

Systems Engineering Modeling Useful in Combating Terrorism

James Long
President, Vitech Corporation
2070 Chain Bridge Road
Suite 320
Vienna, VA 22182

William F. Mackey
Computer Sciences Corporation and
University of Maryland
8800 Teresa Court
Alexandria, VA 22308

Abstract. Following the terrorist events of September 11, 2001, several members of INCOSE have become involved in international, regional, and local activities to respond to those events that have shaken the international community. As part of the newly formed INCOSE Anti-Terrorism International Working Group (ATIWG) established in October 2001, efforts at the University of Maryland University College and Vitech Corporation have produced notable models and products useful to INCOSE. ATIWG meetings at the INCOSE Workshop held in Mesa, AZ, during January 2002 stimulated all who attended and generated still more useful views of the problem space. The ATIWG convened a special panel at INCOSE 2002 in Las Vegas, NV, under the theme documented in a companion paper entitled “The Role of Systems Engineering in Combating Terrorism.”

This paper’s thesis is that the multidisciplinary approach of systems engineering is useful in evaluating the terrorist threats, identifying system vulnerabilities, and reducing or eradicating international terrorism. In addition, the ability to model those events may assist in determining the functional design of the terrorist threat and perhaps permit insight into the physical design as well. The functional design (or *modus operandi*) is frequently unchanged from one terrorist activity to another, and only physical design changes. This then offers the potential to predict future terrorist acts. The authors are in the process of examining all facets of the issue by applying the multidisciplinary approach of systems engineering to the resolution of this meaningful international issue.

Introduction to Terrorism

Terrorism is the systematic use of force and violence to create fear as a means of coercion. It emerged as a concept in 1793-94 during the Reign of Terror in France. Since that time, dissident groups have used terrorism to violently intimidate populations or governments into granting their demands. The systematic use of violence has undergone a transformation since World War II and has made violence even more fearsome and inhuman. The calculated murder of political personalities and military personnel to achieve political objectives has given way to the random killing of innocent people and civilian populations.

Terrorism is a world phenomenon with over 360 major incidents resulting in loss of life and injury committed worldwide since 1967. These events have occurred in Germany, Scotland, Japan, Israel, Pakistan, and literally in all parts of the world. Major terrorist attacks are not unfamiliar to U.S. citizens either. Major terrorist attacks on U.S. citizens and property are shown in Table 1. It should be noted that these attacks also caused death and injury to citizens of many different nations, as well as damage to property of other nations.

Date	Attack	Killed	Injured
August 7, 1988	U.S. Embassy bombings	252	5,000 +
February 27, 1993	World Trade Center (WTC) bombing	6	1,000 +
April 19, 1995	Oklahoma City bombing	168	300 +
July 27, 1996	Atlanta Olympic Park bombing	1	0
January 16, 1997	Atlanta Abortion Clinic bombing	0	0
October 12, 2000	USS Cole bombing	17	39
September 11, 2001	WTC aircraft attacks	2,794	6,000 +
September. 11, 2001	Pentagon and Pennsylvania aircraft attacks	224	100 +
October 2-24, 2002	Washington metro area sniper attacks	10	3

Table 1: Major Terrorist Attacks on the United States Since 1985

These violent events raise several meaningful questions:

- Who are the terrorists responsible?
- What is their motive?
- What must be done to defeat them?

These questions are answered in the companion paper (Mackey et al. 2003).

INCOSE's Response to the Events of September 11

The development of a focus on public interest challenges by the international membership of INCOSE began in the late 1990s. A public interest challenge was defined, within a small working group, as “an unsolved problem that has negative effects on people of various cultures and geographical locations and that is amenable to the application of systems engineering.” The development of the Public Interest Project and examples of such challenges is elaborated in a companion paper (Mackey et al. 2003).

The Immediate Reaction of INCOSE to the Events of September 11. The events of September 11 acted as a catalyst in bringing the Public Interest Project to life. The INCOSE Technical Board has chartered the Anti-Terrorism International Working Group (ATIWG). Its mission is to demonstrate the use of systems engineering principles, techniques, and practices to the reduction or eradication of international terrorism. The systems engineering approach is most amenable to such evaluations because of its ability to incorporate multiple disciplines to examine all facets of the problem space.

The Results of INCOSE Activity to Date. The September 11 events have prompted several meetings in INCOSE chapters (e.g., the Washington Metro Area Chapter) and working sessions at international workshops and symposia. INCOSE also sponsored the Anti-Terrorism Panel in Las Vegas, NV, on August 1, 2002. As a result of these activities, several models and analyses have been completed by various members of INCOSE. The University of Maryland University College (UMUC) systems engineering graduate students completed a class project, developed the *Anti-Terrorism Concept Exploration Document*, and transferred publishing rights to INCOSE. Members of the ATIWG hope that in the future INCOSE will be able to create partnerships with government and/or community organizations needing voluntary engineering

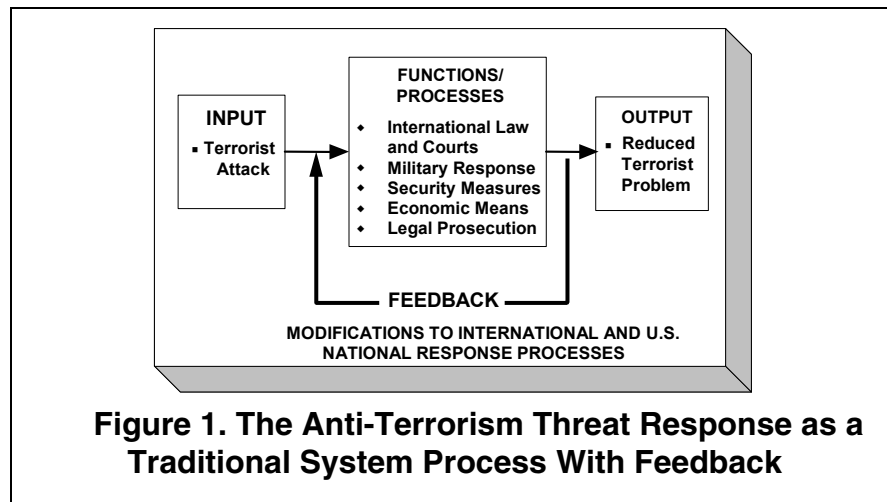
assistance to address this challenge. Meetings involving several INCOSE members are ongoing in an effort to create these partnerships.

Terrorism Behavior Modeled As a System

A system, as defined by INCOSE, is an interacting combination of elements viewed in relation to function. The interaction between a terrorist organization and organizations meant to combat terrorism may be modeled as a traditional system with feedback response. An anti-terrorism behavioral model has the following intentions:

- Reduce or eradicate the effects of international terrorism
- Eliminate the stimuli that initiate the development of international terrorism

Most legal processes may be discussed as a system and analyzed on a consistent basis (Mackey 2000). A simplified model is shown in Figure 1 as an international response, including the U.S. response, to a terrorist attack on any country, such as the events of September 11, 2001, or the Bali bombing of October 2002. The main components—input, process, and output—of a traditional system with feedback response are useful in such a discussion. The external constraints and mechanisms used to support a system are also to be considered. The ease with which the systems engineering concept can be applied to combating terrorism or any other crime has an obvious advantage of communicating legal issues to an engineering community in familiar terms (Mackey 2000) and communicating system issues to legislators, businessmen, and military leaders in a manner they can understand. The simplified model featured in Figure 1 expresses the resolve to reduce the terrorist problem by using international law and courts, economic sanctions, military actions, and legal prosecution against the terrorists involved. It also implies the use of security measures to reduce the vulnerabilities of a nation's system elements (e.g., computers, aircraft, buildings) to attack. By modifying the feedback response to terrorist attacks, the expectation is to reduce terrorist effects to zero.



The United States and the United Nations are presently responding to the direct and immediate threats of terrorism. The authors believe that the long-term approach to resolving the terrorism problem can only be accomplished by a dual-feedback mechanism that includes

- Understanding the thought processes of the terrorists who perpetrate such crimes
- Understanding the thought processes of the nations and peoples being attacked

Creating the Anti-Terrorism System Concept Model must incorporate the understanding of multiple complex disciplines and issues. Such a model must reach back to the stimuli that create such terrorist threats as well as addressing the threats and vulnerabilities of existing systems. Both feedback responses must be used to permanently reduce and eliminate the damages resulting from terrorist events.

Figure 2, a more comprehensive model, shows the anti-terrorism process intended to combat the terrorist threats, alter the system vulnerabilities, and affect the stimuli that create such threats. The main elements of the system can be characterized as follows:

- Input—Stimuli that initiate potential terrorists’ desires to commit acts of terrorism to satisfy their needs and requirements
- Output—Damages arising from loss of life, personal injury, and destruction of property resulting from a terrorist’s activities
- Functions—Activities and processes conducted to combat international terrorism
- External constraints—International law, economics, environmental prohibitions, geography, etc.
- Mechanisms—People, technologies and processes used to combat international terrorism
- Feedback controls—Modifications that can increase or decrease terrorism activity

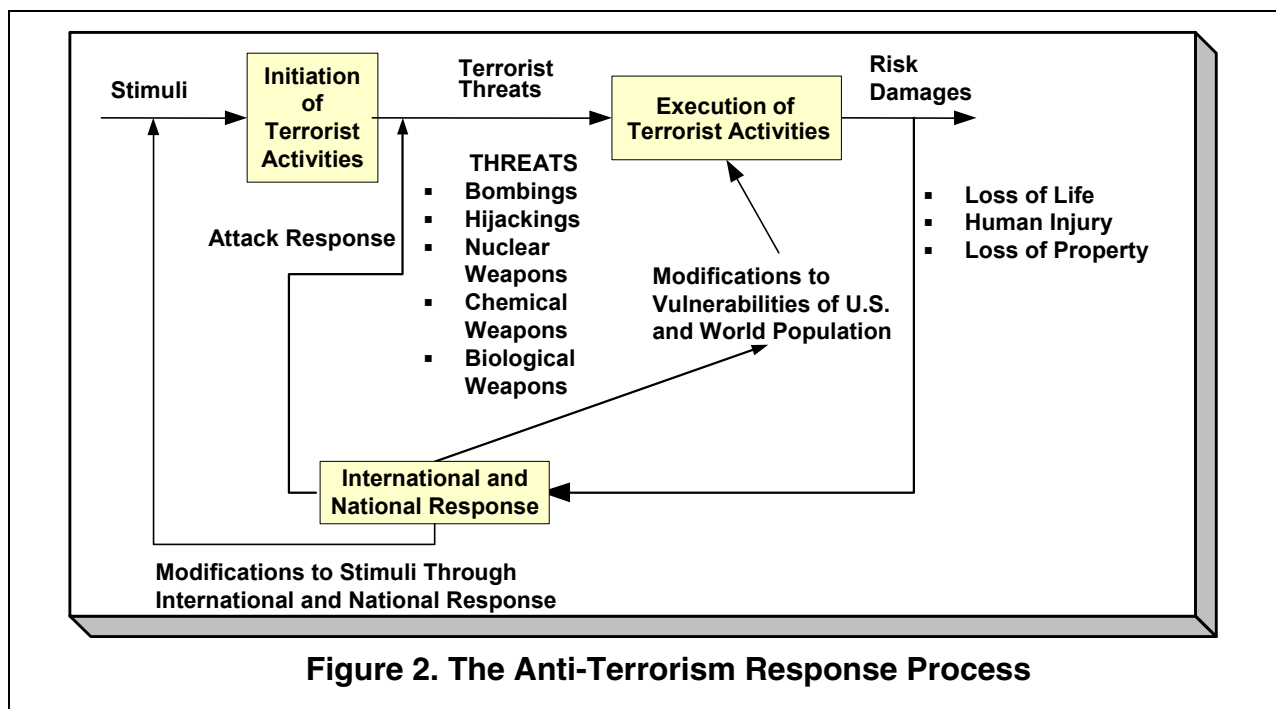


Figure 2 demonstrates several options to modify the behavior of terrorist organizations:

- The international community can attempt to modify the environment of terrorist organizations through peaceful means such as education, efforts to improve the life of the Third World countries that sponsor terrorism, and diplomacy measures. To be successful, the cause-and-effect relationships must be well understood. In this way, these measures might eliminate the stimuli that create and maintain terrorist activities.

- The international community can act directly against the threats by measures such as isolating the terrorist organizations, establishing economic sanctions, and attacking the terrorist cells where they exist.
- The international community can modify the vulnerabilities of each nation's assets to make them less susceptible to attack, such as making transit into the country far more difficult, improving the integrity of airplane cockpit doors, and providing the entire population with biological and chemical antidotes to such attack.

To be sure, all three approaches must take place and all will be costly. The tradeoffs of applying resources to each approach is a challenge to which systems engineering can add value. If the correct programs can be identified to reduce the stimuli, a post WWII Marshall Plan might be less costly and more long lasting. Insufficient resources exist to make all facilities invulnerable to attack.

Analysis Conducted by Graduate SE Students of UMUC

The UMUC Class Project. Following the events of September 11, the systems engineering (SE) graduate students at the UMUC agreed to address the challenge of combating terrorism by creating a class project to be examined by the entire class. The results of this study are recorded in the document *INCOSE Anti-Terrorism International Working Group Concept Document, Preliminary Draft*, December 5, 2001. This document is in the possession of W. Mackey and most members of the ATIWG. The mission of the anti-terrorism class project was to demonstrate the use of systems engineering principles, techniques, and practices to the reduce or eradicate international terrorism.

Scope of Class Project. The challenge to reduce or eradicate international terrorist activities is complex and involves many facets of human activity and expertise including the following:

- Economics
- Political science
- Religions and cultures
- Psychology and sociology
- Geography and geology
- Military and defense
- International law
- Terrorism and counter-terrorism
- Telecommunications and computer technologies and engineering
- Aviation and space technologies and engineering
- Intelligence collection, analysis, and distribution
- Security engineering (administrative, communications, environmental, personnel, and physical)
- Biological, chemical, and nuclear technologies and engineering

Expertise and study in all of these disciplines and yet-to-be-identified skills will be necessary to understand the motives, objectives, strategies and operations of the terrorist groups. Most of these disciplines will also be required to identify the threats, vulnerabilities, and risks to the populations and systems employed by the industrialized countries. The strategies for mitigating

and eradicating the risks through security measures and engineering will require expertise of a different nature. The graduate students agreed to take assignments in many facets of the multidiscipline.

Each graduate student was requested to satisfy his/her domain of interest using the following format:

- Statement of issue—What is the relevance of this domain (e.g., economics, religion, and cultures) to the challenge of combating terrorism?
- Discussion of issue—What analyses have been or should be performed in relation to combating terrorism?
- Requirements for resolution of issue(s)—What is necessary to a solution in this domain?
- Systems engineering challenges—What kinds of projects might be attempted by a small group of systems engineers in this domain?
- Technical performance metrics—What are the useful metrics in this domain to determine whether terrorism is getting better or worse?
- Author, references, and contacts—What are the key sources used in addressing this domain?

This document is presently being reviewed and expanded by the members of the ATIWG.

The Core Approach to Modeling the Events Leading Up To and During September 11

The objective of this experiment was to apply elements of the system engineering process to three terrorist situations to evaluate the possible utility to the practice of intelligence analysis.

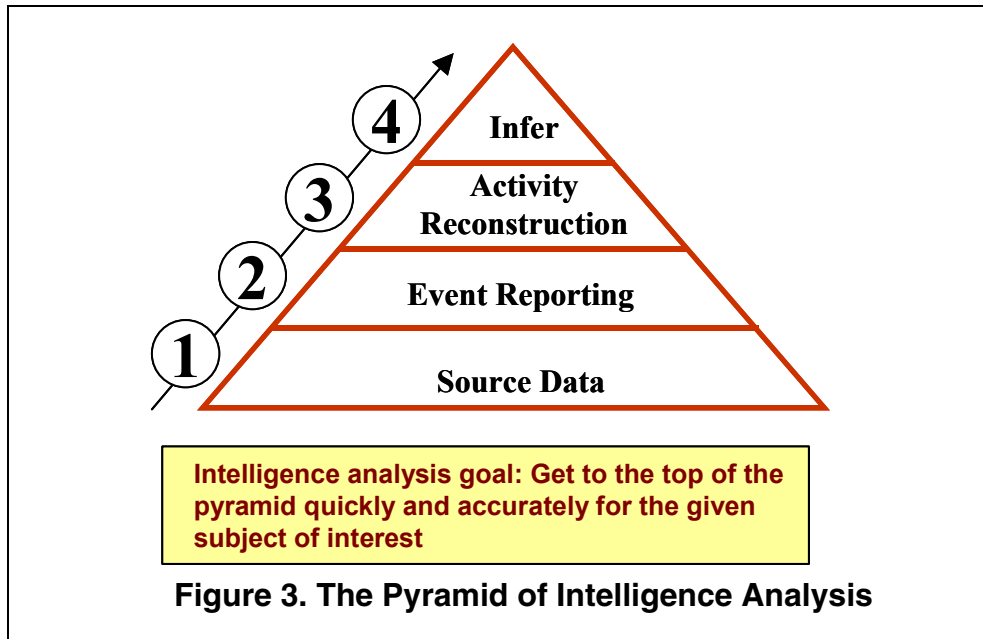
Overview. First, it should be noted that successful intelligence analysis is about prediction of the future—not documenting the past. While intelligence analysis begins with intercepted or gathered raw data, it needs to evolve from this data to the ability to generate predictions of possible/likely actions of the opponent, as shown in Figure 3.

However, to make predictions about possible future events, a model of the opponent must be built based on historical data and hypothesis testing. The application of systems engineering principles and practices involves the following:

- The enemy and target of the enemy can be viewed as interacting dynamic systems.
- Models of the enemy and other participants are reverse-engineered from multisource sampled data and information.
- Systems are represented as separate functional and physical models. System functions change slowly with time, while physical elements could change dramatically.
- Making and testing hypotheses is a key element of refining and converging the models.
- Total analysis is never completed.

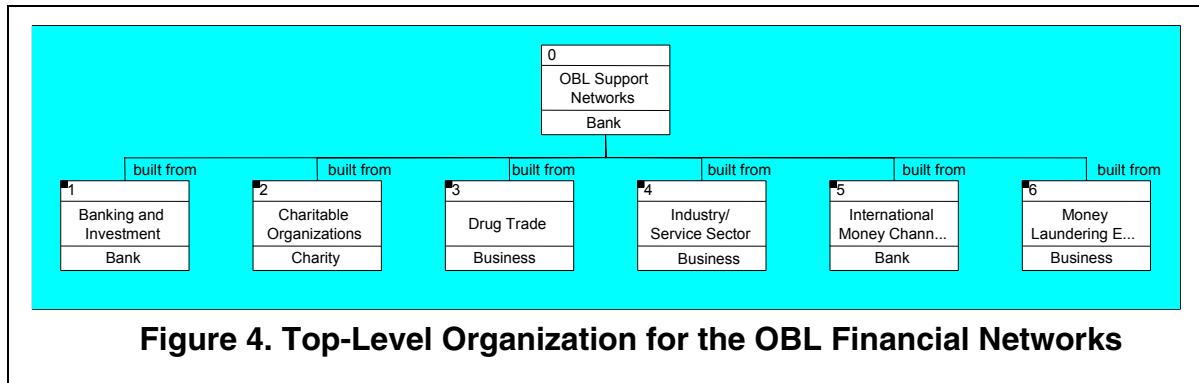
Three different databases were used to illustrate the concepts:

1. Osama bin Laden: Financial Support Networks (Treasury Department Congressional Testimony)
2. Terrorist Pilot Training (Washington Post)
3. WTC Terrorist Cell Activities (Washington Post)



Model 1: Osama bin Laden – Financial Support Networks

This database consists primarily of the elements of the Osama bin Laden (OBL) financial network and its organization as shown in Figure 4.



Postulating a functional model for this network provides a context for these physical elements and their relationships as shown in Figure 5.

The original database consists primarily of data and information and, therefore, is at Level 1 in Figure 3. Augmenting this data with the functional model adds another dimension and provides extra insight.

Model 2: Views From Terrorist Training Data

This database consists of events that allow reconstruction of activities, placing it at Levels 2 and 3 in Figure 3. This permits modeling of system-on-system, represented as an N2 diagram in Figure 6.

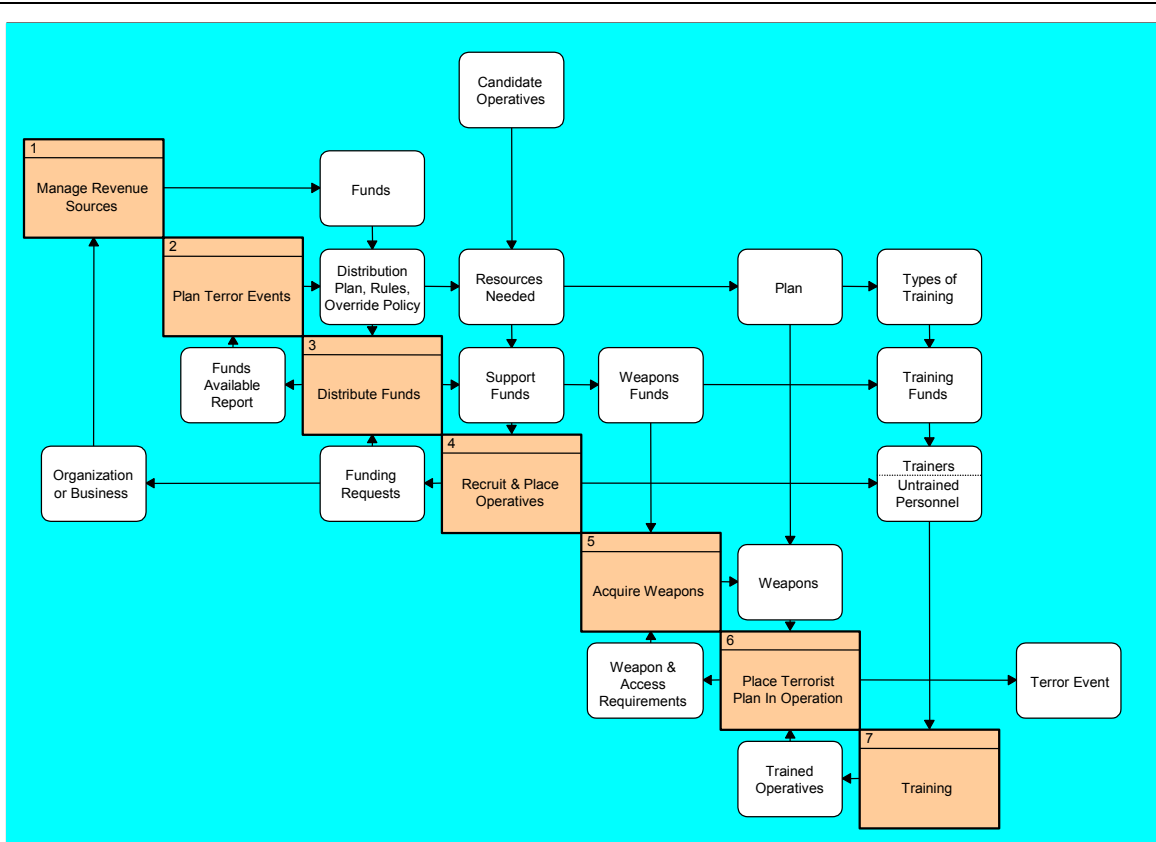


Figure 5. Postulating the OBL Functional Model Puts the Organization in Context

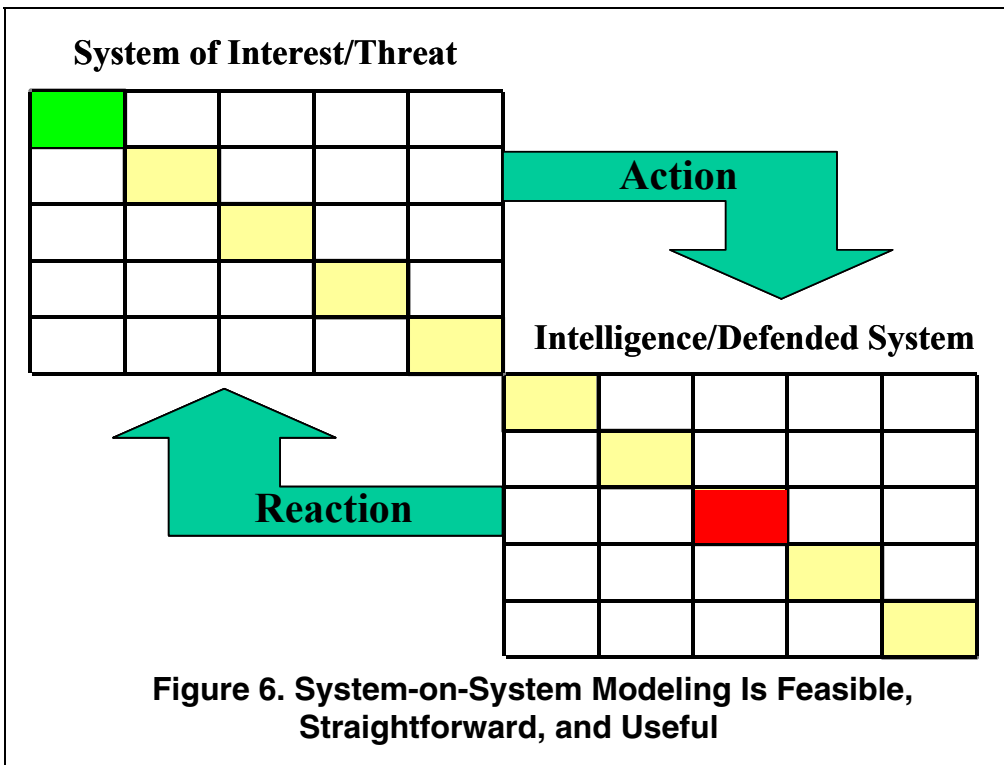


Figure 6. System-on-System Modeling Is Feasible, Straightforward, and Useful

Figure 7 presents al Qaeda, the terrorist (Mohamed Atta's) cell, and the U.S. pilot training schools as systems in an enhanced function flow block diagram (EFFBD). This context-level diagram shows the interface data flows among the systems, but sequences are not shown until the system functions are decomposed at lower levels of the hierarchy.

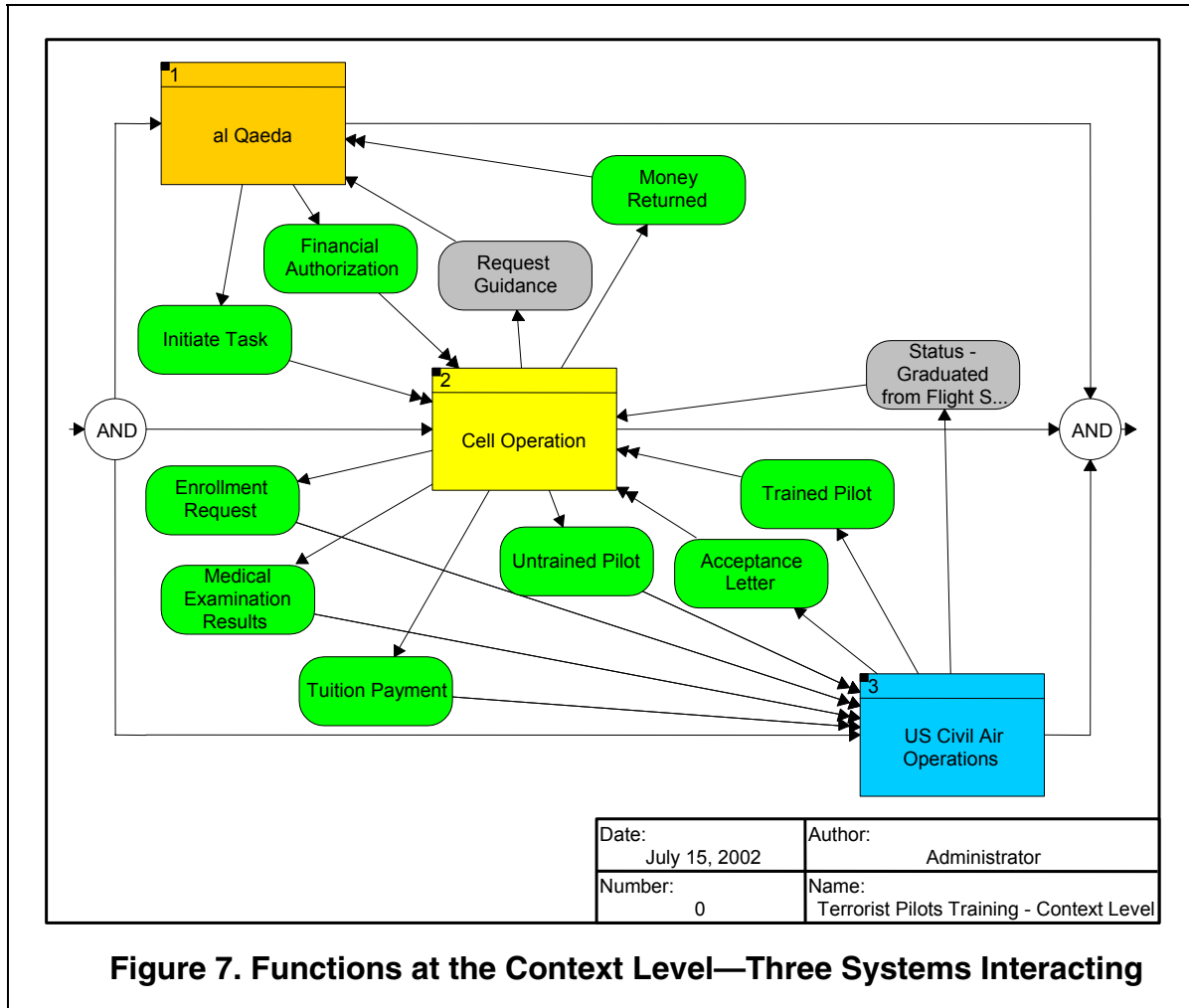


Figure 8 is an N2 interface diagram. While both the EFFBD and N2 diagrams show that no interfaces exist between al Qaeda and pilot-training systems, it is easier to see this lack of interaction in the N2 diagram. The features of the N2 chart make it the tool of choice in reverse-engineering of systems with sparse or incomplete data. The EFFBD is a good view for showing scenarios and time sequences and, therefore, is the best view for making projections and predictions. Figure 9, the second-level EFFBD, shows the additional insight available.

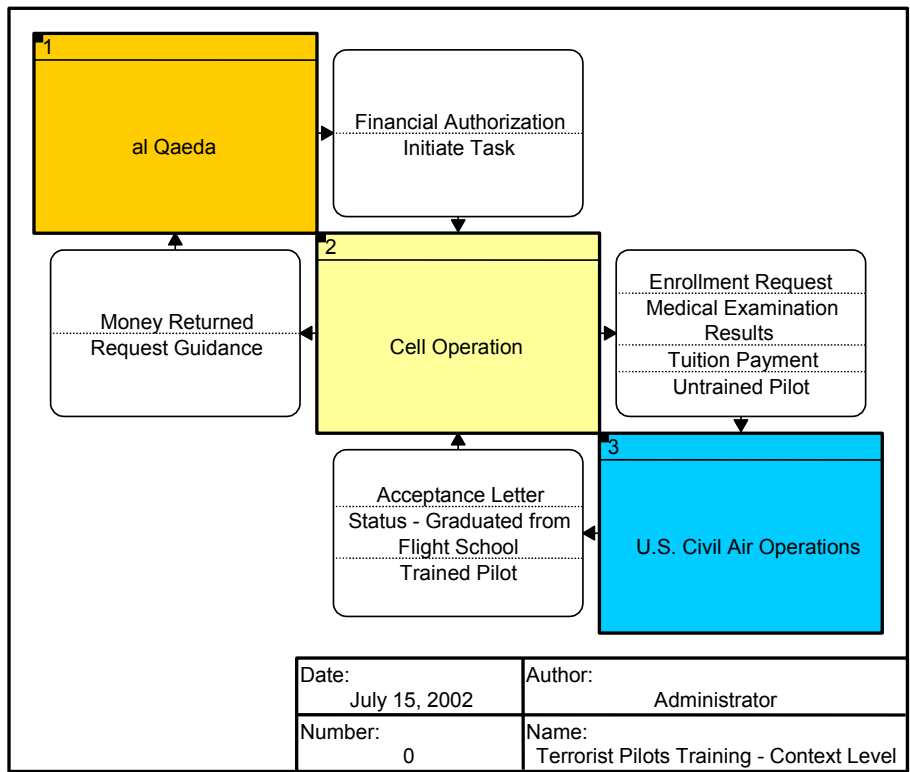


Figure 8. N2 Interface Diagram—Lack of Interaction Between al Qaeda and U.S. School Is Easily Visible

Model 3: Terrorist Cell Activities Leading to the World Trade Center and Pentagon Attacks

The third database contained event-reporting and activity reconstructions, placing it at Levels 2 and 3 in Figure 3. It contains sufficient information to develop EFFBDs to the third level of detail/hierarchy. This amount of detail allows execution of a simulation of the cell activities to the level of individual terrorists. Figures 10, 11, and 12 show details of the activity models. Note that Figure 11 is not expected to be readable but shows the level of detail to which existing information can be expanded to include the activities of each individual terrorist. Figure 12 shows that this model presents the data known (in dark boxes) and reveals information holes (in white boxes, such as data and its location in time, missing activities, etc.).

Results of the Experiment

The experiment was considered successful. The multiple graphical system engineering views available from the models provided additional insight. Treating the interactions of organizations and antagonists with system-on-system analysis simplifies the presentation of information and assists in clarifying the activities of the attackers and their operational scenarios.

The expected benefits of building models of the systems using the N2 chart for reverse-engineering systems and EFFBDs for simulation and prediction were confirmed.

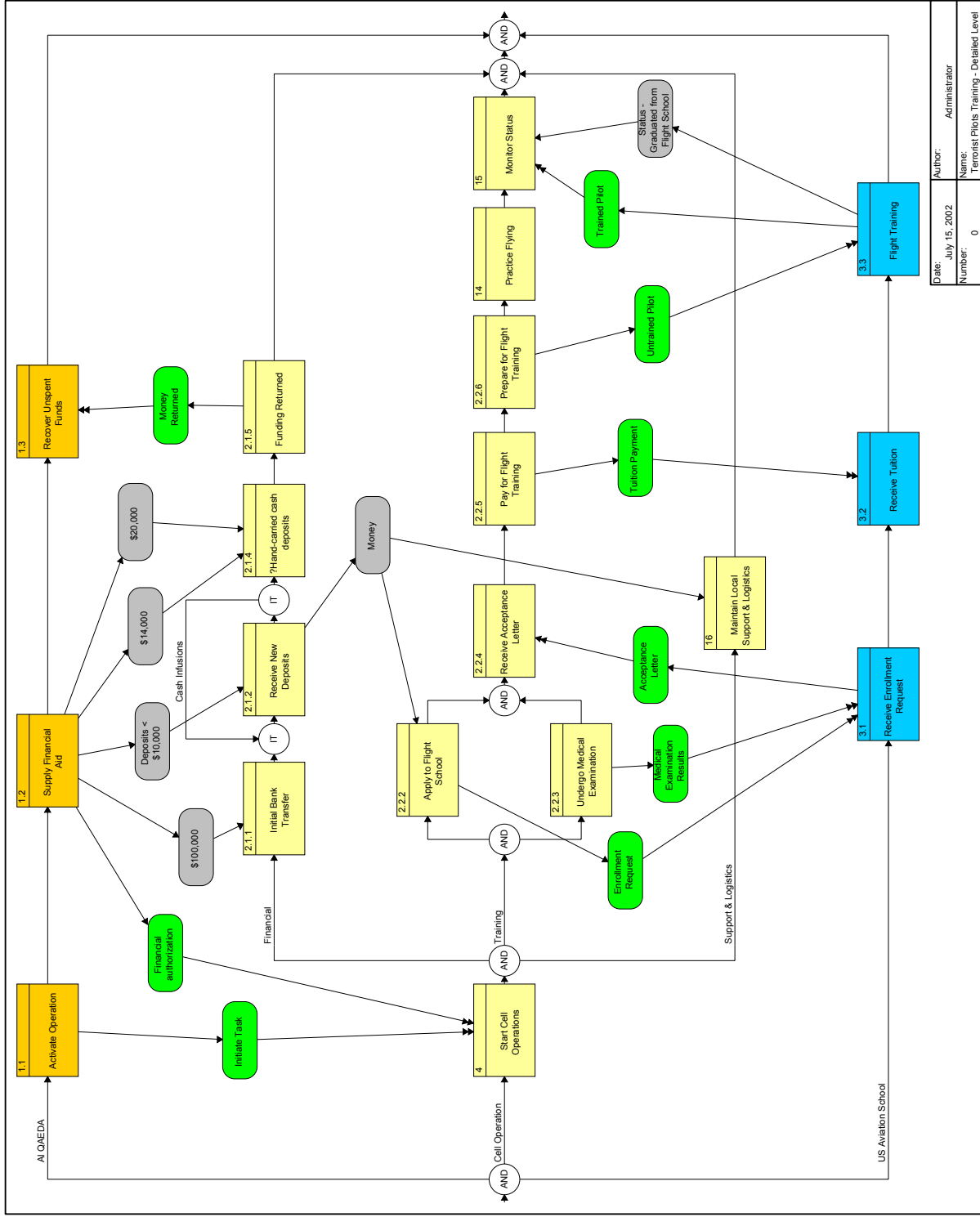
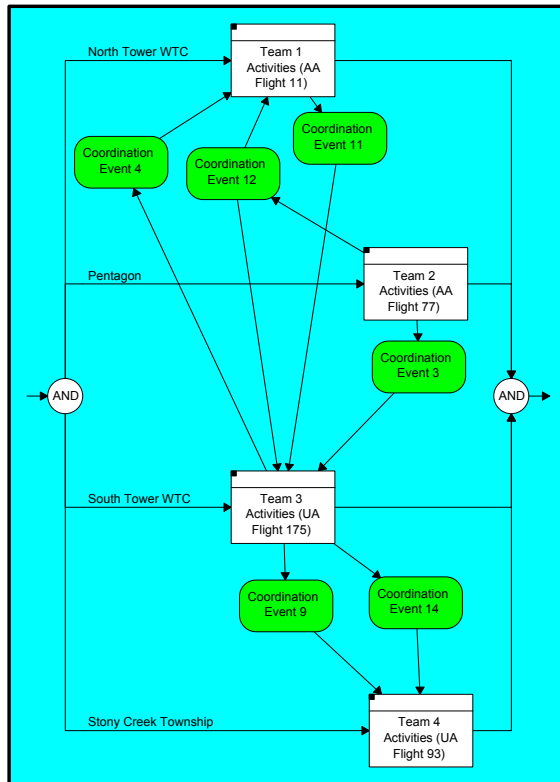
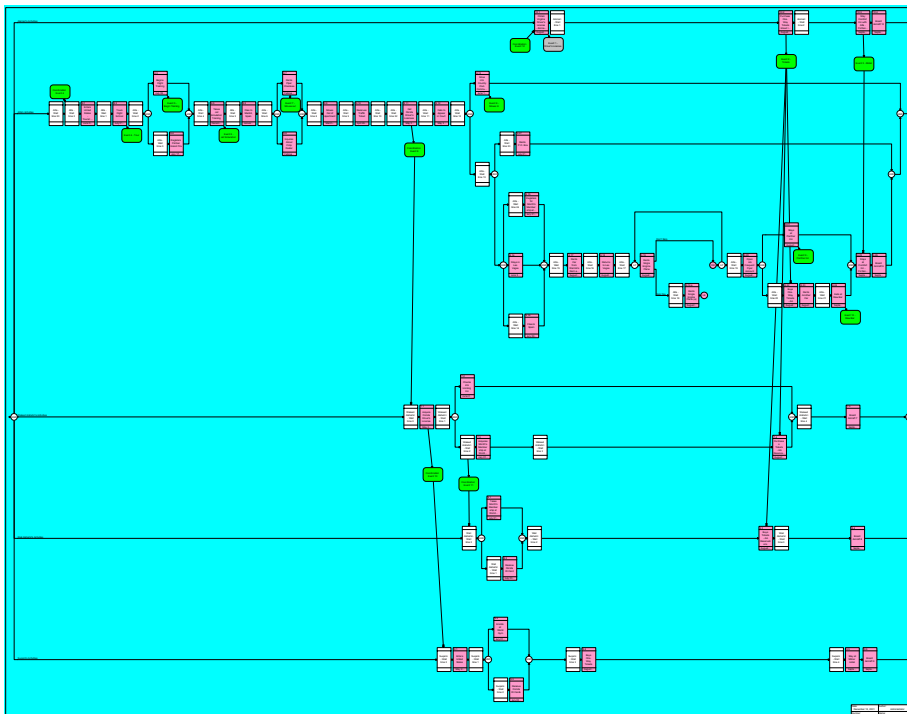


Figure 9. Functional Architecture at the Next Level Shows Sequencing and Partitioning of Roles



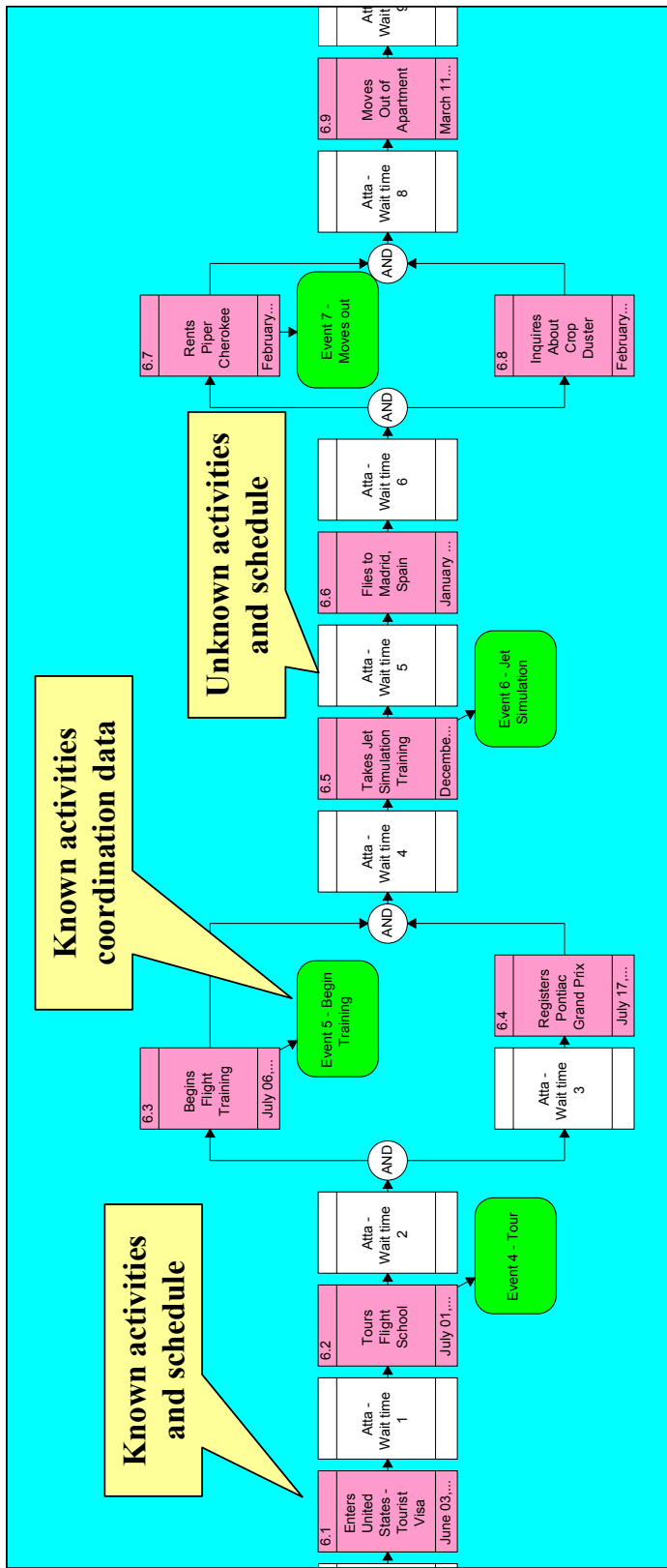
- Behavior and N2 modeling included hierarchies down to the individual terrorist level (see COREsim simulator output for Atta).
- The cell is made up of 19 terrorists organized in 4 coordinated teams.
- The total timeline from the first terrorist entry into the U.S. until the attack on the WTC and Pentagon involved about 33 months.

Figure 10. Activities of WTC Hijackers—Top Level



- Each main branch represents the activities of one terrorist (five on this plane).
- Linked activities between terrorists are indicated by interfacing items.

Figure 11. Activities of Team 1 (AA Flight 11)—At the Next Level of Detail



NOTE:

- Behavior diagrams and scenarios are represented in a graphical language that is executable, allowing automatic simulation of the graphical model.

Figure 12. Details of a Segment of Atta's Timeline

Requirements for Inference and Prediction

To achieve the inference and prediction, it is necessary to identify events relating to some combination of the following:

- Target
- Weapon
- Schedule
- Team
- Postulated scenarios

In addition,

- Inference requirements are interdependent. Once some are satisfied, others become constrained.
- Observables need to be placed in context.
- Functional scenarios and models must have realizable physical allocations. Since scenarios were not postulated in the experiment, there was no opportunity to test hypotheses and make predictions.

Summary

This paper demonstrates that the reduction and eradication of international terrorism is a multidisciplinary challenge. The authors strongly believe that the discipline of systems engineering is amenable to these kinds of challenges. The system architectures of facilities, information systems, and transportation capabilities must present less vulnerability to terrorist threats in the future. How the international community addresses these kinds of threats may determine whether they are transient phenomena or long lasting.

INCOSE has been addressing these kinds of issues in working groups since 1998, and individually through professional papers since its inception in 1991. The INCOSE ATIWG is seeking partnerships with government and community organizations needing voluntary engineering assistance.

A behavioral model, N2 diagrams, and EFFBDs are all useful in evaluating the information available and attempting to understand the functional and physical design of the terrorist act. From these models, it is hoped that further analysis would help to determine the correct responses to the act(s) and to uncover the functional design (or *modus operandi*).

References

- Netanyahu, Benjamin, *Fighting Terrorism*, 2001 edition, Farrar, Straus and Giroux
- Mackey, William et al., "The Role of Systems Engineering in Combating Terrorism," *INCOSE 13th Annual International Symposium Proceedings*, Washington, DC, July 2003

Biographies

Mr. James Long is the President of Vitech Corporation and developer of the system engineering support tool CORE[®]. He has been a performing systems engineer and innovator since creating the first behavior diagrams (then called Function Sequence Diagrams) at TRW in 1967. He played a key technical and management role in the maturing and application of that system engineering process and technology at TRW and Vitech.

Mr. Long's 45 years of engineering, systems engineering, and management experience include positions at Allison Division of General Motors, TRW, TITAN Systems, and Vitech Corporation. His engineering experience includes assignments in flight test engineering, electric propulsion space trajectories, air defense, ballistic missile defense, undersea surveillance, satellite surveillance systems, and military C3I systems.

Mr. Long has undergraduate and graduate engineering degrees from GMI and Purdue University and has been selected as an Eminent Engineer by Tau Beta Pi, the honorary engineering scholastic society. This designation is in recognition for career achievement in engineering.

He is a member of INCOSE and the INCOSE Corporate Advisory Board (CAB). He also served as vice-president and then president of the Washington Metropolitan Area Chapter, the largest chapter of INCOSE.

William Mackey, Ph.D., J.D., is a Senior Member of the Executive Staff of Computer Sciences Corporation and Professor at the University of Maryland University College teaching systems engineering. He attended the U.S. Naval Academy and has B.S. and M.S. degrees in physics from the University of Pittsburgh and the Rensselaer Polytechnic Institute. He received his Ph.D. degree in systems engineering from the University of Pennsylvania and his J.D. degree from the Washington College of Law, American University. Dr. Mackey has a 35-year career in scientific research, engineering, and management applied to aerospace, transportation, energy, systems integration, and law. He is a member of both the District of Columbia and the State of Virginia legal bars. Dr. Mackey formed the INCOSE Anti-Terrorism International Working Group in October 2001 and is its present Chair.