1. Topic: C2 Decision Making & Cognitive Analysis

2. Title : Effects Based Operations for Transnational Terrorist Organizations: Assessing Alternative Courses of Action to Mitigate Terrorist Threats

3. Authors: **Larry K. Wentz and Lee W. Wagenhals**

4. Organization: C3I Center, George Mason University

5. Address: System Architectures Laboratory
C3I Center, MSN 4B5
George Mason University
Fairfax, VA 22030-4444

Larry Wentz
703-993-1725 (v)
703-993-1706 (f)
lwentz@bellatlantic.net

Lee W. Wagenhals
703-993-1712 (v)
703-993-1706 (f)
lwagenha@gmu.edu

6. POC: Larry K. Wentz

Effects Based Operations for Transnational Terrorist Organizations: Assessing Alternative Courses of Action to Mitigate Terrorist Threats

Larry K. Wentz, Lee W. Wagenhals
<lwentz><lwagenha>@gmu.edu
C3I Center, George Mason University
Fairfax, Virginia 2203-4444

Abstract

A terrorist network can be described in terms of its operational and system architectures but the mapping between these architectures is less well known and understood since the operational architecture can be mapped into numerous system architectures that are flexible and reconfigurable and contain target sets that are both hard and soft targets such as political, religious, social and economic networks. Traditional attrition-based warfare focuses on destroying the hard targets of the system architecture of the adversary but terrorists are very much unlike the military forces modeled in force-on-force type engagements and hence, to suppress, if not destroy, transnational terrorism it will be necessary to attack and destroy not their system architecture but their operational architecture–their ability to conduct operational activities in support of their goals.

The concept of effects based operations lends itself well to modeling and assessing approaches to destroying, degrading or disrupting terrorist acts. The George Mason University effects-based course of action planning and assessment research tool, called CAESAR II/EB, has been used to construct influence nets and courses of action to mitigate terrorist attacks.[1] Some findings from this exploratory research are presented in this paper. This is work in progress and much remains to be done.

Introduction

Transnational terrorism is a multidimensional problem for which motivation is a key enabler. Terrorists are inspired by many different motives, some rational but most not, and they have goals. Some terrorists are rational thinkers and they carefully assess whether they can induce enough anxiety to attain their goal without causing a backlash that will destroy the cause and the terrorist themselves. Others may be motivated for psychological reasons that are derived from personal dissatisfaction with their life or accomplishments. Culture is another key motivator and in this regard, there is a tendency for western societies to reject, as unbelievable, things such as vendettas, martyrdom and self-destructive group behavior. Terrorism thrives in a sea of perceived injustice and religion is probably the most volatile of culture identifiers.

---

[1] This work was supported by the Office of Naval Research under grant No. N00014-03-1-0033

Security is another important consideration that influences terrorist organizational arrangements (cellular structures seem to dominate) and recruitment and training (tend to be extremely security-sensitive activities). There is a strong incentive by the members of the networks to keep their structure and operations secret and unobservable. As a result, intelligence operations against these organizations and their leaders, members and supporters are extremely complex and difficult. Terrorist communications are multidimensional and include means such as email, Internet web sites, commercial telecommunications, cellular, courier, radio/TV and other covert or non-traditional means. They use the mass media to generate fear and panic in a free-minded public and also exploit the global media and information highways to carry news of their violence along with propaganda of the deeds. On the other hand, media coverage of terrorism by the free world can be used to educate the public, temper public anxiety, and influence actions to prevent and counter terrorist actions.

Transnational terrorist networks are hard to define in terms of geographical boundaries or through their physical assets. What characterizes these networks is not so much their system architecture but their operational architecture. Inactive nodes can come to life temporarily to carry out an operation at some location and then may go inactive again or self-destruct. Or, in some cases, a system node may augment itself with additional physical assets to carry out an operation and then discard these assets or disengage from them. At the operational level, the relationships that tie the network together, the interconnections, can be a set of beliefs, a financial infrastructure and a communications infrastructure. It is, therefore, dangerous to see them only as madmen bent on destruction.

The terrorist are very much unlike the military forces modeled in force-on-force type engagements where traditional attrition-based warfare focuses on destroying the system architecture of the adversary and the relationship (mapping) between the operational and system architecture is well known and well understood. The terrorists deliberately avoid engaging enemy military forces in combat and do not function in the open as armed units. For the terrorist network, the operational architecture maps into numerous system architectures. Therefore, an important objective in suppressing, if not destroying, transnational terrorism is to attack and destroy not their system architecture but their operational architecture—the ability to conduct operational activities in support of their goals.

For military opponents, a well defined mapping between the operational and system architecture leads directly to concepts such as physical Centers of Gravity, prioritized target lists and the like. But, when the adversary is characterized primarily by an operational architecture that maps into many system architectures or to flexible system architectures that can be easily reconfigured, there is a need to change the way they are analyzed and modeled. The concept of effects based operations is well suited to addressing this problem. Instead of focusing on the servicing of a well-defined a priori target list, the focus is on the effects to be achieved. The target list still exists and includes both hard and soft targets: from weapons systems, to C2 nodes, to leadership nodes, to infrastructure nodes, to political, social, and economic nodes, to the contents of communications, information, and databases. But, the target list is only an intermediate construct, a means to an end that can change rapidly as effects on the adversary are achieved or not. Indeed, the list of possible actions to be used against the adversary

centers of gravity (political, military, economic, social, information, and infrastructure) includes all instruments of national (or coalition) power: diplomatic, information, military, and economic. The availability of all instruments gives added flexibility in trying to achieve the desired effects and to avoid undesirable ones. But, it also makes the Course of Action (COA) problem and the subsequent planning problem much harder. There are now many alternatives, many choices. The choice of a set of actions, their sequencing, and their time phasing become problems in their own right.

Hence, effects based operations for transnational terrorism threat mitigation requires not only a deep understanding of the terrorist motivation, methods, organization and other factors but also needs an understanding of the friendly capabilities and infrastructure and likely vulnerabilities that might be of interest to terrorist. Additional work needs to be done to develop a more informed understanding of the appropriate relationships of motivators, organization dynamics and capabilities of terrorists and courses of action. There are a number of tools that address pieces of the problem but the current suite of tools available in the community do not fully address an integrated approach to counter terrorism course of action planning and assessment.

During the George Mason University (GMU) support to the Joint Forces Command-sponsored Millennium Challenge 2002 experiment,[2] an attempt was made to use the GMU effects-based course of action planning and assessment research tool, called CAESAR II/EB, to construct an influence net for developing and assessing courses of action to deter a terrorist attack within the region of blue force operation for the experiment. The results of this effort were used in support of follow-on GMU research into developing influence networks to examine courses of action that might be considered to deter an act of terrorism.[3] Findings from literature searches and other research activities have been used as an integral part of the research effort presented herein. Documents on the *Terrorism Research Center* Internet web site (www.terrorism.com) and RAND publications by Bruce Hoffman and Brian Jenkins were particularly helpful as were the numerous other documents listed in the References. These information sources were used extensively to develop the terrorism insights needed to build the case study model presented herein. Based on principles set forth in the US "*National Strategy for Combating Terrorism*," alternative high-level courses of action that brought to bear elements of national power were developed and assessed using the case study model. This paper explores some of the challenges of developing and assessing EBO courses of action to mitigate terrorist threats and provides an example of a counter terrorism influence net and some findings from an assessment of COAs aimed to prevent terrorist actions. This is work in progress and much remains to be done.

CAESAR II/EB, The Tool

The CAESAR II/EB tool was originally designed to support the analysis of an adversary's actions and reactions to Blue's activities so that COA options could be evaluated in a rigorous manner. It was inspired by the need to support the development of Information Operations (IO) influence planning and its integration with traditional

---

[2] This work was supported by the Air Force Office of Scientific Research under grant No. F49620-02-1-0332
[3] This work was supported by the Office of Naval Research under grant No. N00014-03-1-0033

military operations. The tool incorporates influence nets as a probabilistic modeling technique and a discrete event system modeling technique, Colored Petri Nets (CP net), to support the temporal aspects of COA evaluation. These two techniques enable the modeler to create the structure of actions, effects, beliefs and decisions and the influencing relationships between them. The strength of the influencing relationships is also captured. The influence net provides a static equilibrium probabilistic model that indicates the probability of effects given sets of actions. A mapping has been established and an algorithm has been encoded for automatically converting the influence net to a CP net. After an influence net is converted to a CP Net, temporal analysis can be conducted that provides the probability of effects over time given a timed sequence of actions. This tool was designed to develop and assess COAs at the operational and strategic level.

The influence net provides an environment for modeling of the causal and influencing relationships between actions by our forces (Blue) and effects on the adversary (Red). It uses a graphical representation comprised of nodes that represent actions or effects and causal or influencing relationships between the nodes. In addition to the network structure of the model, estimates of the "strength" of the causal and influencing relationships is added and enables an underlying probabilistic model base on Bayesian mathematics to be used for analysis. The construct shown in Figure 1 is used. Starting from the set of desired and undesirable effects that reflect the goals of the mission, analysts work backwards to relate the effects to actions that are under our control. Once the Influence net has been completed, it can be used to evaluate the impact of actions on the effects (decisions) of interest using its underlying Bayesian mathematics.

Once the analysis of the Influence net has been completed and the actionable events for the COA have been selected, planners assess the availability of resources to carry out the tasks that will result in the occurrence of the actionable events. The resultant plan will indicate when each actionable event will occur. Clearly, it is not only the selection of the set of actions that will lead to achieving the overall desired effects while not causing the undesired ones that is important. The timing of those actions is critical to achieving the desired outcomes.

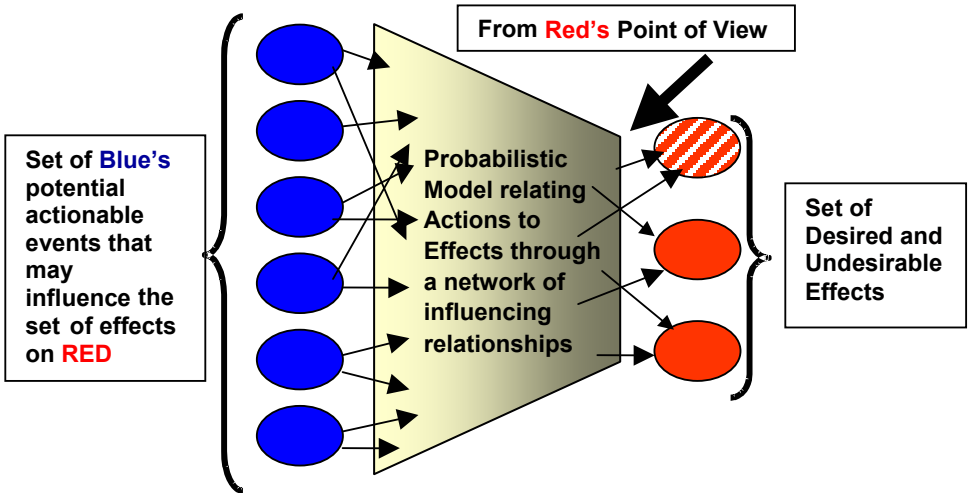

Figure 1. Modeling Actions and Effects

An algorithm has been implemented4 that converts an influence net into a

[4] Wagenhals, L. W., Shin, I., and Levis, A. H. (1998). "Creating Executable Models of Influence Nets with Coloured Petri Nets," *Int. J. STTT,* Springer-Verlag, Vol. 1998, No. 2, pp. 168-181.

discrete event dynamical system model. The particular mathematical model used is that of CP Nets and their software implementation in Design/CPN 5. The nodes in the Influence net become transitions in the CP Net and the places hold tokens that carry the marginal probabilities. Since the Influence net does not contain temporal information, it must be provided as an input to the CP Net.

Figure 2 shows the combination of models and results produced by the CAESAR II/EB tool. An Influence net model for a given situation is shown in the upper left of Figure 2. Each node represents an action, event, belief, or decision. A declarative sentence in the form of a proposition is used to express the meaning of each node. The directed arcs between two nodes mean that there is an influencing or causal relation between those nodes. The truth or falsity of the parent node can affect the truth or falsity of the child node. The Influence net has been arranged with potential Blue actions on the left and the key Red decisions on the right. This is to indicate visually that the effects of the actions are expected to propagate to intermediate effects over time until their impact reaches the key decisions. This captures the cascading and accumulation of effects. There are six actionable events on the left side of the Influence net. These are candidate actions (or results of actions) that can comprise a COA that can impact the three Red decisions of interest.

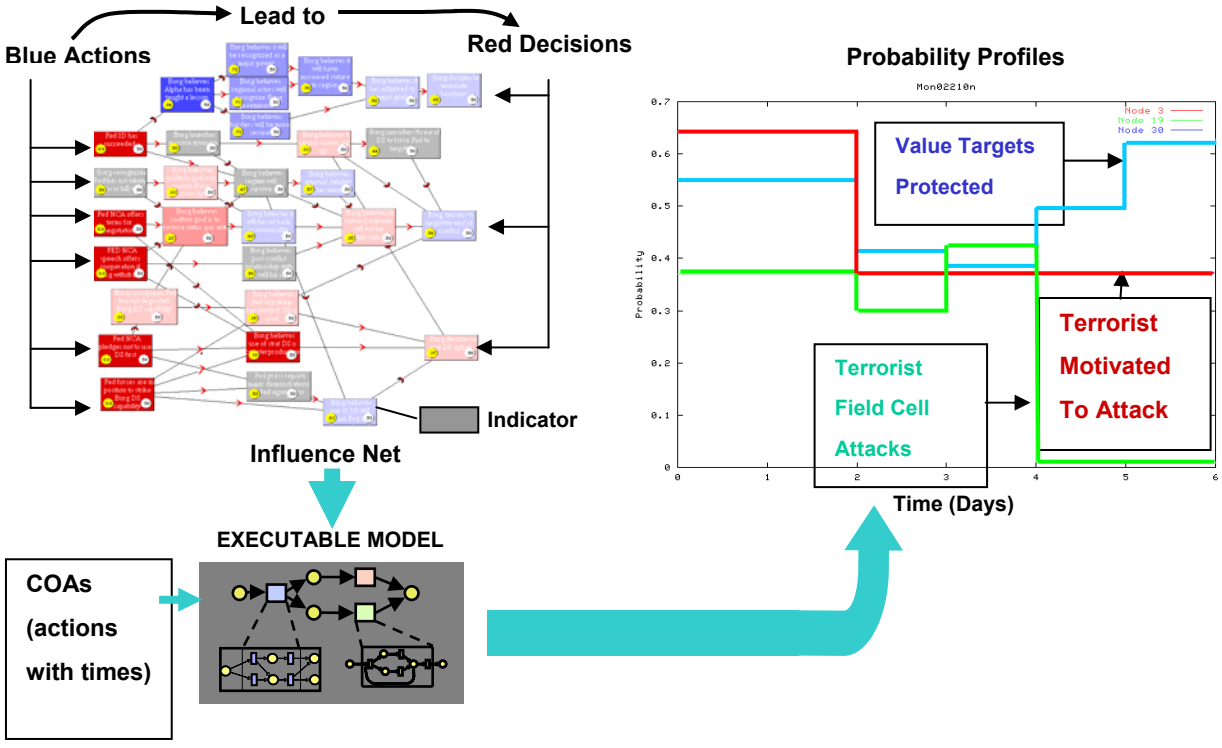

Figure 2. CAEAR II/EB Products

[5] Jensen K. (1997). *Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use. Volumes 1, 2, and 3. Basic Concepts*. Monographs in Theoretical Computer Science, Springer-Verlag, Berlin, Germany.

Once the analysis of the Influence net has been completed and the actionable events for the COA have been selected, the Influence net is automatically converted to an executable model (CP net) so that a temporal analysis of the COA can be performed. Using the executable model, the analyst is able to generate the probability profiles that show the marginal probability for any node in the net as a function of time. These profiles can indicate how long it will take for the effects of the actionable events to affect various nodes in the Influence net. The analyst will most likely concentrate on the probability profiles of the key decision nodes, the nodes with no children. The probability profiles shown in Figure 2 were generated for the COA proposed by the planners. The annotations have been added to indicate the three separate probability profiles. Different timing of the actions can alter the probability profiles. As a result, some will be more desirable than others while others may be unacceptable, so the planners will try to adjust the scheduling of actions.

Terrorism Definitions

There are numerous definitions for terrorism. The *U.S. National Security Strategy* defines terrorism as simply "premeditated, politically motivated violence against innocents." U.S. government organizations and the UN define terrorism slightly differently.[6] For example:

> **U.S. Department of Defense**: The calculated use of violence or the threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.
>
> **U.S. Department of State**: Premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience.
>
> **U.S. Federal Bureau of Investigation**: The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
>
> **United Nations**: A unique form of crime. Terrorist acts often contain elements of warfare, politics and propaganda. For security reasons and due to the lack of popular support, terrorist organizations are usually small, making detection and infiltration difficult. Although the goals of terrorism are sometimes shared by wider constituencies, their methods are generally abhorred.

The challenge of grasping the nature and parameters of the war on terrorism is certainly not eased by the absence of a commonly accepted definition or by its depiction as a Manichaean struggle between good and evil, "us" versus "them."[7] Consensus on the definition of terrorism is not necessary to conduct counter terrorism operations against specific terrorist organizations but a lack of consensus can impede the study of the phenomenon itself.

---

[6] "*The Terrorist Recognition Handbook*" by Malcolm Nance (2003)

[7] Record, Jeffrey (2003). "Bounding the Global War on Terrorism," Army War College, Strategic Studies Institute.

Counter terrorism is not war in the traditional sense of military operations between states or between a state and an insurgent enemy for ultimate control of that state. Terrorist organizations do not field military forces as such and are trans-state organizations that are pursuing non-territorial ends. As such, and given their secretive, cellular, dispersed, and decentralized "order of battle," they are not subject to conventional military destruction.

Based on findings from the research of literature on terrorism, what terrorism is and is not can be summarized as follows:

•**Terrorism is:**

–Calculated use of covert criminal violence or threat of violence
–Deliberately selected as a tactic to effect change
–Targeting of innocent people, including military personnel
–The use of symbolic acts to attract media and reach a large audience
–Illegitimate combat, even in war
–Never justified

•**Terrorism is not:**

–Common crimes
–Conducting acts legal under national and international law
–Civil disturbances or spontaneous rioting
–Freedom of speech or nonviolent civil disobedience
–Protests and assembly to present opposing views and express dissent

The following terms are used by U.S. organizations such as the Defense Department, Intelligence Agencies and the Law Enforcement community to describe classes of measures taken to address terrorist acts.

Antiterrorism: Defensive and preventive measures taken to reduce vulnerability to terrorist attacks.

Counter-terrorism: Offensive measures taken in response to a terrorist attack, after it occurs.

Combating terrorism: The U.S. government program against terrorism that includes antiterrorism, counter-terrorism, and all other aspects of tracking, defense, and response to terrorism throughout the threat spectrum.

Force Protection: The U.S. DOD program for the defense of military and government assets from terrorist and unconventional warfare attack—detect, deter, and defend.

Terrorist Considerations

Numerous reports from the *Terrorism Research Center* Internet web site and books and articles published on the subject of terrorism were used to develop the insights presented herein. Of particular value were the following:

- Terrorism Research Center Internet web site
    - The Basics: Combating Terrorism, an essay from the U.S. Army Field Manual 100-20, Stability and Support Operations
    - Terrorist Intelligence Operations, reprint from the Interagency OPSEC Support Staff, Intelligence Threat handbook

- Microsoft Encarta Online Encyclopedia 2003
    - Terrorism by Bruce Hoffman
- RAND
    - "Countering al Qaeda" by Brian Jenkins
    - "Countering the New Terrorism" by Ian Lesser and et al
    - "Deterrence and Influence in Counter Terrorism" by Paul Davis and Brian Jenkins
- Books
    - "Inside al Qaeda" by Rohan Gunaratna
    - "Inside Terrorism" by Bruce Hoffman
    - "Terrorism, War and the Press" by Nancy Palmer
    - "The Terrorist Recognition Handbook" by Malcolm Nance
    - "Framing Terrorism" by Norris Pippa and et al

Terrorists prefer simple strategies that appear sophisticated but are simple in planning and execution. They seek dramatic and wide publication by media to transmit fear and publicize their cause. Their apparent lack of logic enhances the terror in terrorism. Terrorist acts are seemingly random and they feel their goal will be reached by conducting enough attacks. They achieve their most dramatic impact through the use of speed, surprise and violence of attack. The terrorist only needs to get lucky once but the antiterrorist forces need to be lucky all of the time.

The goals of the terrorist organizations focus on recognition, coercion, extortion, intimidation, provocation, and insurgency support for their cause. Their objectives are to create a climate of fear in a targeted group or nation through a sustained campaign of violence and to destroy the social and political order by attacking and destroying commerce, property and infrastructure. They seek revenge for previous incidents or situations affecting terrorist organizations or its causes and try to negatively affect processes that the terrorist organization sees as against its interests**.** Attempts are made to eliminate specific individuals or groups and to demonstrate the weakness of legitimate governments. Terrorist organizations try to ensure governments overreact and oppress their own people. They continuously try to gain new recruits, money or weapons. Some terrorist organizations attack just to achieve the satisfaction of harming their enemy. Attacks also serve to demonstrate that the terrorist group is still active.

Terrorist groups can be indigenous or transnational. They can be state-sponsored, state-directed or have no state relationship. Those organizations that are state-sponsored tend to operate independently but receive support such as weapons, training, money, and safe-havens. Those that are state-directed, act as agents of the state and receive intelligence,

logistics and operational support. The groups not sponsored act autonomously and receive no significant support.

Motivation is a major consideration in terrorist organizations. Some are rational and think through goals and objectives, conduct course of action planning and assessments and risk and cost benefit analysis. They are careful when inducing anxiety to achieve their goals to attempt to ensure that it does not cause a backlash that may destroy them or their cause. Others are psychologically motivated and are dissatisfied with life and accomplishments and crave violence to relieve anger. They tend to need to belong to a group and require group acceptance, demand unanimity, are intolerant of dissent, and have a polarized "we versus them" outlook. Culture is another key motivator. Western cultures are reluctant to appreciate the intense effect of culture on behavior. In their view irrational behavior as a means to achieve objectives is counter culture. They believe rational behavior guides human actions and reject the notions of vendettas, martyrdom, self-destructive group behavior, and dissolution of a viable state for ethnic purity. For the terrorists, fear of cultural extermination leads to violence — the perception that "outsiders" are against them. Religion can be the most volatile of cultural identifiers — the belief in moral certainty and divine sanctions.

Security is a primary concern of terrorist organizations. Although cell operations are the least understood part of terrorism, it is believe terrorist organizations are best served by cellular structures that operate in secret as small team. This way, members do not know and cannot identify more than a few the other members. They can operate as a group on orders of a commander or independently. Defections are rare and it's difficult to penetrate cells. Fundamental units such as Command and Control, Tactical Operations, Intelligence, and Logistics are employed. A highly trusted and experienced leader generally runs the Intelligence cell and members of this cell rarely participate in attacks — there is a need to protect identity of members. Terrorists tend to organize to function in the environment where they plan to carry out their attacks — this is situation specific. Numerous means are used to communicate. Direct means such as face-to-face, Internet, cell phones and telephones can be used. Indirect means such as courier, trusted agent, Internet, cell phones, telephones, mail, dead drops, newspapers, books, and Radio/Television are used as well. Charismatic leaders are needed to unite the effort otherwise behavior is a reflection of the group dynamics. The support structure is a mix of state-sponsors and sympathizers. The recruitment process is highly security-sensitive. Training of the terrorist organizations can vary from military style at sophisticated facilities to inspirational talks before activation — motivating "throw away" operatives.

Terrorist potential targets generally fall into hard targets that are security conscious and difficult to attack successfully and soft targets that are people, structures, or locations that have less security and are open to public. Target selection is based on motive (ultimate goal/objective), opportunity (feasibility) and means (covert capabilities). The targets they choose can be categorized as follows:[8]

---

[8] Nance, Malcolm (2003). "The Terrorist Recognition Handbook," The Lyons Press, Gilford, Connecticut.

•**Strategic value:** Long-term impact target sets that include executive leadership, strategic reserves, cities, and national command centers.

•**High payoff:** Immediate impact target sets such as energy and economic centers.

•**High value:** Contribute to degradation of societies ability to respond militarily or sustain itself economically. Targets include military, law enforcement and emergency response centers, Federal Government centers and critical commerce personalities.

•**Low value:** Contribute to localized fear and harassment of society and target sets include local transportation and non-critical infrastructure.

•**Tactical value:** Degrade local law enforcement capabilities to respond and includes target sets such as individual or small numbers of military or police, low level civil, military and law enforcement leadership personnel and centers, and military bases and equipment.

•**Symbolic value:** Heighten public fear and targets include innocent people, national treasures and landmarks, prominent public structures, and national representatives or diplomats.

•**Ecological value:** Damage natural resources of a society such as large bodies of natural resources and wide areas of agricultural resources and industry.

The terrorist target selection will likely be driven by the ultimate goal of its leadership, the feasibility of achieving success based on reports from the intelligence cells, and the ability to covertly deploy necessary cells to carry out the act.

Terrorist attack profiles are driven by the time to develop and execute a plan and they can use hard entry where they go in loud immediately with assaults using a range of weapons or use a soft (stealth) entry where penetration is not known until the attack occurs. They employ strategies that include misdirection (feints), deception (mask who or intent), and large numbers of identical incidents over a period of time. Planning and execution times can range from a few hours (hasty) to weeks (normal) to months and even years (deliberate). The terrorist methods and tactics vary. They have already demonstrated the use of hijackings, kidnappings, bombings, surface-to-air missiles, man portable air defense systems, arson, assassinations, armed assaults, and barricade-hostage incidents to attack critical infrastructure or capabilities, popular or high profile individuals, or important facilities or symbols. Weapons of mass effects (e.g., human suicide/martyr bombers, truck/car bombs, aviation attacks, maritime attacks, psychological, agriculture, ecological, economic, cyber) have been used as well and there is concern that they may in the future use weapons of mass destruction (e.g., chemical, biological, nuclear).

Initiation, escalation, de-escalation and termination of terrorist actions are determined by the leadership intent, the group capabilities (resources and expertise) and opportunities presented for attack. Terrorists have attacked both strategic and tactical targets worldwide — the intent is to make their presence felt. Western governments security services have been reticent about sharing intelligence and judicial authorities rarely entertain request

for extradition that adds to the difficulties of fighting the war on terrorism. Another important factor is the global media who are largely unaccountable to society and provide an unsophisticated form of terrorist Intelligence Surveillance and Reconnaissance, e.g., through transmission of live images of terrorism related events and by talking head analysis and special coverage assessments. Terrorist use symbolic acts to attract media and reach a large audience. They exploit the media to gain public attention, publicize their cause, and influence and spread fear. The media often make the mistake of seeking deeper goals in a terrorist operation than the terrorist set for them. This makes the terrorist appear powerful and untouchable. Media actions can also contribute to amplifying fear—a terrorist objective.

U.S. National Strategies

Following the terrorist attacks of September 11, 2001, the Bush administration developed and published seven national strategies that relate, in part or in whole, to combating terrorism and homeland security. These were:

- The *National Security Strategy of the United States of America*, September 2002.
- The *National Strategy for Homeland Security*, July 2002.
- The *National Strategy for Combating Terrorism*, February 2003.
- The *National Strategy to Combat Weapons of Mass Destruction*, December 2002.
- The *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February 2003.
- The *National Strategy to Secure Cyberspace*, February 2003.
- The *2002 National Money Laundering Strategy*, July 2002.

The *U.S. National Strategy for Combating Terrorism* is mainly offensive oriented but does include defensive homeland security objectives as well as objectives for protecting U.S. citizens abroad.[9] The principles of this strategy were used as a guide in the development of the case study counter terrorism influence net, scenarios and courses of action assessments discussed herein. The intent of the national strategy is to prevent, spoil actions, deter, and respond; neutralize or destroy terrorist groups; prevent attacks and minimize effects should one occur; weaken terrorist organizations and their political power; and make potential targets more difficult to attack. The goals and objectives of the 4D strategy (Defeat, Deny, Diminish and Defend) include:

Defeat terrorists and their organizations

- •Attack sanctuaries, leadership, C3, logistics, and finances
- •Disrupt ability to plan and operate
- •Disperse and isolate terrorist
- •Coordinate and use regional partners to neutralize terrorists

[9] GAO-04-40ST. "Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism," February 2004.

Deny further sponsorship, support and sanctuaries to terrorists

- •End state sponsorship of terrorism
- •Ensure regional states accept responsibilities to take action
- •Interdict and disrupt material support for terrorist

Diminish the underlying conditions that terrorist seek to exploit

- •Enlist international community to focus on areas most at risk
- •Work with partners to keep combating terrorism
- •Win the war of ideas

Defend U.S. citizens and interest at home and abroad

- •Attain domain awareness
- •Protect the homeland and extend our defenses to insure we identify and neutralize the threat as early as possible

Success is dependent upon sustained, steadfast, and systematic application of all the elements of national power—diplomatic, economic, information, financial, law enforcement, intelligence, and military—simultaneously across all fronts.[10]

Terrorist Threat Considerations and Trends

The number of international terrorist attacks has declined but the level of violence and lethality has increased.[11] Primary sources of terrorist organizations are organized groups that have political, ethnic, and religious agendas; state sponsored organizations; transnational groups with broader goals; and Islamic terrorist groups that have become a growing threat. Al-Qaeda is gaining in global presence. These groups are loosely organized; recruit membership from many different countries; and obtain support from informal international networks.

Terrorists have employed a wide variety of tactics to attack American targets worldwide that range from violent demonstrations to kidnapping to hostage taking to murder to armed attacks to bombings. Bombings are the most common type of attack (67% of all attacks against Americans).[12] Terrorist attack American businesses most frequently (more than 89% of the attacks) since businesses tend to be less protected and soft targets. U.S. government, diplomatic and military facilities tend to be protected and harder targets and less likely to be attacked. Terrorism varies by region of the world but most attacks occur in Latin America (87%).[13]

The reduced international barriers of the post-cold war landscape provide opportunities to exploit reduce political and economic barriers and facilitate movement of people, money, information and material across international borders. The global business networks facilitate international terrorism by providing safe havens for planning operations and allowing the terrorists to take advantage of global banking,

---

[10] "National Strategy for Combating Terrorism," February 2003.
[11] GAO-03-165, "Combating Terrorism: Interagency Framework and Agency Programs to Address the Overseas Threat," May 2003.
[12] Ibid
[13] Ibid

communications, and transportation to carry out operations. Trafficking in narcotics, persons and weapons and organized crime are key sources of finance for operations.[14]

Other aggravating factors included technology advances and weak international law enforcement institutions. Information technology and communications facilitates global reach and terrorists are becoming more sophisticated in use of computer and telecommunications technology. Cell phones and Internet are used for planning, coordination, and execution. There are serious vulnerabilities in our critical infrastructure due to the reliance in information technology. The terrorists are adept at using technology for counterintelligence. Weak law enforcement institutions due to ineffective police and judicial systems in many foreign countries is a problem. Many of these institutions lack resources. There are outdated laws in many countries and some foreign governments are plagued by corruption. Law enforcement is constrained by national boundaries. Terrorists take advantage of institutional limitations and weaknesses to find and establish sanctuaries.

Recent U.S. actions seem to have resulted in a decline in state-sponsorship of terrorism. Threats of sanctions and retaliation have reduced willingness of nations to support terrorist organizations. Terrorists have become less dependent on sponsorship by sovereign states and a new phenomenon is emerging—terrorist sponsoring a state (e.g., Taliban in Afghanistan). Terrorist groups operating on their own in loosely affiliated groups is on the increase as dependency on state sponsorship decreases. The terrorist organizations recruit membership from many different countries and obtain support form an informal network of like-minded extremists. There is a shift from aircraft hijacking and hostage taking to indiscriminate terrorist attacks that yield maximum destruction, casualties, and impact. This has generated a concern that there may be a shift to unconventional weapons of mass effects or even mass destruction. Alliances with transnational crime are providing the terrorist with access to various international crime organizations to help finance their operations.

Counter Terrorism Actions

The key to defeating terrorists lies in the realms of intelligence and police work, with military forces playing an important but nonetheless supporting role. Military destruction of al-Qaeda training and planning bases in Afghanistan have been successes in the war on terrorism but good intelligence—and luck—has formed the basis of virtually every other U.S. success against al-Qaeda.[15] Intelligence-based arrests and assassinations, not military divisions destroyed or ships sunk, are the cutting edge of successful counter terrorism actions. The war on terrorism is analogous to the international war on drugs. An effective strategy for counter terrorism needs to mobilize all elements of national power as well as the services of many other countries. Hence, to suppress, if not destroy, transnational terrorism it will be necessary to attack and destroy not their system architecture but their operational architecture–their ability to conduct operational activities in support of their goals.

---

[14] Ibid

[15] Record, Jeffrey (2003). "Bounding the Global War on Terrorism," Army War College, Strategic Studies Institute.

There are numerous factors to consider as one builds a strategy for attacking the terrorist operational architecture. It is of utmost important to know your enemy in terms of motivation, his strengths and weaknesses, social networks of influence, sources of financing, logistics and other support, recruiting process, means of communicating, and organization structure and behavior. It is important to identify and locate terrorists and terrorist organizations then destroy them and their organizations. This requires an aggressive offensive strategy that aims to disrupt, dismantle, and destroy terrorist capabilities to carry out their operational activities by attacking their sanctuaries, leadership, C3I, material support, and finances.

The strategy needs to employ diplomatic, military and law enforcement means to eliminate sources of financing. As noted earlier, actions need to be taken to choke off the lifeblood of terrorist groups by employing the full range national power to end the state sponsorship of terrorism, to establish and maintain international accountability, to strengthen and sustain international effort to fight terrorism, to interdict and disrupt material support for terrorists, to eliminate terrorist sanctuaries, and eliminate conditions that terrorist can exploit.

Major threats to U.S. and world order today come from weak, collapsed, or failed states. Of concern is the fact that weak or absent government institutions in developing countries form the thread that links terrorism and weapons of mass destruction. Before 9/11, the U.S. viewed with less concern the chaos in far away places such as Afghanistan, but with the intersection of terrorism and weapons of mass destruction, these areas have become of major concern to the U.S. national security interests. Our tolerance for failed states has been reduced by the global war on terrorism and necessitates that we not leave weak and failed nations crumbling and ungoverned. Terrorists seek out such places to establish training camps, recruit new members, and tap into a black market where all kinds of weapons can be found for sale.[16] Courses of action to counter terrorism need strong consideration of ways to help rebuild and strengthen weak states and to identify and diminish conditions contributing to weak states by helping resolve poverty, deprivation, social disenfranchisement, and unresolved political and regional disputes. Partnering with the international community will be key. The strategy needs to win the war of ideas by employing actions that de-legitimize terrorism, kindle the hopes and aspirations of freedom, and support moderate and modern governments, especially in the Muslim world and in this regard assure Muslims that American values are not at odds with Islam. It will be necessary to reverse the spread of extremist ideology and to seek non-support, non-tolerance, and active opposition to terrorism from the international community. Use of effective, timely public diplomacy and government-supported media to promote the free flow of information and ideas will be needed as well.

The best defense is a good offense. This means investment of political will and resources to improve intelligence and warning and intelligence sharing among the military, law enforcement and our international partners. It will be necessary to integrate information sharing across the federal government and to effectively use intelligence, information and data across all agencies. Continuous law enforcement, intelligence and military pursuit of terrorists and their supporters will be necessary and needs to include a

---

[16] The Atlantic Monthly article "Nation Building 101" by Francis Fukuyama

coordinated and focused effort of federal, state and local government, the private sector, and the American people. We will need to mobilize and organize to secure the homeland. In this regard, protection of vital systems and infrastructure is a shared responsibility of the public and private sectors. Plans need to be developed for alerting, containing and if necessary, repelling attacks. Measures to ensure the integrity, reliability, and availability of critical physical and information-based infrastructure at home and abroad need to be enhanced.

As noted earlier, intelligence is a key element of success in counter terrorism actions. The safe house is one of the key nodes of a terrorist operation and if seized may compromise cells, plans and materials. A safe house may be detected by informants, suspicious neighbors or through surveillance. Logistic cells have a higher probably of detection because they often deal with low-level criminals and open market purchasing. Modern terrorist have become creative in the use of advanced information technology to conduct command and control of their operations making it difficult to detect activities. Terrorist can use diverse methods to finance their operations that include sources such as charitable organizations, organized crime, state sponsors, and legitimate business investments. Terrorist activity detection opportunities include:

- •Leadership behavior
- •State sponsors and other supporters
- •Political and religious influence networks
- •Safe houses
- •Supply chains
- •Logistics cells
- •Storage of supplies
- •Transportation and mobility
- •Command, control, communications and intelligence
- •Media relations and uses
- •Financing
- •Recruiting
- •Training camps

The challenge to the intelligence and law enforcement community becomes one of asset management and focus and the ability to effectively share information and leverage the resources of the military, law enforcement and international community.

A measure of success for a counter terrorism strategy will be diminished incidence and scope of terrorist attacks. However, analytically, this is an unsatisfactory measure of success since there is no way to prove a cause effect relationship. Additionally, a successful counter terrorism strategy can have self-defeating unintended consequences such as the terrorists changing their behavior and strategies that make them even harder to identify and neutralize. The GMU tool, CAESAR II/EB, may be of help to understand possible cause effect relationships of proposed courses of action and to identify potential unintended and undesired consequences. Successful results in this regard are highly depended upon the subject matter expert contributions and the creativity of the analyst constructing the influence net and the assessing the courses of action—it's an art not a science.

Counter Terrorism Case Study

The purpose of the case study was to demonstrate the utility and examine the challenges of using CAESAR II/EB to develop and assess EBO-based Courses of Action (COA) to mitigate an attack by a terrorist field cell by employing a broad-based strategic level attack profile that used both lethal and non-lethal means to disrupt and destroy the operational and systems architectures of the terrorist organization. The strategies tested employed the elements of National Power (Diplomatic, Information, Military, and Economic) to attack the terrorist organizations centers of gravity (Political, Religious, Military, Economic, Social, Infrastructure and Information). The study examined reactive, proactive, preemptive, and preventative tactics and examined the role of intelligence, the media, and the use of non-lethal means, such as, IO, Political, Legal, and International Collaboration. Homeland Security preparedness measures to defend high value targets was addressed as well.

Building the Model

Extensive research of the literature on historical experience with terrorism and strategies and frameworks for modeling counter terrorism actions was necessary in order to develop the understanding needed to create influence nets that could be used to assess counter terrorism courses of action and to examine the assessments for possible unintended consequences of actions taken against the terrorists and their organizations. Two RAND publications were of extreme value in the development of the case study influence net: the Paul Davis book titled "*Deterrence and Influence in Counter Terrorism*" and the Brian Jenkins book titled "*Countering al-Qaeda*." A *Signal Magazine* article from the December 2001 issue by Dr Roger Smith, Titan Systems Corp., titled "*Counter Terrorism Modeling and Simulation: A New Type of Decision Support Tool*" was useful as well.

There are a number of interrelated challenges in constructing a counter terrorism influence net. First, is being able to think in terms of how the individuals and organizations to be modeled and attacked perceive they can be influenced and attacked—view the situation from the terrorist perspective. Second, is identifying the actors and the types and sequence of actions that can be taken to create the desired influence and behavior change. Additionally, thinking about whether terrorists and their organizations can be deterred, destroyed, or otherwise influenced requires a decomposition of the terrorist operations and supporting systems into classes of influence to be attacked.[17] Estimating the relative degree of impact of actions and events to influence outcomes needed to be developed and this proved to be a challenge as well—open literature documentation discusses the subject in qualitative terms.

The model for the case study was done at the strategic level and addressed broad-front national level actions needed to achieve an outcome that deterred a terrorist field cell from attacking. Past experiences using CAESAR II/EB to develop models in support of

[17] Davis, Paul and Jenkins, Brian (2002). "Deterrence and Influence in Counter Terrorism," RAND.

Naval War College Global war games[18] and Joint Forces Command experiment MC02[19] demonstrated that it was difficult to model at the operational level and much more difficult at the tactical level, and therefore, this effort focused on the strategic level.

The types of influence that needs to be considered can have both a positive and negative impact on the desired effect or event and determining the appropriate balance of these influences to achieve the desired effect is a challenge. It's largely a trial and error experimentation process. For example, the higher the terrorist motivation and ability to attack, the less effective deterrence is likely to be. On the other hand, if the terrorist target of interest is well protected, the greater the deterrence. The influence net created for the case study is depicted in Figure 3 and was used to assess courses of action that reduced the probability that a terrorist field cell would attack.

The terrorist centers of gravity to be influenced and attack strategies ranged from using soft means to attack the political, social, belief, and financial structures to hard kill military means that disrupted or destroyed training facilities, logistics operations, weapons caches, and C3I capabilities needed to conduct operations. Threats to things terrorist care about, such as, loved ones, the terrorist cause itself, and the terrorist personal power and possessions are important deterrence factors and were the target of the IO campaign to influence perceptions, legal actions to seize possessions, and military and law enforcement actions to enforce messages in the IO campaign—actions need to support words. Other factors such as senior terrorist leadership support of terrorist cells and cause, continuation of state sponsorship of terrorists, continued approval by supporters of the terrorist and their cause, terrorist ability to conduct C3I of their operation, and the ability of the terrorist to finance operations are enablers and as such need to be attacked by an appropriate combination of all means available, especially the non-lethal means where and when possible. Public fear and anxiety are terrorist enablers that require careful attention and actions to keep the public informed and in this regard, both the government actions and the media messages play an important role in informing and influencing public understanding. Protection of high value targets is deterrence and this requires proactive government (federal, state and local) attention to protection policies, response plans and capabilities, and strategies and investments to protect critical infrastructure and key leadership personnel. Industry also has a role to play in investing in protection of facilities, capabilities, and key personnel. Awareness campaigns to educate and inform the public and make the terrorist aware that antiterrorism investments are being or have been made is important as well.

---

[18] Wagenhals, L. W. and Levis, A. H. (2002). "Modeling support of Effects Based Operations in War Games," 7th Command and Control Research and Development Symposium, Naval Post Graduate School, Monterey, CA, June 2002.

[19] Wentz, L. K. and Wagenhals, L.W. (2003). " Effects Based Information Operations," 8th International Command and Control Research and Technology symposium, National Defense University, Washington, D.C., June 2003.

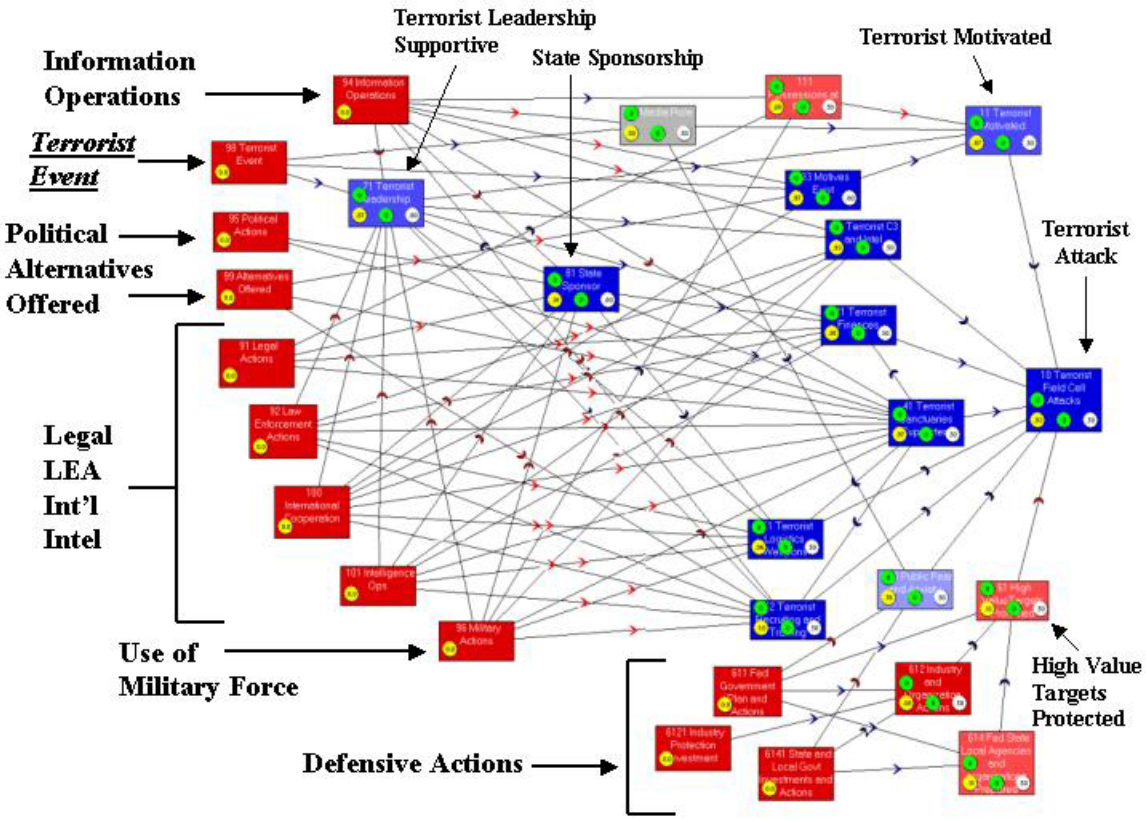

Figure 3. Counter Terrorism Influence Net

These considerations were built into the influence relationships and actions illustrated in the influence net shown in Figure 3. The desired outcome of the courses of action implemented is to drive the probability that a "terrorist field cell" will attack as low and as quickly as possible without creating unintended consequences such as windows of opportunity and vulnerabilities for the terrorist to attack. Key high level influence elements in the upper right hand quadrant of the influence net shown in Figure 3 include terrorist motivated to attack, finances available to conduct operations, recruiting and training capability providing new terrorist, the terrorist C3I capabilities able to support command and control of operations, logistics functioning and weapons available to support an attack, sanctuaries available to attack from, and continued approval of supporters such as political and religious leaders and other supporters of their cause exists. The lower right hand quadrant addresses perceptions of uncertainty and risk in terms of public fear and anxiety in response to terrorist threat warnings and terrorist belief that government and industry made the antiterrorism investments needed to protect high value targets (infrastructure—power, water, transportation—and leadership). The upper left hand quadrant includes influence elements such as state sponsorship, terrorist leadership support and media reporting of terrorist threats and terrorist perception of threats to things they care about.

The left side of the influence net and lower right quadrant of the net show the different domains of actionable events. There are hard kill actions aimed at destroying terrorist targets that are largely military actions but law enforcement plays a role as well. The Intelligence action is the means to identify and monitor targets of opportunity, to develop social network understanding, to assess terrorist C2 tactics, procedures, and capabilities, and to develop situation awareness and actionable intelligence and warning. International cooperation is an enforcement enabler to provide an integrated global reach to leverage the use of other nations to help attack terrorist elements in their geographic area, to collect and share intelligence on terrorists, and to influence state sponsors and other supporters of terrorism to stop. Legal and law enforcement actions use international and national laws, law enforcement and judicial systems to disrupt terrorist organizations by arresting leadership and other members, disrupting terrorist recruiting activities, dismantling training camps, preventing cross border operations such as weapons trafficking and movement of terrorists, and dismantling of the terrorist financial networks. The political actions aim to gain international support to impose sanctions and to influence state sponsors and nations providing sanctuaries and other support to terrorist organizations and operations. The Information Operations actions focus on perception management of regional and local political and religious leaders, influencing the beliefs of the terrorist leaders, state sponsors, and members of the terrorist organizations and their supporters, and disruption of the recruiting of terrorists. An action referred to as "Alternatives Offered" aims to provide hope and improvements in quality of life of those suffering from poverty, deprivation and suppression of human rights who in turn support the terrorist cause and are a source of terrorist recruits. The provision of hope and improved the quality of life could serve to influence a large number of these people to quit supporting the terrorists and their cause. The lower right quadrant addresses federal, state and local government and industry actions (policies, contingency response plans, command, control and intelligence capabilities, and investments in infrastructure and key personnel protection) needed to implement antiterrorism measures to secure and protect high value targets and to be able to more effectively respond to indications of possible terrorist attacks.

The upper left hand quadrant has an action titled "terrorist event" and this was used as an intelligence and warning (I&W) indicator that a major terrorist attack was about to happen. Activation of this action served two purposes. First, its activation was used to positively influence the terrorist leadership support and motivation of the members of terrorist organizations and to influence the media response to generate radio and television public awareness messages and "talking head" discussions of the possibility and implications of an attack. The media response in turn had an additional positive influence on the motivation of the terrorists and in publicizing their cause. It also had a negative influence that contributed to the generation of public fear and anxiety.

A scenario-based approach was used to assess various courses of action so the second use of I&W actions was a trigger to initiate various courses of action strategies to be tested—reactive, proactive, preemptive, and preventative. In this role, the I&W action was used in two modes, the action could be turned on for the entire assessment timeframe or it could be turned on and off several times over the assessment timeframe to simulate multiple occurrences of threat warnings coming and going. The former mode was used to assess the impact of individual and various combinations of actions in response to the

threat of a terrorist attack. The latter mode was used to assess the relative effectiveness of implementing course of action strategies that reacted to multiple warnings of terrorist attacks.

Sample COA Assessments

A number of assessments of the relative impact of individual and multiple actionable events on reducing the probability of attack and the sequencing and timing of these events were conducted as part of the research. Several different scenarios were also postulated based on the *U.S. National Strategy for Combating Terrorism* and used to formulate courses of action tested and assessed. Two examples of scenario-based courses of action assessments follow to illustrate the use of the tool and types of analysis conducted. The first example examines a strategy that reacts to multiple terrorist threat warnings and the second is a preemptive strategy in response to an initial threat warning and aims to minimize the probability of an attack as quick as possible given there will be a subsequent indication that an attack might occur. The two examples used different scenarios and sequencing and timing of the actionable events. The objective was not to select the optimum strategy and course of action or to imply one strategy was better than the other but to simply illustrate the use of the tool to conduct a comparison of these two strategies based on the probability of a terrorist attack over time and to provide some analysis of the relative effects of various courses of action.

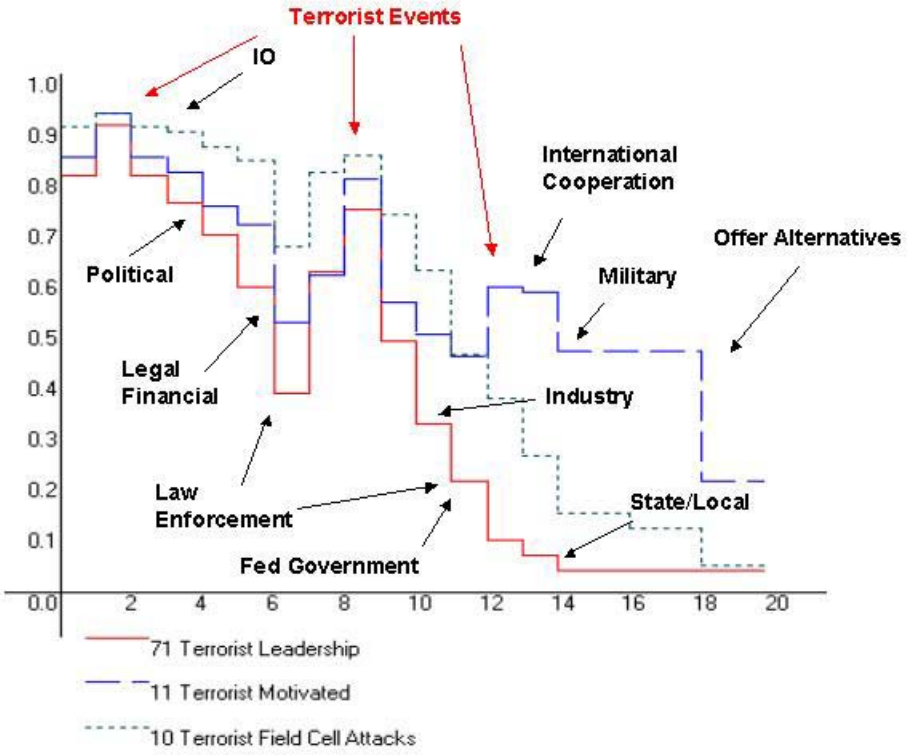

Figure 4. Reactive Strategy

The probability profiles in Figure 4 show the temporal analysis of terrorist leadership support, terrorist motivation and terrorist field cell likelihood to attack. Three single timeslot terrorist warning events occurred at times 1, 8 and 12 and these terrorist warning events were used to trigger a scenario-driven predetermined reactive course of action. The reaction strategy tested chose to use soft means first and then hard kill. IO followed by Political actions were initiated in reaction to the first terrorist threat warning event but these actions alone were not significant enough to cause a major reduction in the likelihood of a terrorist attack. The actionable events did serve to set some initial conditions for deterring an attack by reducing terrorist leadership willingness to support terrorist activities and there was some negative impact to terrorist motivation—largely driven by the IO campaign.

Legal and financial actions against the state sponsors and supporters and terrorist support elements such as sanctuaries and the financial networks were initiated at time 6. These actions combined with a short duration law enforcement action at time 6-7 against terrorist leadership and support elements appeared to have an important temporary impact on terrorist leadership, motivation and likelihood of attack. One might conclude that if the law enforcement action had continued (or its initial effects persisted) it would have helped reduce the relative influence of the second terrorist event that occurred at time 8. With the law enforcement action ending at time 7, it is suggested that a window of opportunity (or vulnerability) opened between time 7 and the next terrorist threat warning at time 8. As a result, the relative impact of the second threat warning was a more significant influence in raising the probability of attack.

Following the second terrorist event, the scenario proposed actions by government and industry to protect high value targets and this had a high payoff in reducing the probably of a terrorist attack. These actions increased the risk to the terrorists if they attacked. In this case, the scenario suggested that industry would respond quicker (loss of revenue driven) to the threats than government bureaucracies and that the federal government would be able to respond quicker than state and local governments and this drove the sequencing of antiterrorism protection actions. Law enforcement actions were also reactivated at time 11 to aggressively pursue terrorist leadership and support elements.

Although the third terrorist event increased terrorist motivation, the actions in place kept the probably that the terrorist would attack low—leveraged terrorist belief that attacking protected targets would be a high risk. Military action was initiated at time 14 to attack terrorist leadership and to reduce the ability of terrorists to conduct operations. The likelihood of a terrorist attack was further reduced when international cooperation and the offering of alternatives to improve the quality of life of terrorist supporters took place. These actions served to erode support for the terrorist cause and significantly reduced terrorist motivation.

Embedded within the temporal analysis shown in Figure 4 are multiple actions related to use of intelligence. The scenario assumed that there were limited intelligence assets available to support the counter terrorism and antiterrorism actions and that the use of these assets would therefore be driven by increased awareness that there was a need to focus on terrorism related targets. It was assumed that at time 0 that a minimum level of intelligence was being used (25%). Following the first terrorist event the use increased (50%) at time 5 but then went back down (25%) at time 7 when no attack occurred.

Following the second terrorist warning event, the use was escalated (75%) and after the third warning its usage went to the max (100%).

The analysis suggests that an effective antiterrorism protection campaign can have a significant impact in reducing the likelihood of a terrorist attack but this alone is not sufficient. Other means need to be employed to dismantle the terrorist operational architecture—their ability to conduct operational activities in support of their goals.

The scenario for the second example employed a preemptive strategy in response to a terrorist threat warning. In this case, proactive use of the elements of national power were brought to bear early with an aggressive combined use IO, intelligence, political, military, legal, financial and law enforcement actions to achieve an early deterrence in the probability of attack by going after the leadership, state sponsors, reducing terrorist motivation and disrupting their ability to conduct operations. The aggressive strategy was intended to buy time to allow the bureaucratic process to take the actions necessary to initiate protection of high value targets and to engage the cooperation of the international community that would in turn serve to reduce the likelihood of an attack by further reductions in state sponsorship, terrorist supporters and support activities and the elimination of sanctuaries.

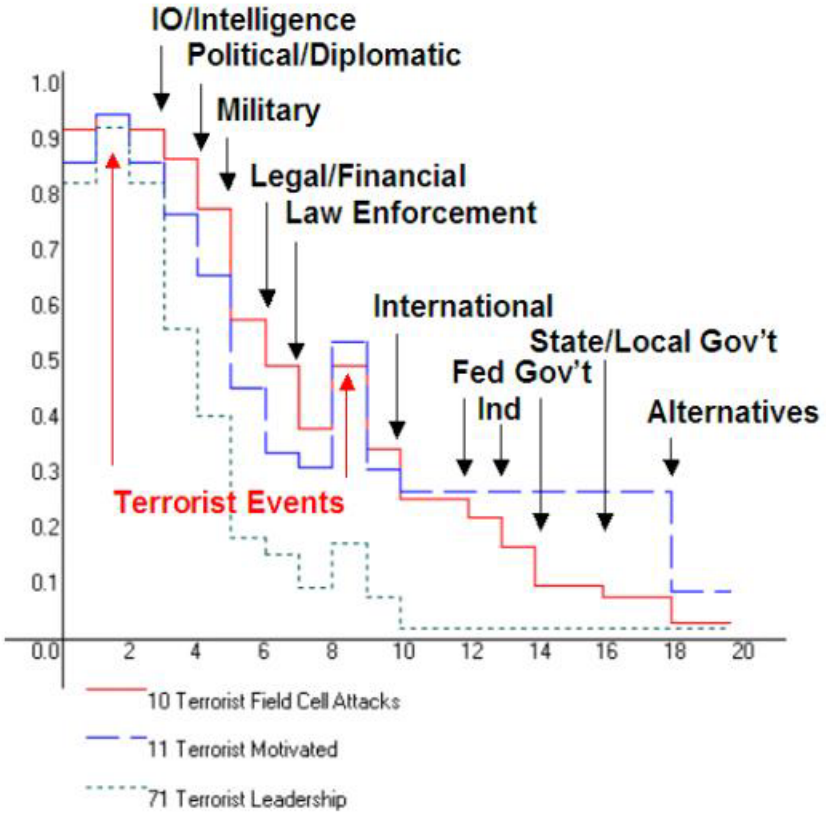

Figure 5. Preemptive Strategy

The probability profiles in Figure 4 show the temporal analysis of terrorist leadership support, terrorist motivation and terrorist field cell likelihood to attack. There are two terrorist warning events, one at time 1 and a second at time 8. The first terrorist warning event triggered the response to aggressively attack. The resulting effect was to drive the probability that the terrorist would attack below 50% and even with the second attack warning the probably of attack did not rise above 50%. Initiation of international cooperation at time 10 served to further reduce terrorist leadership willingness to support terrorist attack actions and this influenced a reduction in terrorist motivation and willingness to attack. As was the case in the first example, initiation of antiterrorism protection actions caused a reduction in the likelihood of a terrorist attack and the offering of alternatives to improve the quality of life of terrorist supporters served to further reduce terrorist motivation. The results suggest that the aggressive attack strategy was successful in achieving an early dismantling of the terrorist ability to conduct operations and significantly reduced the leadership support and other support of terrorist actions. Although the probability that the terrorist would attack was driven below 50% before the second terrorist warning event, the results also suggest that an aggressive antiterrorism program is needed to compliment the aggressive counter terrorism program. Both examples suggest that neither alone is sufficient.

The CAESAR II/EB tool has an ability to do a sensitivity analysis of the relative impacts of individual and combinations of actions. A sensitivity analysis of the case study model suggested that international cooperation and IO were key actions that if used in combination with other lethal and non-lethal actions could be a force multiplier and important contributor to reducing the probably the terrorist cell would attack.

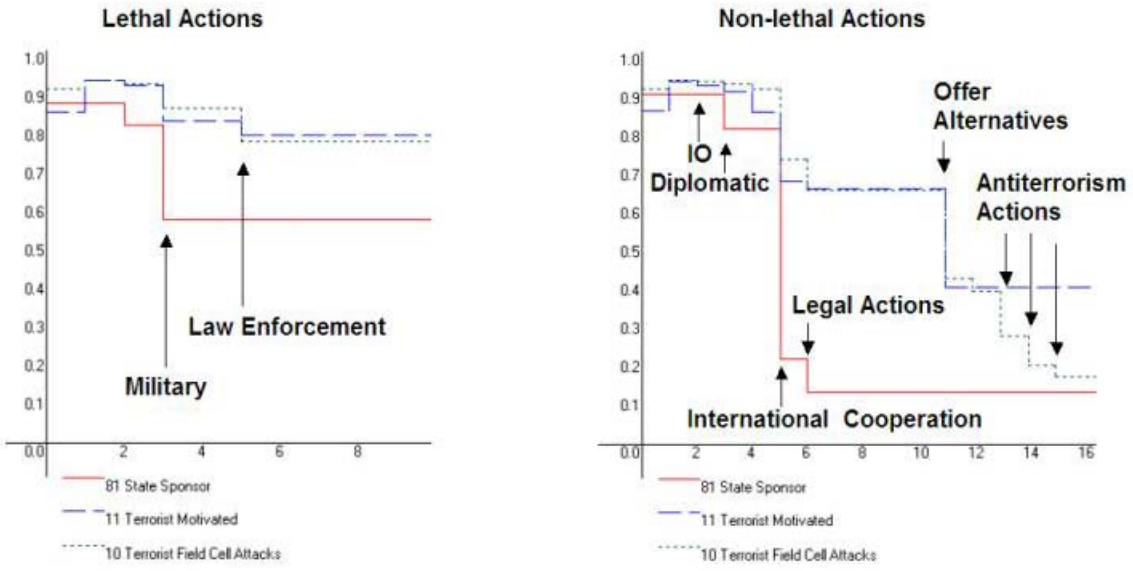

Figure 6. Comparison of use of Lethal and Non-lethal Means

Figure 6 compares the use of lethal and non-lethal means in response to the belief a terrorist event might occur. The probability profiles show the temporal analysis of state

sponsorship, terrorist motivation and terrorist field cell likelihood of attack. In both cases, a terrorist warning event occurs at time 1 and at time 2 intelligence actions were initiated in response to this warning. The comparison suggests that although the follow on military and law enforcement actions reduced the willingness of state sponsors to support terrorist activities, these actions alone were not sufficient to significantly impact the terrorist willingness to attack. On the other hand, the use of non-lethal means such as IO, political/diplomatic, international cooperation and legal/financial actions appeared to be significantly more effective in terms of reducing state sponsorship willingness to support the terrorist activities but here too these alone were not sufficient to significantly reduce the probability the terrorist might attack. The follow on offering of alternatives to improve the quality of life of terrorist supporters drove the terrorist motivation down and the probability of attack below 50%. The antiterrorism protective actions served to further reduce the likelihood of attack—increased risk to terrorist but not a de-motivation of support of the cause. One might conclude from this assessment that non-lethal means can be a significant contributor to reducing the probability that the terrorist might attack. Comparing these results with the preemptive strategy illustrated in Figure 5 also suggests that combining early military and law enforcement actions with non-lethal means such as IO, political, international cooperation and legal actions provided a synergistic effect (i.e., non-lethal means can be force multipliers) that achieved an early dismantling of the terrorist ability to conduct operations and reduced the willingness of the supporters to continue their support of terrorist actions and hence, satisfied the end objective to significantly reduce the probability that the terrorist would attack.

Observations

As noted earlier, creating influence nets and assessing courses of action is an art not a science. As such, the experience of the model builder is key as well as availability of subject matter experts to help guide the development of the models, the selection of courses of action and subsequent assessments. In many cases, the subject matter experts are not readily available and the modeler needs to do the research to prepare to develop the influence nets and conduct the course of action planning and assessments. This was the situation for the Counter Terrorism case study presented herein—a large part of the effort was researching the subject area. Model building is also a timely and complex task. In the authors' view, the current tools work best at the strategic level and to a limited extent at the operational level. The pace of tactical operations coupled with the author's experience using and observing the use of such tools in exercises and experiments suggests that these tools can be cumbersome to use operationally and hence, limit their value added in the high OPTEMPO environment of the tactical level of operation.[20]

The value added of CAESAR II/EB was successfully demonstrated at the strategic level when it was used to support the Naval War College Global Wargames and at the operational level when it was used to support the Joint Task Force Information Operations cell at the Millennium Challenge 2002 experiment at JFCOM. It must be

---

[20] Wentz, L. K. and Wagenhals, L.W. (2003). " Effects Based Information Operations," 8th International Command and Control Research and Technology symposium, National Defense University, Washington, D.C., June 2003.

remembered, however, that tools, such as CAESAR II/EB, are research tools and not ready for prime time operational use. Hence, the man-machine interfaces are not that user friendly and visualization of the results have limitations—CAESAR II/EB is cumbersome to use and generates probability profiles as its visualization output. Results must also be used carefully since this is just one means for trying to gain insights into effects actions might have on achieving a desired outcome. It's a prediction with varying degrees of uncertainty.

Challenges related to constructing influence nets are numerous. Understanding the situation is key to identifying the effects to be modeled and to develop the causal relationships and predict the truth or falsity of parent node effects on the child nodes. Selections of actions and the timing of the sequencing of these actions require some creativity on the part of the modeler as well. The process usually is to build a little and test a little with lots of trial and error experimentation to refine the model and to develop and select courses of action to be assessed. Models have limitations as well. For example, for CAESAR II/EB, persistence or the continuation of the effect after the action is removed is not modeled. Actions can be turned on and off several times over time but the persistence factor is not modeled. The model does not differentiate between the effects of the sequencing of two actions (e.g., action A before B versus B before A gives same final result although intermediate probabilities may be quite different) that in a real life situation may not be the case. On the other hand, the insights and interchanges among the decision makers, analysts and planners and synergy derived from the process of developing models and assessing the courses of action is probably one of the most important benefits to be realized from using a tool such as CAESAR II/EB.

The Counter Terrorism model developed using CAESAR II/EB and related courses of action planning and assessments appear to provide useful insights into the effects of lethal and non-lethal actions and their timing on desired deterrence outcomes as well as to help identify unintended and undesirable consequences of actions taken. The analysis presented herein suggests that counter terrorism and antiterrorism strategies need to address both the operational and technical architectures of the terrorist operations and organizations as well as one's own architectures. The experience has enabled the GMU researchers to expand their repertoire of modeling types and techniques to provide support to different classes of problems. CAESAR II/EB has limitations and work is in progress at GMU to explore enhancements to the utility of the tool including incorporation of modeling persistence and improving the user friendliness and visualization of results in support of effects based COA planning and assessments. Similar research and modeling efforts at the Air Force Rome Labs have already addressed some of these short falls. Their Causal Analysis Tool has incorporated modeling persistence and improved user interfaces and visualization and additional research is addressing improvements to the operational utility of CAT to support effects based air operations planning and assessments.

Acknowledgement

The contribution of Mr. Sajjad Haider of the GMU System Architectures Laboratory in the development of CAESAR II/EB and its use is gratefully acknowledged.

Reference

Anonymous (2003). "Terrorist Hunter," Harper Collins Publisher.

Cordesman, Anthony (2001). "A new US Strategy for Counter Terrorism and Asymetric Warfare," Center for Strategic and International Studies, Washington, D.C.

Davis, Paul and Jenkins, Brian (2002). "Deterrence and Influence in Counter Terrorism," RAND.

Ehrenfeld, Rachel (2003). "Funding Evil," Bonus Books.

Gunaratna, Rohan (2002). "Inside al Qaeda," Berkley Books.

Hess, Stephen and Kalb, Marvin (2003). "The Media and the War on Terrorism," Brookings Press.

Hoffman, Bruce (1998). "Inside Terrorism," Columbia University Press.

Hudson, Rex (1999). "Who Becomes a Terrorist and Why," The Lyons Press, Gilford, Connecticut.

Internet. "Terrorism Research center," www.terrorism.com

Jenkins, Brian (2002). "Countering al Qaeda," RAND.

Ledeen, Michael (2003). "The War Against the Terror Masters," Truman Talley Books.

Record, Jeffrey (2003). "Bounding the Global War on Terrorism," Army War College, Strategic Studies Institute.

Lesser, Ian and et al (1999). "Countering the New Terrorism," RAND.

Nance, Malcolm (2003). "The Terrorist Recognition Handbook," The Lyons Press, Gilford, Connecticut.

Norris, Pippa and et al (2003). "Framing Terrorism," Routledge Press

Palmer, Nancy (2003). "Terrorism, War, and the Press," Harvard University.

Wagenhals, L. W. and Levis, A. H. (2002). "Modeling support of Effects Based Operations in War Games," 7th Command and Control Research and Development Symposium, Naval Post Graduate School, Monterey, CA, June 2002.

Wentz, L. K. and Wagenhals, L.W. (2003). " Effects Based Information Operations," 8th International Command and Control Research and Technology symposium, National Defense University, Washington, D.C., June 2003.