures of human rights standards and democracy tend to be less exposed to domestic ideological terrorism. Terrorism is closely linked to a set of core legitimacy problems: lack of continuity of the political system tends to encourage ideological terrorism, while the lack of integration of political fringes also tends to encourage ideological terrorism. Ethnic diversity, however, tends to increase the potential for ethnic terrorism. Political-based societal theories contend that political stability and societal integration are key to discouraging terrorism (50 p. 37).

Historical-based societal theories of terrorism contend that certain social habits, norms, and historical traditions tend to encourage a higher level of civil violence and terrorism. While causalities have been suggested, they have not been established, and there are few general theories on the relationships between prevalent social norms and traditions and the occurrence of terrorism. More empirical evidence is needed to establish sound theories in this field (50 pp. 37-38).

Ecologically-based societal theories of terrorism contend that technological changes associated with modernization have created new and unprecedented conditions for terrorism (such as a multitude of targets, mobility, communications, anonymity, and audiences). Technological developments offer new and more efficient means and weapons for terrorist groups, but at the same time increase the counter-terrorist capabilities of states. Transnational organized crime and terrorism are partly inter-linked phenomena and growth in transnational organized crime may contribute to increased levels of terrorism (50 p. 38).

Systemic theories of terrorism examine the character of the international system including foreign policies of states and global circumstances that generate an environment conducive for terrorist activity. The character of the international system is significant. A system characterized by strong bipolar hegemony and a high level of bipolar conflict in world politics, such as the US-USSR standoff during the Cold War, is more exposed to international terrorism. Similarly, state sponsorship of international terrorism has been a significant cause of terrorism. The existence of weak and collapsed states tends to encourage both internal armed conflicts and international terrorism (50 p. 26).

Certainly we can identify elements of various terrorism theories within the current National Security Strategy. The influence of economic-based societal theories appear evident in the strategy's goal of strengthening education and human capital at home, achieving balanced and sustainable growth, and promoting dignity by meeting basic needs. These objectives will presumably decrease incentives for both domestic and international terrorism. Politically-based societal theories seem to drive objectives to disrupt, dismantle, and defeat al-Qaeda and its affiliates in Afghanistan, Pakistan, and around the world, and promote democracy and human rights abroad. These objectives are aimed at eliminating bases for terrorist operations, and alleviating conditions that promote terrorism. Systemic theories of terrorism seem to apply to objectives for advancing peace, security, and opportunity in the greater Middle East, investing in the capacity of strong and capable partners, ensuring strong alliances, and sustaining broad cooperation on key global challenges. Such efforts support a more stable and cooperative international system less likely to spawn terrorists (44).

Collectively, terrorism theories address motivations why people turn to terrorism. The underlying assumption is that if you can isolate the cause, you can eliminate the effect. National

security strategy may indeed reduce the overall incidence of terrorism by alleviating societal and systemic pressures, but it cannot directly affect the decision of individuals to turn to terrorism. Psychological theories deal with individual choice, but to date they have not identified a "terrorist personality" or profile (51 p. 35).

> *It is uncertain whether terrorism theories will ever discover a root cause. Consequently, additional insight may be found by not seeking what makes terrorists, but by examining how terrorists act.*

Thwarting the next terrorist attack is a goal only slightly less desirous than eliminating terrorism. Since 9/11, much research has been undertaken in terrorism risk modeling to help predict and subsequently deter or defeat terrorist actions. These efforts have yielded valuable insights beneficial to counterterrorism and homeland security strategies. Terrorism risk modeling has been undertaken in various forms: 1) deterministic modeling, 2) stochastic games, 3) network analysis, and 4) gaming theory (9).

Deterministic modeling has long been used by the insurance industry to assess risk. For example, insurance companies calculate Probable Maximum Loss (PML) for earthquakes by 1) identifying the fault posing the greatest threat, 2) assigning the maximum credible earthquake to the fault, and 3) calculating portfolio loss assuming this size event occurs on this fault. PML estimation amounts to a series of problems in the domain of engineering, physical, chemical, and biological sciences. The same method can be applied to terrorist attacks such as evaluating the blast effect of a bomb detonation, the extent of fire from a fuel tanker explosion, the radiation fall-out from a radiological dispersal device, the spread of contagion from a smallpox outbreak, etc. These problems may still be technically complex and challenging, but the core mathematical models for blast analysis, conflagration, atmospheric dispersion, pollution transport, epidemiology, etc. are well established (9 p. 2). Notable is the research carried out by the RAND Center for Terrorism Risk Management Policy, which is a joint project of the RAND Institute for Civil Justice, RAND Public Safety and Justice, and Risk Management Solutions (RMS). A detailed RAND study based on the RMS model has developed an approach for making allocation decisions robust against uncertainty in model parameterization. A considerable volume of terrorism risk research has also been undertaken to support national public policy, notably at the University of Southern California's Center for Risk and Economic Analysis of Terrorism Events (CREATE), a DHS University Center of Excellence (52 p. 7). Another method, Probabilistic Risk Analysis, initially developed for the purpose of assessing the safety of nuclear reactors has also been applied to terrorism risk modeling (53 p. 11). Deterministic models, however, are packed with assumptions, and often resort to expert judgment to assign probabilities to terrorist attack scenarios, introducing a range of variability and subjectivity to the results. Furthermore, the deterministic approach largely removes the human behavioral component from estimation. The uncertainty introduced by assumptions is one reason why a deterministic approach can only be partially satisfactory (9 p. 3).

Unlike naturally occurring or accidental events, such as floods, earthquakes, or system failures, terrorism is fundamentally adversarial and adaptive (53 p. 5). Randomness plays a significant part in any human conflict. But there are causal factors as well, which shape the conflict landscape, including the temporal pattern of successful attacks (9 p. 4). Stochastic games were first introduced to the literature by Lloyd S. Shapley in 1953. The first paper on stochastic games considers two-person zero-sum stochastic games. Two-person indicates that there are two players, and zero-sum denotes that a player's gain is the cost to the other player. Play proceeds

in stages, from one state to the other according to the transition probabilities controlled jointly by the two opponents. The game consists of states and actions associated with each player. Once in a state, each player chooses their respective action. The play then moves into another state which some probability that is determined by the actions chosen and by the state in which they are chosen. Given that opponents make their respective decisions in a given stage, a cost is incurred to each player. An opponent discounts his projected cost by a factor Beta. The usual interpretation of Beta is that decision makers consider that costs incurred in future stages have less value in the present stage. Another interpretation of Beta in homeland security applications is the interest rate interpretation that determines the return on investment that could have been earned if the decision maker had not invested the funds in security investments (53 p. 7). Similarly, the time development of the al-Qaeda conflict is a stochastic process which may be described by a controlled Markov chain model[25]. At any moment in time, the predator (i.e., al-Qaeda) is in some specific state of attack preparedness, while the prey (i.e., USA) is in some corresponding state of defense preparedness. In a democracy, there are rigorous checks and balances imposed on law enforcement and security services. Accordingly, the counterterrorism response has to be commensurate with the terrorism threat: draconian measures (e.g., detention without trial) are only tolerable when the threat level is high. Democracies are prevented constitutionally from mounting an unlimited war on terrorism. Whatever state al-Qaeda occupies, police and security forces counter the prevailing threat with actions which aim to control terrorism. Because of these controlling counter-actions, the frequency of attack occurrence is not Poissonian[26], as is generally assumed for natural hazards. In mathematical terms, these counter-actions are termed Markov feedback policy[27] (9 p. 4). Stochastic processes and Markov chains, however, require continual adjustment and parameter tuning to reflect observed behavior. The question of their utility, therefore, is whether they are best utilized as explanatory models rather than predictive tools.

Network analysis seeks to gain insight into the dynamics of a terrorist network by looking inside and analyzing the social network of interconnections between nodes corresponding to individual terrorists. Al Qaeda has shown flexibility in adapting to counterterrorism action, and has been compared to the ability of a virus to mutate faster than its environment changes. This adaptation process can be simulated by evolving the social network according to a set of basic rules. Nodes communicate with one another to exchange information, financial and logistical resources, subject to the risk that any communication might be detected by security services. Local cells are autonomous to a substantial degree, and recruit attack team members and carry out target reconnaissance. Macroterrorism attacks are planned, but the larger and more ambitious that an attack becomes, the higher the chance of it being compromised by one of the attack team. If any node is removed from the network, there is a chance that any node connected to it might also be named and removed. Thus the more hierarchical the network, the greater the chance of

[25] A Markov chain, named for Andrey Markov, is a mathematical system that undergoes transitions from one state to another, between a finite or countable number of possible states. It is a random process characterized as memoryless: the next state depends only on the current state and not on the sequence of events that preceded it. This specific kind of "memorylessness" is called the Markov Property (Wikipedia).

[26] The Poisson Distribution is a discrete probability distribution that expresses the probability of a given number of events occurring in a fixed interval of time and/or space if these events occur with a known average rate and independently of the time since the last event (Wikipedia).

[27] A feedback policy is a maximizing function for a Markov chain. The point of this statement is that stochastic processes can reveal behavioral influences separate from deterministic processes, such as earthquakes.

destabilization through the arrest of senior leaders (9 pp. 7-8). The opportunity for surveillance experts to spot a community of terrorists, and gather sufficient evidence for courtroom convictions, increases nonlinearly with the number of operatives; above a critical number, the opportunity improves dramatically. This nonlinearity emerges from analytical studies of networks using modern graph theory methods. Below the tipping point, the pattern of terrorist links may not necessarily betray much of a signature to the counterterrorism services. However, above the tipping point, a far more obvious signature may become apparent in the guise of a large connected network cluster of dots, which reveals the presence of a form of community. As exemplified by the audacious attempted replay in 2006 of the Bojinka plot[28], too many terrorists spoil the plot. Intelligence surveillance and eavesdropping of terrorist networks thus constrain the pipeline of planned attacks that logistically might otherwise seem almost boundless. For example, in the three years before the 7/7/05 London attack[29], eight plots were interdicted. Thanks to the diligence of the security services, which deter the planning of large numbers of attacks, and interdict most of those that are planned, the frequency of successful terrorist attacks is kept low. Only a small proportion of attacks succeed, and these tend to be those involving fewer operatives (52 pp. 5-6). Such network analysis, though, has to cope with the problem of missing data. Massive amounts of uncertainty and a dearth of data plague network analysis (9 p. 8). The amount and type of data required to support network analysis comes at the cost of personal civil liberty. As happened after 9/11 and 7/7, after each major terrorist attack, democracies will respond by rebalancing the desire for liberty with the need for security (52 p. 6).

> *Unlike above methods, game theory incorporates human behavior directly into its mathematical analysis.*

The two fundamental precepts underlying game theory are 1) that protagonists are rational and 2) intelligent in strategic reasoning. In applying game theory to terrorism, it is important to leave behind popular notions of rationality, and to return to formal mathematical definitions of rational behavior, namely that actions are taken in accordance with a specific preference relation called "utility". There is no requirement that a terrorist's preference relation should involve economic advantage or financial gain. Nor is it necessary that a terrorist's preference relation conform with those of society at large. Game theory is not restricted to any one cultural or religious perspective. The test of any mathematical risk model is its explanatory and predictive capability. Among its insights, game theory predicts that, as prime targets are hardened, rational terrorist will tend to substitute lesser softer targets. Explicit admission of this soft target strategy has since come from Khalid Sheikh Mohammed, the al-Qaeda operations chief and mastermind behind 9/11 after his capture in March 2003. As with burglar alarms, self-protection has the externality of shifting risk to one's neighbors. Further validation of the terrorism target prioritization model is provided by analysis of the Irish Republican Army campaign in Ulster and

[28] The Bojinka plot was a planned large-scale Islamist terrorist attack by Ramzi Yousef and Khalid Shaikh Mohammed to blow up 12 airliners and their approximately 4,000 passengers as they flew from Asia to the United States. Khalid Shaikh Mohammed evolved this plot into the 9–11 airliner attacks (Wikipedia).

[29] The 7 July 2005 London bombings (often referred to as 7/7) were a series of coordinated suicide attacks in the United Kingdom, targeting civilians using London's public transport system during the morning rush hour. On the morning of Thursday, 7 July 2005, four terrorists detonated four bombs, three in quick succession aboard London Underground trains across the city and, later, a fourth on a double-decker bus in Tavistock Square. Fifty-two people, as well as the four bombers, were killed in the attacks, and over 700 more were injured.

England[30], and the GIA campaign in France[31]. The success of this game theory model illustrates the future potential for quantitative terrorism model development (9 p. 7).

> *Game theory is an appropriate tool for examining terrorism for a number of reasons. First, game theory captures the strategic interactions between terrorists and a targeted government, where actions are independent and, thus, cannot be analyzed as though one side is passive. Second, strategic interactions among rational actors, who are trying to act according to how they think their counterparts will act and react, characterize the interface among terrorists or among alternative targets. Third, in terrorist situations, each side issues threats and promises to gain a strategic advantage. Fourth, terrorists and governments abide by the underlying rationality assumption of game theory, where a player maximizes a goal subject to constraints. Fifth, game-theoretic notions of bargaining are applicable to hostage negotiations and terrorist campaign-induced negotiations over demands. And sixth, uncertainty and learning in a strategic environment are relevant to all aspects of terrorism, in which the terrorists or government or both are not completely informed* (54 pp. 1-2).

5 Game Theory

Game theory is the formal study of conflict and cooperation. Game theoretic concepts apply whenever the actions of several agents are interdependent. These agents may be individuals, groups, firms, or any combination of them. The concepts of game theory provide a language to formulate, structure, analyze, and understand strategic scenarios (55 p. 4).

Game-theoretic insights can be found among commentators going back to ancient times (56 p. 2). However, the earliest example of a formal game-theoretic analysis is the study of duopoly by Antoine Cournot in 1838[32]. The mathematician Emile Borel suggested a formal theory of games in 1921, which was furthered by the mathematician John von Neumann in 1928 in a "theory of parlor games." Game theory was established as a field in its own right after the 1944 publication of Theory of Games and Economic Behavior by von Neumann and the economist Oskar

[30] The Provisional Irish Republican Army (IRA) is a paramilitary organization whose aim was to remove Northern Ireland from the United Kingdom and bring about a socialist republic within a united Ireland by force of arms and political persuasion. The IRA's initial strategy was to use force to cause the collapse of the Northern Ireland administration and to inflict enough casualties on the British forces that the British government would be forced by public opinion to withdraw from the region. From 1971–1994, the IRA launched a sustained offensive armed campaign that mainly targeted the British Army, the Royal Ulster Constabulary (RUC), the Ulster Defence Regiment (UDR), and economic targets in Northern Ireland. The first half of the 1970s was the most intense period of the IRA campaign. On 28 July 2005, the IRA Army Council announced an end to its armed campaign, stating that it would work to achieve its aims using "purely political and democratic programs through exclusively peaceful means (Wikipedia).

[31] The Armed Islamic Group (GIA from French Groupe Islamique Armé) is an Islamist organization that wants to overthrow the Algerian government and replace it with an Islamic state. The GIA adopted violent tactics in 1992 after the military government voided the victory of the Islamic Salvation Front, the largest Islamic opposition party, in the first round of legislative elections held in December 1991. The group uses assassinations and bombings, including car bombs, and it is known to favor kidnapping victims and raping them. The GIA is considered a terrorist organization by the governments of Algeria, France and the United States (Wikipedia).

[32] A duopoly is a market dominated by only two sellers. Cournot showed that two firms assume each others' output and treat this as a fixed amount, and produce in their own firm according to this assumption (Wikipedia).

Morgenstgern. This book provided much of the basic terminology and problem setup that is still in use today (55 p. 4).

In 1950, John Nash demonstrated that finite games always have an equilibrium point, at which all players choose actions which are best for them given their opponents' choices. This central concept of noncooperative game theory has been a focal point of analysis since then. In the 1950s and 1960s, game theory was broadened theoretically and applied to problems of war and politics. Since the 1970s, it has driven a revolution in economic theory. Additionally, it has found applications in sociology and psychology, and established links with evolution and biology. Game theory received special attention in 1994 with the awarding of the Nobel prize in economics to Nash, John Harsanyi, and Reinhard Selten (55 pp. 4-5).

At the end of the 1990s, a high-profile application of game theory was the design of auctions. Prominent game theorists have been involved in the design of auctions for the use of bands of the electromagnetic spectrum to the mobile telecommunications industry. Most of these auctions were designed with the goal of allocating these resources more efficiently than traditional governmental practices, and additionally raised billions of dollars in the United States and Europe (55 p. 5).

The internal consistency and mathematical foundations of game theory make it a prime tool for modeling and designing automated decision-making processes in interactive environments. As a mathematical tool for the decision-maker the strength of game theory is the methodology it provides for structuring and analyzing problems of strategic choice (55 p. 5).

The process of formally modeling a situation as a game requires the decision-maker to enumerate explicitly the players and their strategic options, and to consider their preferences and reactions. The discipline involved in constructing such a model already has the potential of providing the decision-maker with a clearer and broader view of the situation. This is a "prescriptive" application of game theory, with the goal of improved strategic decision making (55 p. 5).

The object of study in game theory is the game, which is a formal model of an interactive situation. It typically involves several players; a game with only one player is usually a decision problem. The formal definition lays out the players, their preferences, their information, the strategic actions available to them, and how these influence the outcome (55 pp. 5-6).

Games can be described formally at various levels of detail. A coalitional (or cooperative) game is a high-level description, specifying only what payoffs each potential group, or coalition, can obtain by the cooperation of its members. Cooperative game theory investigates such coalitional games with respect to the relative amounts of power held by various players, or how a successful coalition should divide its proceeds. This is most naturally applied to situations arising in political science or international relations, where concepts like power are most important (55 p. 6).

In contrast, noncooperative game theory is concerned with the analysis of strategic choices. The paradigm of noncooperative game theory is the details of the ordering and timing of players' choices are crucial to determining the outcome of a game. The term "noncooperative" means this branch of game theory explicitly models the process of players making choices out of their own interest. Cooperation can, and often does, arise in noncooperative models of games, when players find it in their own best interests (55 pp. 6-7).

Branches of game theory also differ in their assumptions. A central assumption in many variants of game theory is that the players are rational. A rational player is one who always chooses an action which give the outcome he most prefers, given what he expects his opponents to do. The goal of game-theoretic analysis in these branches, then, is to predict how the game will be played by rational players, or, relatedly, to give advice on how best to play the game against opponents who are rational (55 p. 7).

The strategic form (also called the normal form) is the basic type of game studied in noncooperative game theory. A game in strategic form lists each player's strategies, and the outcomes that result from each possible combination of choices. An outcome is represented by a separate payoff for each player, which is a number (also called utility) that measures how much the player likes the outcome (55 p. 7).

The extensive form, also called a game tree, is more detailed than the strategic form of a game. It is a complete description of how the game is played over time. This includes the order in which players take actions, the information that players have at the time they must take those actions, and the times at which any uncertainty in the situation is resolved. A game in extensive form may be analyzed directly, or can be converted into an equivalent strategic form (55 p. 7).

Since all players are assumed to be rational, they make choices which result in the outcome they prefer most, given what their opponents do. In the extreme case, a player may have two strategies A and B so that, given any combination of strategies of the other players, the outcome resulting from A is better than the outcome resulting from B. Then strategy A is said to dominate strategy B. A rational player will never choose to play a dominated strategy. In some games, examination of which strategies are dominated result in the conclusion that rational players could only ever choose one of their strategies (55 p. 8).

Consideration of dominating strategies alone can yield precise advice to players on how to play the game. In many games, however, there are no dominated strategies, so these considerations are not enough to rule out any outcomes or to provide more specific advice on how to play the game. On the other hand, a Nash equilibrium recommends a strategy to each player that the player cannot improve upon unilaterally, that is, given that the other players follow the recommendation. Since the other players are also rational, it is reasonable for each player to expect his opponents to follow the recommendation as well (55 p. 12). A Nash equilibrium, also called strategic equilibrium, is a list of strategies, one for each player, which has the property that no player can unilaterally change his strategy and get a better payoff (55 p. 3).

A Nash equilibrium may not be unique. If a game has more than one Nash equilibrium, a theory of strategic interaction should guide players towards the "most reasonable" equilibrium upon which they should focus. A large number of papers in game theory are concerned with "equilibrium refinements" that attempt to derive conditions that make one equilibrium more plausible or convincing than another (55 p. 14).

A game in strategic form does not always have a Nash equilibrium in which each player deterministically chooses one of his strategies. However, players may instead randomly select from among these pure strategies with certain probabilities. Randomizing one's own choice is what is called a mixed strategy. Nash showed in 1951 that any finite strategic-form game has an equilibrium if mixed strategies are allowed (55 p. 17).

Games in strategic form have no temporal component. In a game of strategic form, the players choose their strategies simultaneously, without knowing the choices of the other players. The more detailed model of a game tree, also called a game in extensive form, formalizes interactions where the players can over time be informed about the actions of others. In an extensive game with perfect information, every player is at any point aware of the previous choices of all other players. Furthermore, only one player moves at a time, so there are no simultaneous moves (55 p. 22).

Typically, players do not always have full access to all the information which is relevant to their choices. Extensive games with imperfect information, model exactly which information is available to the players when they make a move. Modeling and evaluating strategic information precisely is one of the strengths of game theory. John Harsanyi's pioneering work in this area was recognized in the 1994 Nobel awards (55 p. 29).

Informing homeland security strategy with mathematical modeling of human behavior, as with game theory, can confer many advantages. First, mathematical models can describe basic behavioral processes in a more precise way than can be done with simple verbal descriptions. Second, it sometimes is difficult to derive unambiguous predictions from theories that are expressed in words, but the implications of competing theories (and differences between them) often become clear when the theories are presented in mathematical form. Third, critical tests that compare the quantitative predictions of two or more different models can indicate which hypotheses about a behavioral process are viable and which are not. Fourth, studies that test the quantitative predictions of mathematical models can identify insufficiencies in current theories and draw our attention to factors affecting behavior that might otherwise have been overlooked. And fifth, at their best, mathematical models can provide a common framework for describing diverse behavioral phenomena (57 pp. 287-288).

6 Applying Game Theory to Terrorism

Social scientists have written many papers on applications of game theory to terrorism (53 p. 12). One of the pillars of US antiterrorism policy is never to negotiate or capitulate to the demands of hostage-taking terrorists. The logic to this policy is that if a target adheres to its stated no-negotiation policy, then would be hostage takers would have nothing to achieve and so would stop abducting hostages. The outcome implicitly assumes that terrorists only gain from achieving their demands and that the subgame perfect equilibrium is to pledge not to concede. Obviously, something is incomplete about this logic because terrorists continue to take hostages and even the staunchest advocates of the no-negotiation policy have reneged on their pledge. Lapan and Sandler (1988) elucidate the policy's incompleteness with a game in extensive form where the government first chooses the level of deterrence, which, in turn, determines the logistical failure or success of terrorists when they engage in a hostage mission. A higher level of deterrence elevates the likelihood of logistical failure. Based on their perceived likelihoods of logistical and negotiation success, the terrorists decide whether to attack. If their expected payoffs from the hostage taking are positive, then they attack. The game can end in four ways: 1) no attack, 2) an attack that results in a logistical failure, 3) a successful attack that ends with the terrorists obtaining their demands, and 4) a successful attack that results in no concessions. Information is incomplete because the government does not know the payoffs associated with not capitulating prior to hostage incidents. Lapan and Sandler (1988) demonstrate that the

effectiveness of the no-negotiation strategy hinges on the credibility of the government's pledge, the absence of incomplete information, the terrorists' gain being solely tied to a negotiation success, and sufficient deterrence spending to eliminate logistical success. In practice, each of these implicit assumptions is suspect, casting doubt on the policy as a whole (54 pp. 2-3).

Another application of game theory involves terrorists' choice of targets for a three-player game involving two targeted nations and a common terrorist threat (Sandler & Lapan, 1988; Sandler & Siqueira, 2003). Each nation independently chooses its deterrence expenditures, which again determines the terrorists' logistical failure probability on that nation's soil. The terrorists pick the venue with the highest expected payoff for their attack. Each nation's choice of deterrence confers benefits and costs on the other target. By transferring the attack abroad, each nation imposes an external cost on its counterpart; however, by limiting attacks and their severity at home, each nation provides an external benefit to foreign residents. Moreover, an external benefit arises whenever the deterrence efforts of the nations sufficiently degrade the terrorists' expected benefits, so that they attack no one. The more fanatical are the terrorists, the less likely is the no-attack scenario. Sandler and Lapan (1988) show that the Nash equilibrium where each nation chooses its deterrence in isolation may result in too much or too little deterrence when compared with a social optimum, depending on the pattern of external costs and benefits. If, for example, attacks in either country leads to no collateral damage on foreign residents or interests, then the countries will engage in a deterrence race as each tries to transfer the potential attack abroad, where it has no residents. In a globalized society where a country's risks from a terrorist attack are equal everywhere, independent deterrence choices imply too little deterrence as each country fails to account for the protection that its efforts confer on foreign residents (54 pp. 4-5).

The game-theoretic approach reveals a couple of paradoxes. Countries may work at cross purposes when deterring terrorist attacks. Although the United States is the target of approximately 40% of all transnational terrorist attacks, virtually all of these attacks occurred abroad in recent years with 9/11 being a noticeable exception (Sandler, 2004). US over-deterrence means that it experiences attacks where it has little authority to do anything about them. Additionally, efforts to share intelligence on terrorists' preferences and resources may exacerbate this over-deterrence if deterrence decisions are not coordinated as nations use this information to augment efforts to transfer the attacks abroad (Sandler, & Lapan, 1988; Enders, & Sandler, 1995). This is a standard second-best result in economics in which there are two relevant policy variables – share intelligence and coordinate deterrence – but joint action only involves a single variable. This result highlights the beauty of a strategic approach. Standard intuition suggests that pooling information should enhance welfare, but this is not the case if this sharing worsens the deterrence race that wastes resources without necessarily increasing security against a determined terrorist group (54 p. 5).

Another game-theoretic representation analyzes a situation of asymmetric information where the terrorists know their true strength, but the targeted government must guess the terrorists' resources based on the level of their attacks. These attacks are intended to apply sufficient pressures, in terms of costs, to a government, so that it concedes to terrorist demands. In a deterministic setting, the outcome of the struggle between the adversaries would be known even before the first play of the game, because, in the absence of ties, a finite game of perfect information has a unique subgame perfect equilibrium. If, for example, the government is aware that the terrorists possess sufficient resources to force the government to surrender eventually, then the optimal strategy is for the government to concede at the outset and suffer no attack

damage. If, moreover, a well-informed terrorist group understands that it has insufficient resources to obtain its political demands, then it is optimal either to abandon the campaign or expend all of its resources at the outset (54 pp. 5-6).

A more interesting and relevant scenario is when the government is incompletely informed about the terrorists' capability. Lapan and Sandler (1993) analyze this scenario in which a signaling equilibrium may allow a government to limit its expected costs from attacks, even though the likelihood of surrender may increase. In this scenario, the extent of terrorist incidents may provide information to the government about the type of terrorist group – strong or weak – that it confronts. Attacks therefore serve as a signal that the government can process to adjust its posterior beliefs concerning the resources of the terrorists. Such updated beliefs permit the government to decide whether to capitulate or resist. The terrorists face an interesting tradeoff – the use of large amounts of their resources at the outset may correctly or incorrectly convince the government that they are strong, but this outlay results in less future attacks if the government is unconvinced. A perfect Bayesian[33] equilibrium for the two-period signaling game is derived in which the government prefers the associated partial pooling equilibrium, where the government surrenders to groups whose first-period attacks exceed a certain threshold, over the never-surrender equilibrium. The pooling equilibrium is associated with some regret when the government misjudges the terrorists' true strength based on initial attacks. Intelligence is valued, because it can reduce this regret by curtailing the variance of government priors (54 p. 6).

Another interesting application of game theory to terrorism involves accommodations reached between terrorists and a host government (Lee, 1988; Lee, & Sandler, 1989). In such scenarios, a terrorist organization has an implicit understanding that it can operate with impunity, provided that its attacks do not create collateral damage for the host country. This accommodation can undo efforts of other countries to retaliate against a terrorist group by reducing their cooperative payoffs. Thus, nations now have three options in their reaction to terrorists and their sponsors: do nothing, retaliate against the terrorists and their sponsors, or accommodate the terrorists. The last option helps the terrorists at the expense of the cooperating nations. Lee (1988) shows that this third option dominates the other two, thereby resulting in a Prisoner's Dilemma[34] where some

[33] In game theory, a Bayesian game is one in which information about characteristics of the other players (i.e. payoffs) is incomplete. Following John C. Harsanyi's framework, a Bayesian game can be modeled by introducing Nature as a player in a game. Nature assigns a random variable to each player which could take values of types for each player and associating probabilities or a probability density function with those types (in the course of the game, nature randomly chooses a type for each player according to the probability distribution across each player's type space). Harsanyi's approach to modeling a Bayesian game in such a way allows games of incomplete information to become games of imperfect information (in which the history of the game is not available to all players). The type of a player determines that player's payoff function and the probability associated with the type is the probability that the player for whom the type is specified is that type. In a Bayesian game, the incompleteness of information means that at least one player is unsure of the type (and so the payoff function) of another player. Such games are called Bayesian because of the probabilistic analysis inherent in the game. Players have initial beliefs about the type of each player (where a belief is a probability distribution over the possible types for a player) and can update their beliefs according to Bayes' Rule as play takes place in the game, i.e. the belief a player holds about another player's type might change on the basis of the actions they have played. The lack of information held by players and modeling of beliefs mean that such games are also used to analyze imperfect information scenarios (Wikipedia).

[34] The prisoner's dilemma is an example of a game, analyzed in game theory that shows why two individuals might not cooperate, even if it appears that it is in their best interest to do so. It was originally framed by Merrill Flood

nations seek such accommodations and, in so doing, undo the accomplishments of others to curtail the terrorist threat. Once again, pursuit of self-interest may harm others owing to strategic considerations (54 pp. 6-7).

Sandler's game theoretic analysis of terrorism, and those of others, follow some common themes. First, addressing one or more strategic interaction means eschewing an analysis of other strategic interactions. Models must be made tractable so that a choice of players must be made; that is, conclusions may drastically change as the strategic players change. Generally, just two or three strategizing players are considered at a time. Second, the use of multiple stages allows for more strategic players, but in each stage, there are generally two kinds of actively strategizing agents. Third, the number of continuous choice variables is limited; thus, a new continuous-choice variable requires making some other variable into a discrete-choice variable. Fourth, game-theoretic analyses of terrorism yield results that may be counterintuitive; for instance, augmenting information about terrorists' targeting preferences may actually exacerbate the inefficient behavior of targeted governments. Once the underlying strategic interaction is understood, the findings become intuitive. As a tool, game theory allows one to uncover nonobvious insights (58 p. 2).

7 Focusing on Homeland Security Strategy

The impressive work amassed by Sandler and others to date have made an indirect impact on homeland security strategy. We wish to extend their techniques to more directly inform homeland security strategy with respect to macroterrroism. A cursory examination of Sandler's applications reveals no underlying theme to problem selection. In part their methods are restricted by the ability to frame specific problems within a small set of parameters amenable to mathematical computation (58 p. 2). We propose a guiding theme to identify new problems sets amenable to game theoretic analysis and more directly inform homeland security strategy. We propose the following guiding heuristic:

> *Macroterrorism is a crime, and as such, may be thwarted by eliminating either means, motive, or opportunity.*

Macroterrorism is a form of terrorism. Terrorism, both international and domestic, is a crime under Title 18 United States Code (Crimes and Criminal Procedure), according to the following definitions:

> *(1) the term "international terrorism" means activities that—*
>
> > *(A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;*
> >
> > *(B) appear to be intended—*
> >
> > > *(i) to intimidate or coerce a civilian population;*
> > >
> > > *(ii) to influence the policy of a government by intimidation or coercion; or*

---

and Melvin Dresher working at RAND in 1950. Albert W. Tucker formalized the game with prison sentence payoffs and gave it the "prisoner's dilemma" name (Wikipedia).

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and

(C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum;

…

(5) the term "domestic terrorism" means activities that—

(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;

(B) appear to be intended—

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and

(C) occur primarily within the territorial jurisdiction of the United States.

The above heuristic is motivated by the "fire triangle". At the end of the 18th century, Antoine-Laurent Lavoisier (1743–1794) unveiled the mystery of fire, discovering that its anatomy- and minimum common denominator- constituted a triangle whose sides corresponded to heat (H), fuel (F) and oxygen (O). Lavoisier also deducted the biconditional characteristic of fire, i.e., it can occur if, and only if, all three elements are present, H, F, O ↔ Fire. Since then the fire triangle has been the foundation of all firefighting techniques (59 p. 13).

Means, motive, and opportunity (MMO) provide a similar basis for helping convict suspected criminals in a court of law. By themselves, MMO are not grounds for legal conviction. Many people have means, motive, and opportunity to commit crime, but yet they do not do so. Means, motive, and opportunity have no basis in law. However, they do have basis in court. In rhetorical theory, means, motive, and opportunity are classified as "topoi", a set of common arguments that assist lawyers with examining suspects. Did the accused have a motive, or reason to commit the crime; was it to their advantage? Did the suspect have the means to commit the crime; did they possess the weapon and ability to use it? Did the suspect have opportunity to commit the crime; were they in the right place at the right time? MMO belong to a collection of Denial topoi. In a Denial case, the lawyer's key task is to prove that the accused did indeed perform the alleged act. The Denial topoi, MMO, help frame a case for a jury, and together with credible evidence, build the burden of proof against the accused. By the same token, the Denial topoi may be equally employed by the defense to disprove the prosecution's theory. Defense need only poke a hole in a single argument to deflate the entire case. Typically, defense will resort to an "alibi" to disprove opportunity. MMO are not legal grounds for conviction, but they are heuristic tools that help lawyers convince juries the strength or weakness of a case (60).

The strength of the MMO topoi to prove or disprove a case is based on a long standing assumption that crime is only possible when all three elements are present. Remove one element

and it is impossible to prove the case since it was impossible to commit the crime. Certainly it is within means and possible for people to create disaster unintentionally, that is without malicious intent or motive. This, however, is an accident. And while these people can still be prosecuted and held accountable for their actions, their sanctions may be less severe because of an absence of malice[35]. Even so, accidents still require means and opportunity. Theories of accident causation generally attribute means to faulty or poorly designed systems (equipment, environment, or combination), and opportunity to careless, incapacitated, or inadequate personnel. Again, if either element is removed or mitigated, the accident will not happen (61 pp. 4-9).

> *We propose using the Denial topoi, means, motive, and opportunity, to identify a coherent set of macroterrorism problems, then analyzing those problems using the game theoretic approach to gain new insights to directly inform homeland security strategy.*

Together, WMD and CI provide a means for terrorists to inflict unprecedented death and destruction on the country. Before we examine how homeland security strategy may be shaped to possibly preclude this possibility, let us take a closer look at the mechanisms themselves.

8 WMD and CI Avenues of Attack

As introduced previously, macroterrorism incidents are those that can cause more than 500 deaths and $1B in damages (9 p. 5). As was noted earlier, weapons of mass destruction and critical infrastructure provide ready avenues of attack for small groups and individuals wishing to inflict macroterrorism. WMD include chemical, biological, radiological, and nuclear weapons. CI includes 18 distinct sectors as identified in the current Department of Homeland Security National Infrastructure Protection Plan (21 p. 3).

[35] On the evening of December 2, 1984, the Union Carbide India Limited (UCIL) chemical plant in Bhopal, India, leaked methyl isocyanate gas, an intermediate compound in the production of pesticides, killing an estimated 2,259 nearby residents. Various sources estimate 3,000 people died from direct exposure within weeks, and another 8,000 died later from gas-related diseases. UCIL was the Indian subsidiary of the Union Carbide Corporation (UCC), an American business later purchased by Dow Chemical Company in 2001. In June 2010, seven ex-employees, including the former UCIL chairman, were convicted in Bhopal of causing death by negligence and sentenced to two years imprisonment and a fine of about $2,000 each, the maximum punishment allowed by law. Civil and criminal cases remain pending in the United States District Court, Manhattan and the District Court of Bhopal, India (Wikipedia).

1. Agriculture and Food
2. Defense Industrial Base
3. Energy
4. Healthcare and Public Health
5. National Monuments and Icons
6. Banking and Finance
7. Water
8. Chemical Plants
9. Commercial Facilities
10. Critical Manufacturing
11. Dams
12. Emergency Services
13. Nuclear Reactors, Materials, and Waste
14. Information Technology
15. Communications
16. Postal and Shipping
17. Transportation Systems
18. Government Facilities

By itself, CI is not destructive. Only through subversion may CI become destructive. For our purposes, subversion means degrading, destroying, or diverting the intended CI function or capability. A quick review of the above list reveals that some CI, even if subverted, do not pose a danger of macroterrorism. For this reason, we shall remove the following CI from further consideration:

- Defense Industrial Base. Includes 250,000 firms in 215 distinct industries that manufacture and supply military equipment (18 p. 9). Subversion of key businesses may blunt military readiness, but they would not directly threaten a large portion of the civilian population.
- Healthcare and Public Health. Includes 5800 registered hospitals (18 p. 9). Subversion of all or even a large percentage of these facilities might hinder or delay health treatment, but they would not of themselves lead to mass casualties.
- National Monuments and Icons. Some 5,800 historic structures are counted among this sector (18 p. 9) that are more accurately termed "key resources" as they provide no tangible services[36]. Again, their destruction would be a great loss to the nation's heritage, otherwise, they don't represent a larger threat to the citizens of our country.
- Commercial Facilities. About 460 skyscrapers are listed among concerns for terrorist attack (18 p. 9). As was seen on 9/11, the collapse of the Twin Towers in New York City resulted in thousands of deaths. High rises by themselves, though, do not represent a threat. As happened on 9/11, it was subversion of the air transportation system that brought down the Twin Towers. It was the means that brought down the towers, not the towers themselves, that constitute the threat.

[36] The 2002 National Strategy for Homeland Security uses the term "key assets," defined as individual targets whose destruction would not endanger vital systems, but could create a local disaster or profoundly damage the Nation's morale or confidence. The Homeland Security Act and HSPD-7 use the term "key resources," defined more generally to capture publicly or privately controlled resources essential to the minimal operations of the economy or government. "Key resources" is the current terminology.

- Critical Manufacturing. Similar to the Defense Industrial Base, except instead of blunting military readiness, subversion of key businesses would hurt the economy. Damage would not otherwise directly threaten lives or property of the greater population.
- Emergency Services. These encompass more than 87,000 tribal, state, county, and municipal First Responder jurisdictions (18 p. 9). The loss of First Responders would certainly endanger the greater population, however, they would not necessarily precipitate that threat by themselves.
- Communications. This includes 2 billion miles of cable (18 p. 9). Subversion of this infrastructure would have cascading consequences across Information Technology and all that it touches, but it would be restricted to loss of capability. While the impact would be significant, it would not by itself perpetuate further damage.
- Postal and Shipping. These encompass a large infrastructure with 137 million delivery sites (18 p. 9). Again, the economic damage would be considerable, especially to businesses that depend on just-in-time inventories.
- Government Facilities owns and operates some 3,000 facilities including the places where state and national representatives meet to conduct the peoples' business [2003 NSIP]. While the catastrophic loss of a substantial portion of government would significantly affect the country, it would not lead to the collapse of the nation. Constitutions at all levels provide for succession of leadership, and plans for re-establishing central authority developed during the Cold War survive and continue to be practiced to this day [citation].

The remaining critical infrastructure may be subverted directly or indirectly by small groups or individuals to achieve macroterrorism effects. We will now take a closer look at the potential for subversion and resulting consequences of subversion in the remaining CI:

- Food and Agriculture. The potential for terrorist attacks against agricultural targets (agroterrorism) is increasingly recognized as a national security threat, especially after 9/11. Agroterrorism is a subset of bioterrorism, and is defined as the deliberate introduction of an animal or plant disease with the goal of generating fear, causing economic losses, and/or undermining social stability. The goal of agroterrorism is not to kill cows or plants. These are the means to the end of causing economic damage, social unrest, and loss of confidence in government. Human health could be at risk if contaminated food reaches the table or if an animal pathogen is transmissible to humans (zoonotic). While agriculture may not be a terrorist's first choice because it lacks the "shock factor" of more traditional terrorist targets, many analysts consider it a viable secondary target. Agriculture has several characteristics that pose unique vulnerabilities. Farms are geographically disbursed in unsecured environments. Livestock are frequently concentrated in confined locations, and transported or commingled with other herds. Many agricultural diseases can be obtained, handled, and distributed easily. International trade in food products often is tied to disease-free status, which could be jeopardized by

an attack. Many veterinarians lack experience with foreign animal diseases that are eradicated domestically but remain endemic in foreign countries (62 p. 2).

- Energy. Electricity is vital to the commerce and daily functioning of United States. The modernization of the grid to accommodate today's uses is leading to the incorporation of information processing capabilities for power system controls and operations monitoring. The "Smart Grid" is the name given to the evolving electric power network as new information technology systems and capabilities are incorporated. While these new components may add to the ability to control power flows and enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to computer-related attack since they are built around microprocessor devices whose basic functions are controlled by software programming (63 p. 2). Industrial control (IC) systems are particularly vulnerable to cyber attack because of their intelligence and communications capabilities. IC systems perform a number of functions in the electrical grid, ranging from microprocessor-based control systems which control the actuation and operation of one or more devices, to more sophisticated industrial IC systems which can manage entire industrial processes or automated systems. SCADA systems are a well-known application of remote IC used to monitor and control electric transmission system components. While cyber-intrusions into the U.S. grid have been reported in recent years, no impairment or other damage has been publicly reported as a result of the attacks. By exploiting loopholes in cyber security, cyber attackers could breach the privacy of customer's power usage data and access large numbers of meters, perhaps sending deliberately misleading information to the grid. This could potentially overload systems or cause grid operators to respond to false readings. However, concerns exist as to the potential damage that could result in the future from malware left behind by such intrusions or doorways created in systems which could be exploited. The revelation of the complexities of the Stuxnet worm and the alleged targeting of the control systems of a nuclear power plant in Iran have raised additional concerns about the vulnerability of electric power systems worldwide (63 p. 6). The Stuxnet worm reportedly affected the logical decision making functions of the control systems of one particular type of manufacturing facility. Theoretically, Stuxnet-like malware could be adapted to impair other types of process or control systems in malicious or unpredictable ways. Malware modified in such ways could overload and damage targeted equipment and systems in critical infrastructure. The Department of Homeland Security conducted a simulated cyber attack on an electric generator control room and partially destroyed a large diesel-electric generator secured for the test as a demonstration of existing power system vulnerabilities (63 p. 7).
- Banking and Finance. Long before 9/11, analysts identified financial sector system vulnerabilities as elements of national economic security in the work of the President's Commission on Critical Infrastructure Protection in 1996 and 1997. Financial institutions operate as intermediaries — accepting funds from various sources and making them available as loans or other investments to those who need them. The test of their

collective operational effectiveness is how efficiently the financial system as a whole allocates resources among suppliers and users of funds to produce real goods and services. America has grown far beyond a bank-centered financial economy: financial value has largely become resident on computers as data rather than physical means of payment. This element of the financial system is an area of particular vulnerability. Financial institutions face two categories of emergencies that could impair their functioning. The first is directly financial: danger of a sudden drop in the value of financial assets, whether originating domestically or elsewhere in the world, such that a global financial crisis might follow. The second is operational: failure of physical support structures that underlie the financial system. Either could disrupt the nation's ability to supply goods and services and alter the behavior of individuals in fear of the disruption (or fear of greater disruption). They could reduce the pace of economic activity, or at an extreme, cause an actual contraction of economic activity. Financial regulators generally address the former set of problems through deposit insurance and other sources of liquidity to distressed institutions, safety and soundness regulation, and direct intervention. They address the latter, operational, set through remediation (as with the Y2K problem[37]), redundancy, and other physical security. Under the worst case scenarios, the Federal Reserve (Fed) can relieve the economic effects of either set by acting as lender of last resort to supply liquidity to the financial system, employing monetary policy to expand domestic demand (as it did following the 9/11 terrorist attacks). In the Terrorism Risk Insurance Act of 2002 (TRIA), Congress expanded the Fed's ability to act as lender of last resort to the financial and real economies. Congress may also legislate direct federal assistance to protect the financial infrastructure. It has done so to prevent troubled entities such as Chrysler, the Farm Credit System, and New York City from defaulting, thus harming their lenders, and potentially causing failure in major parts of the financial system and the economy. Collapse of one prominent entity could evoke a contagion effect, in which sound financial institutions become viewed as

[37] The Year 2000 problem (also known as the Y2K problem, the Millennium bug, the Y2K bug, or simply Y2K) was a problem for both digital (computer-related) and non-digital documentation and data storage devices stemming from the practice of abbreviating a four-digit year to two digits. In computer programs, the practice of representing the year with two digits becomes problematic with logical errors arising upon "rollover" from x99 to x00. This caused some date-related processing to operate incorrectly for dates and times on and after January 1, 2000 and on other critical dates which were billed "event horizons". Without corrective action, long-working systems would break down when the "...97, 98, 99, 00..." ascending numbering assumption suddenly became invalid. Companies and organizations worldwide checked, fixed, and upgraded their computer systems. The number of computer failures that occurred when the clocks rolled over into 2000 in spite of remedial work is not known; among other reasons is the reticence of organizations to report problems. There is evidence of at least one date-related banking failure due to Y2K. There were plenty of other Y2K problems, but the fact that none caused major incidents is seen by some as vindication of the Y2K preparation. However, some questioned whether the relative absence of computer failures was the result of the preparation undertaken or whether the significance of the problem had been overstated (Wikipedia).

weak — today's equivalent of a bank run, in which panicked customers withdraw funds from many entities, probably causing others to fail as well. (64 pp. 1-2)

- Water. Damage to or destruction of the nation's water supply and water quality infrastructure by terrorist attack or natural disaster could disrupt the delivery of vital human services in this country, threatening public health and the environment, or possibly causing loss of life. Across the country, water infrastructure systems extend over vast areas, and ownership and operation responsibility are both public and private, but are overwhelmingly non-federal. Since the attacks, federal dam operators and local water and wastewater utilities have been under heightened security conditions and are evaluating security plans and measures. There are no federal standards or agreed-upon industry practices within the water infrastructure sector to govern readiness, response to security incidents, and recovery. Efforts to develop protocols and tools are ongoing since the 9/11 terrorist attacks (65 p. 1). A fairly small number of large drinking water and wastewater utilities located primarily in urban areas (about 15% of the systems) provide water services to more than 75% of the U.S. population. Arguably, these systems represent the greatest targets of opportunity for terrorist attacks, while the larger number of small systems that each serve fewer than 10,000 persons are less likely to be perceived as key targets by terrorists who might seek to disrupt water infrastructure systems. However, the more numerous smaller systems also tend to be less protected and, thus, are potentially more vulnerable to attack, whether by vandals or terrorists. A successful attack on even a small system could cause widespread panic, economic impacts, and a loss of public confidence in water supply systems (65 p. 2). Since the 2001 terrorist attacks, many water and wastewater utilities have switched from using chlorine gas as disinfection to alternatives which are believed to be safer, such as sodium hypochlorite or ultraviolet light. However, some consumer groups remain concerned that many wastewater utilities, including facilities that serve heavily populated areas, continue to use chlorine gas. Damage to a wastewater facility prevents water from being treated and can impact downriver water intakes. Destruction of containers that hold large amounts of chemicals at treatment plants could result in release of toxic chemical agents, such as chlorine gas, which can be deadly to humans if inhaled and, at lower doses, can burn eyes and skin and inflame the lungs (65 pp. 4-5)
- Chemical Plants. The potential harm to public health and the environment from a sudden release of hazardous chemicals has long concerned the US Congress. The sudden, accidental release in December 1984 of methyl isocyanate in an industrial incident at the Union Carbide plant in Bhopal, India, and the attendant loss of thousands of lives and widespread injuries spurred legislative proposals to reduce the risk of chemical accidents in the United States (66 p. 1). Potential terrorist acts against chemical facilities might be classified roughly into two categories: direct attacks on facilities or chemicals on site, or efforts to use business contacts, facilities, and materials (e.g., letterhead, telephones, computers, etc.) to gain access to potentially harmful materials. In either case, terrorists may be employees (saboteurs) or outsiders, acting alone or in collaboration with others.

In the case of a direct attack, traditional or nontraditional weapons may be employed, including explosives, incendiary devices, firearms, airplanes, computer programs, or weapons of mass destruction (nuclear, radiological, chemical, or biological). In obtaining chemicals, a terrorist's intent may be their use as weapons or to make weapons, including but not limited to explosives, incendiaries, poisons, and caustics. Access to chemicals might be gained by physically entering a facility and stealing supplies, or by using legitimate or fraudulent credentials (e.g., company stationary, order forms, computers, telephones or other resources) to order, receive, or distribute chemicals (66 p. 2).

- Dams. The federal government has built hundreds of water projects, primarily dams and reservoirs for irrigation development and flood control, with municipal and industrial water use as an incidental, self-financed, project purpose. Many of these facilities are critically entwined with the nation's overall water supply, transportation, and electricity infrastructure. The largest federal facilities were built and are managed by the Bureau of Reclamation (Reclamation) of the Department of the Interior and the U.S. Army Corps of Engineers (Corps) of the Department of Defense. Reclamation reservoirs, particularly those along the Colorado River, supply water to millions of people in southern California, Arizona, and Nevada via Reclamation and non-Reclamation aqueducts. Reclamation's inventory of assets includes 471 dams and dikes that create 348 reservoirs with a total storage capacity of 245 million acre-feet of water. Reclamation projects also supply water to 9 million acres of farmland and other municipal and industrial water users in the 17 western states. The Corps operates 276 navigation locks, 11,000 miles of commercial navigation channel, and approximately 1,200 projects of varying types, including 609 dams. It supplies water to thousands of cities, towns, and industries from the 9.5 million acre-feet of water stored in its 116 lakes and reservoirs throughout the country, including service to approximately 1 million residents of the District of Columbia and portions of northern Virginia. The largest Corps and Reclamation facilities also produce enormous amounts of power. For example, Hoover and Glen Canyon dams on the Colorado River represent 23% of the installed electrical capacity of the Bureau of Reclamation's 58 power plants in the West and 7% of the total installed capacity in the Western United States. Similarly, Corps facilities and Reclamation's Grand Coulee Dam on the Columbia River provide 43% of the total installed hydroelectric capacity in the West (25% nationwide). Still, despite its critical involvement in such projects, especially in the West, the federal government is responsible for only about 5% of the dams whose failure could result in loss of life or significant property damage. The remaining dams belong to state or local governments, utilities, and corporate or private owners. Attacks resulting in physical destruction to any of these systems could include disruption of operating or distribution system components, power or telecommunications systems, electronic control systems, and actual damage to reservoirs and pumping stations. Further, destruction of a large dam could result in catastrophic flooding and loss of life (65 p. 2).
- Nuclear Reactors, Materials, and Waste. Protection of nuclear power plants from land-based assaults, deliberate aircraft crashes, and other terrorist acts has been a heightened

national priority since the attacks of September 11, 2001 (67 p. 1). The major concerns in operating a nuclear power plant are controlling the nuclear chain reaction and assuring that the reactor core does not lose its coolant and "melt down" from the heat produced by the radioactive fission products within the fuel rods. US plants are designed and built to prevent dispersal of radioactivity, in the event of an accident, by surrounding the reactor in a steel-reinforced concrete containment structure, which represents an intrinsic safety feature. Two major accidents have taken place in power reactors, at Three Mile Island (TMI) in 1979[38] and at Chernobyl in the Soviet Union in 1986[39]. Although both accidents resulted from a combination of operator error and design flaws, TMI's containment structure effectively prevented a major release of radioactivity from a fuel meltdown caused by the loss of coolant. In the Chernobyl accident, the reactor's protective barriers were breached when an out-of-control nuclear reaction led to a fierce graphite fire that

[38] The Three Mile Island accident was a core meltdown in Unit 2 of the Three Mile Island Nuclear Generating Station in Dauphin County, Pennsylvania near Harrisburg, United States in 1979. The accident resulted in the release of approximately 2.5 million curies of radioactive gases, and approximately 15 curies of iodine-131. There was an evacuation of 140,000 pregnant women and pre-school age children from the area. In the end, the reactor was brought under control, although full details of the accident were not discovered until much later, following extensive investigations by both a presidential commission and the NRC. The Kemeny Commission Report concluded that "there will either be no case of cancer or the number of cases will be so small that it will never be possible to detect them. The same conclusion applies to the other possible health effects". Several epidemiological studies in the years since the accident have supported the conclusion that radiation released from the accident had no perceptible effect on cancer incidence in residents near the plant, though these findings are contested by one team of researchers. Cleanup started in August 1979 and officially ended in December 1993, with a total cleanup cost of about $1B. The accident crystallized anti-nuclear safety concerns among activists and the general public, resulted in new regulations for the nuclear industry, and has been cited as a contributor to the decline of new reactor construction that was already underway in the 1970s (Wikipedia).

[39] On 26 April 1986, the Chernobyl Nuclear Power Plant in Ukraine exploded and caught fire, releasing large quantities of radioactive contamination into the atmosphere and spreading it over much of the Western Soviet Union and Europe. It is considered the worst nuclear power plant accident in history, rivaled only by the Fukushima Daiichi nuclear disaster in March 2011The battle to contain the contamination and avert a greater catastrophe ultimately involved over 500,000 workers and cost an estimated 18 billion rubles, crippling the Soviet economy. From 1986 to 2000, 350,400 people were evacuated and resettled from the most severely contaminated areas of Belarus, Russia, and Ukraine. According to official post-Soviet data, about 60% of the fallout landed in Belarus. The accident raised concerns about the safety of the Soviet nuclear power industry, as well as nuclear power in general, slowing its expansion for a number of years and forcing the Soviet government to become less secretive about its procedures. The government cover-up of the Chernobyl disaster was a "catalyst" for glasnost, which "paved the way for reforms leading to the Soviet collapse." Russia, Ukraine, and Belarus have been burdened with the continuing and substantial decontamination and health care costs of the Chernobyl accident. Thirty one deaths are directly attributed to the accident, all among the reactor staff and emergency workers. A UN report places the total confirmed deaths from radiation at 64 as of 2008. The World Health Organization suggests it could reach 4,000 civilian deaths, a figure which does not include military clean-up worker casualties. A 2006 report predicted 30,000 to 60,000 cancer deaths as a result of Chernobyl fallout. A Greenpeace report puts this figure at 200,000 or more. A Russian publication, Chernobyl, concludes that 985,000 premature cancer deaths occurred worldwide between 1986 and 2004 as a result of radioactive contamination from Chernobyl (Wikipedia).

caused a significant part of the radioactive core to be blown into the atmosphere (67 p. 4). US nuclear power plants were designed to withstand hurricanes, earthquakes, and other extreme events. But deliberate attacks by large airliners loaded with fuel, such as those that crashed into the World Trade Center and Pentagon, were not analyzed when design requirements for today's reactors were determined. A taped interview shown September 10, 2002, on Arab TV station al- Jazeera, which contains a statement that Al Qaeda initially planned to include a nuclear plant in its 2001 attack sites, intensified concern about aircraft crashes. According to former NRC Chairman Nils Diaz, NRC studies "confirm that the likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low." Even so, NRC announced on April 24, 2007, that it would issue a proposed rule requiring license applicants for new reactors to assess potential design improvements that would improve protection against impact by large commercial aircraft. However, even if the reactor is secure from aircraft impact, the same may not be true for spent fuel. When no longer capable of sustaining a nuclear chain reaction, "spent" nuclear fuel is removed from the reactor and stored in a pool of water in the reactor building and at some sites later transferred to dry casks on the plant grounds. Because both types of storage are located outside the reactor containment structure, particular concern has been raised about the vulnerability of spent fuel to attack by aircraft or other means. If terrorists could breach a spent fuel pool's concrete walls and drain the cooling water, the spent fuel's zirconium cladding could overheat and catch fire (67 p. 5). The National Academy of Sciences released a report in April 2005 that found that "successful terrorist attacks on spent fuel pools, though difficult, are possible," and that "if an attack leads to a propagating zirconium cladding fire, it could result in the release of large amounts of radioactive material." (67 p. 6)

- Information Technology. The FBI reports that cyber attacks attributed to terrorists have largely been limited to unsophisticated efforts such as e-mail bombing of ideological foes, denial-of-service attacks, or defacing of websites. However, it says, their increasing technical competency is resulting in an emerging capability for network-based attacks. The FBI has predicted that terrorists will either develop or hire hackers for the purpose of complementing large conventional attacks with cyber attacks. The Internet, whether accessed by a desktop computer or by the many available handheld devices, is the medium through which a cyber attack would be delivered. However, for a targeted attack to be successful, the attackers usually require that the network itself remain more or less intact, unless the attackers assess that the perceived gains from shutting down the network entirely would offset the accompanying loss of their own communication. A future targeted cyber attack could be effective if directed against a portion of the US critical infrastructure, and if timed to amplify the effects of a simultaneous conventional physical or chemical, biological, radiological, or nuclear terrorist attack. The objectives of a cyber attack may include the following:
    - loss of integrity, such that information could be modified improperly;

- loss of availability, where mission-critical information systems are rendered unavailable to authorized users;
- loss of confidentiality, where critical information is disclosed to unauthorized users; and
- physical destruction, where information systems create actual physical harm through commands that cause deliberate malfunctions.

Publicity would also potentially be one of the primary objectives for a terrorist cyber attack. Extensive media coverage has shown the vulnerability of the US information infrastructure and the potential harm that could be caused by a cyber attack. This might lead terrorists to believe that even a marginally successful cyber attack directed at the United States would garner considerable publicity. Some suggest that were such a cyber attack by an international terrorist organization to occur and become known to the general public, regardless of the level of success of the attack, concern by many citizens and cascading effects might lead to widespread disruption of critical infrastructures. For example, reports of an attack on the international financial system's networks could create a fiscal panic in the public that could lead to economic damage. The recent emergence of the Stuxnet worm may have implications for what potential future cyber attacks might look like. Stuxnet is thought to be the first piece of malicious software (malware) that was specifically designed to target the computer-networked industrial control systems that control utilities, in this case nuclear power plants in Iran. Although many experts contend that the level of sophistication, intelligence, and access required to develop Stuxnet all point to nation states, not only is the idea now in the public sphere for others to build upon, but the code has been released as well. An industrious group could potentially use this code as a foundation for developing a capability intended to degrade and destroy the software systems that control the US power grid, to name one example (68 pp. 5-6).

- Transportation Systems. The nation's air, land, and marine transportation systems are designed for accessibility and efficiency, two characteristics that make them highly vulnerable to terrorist attack. Aviation security has been a major focus of transportation security policy following the terrorist attacks of September 11, 2001. In the aftermath of these attacks, the 107th Congress moved quickly to pass the Aviation and Transportation Security Act (ATSA; P.L. 107-71) creating the Transportation Security Administration (TSA) and mandating a federalized workforce of security screeners to inspect airline passengers and their baggage. The act gave the TSA broad authority to assess vulnerabilities in aviation security and take steps to mitigate these risks. The July 2005 bombing of trains in London and the bombings of commuter trains and subway trains in Madrid and Moscow in 2004 highlighted the vulnerability of passenger rail systems to terrorist attacks. The volume of ridership and number of access points make it impractical to subject all rail passengers to the type of screening airline passengers undergo. A leading issue with regard to securing truck, rail, and waterborne cargo is the desire of

government authorities to track a given freight shipment at a particular time. Most of the attention with regard to cargo vulnerability concerns the tracking of marine containers as they are trucked to and from seaports. Security experts believe this is a particularly vulnerable point in the container supply chain. Hazardous materials (hazmat) transportation raises numerous security issues. There are issues regarding routing of hazmat through urban centers, and debate persists over the pros and cons of rerouting high hazard shipments (69 p. 3).

The continuing possibility of terrorist attacks using nuclear, biological, or chemical weapons is an ongoing concern in the national security policy arena in the face of a clear trend among terrorists to inflict greater numbers of casualties. Worldwide, the likelihood of terrorists being capable of producing or obtaining WMD may be growing due to looser controls of stockpiles and technology in the former Soviet states specifically, and the broader dissemination of related technology and information in general. However, WMD remain significantly harder to produce or obtain than what is commonly depicted in the press. The Central Intelligence Agency has reported that it is likely that most terrorists will continue to choose conventional explosives over WMD, but warns that the al-Qaeda network has made obtaining WMD capability a very high priority (17 p. 2).

- Chemical. Toxic industrial chemicals such as chlorine or phosgene are easily available and do not require great expertise to be adapted into chemical weapons. Aerosol or vapor forms are the most effective for dissemination, which can be carried out by sprayers or an explosive device. Nerve agents are more difficult to produce, and require a synthesis of multiple precursor chemicals. They also require high-temperature processes and create dangerous by-products, which makes their production unlikely outside an advanced laboratory. Blister agents such as mustard can be manufactured with relative ease, but also require large quantities of precursor chemicals. The production and transfer of precursor chemicals is internationally monitored under the Chemical Weapons Convention and the informal international export control regime of the Australia Group, providing some degree of control over their distribution (17 p. 6).
- Biological. Experts say terrorists working outside a state-run laboratory would have to overcome extraordinary technical and operational challenges to effectively and successfully weaponize and deliver a biological agent to cause mass casualties. Despite the 2001 anthrax attacks, this statement may still hold some validity. While many biological agents can be obtained or grown with relative ease, several significant steps remain on the way to weaponization and effective use of these agents. The main challenge is effective dissemination, which requires an aerosol form. The formulation of agents for airborne dispersal requires dissolving optimal amounts of agent in a specific combination of different chemicals (with each agent requiring a unique formulation). Moreover, aerosol disseminators need to be properly designed for the agent used, and suitable meteorological conditions must be present to carry out a successful biological mass casualty attack. Of particularly great concern is the threat of highly contagious

diseases, particularly smallpox. Anthrax is not contagious from person to person, consequently its spread can be relatively easily contained. With a disease like smallpox, however, contagion can spread very rapidly. The breath or coughing of an infected person at the fever stage of the disease is sufficient to infect those around him or her. The disease has an incubation period of 12-14 days, during which an infected person experiences no symptoms. Consequently, a clandestine smallpox release in a major transportation hub could infect hundreds, and would, in two weeks' time, result in disease outbreaks wherever the passengers eventually traveled. Smallpox has been eradicated as a naturally occurring disease, and the only two known existing cultures of the virus are held by the United States and Russia. Even so, concerns over the security of the Russian samples and the possibilities of unknown samples, have kept smallpox in the forefront of threat considerations. Though the probability of terrorists gaining access to the virus may be very low, the severity of the potential consequences has nevertheless led the federal government to stockpile 300 million smallpox vaccine doses (17 pp. 5-6).

- Radiological. Explosive-driven "dirty bombs" are an often-discussed type of radiological dispersion device (RDD), though radioactive material can also be dispersed in other ways. Radioactive material is the necessary ingredient for an RDD. This material is composed of atoms that decay, emitting radiation. Some types and amounts of radiation are harmful to human health. Terrorists have shown some interest in RDDs. They could use them in an attempt to disperse radioactive material to cause panic, area denial, and economic dislocation. While RDDs would be far less harmful than nuclear weapons, they are much simpler to build and the needed materials are used worldwide. Accordingly, some believe terrorists would be more likely to use RDDs than nuclear weapons. Key points include:
    - RDDs could contaminate areas with radioactive material, increasing long-term cancer risks, but would probably kill few people promptly. Nuclear weapons could destroy much of a city, kill tens of thousands of people, and contaminate much larger areas with fallout.
    - Cleanup cost after an RDD attack could range from less than a billion dollars to tens of billions of dollars, depending on area contaminated, decontamination technologies used, and level of cleanup required (70 p. 2).

  Despite the seeming ease of launching a successful RDD attack, terrorists have not done so. The reasons are necessarily speculative, but may include difficulties in handling radioactive material, lack of sufficient expertise to fabricate material into an effective weapon, a shift to smaller-scale but simpler attacks using standard weapons and explosives, and improved security. Of course, such factors cannot guarantee that no attack will occur (70 p. 2).

- Nuclear. While a nuclear weapon is the most destructive of all WMD, obtaining one poses the greatest difficulty for terrorist groups. The key obstacle to building such a weapon is the availability of a sufficient quantity of fissile material—either plutonium or

highly enriched uranium. Some experts believe that if allowed access to the necessary quantities of fissile material, extraordinarily capable groups could build a crude nuclear weapon (17 p. 4).

9 Macroterrorism Risk Model

If we take a closer look at the remaining WMD and CI, we observe an order or preference that may be expressed by terrorists based upon the potential scope of destruction for each method of attack. For example, a successful attack on Food and Agriculture or Energy could have potential nationwide impact compared to sabotaging a Water aqueduct or Chemical Plant. Consequently, we will now classify our list of WMD and CI into two orders of preference with the first order of preference representing greater potential lethality:

First Preference

- Food & Agriculture
- Energy
- Banking & Finance
- Nuclear Reactors, Materials, & Waste
- Information Technology
- CBRN Weapons

Second Preference

- Water Infrastructure
- Chemical Plants
- Dams
- Transportation Systems

Similarly, we notice that there is an ordered relationship between the various methods of attack. The corresponding relationships are expressed as follows:

1. Terrorists are Agents who seek to harm innocent civilians.
2. Terrorists must acquire Weapons or Materials to achieve their means.
3. Materials must be manufactured into Weapons.
4. Weapons may be employed directly or indirectly against civilians.
5. Terrorists may choose Targets that indirectly affect civilians.
6. Terrorists may choose to Target civilians directly.

The resulting graph is called the Macroterrorism Risk Model. The Macroterrorism Risk Model facilitates heuristic analysis using the Denial Topoi of means, motive, and opportunity to identify government policy opportunities with respect to homeland security strategy.

10 MRM Analysis

Examining the Macroterrorism Risk Model with respect to means, motive, and opportunity, we notice four areas where government can shape policy to prevent or protect against catastrophic terrorism: 1) controlling means by which terrorists may *acquire* weapons, 2) controlling means by which terrorists may *manufacture* weapons, 3) protecting *targets* which terrorists may choose to attack, and 4) controlling direct and indirect means by which terrorists may *harm* a large portion of the nation's population.

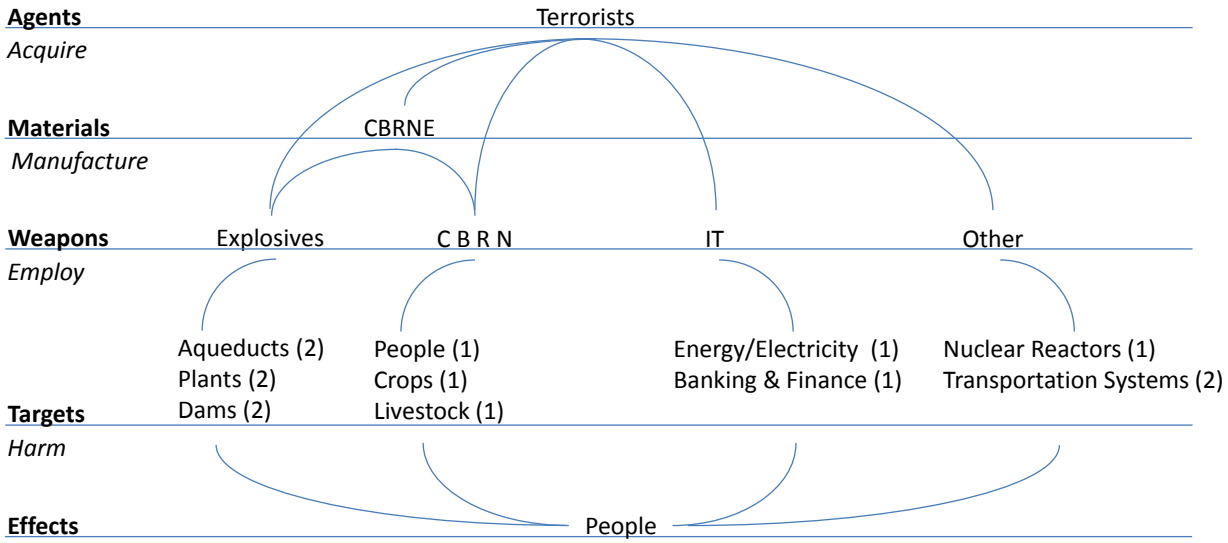

Figure 1: Macroterrorism Risk Model

Terrorist target selection has already been examined using the game theoretic approach. Essentially hardening one set of potential targets only transfers terrorist's attention to less protected, easier targets. The target set in this case is very large, and would be impractical to protect against determined terrorist attack (54 pp. 4-5).

Weapons manufacturing requires only materials, tools, and knowledge. Materials acquisition represents a strong area for government policy intervention, addressed in the next paragraph. Government policies restricting access to tools and knowledge are much less promising. This is because 1) the knowledge is already prevalent in the public domain, and 2) the required tools have dual-use across a wide variety of applications. Government policies to prevent the manufacture of WMD, particularly high explosives would be mostly ineffective.

As previously indicated, government policies addressing the means for acquiring WMD could prove more lucrative in preventing catastrophic terrorism. The fact that neither nuclear nor radiological weapons have been employed to date may be attributable to current policies restricting access to CBRN weapons and materials (70 p. 2). The Macroterrorism Risk Model

suggests that new policy insights may be gained using a game theoretic approach examining the choice of terrorist weapons' selection.

> *The question that presents itself is whether government policies can influence terrorists' weapons selection similar in manner to target selection, and whether government policies might be crafted to direct terrorists to less destructive means.*

Such game-theoretic analysis would examine terrorists' **motives** for weapons selection given varying difficulties of access.

The ultimate target of macroterrorism is the civilian population. The opportunity for subverting critical infrastructure to achieve terrorist goals is rooted in systems' ad hoc organization: very little was centrally planned, and even less was designed to withstand deliberate attack. This can be changed. The nation's critical infrastructure can be overhauled or replaced to become less susceptible to subversion, or at least less hazardous when subverted. Such a condition is called "failsafe". Nuclear reactors are a good example of this potential. Today's commercial reactors depend upon active cooling, which, despite backup systems, may still fail, as occurred at Fukushima in Japan[40] (71 p. 2). The resulting meltdown and release of radioactive material will take decades and billions of dollars to remediate. Pebble reactors, on the other hand, are not only failsafe, they do not require active cooling and will halt without active power. They are also more efficient than water reactors[41]. So, terrorists may be denied **opportunity** by making CI failsafe. This, however, is a very expensive proposition.

[40] The earthquake on March 11, 2011, off the east coast of Honshu, Japan's largest island, reportedly caused an automatic shutdown of eleven of Japan's fifty-five operating nuclear power plants. Most of the shutdowns proceeded without incident. However, the plants closest to the epicenter, Fukushima and Onagawa, were damaged by the earthquake and resulting tsunami. The Fukushima Daiichi plant subsequently suffered hydrogen explosions and probable nuclear fuel damage, releasing significant amounts of radioactive material into the environment.

[41] The pebble bed reactor (PBR) is a graphite-moderated, gas-cooled, nuclear reactor. It is a type of very high temperature reactor (VHTR), one of the six classes of nuclear reactors in the Generation IV initiative. Like other VHTR designs, the PBR uses TRISO fuel particles, which allows for high outlet temperatures and passive safety. The base of the PBR's design is the spherical fuel elements called pebbles. These tennis ball-sized pebbles are made of pyrolytic graphite (which acts as the moderator), and they contain thousands of micro fuel particles called TRISO particles. These TRISO fuel particles consist of a fissile material (such as 235U) surrounded by a coated ceramic layer of silicon carbide for structural integrity and fission product containment. In the PBR, thousands of pebbles are amassed to create a reactor core, and are cooled by an inert or semi-inert gas such as helium, nitrogen or carbon dioxide. This type of reactor is claimed to be passively safe; that is, it removes the need for redundant, active safety systems. Because the reactor is designed to handle high temperatures, it can cool by natural circulation and still survive in accident scenarios, which may raise the temperature of the reactor to 1,600 °C. Because of its design, its high temperatures allow higher thermal efficiencies than possible in traditional nuclear power plants (up to 50%) and has the additional feature that the gases do not dissolve contaminants or absorb neutrons as water does, so the core has less in the way of radioactive fluids. A number of prototypes have been built. China's HTR-10 is the only prototype currently operating (Wikipedia).

The question that may be posed for game theoretic analysis is whether government policies aimed at retrofitting CI to reduce terrorists' opportunity for attack will more or less effectively reduce the threat of catastrophic attack, and at what cost.

The Macroterrorism Risk Model also identifies various **means** for reducing the threat of catastrophic terrorism. MRM makes evident the counterterrorism choices first proposed by the Gilmore Commission in America's New Normalcy. According to the Bremer Commission, the US has a choice of going after terrorists, terrorist weapons, or protecting potential targets (72 p. 11).

The question that may be posed for game theoretic analysis is which government strategy would most stress the capabilities of terrorists, forcing them to withdraw from plans to conduct catastrophic attacks, versus actions that would encourage them to conduct catastrophic attacks. Currently the nation pursues a mixed strategy. Is there a better equilibrium?

11 Thesis Proposal

This paper proposes using game theoretic analysis to better inform homeland security strategy. This paper suggests that terrorism, in all forms, is a criminal act, and thereby recommends using the criminal predicate (Denial Topoi) of means, motive, and opportunity to concentrate game theoretic analysis on the threat of catastrophic terrorism. A Macroterrorism Risk Model identifies relationships between WMD and CI to assist in locating suitable problems amenable to game theoretic analysis. Three specific problems are identified:

1. **Motive.** Can homeland security policies governing availability and access to CBRN materials and weapons affect terrorists' motives regarding their deployment (i.e., "weapons substitution")?
2. **Opportunity.** Can homeland security policies expediting development of failsafe CI reduce the threat of catastrophic attack, and at what cost?
3. **Means.** Should homeland security policies focus more on terrorists, weapons, or targets? Which strategy would most stress the capabilities of terrorists, forcing them to withdraw from plans to conduct catastrophic attacks, versus actions that would encourage them to conduct catastrophic attacks?

This paper proposes conducting game theoretic analysis of the above problems and publishing the results. The research would validate the proposed methodology and the results would have direct application to US homeland security policy. Expanded research using the same methodology could identify even more problems amenable to similar analysis, providing even more insight to homeland security strategy. The schedule of research is proposed as follows:

MS	Description	Start	End
0	Initiate Research	4 Jan 12	4 Jan 12
1	Research Paper 1	4 Jan 12	1 Apr 12
2	Publish Paper 1	1 May 12	1 May 12
3	Research Paper 2	1 Apr 12	1 Jun 12
4	Publish Paper 2	1 Jul 12	1 Jul 12
5	Research Paper 3	1 Jun 12	1 Aug 12
6	Publish Paper 3	1 Sep 12	1 Sep 12
7	Draft Dissertation	1 Aug 12	1 Nov 12
8	Publish Dissertation	1 Dec 12	1 Dec 12

12 Conclusion

We began this proposal with the question "are we safe?" Ten years after 9/11 and the death of Osama bin Laden, is the United States safe from terrorist attack? The answer is "no". On 9/11, nineteen people caused as much damage as the Imperial Japanese Navy on December 7th, 1941. The lesson from 9/11 is not the threat of Islamic extremism, but rather that small groups and individuals can subvert our critical infrastructure to inflict destruction on a scale once reserved to nations. Hope is not a strategy, the threat cannot be ignored. It is a basic function of the US government to protect its citizens, and it acted appropriately to develop homeland security strategy. Today's strategy is similar to the original strategy which has no basis in theory. A theoretic foundation is preferred to help direct the most effective and efficient expenditure of government manpower and funds. International relation theories don't apply since terrorists are not sovereign government entities. Terrorism theories are ineffective as they address what makes terrorists and have yet to determine any root causes. Terrorism modeling, on the other hand, has offered insight into terrorists' actions, especially game theoretic analysis. Among the alternatives, game theory seems to offer the strongest foundation for policy guidance as it accounts for terrorist behavior within a mathematically formulated model. This approach has provided insight to broader counterterrorism policies on 1) negotiating with terrorists, 2) target substitution, 3) international cooperation, and other areas. The problem is that this approach has not been systematically applied to specifically inform homeland security strategy.

13 Bibliography

1. **Eisenhower Study Group.** *Costs of War: Executive Summary.* Providence, RI : Watson Institute, Brown University, 2011.
2. **Federal Bureau of Investigation.** Most Wanted Terrorists. *The FBI.* [Online] May 2, 2011. [Cited: October 29, 2011.] http://www.fbi.gov/news/stories/2011/may/binladen_050211/binladen_050211.
3. **National Security Preparedness Group.** *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations.* Washington, DC : Bipartisan Policy Center, 2011.
4. **Whitlock, Craig.** Panetta: U.S. 'within reach' of defeating al-Qaeda. *The Washington Post.* [Online] July 9, 2011. [Cited: October 29, 2011.] http://www.washingtonpost.com/world/panetta-us-within-reach-of-defeating-al-qaeda/2011/07/09/gIQAvPpG5H_story.html.
5. **Rollins, John.** *Osama bin Laden's Death: Implications and Considerations.* Washington, DC : Congressional Research Service, 2011. R41809.
6. **National Commission on Terrorist Attacks Upon the United States.** *The 9/11 Commission Report.* Washington, DC : US Government Printing Office, 2004.
7. **Miller, Erin and Smarick, Kathleen.** *Background Report: 9/11, Ten Years Later.* s.l. : National Consoritum for the Study of Terrorism and Response to Terrorism (START), 2011.
8. **Kochanek, Kenneth D., et al., et al.** *Deaths: Preliminary Data for 2009.* Atlanta, GA : Centers for Disease Control and Prevention, 2011.
9. *The Evolution of Terrorism Risk Modeling.* **Woo, Gordon.** London, England : Journal of Reinsurance Risk Management Solutions, Ltd., 2003.
10. **US House of Representatives.** Testimony of the Acting DCI William O. Studeman. Washington, DC : s.n., 1995.
11. **The White House.** National Strategy to Combat Weapons of Mass Destruction. Washington, DC : s.n., 2002.
12. **Fidler, David P.** Weapons of Mass Destruction and International Law. *American Society of Intnernational Law.* [Online] February 2003. [Cited: November 2, 2011.] http://www.asil.org/insigh97.cfm.
13. **The United States Commission on National Security/21st Century.** *Road Map for National Security: Imperative for Change.* Washington, DC : s.n., 2001.
14. **Bowman, Steve and Barel, Helit.** *Weapons of Mass Destruction - The Terrorist Threat.* Washington, DC : Congressional Resarch Service, 1999. RS20412.
15. **Howe, David.** *Planning Scenarios: Executive Summaries.* Washington, DC : The Homeland Security Council, 2004.
16. **US Department of Justice.** *Amerithrax: Investigative Summary and Errata.* Washington, DC : s.n., 2010.
17. **Bowman, Steve.** *Weapons of Mass Destruction: The Terrorist Threat.* Washington, DC : Congressional Research Service, 2002. RL31332.
18. **The White House.** *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets.* Washington, DC : s.n., 2003.
19. **Nanto, Dick K.** *9/11 Terrorism: Global Economic Costs.* Washington, DC : Congressional Research Service, 2004. RS21937.

20. **National Commission on Terrorist Attacks Upon the United States.** *The 9/11 Commission Report: Executive Summary.* Washington, DC : s.n., 2004.
21. **Department of Homeland Security.** *National Infrastructure Protection Plan.* Washington, DC : s.n., 2009.
22. **Burke, James.** *Connections, Episode 1, The Trigger Effect.* s.l. : BBC Science & Features Department, 1978.
23. **The White House.** *The National Strategy to Secure Cyberspace.* Washington, DC : s.n., 2003.
24. **Department of Homeland Security.** *National Preparedness Guidlines.* Washington, DC : s.n., 2007.
25. **Easyrider LAN Pro.** The Aurora Power Grid Vulnerability Including Stuxnet; A White Paper. *The "No Network is 100% Secure" Series.* [Online] 2011. [Cited: November 5, 2011.] http://unix.nocdesigns.com/aurora_white_paper.htm.
26. **Shea, Dana A.** *Critical Infrastructure: Control Systems and the Terrorist Threat.* Washington, DC : Congressional Research Service, 2004. RL31534.
27. **North American Electric Reliability Corporation.** *High-Impact, Low-Frequency Risk to the North American Bulk Power System.* 2010.
28. **Kerr, Paul K., Rollins, John and Theohary, Catherine A.** *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.* Washington, DC : Congressional Research Service, 2010. R41524.
29. **The White House.** *Executive Order 13228 Establishing the Office of Homeland Security and the Homeland Security Council.* Washington, DC : s.n., 2001.
30. **Office of Homeland Security.** *National Strategy for Homeland Security.* Washington, DC : s.n., 2002.
31. **Best, Richard A.** *The National Security Council: An Organizational Assessment.* Washington, DC : Congressional Research Service, 2011. RL30840.
32. **Dale, Catherine.** *National Security Strategy: Legislative Mandates, Execution to Date, and Considerations for Congress.* Washington, DC : Congressional Research Service, 2008. RL34505.
33. **Office of Homeland Security.** *National Strategy for Homeland Security.* Washington, DC : s.n., 2002.
34. **Yim, Randall A.** *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism.* Washington, DC : US General Accounting Office, 2004. GAO-04-408T.
35. **107th United States Congress.** Homeland Security Act. *Public Law 107-296.* Washington, DC : s.n., 2002.
36. **Department of Homeland Security.** History: Who Became Part of the Department? *Department of Homeland Security.* [Online] [Cited: April 7, 2005.] http://wwww.dhs.gov/dhspublic/display?theme=59&content=4081&print=true.
37. **The White House.** *The Department of Homeland Security.* Washington, DC : s.n., 2002.
38. **Homeland Security Council.** *National Strategy for Homeland Security.* Washington, DC : s.n., 2007.
39. **The White House.** *The Federal Response to Hurricane Katrina: Lessons Learned.* Washington, DC : s.n., 2006.
40. **US House of Representatives.** *A Failure of Initiative: Final Report of the Select Bipartisan Committeee to Investigate the Preparation for and Response to Hurricane Katrina.* Washington, DC : s.n., 2006.
41. **Department of Homeland Security.** *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland.* Washington, DC : s.n., 2010.
42. **Reese, Shawn.** *Homeland Security Grants: Evolution of Program Guidance and Grant Allocation Methods.* Washington, DC : Congressional Research Service, 2006. RL33583.

43. **Hsu, Spencer S.** Obama Combines Security Councils, Adds Offices for Computer and Pandemic Threats. *The Washington Post.* [Online] May 27, 2009. [Cited: November 11, 2011.] http://www.washingtonpost.com/wp-dyn/content/article/2009/05/26/AR2009052603148.html.
44. **The White House.** *National Security Strategy.* Washington, DC : s.n., 2010.
45. **Office of Management and Budget.** *Historical Tables: Budget of the US Government for Fiscal Year 2011.* Washington, DC : US Government Printing Office, 2010. ISBN 978-0-16-084797-4.
46. **Yarger, Harry R.** *Strategic Theory for the 21st Centry: The Little Book o Big Strategy.* s.l. : US Army Strategic Studies Institute, 2006. ISBN 1-58487-233-0.
47. *Is Anybody Still a Realist?* **Legro, Jeffrey W. and Moravcsik, Andrew.** 2, Boston : International Security, 1999, Vol. 24.
48. *Game Theory, Political Economy, and the Evolving Study of War and Peace.* **de Mesquita, Bruce B.** 4, s.l. : American Political science Review, 2006, Vol. 100.
49. *Military Deterrence of International Terrorism: An Evaluation of Operation El Dorado Canyon.* **Prunckun, Henry W.** 1997, Adelaide, South Australia : Studies in Conflict & Terrorism, 1997, Vol. 20. 1057-610X/97.
50. **Brynjar, Lia and Skjølberg, Katja.** *Why Terrorism Occurs - A Survey of Theories and Hypotheses on the Causes of Terrorism.* Kjeller, Norway : Forsvarets Forsknings Institute, Norwgian Defense Research Establishment, 2000. FFISYS/776/161.1.
51. **Borum, Randy.** *Psychology of Terrorism.* Tampa, FL : University of South Florida, 2004.
52. **Woo, Gordon.** Terrorism Risk. [book auth.] John Wiley. *Wiley Handbook of Science and Technology for Homeland Security.* s.l. : Wiley Online Library, 2008.
53. **Kardes, E.** *Robust Stochasitc Games and Applications to Counter-Terrroism Strategies.* Los Angeles, CA : University of Southern California Center for Risk and Economic Analysis of Terrorism Events, 2005. FEMA Grant N00014-05-0630.
54. *Terrroism and Game Theory.* **Sandler, Todd and Arce, Daniel G.** September, s.l. : Simulation & Gaming, 2003, Vol. 34.
55. **Turocy, Theodore L. and von Stengel, Bernhard.** *Game Theory.* London, England : Computational, Discrete and Applicable Mathematics, 2001. LSE-CDAM-2001-09.
56. **Ross, Don.** Game Theory. *Stanford Encyclopedia of Philosophy.* [Online] May 5, 2010. [Cited: August 1, 2011.] http://plato.stanford.edu/entries/game-theory/.
57. *Mathematical Models and The Experimental Analysis of Behavior.* **Mazur, James E.** 2, s.l. : Journal of the Experimental Analysis of Behavior, 2006, Vol. 85.
58. *Games and Terrorism.* **Sandler, Todd and Siqueira, Kevin.** May, Dallas, TX : Simulation & Gaming Online, 2008. 10.1177/1046878108314772.
59. *The Systemic Theory of Living Systems and Relevance to CAM.* **Rangel, José A.** Caracas, Venezuela : eCAM, 2005, Vol. 2. doi:10.1093/ecam/neh068.
60. **Goodwin, Jean.** Chapter Eight: Deinails and burden of proof. *Iowa State University: Speech Communication 324.* [Online] January 8, 2006. [Cited: October 15, 2011.] http://www.public.iastate.edu/~goodwin/spcom324/eight.pdf.
61. **Cleveland State University.** Theories of Accicent Causation. *Accident Theories.* [Online] 2009. [Cited: October 16, 2011.] http://academic.csuohio.edu/duffy_s/.

62. **Monke, Jim.** *Agroterrorism: Threats and Preparedness.* Washington, DC : Congressional Research Service, 2007. RL32521.
63. **Campbell, Richard J.** *The Smart Grid and Cybersecurity - Regulatory Policy and Issues.* Washington, DC : Congressional Research Service, 2011. R41886.
64. **Jackson, William D.** *Homeland Security: Banking and Financial Infrastructure Continuity.* Washington, DC : Congressional Research Service, 2003. RL31873.
65. **Copeland, Claudia.** *Terrorism and Security Issues Facing the Water Infrastructure Sector.* Washington, DC : Congressional Research Service, 2010. RL32189.
66. **Schierow, Linda-Jo.** *Chemical Plant Security.* Washington, DC : Congressional Research Service, 2004. RL31530.
67. **Holt, Mark and Andrews, Anthony.** *Nuclear Power Plants: Vulnerability to Terrorist Attack.* Washington, DC : Congressional Research Service, 2007. RS21131.
68. **Rollins, John.** *Terrorist Use of the Internet: Information Operations in Cyberspace.* Washington, DC : Congressional Research Service, 2011. R41674.
69. **Peterman, David R.** *Transportation Security: Issues for the 109th Congress.* Washington, DC : Congressional Research Service, 2006. IB10135.
70. **Medalia, Jonathan.** *"Dirty Bombs": Technical Background, Attack Prevention and Response, Issues for Congress.* Washington, DC : Congressional Research Service, 2011. R41890.
71. **Campbell, richard J.** *Fukushima Nuclear Crisis.* Washington, DC : Congressional Research Service, 2011. R41694.
72. **The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction.** *V. Forging America's New Normalcy: Securing Our Homeland, Preserving Our Liberty.* Arlington, VA : The RAND Corporaton, 2003.
73. **Relyea, Harold C.** *Presidential Directives: Background and Overview.* s.l. : Congressional Research Service, 2008. 98-611.
74. **Redhead, Stephen C. and Vogt, Donna U.** *Public Health Security and Bioterrorism Preparedness and Response Act (P.L. 107-88): Provisions and Changes to Preexisting Law.* Washington, DC : Congreassional Research Service, 2002. RL31263.