Decision Support for Countering Terrorist Threats against Transportation Networks

Richard Adler
DecisionPath, Inc., rich@decpath.com

Jeff Fuller
Teledyne Brown Engineering, Inc., jeff.fuller@tbe.com

Follow this and additional works at: <https://digitalcommons.usf.edu/jss>

Part of the [Defense and Security Studies Commons](#), [National Security Law Commons](#), and the [Portfolio and Security Analysis Commons](#)
pp. 43-64

Recommended Citation

Adler, Richard and Fuller, Jeff. "Decision Support for Countering Terrorist Threats against Transportation Networks." *Journal of Strategic Security* 2, no. 3 (2010) : 43-64.

DOI: <http://dx.doi.org/10.5038/1944-0472.2.3.5>

Available at: <https://digitalcommons.usf.edu/jss/vol2/iss3/5>

This Article is brought to you for free and open access by the Open Access Journals at Digital Commons @ University of South Florida. It has been accepted for inclusion in Journal of Strategic Security by an authorized editor of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.

Decision Support for Countering Terrorist Threats against Transportation Networks

Abstract

This article presents a dynamic decision support methodology for counter-terrorism decision support. The initial sections introduce basic objectives and challenges of terrorism risk analysis and risk management. The remainder of the paper describes TRANSEC, a decision support framework for defining, validating, and monitoring strategies focused on managing terrorism risks to international transportation networks. The methodology and software tools underlying TRANSEC are applicable to other homeland security problems, such as critical infrastructure and border protection.

Decision Support for Countering Terrorist Threats against Transportation Networks

By Richard Adler, Ph.D. and Jeff Fuller

Introduction: Challenges for Managing Risks from Terrorism

Improved intelligence sharing is helping Homeland Security authorities identify terrorist threats more effectively. However, this progress accentuates key "downstream" problems for decision-makers:

- Analyzing credible but imprecisely defined terrorist threats.
- Formulating strategies to mitigate risks from terrorist threats and understanding their likely consequences and costs.
- Revalidating and adapting strategies as the risk landscape evolves over time.

Conventional decision support methods and tools lack the horsepower required to address these program-level tasks effectively. For example, spreadsheets and other simulation engines excel at manipulating numeric data, projecting quantitative trends, and the like. However, they fall short in depicting and leveraging critical knowledge about security that is largely qualitative, uncertain, and incomplete. Key examples include intelligence about terrorist objectives, resources, and behaviors; economic forces and technological trends; and the challenges of implementing complex security initiatives. Lacking robust frameworks for analyzing the *dynamics* of terrorism risk and risk mitigation strategies, authorities are seriously hampered in their efforts to protect the nation.

This article presents a dynamic decision support methodology for counter-terrorism decision support. The initial sections introduce basic objectives and challenges of terrorism risk analysis and risk management. The remainder of the paper describes TRANSEC, a decision support framework for defining, validating, and monitoring strategies focused on managing terrorism risks to international transportation networks. The methodology and software tools underlying TRANSEC are applicable to other homeland security problems, such as critical infrastructure and border protection.

Analyzing Risks from Terrorist Attacks

Classic risk assessment methodologies focus on identifying relevant threats and estimating their relative likelihoods and expected impacts.¹ The United States Department of Homeland Security (DHS) has adopted the following analytic construct for assessing risks, not only from terrorist attacks but also from natural disasters such as hurricanes, earthquakes, and epidemics:²

$$\text{Risk} = \text{Threat} \times \text{Consequence} \times \text{Vulnerability}.$$

For terrorism risks, analysts evaluate threats by estimating the capability and intent of terrorists to carry out specific types of attacks against identified targets, such as driving a truck carrying a bomb into a facility in the Port of Miami or firing a shoulder-launched missile (MANPAD) at an aircraft from the perimeter of Los Angeles International Airport. Vulnerability is estimated in terms of physical accessibility and security defenses already in place to deter or prevent attacks. Finally, Consequence hinges on estimated impacts, such as loss of life and economic effects should an attack succeed.

For example, within DHS, the United States Coast Guard (USCG) has developed and deployed a maritime security analysis model (MSRAM).³ MSRAM analyzes the threat of terrorist attacks against 63 classes of potential targets in and around the nation's ports and waterways, including various types of passenger and cargo vessels, terminals and other port facilities, utilities, and other infrastructure. Twenty-three attack modes are proposed, such as aquatic mines or Improvised Explosive Devices (IEDs), small aircraft, bomb-laden trucks, and hijacked vessels used as weapons. MSRAM depicts the threat for each such target-attack mode pairings via quantitative estimates of terrorist intent and capabilities to carry out these scenarios, together with confidence levels in these judgments. These data are supplied by the USCG Intelligence Coordination Center (ICC).

MSRAM estimates vulnerability as a function of three factors: Attack Achievability, System Security, and Target Hardness. Attack Achievability is assessed in terms of factors such as geography, weather, and the complexity of the attack mode. System Security measures the capability of key government and commercial security authorities to interdict attacks. Finally, Target Hardness refers to the target's estimated capability to withstand particular attack modes, such as a bomb blast or release of toxic chemicals, and maintain operations.

Finally, MSRAM assesses the consequences of target-attack mode combinations in terms of estimated deaths, injuries, primary economic and environmental impacts, effects on national security, and symbolic significance. Economic impacts include property damage and immediate costs of disruption and substitution. Primary economic consequences can be mitigated by the capability of security actors to respond effectively to successful attacks; e.g., neutralizing attackers, putting out fires, providing emergency medical services, decontaminating sites, etc. MSRAM also attempts to estimate the secondary economic impacts of attacks, such as the net losses to commercial aviation from disruptions in air travel following the 9/11 attack. Mitigating factors for the component of consequence include redundancy of facilities (e.g., multiple cranes or docks) and preparedness to recover operational capabilities promptly.

The USCG deploys MSRAM as a PC-based application, backed by extensive training. Captains of the Port and their staff apply MSRAM to assess risks at their (local) level on an annual basis. The USCG rolls up MSRAM data and applies it to prioritize critical maritime security investments at local, regional, and national levels.

Managing Risk from Terrorist Threats

Once risks have been assessed through models such as MSRAM, the question naturally arises of reducing exposure to these risks. In other words, how do we *manage* risks once they are analyzed uniformly to allow ranking and other types of comparisons?

In particular, what allocations of and investments in new personnel, training, systems, technologies, and other resources will improve capabilities to prevent attacks and to respond effectively should interdiction efforts fail? How and when will these strategies reduce vulnerabilities and consequences? How robust are these strategies to changes in adversaries' tactics and weapons? Finally, how can risk mitigation activities and investments be managed as a diversified *portfolio* to maximize reduction of risk exposure not only across geographically distributed threats and targets, but also across plausible future conditions?

Managing risks from terrorist threats generally involves two types of situational interventions.⁴ First, exposure to risk can be addressed by reducing vulnerabilities. For example, buildings or building complexes such as ports or airports can be hardened by adding barriers around their perimeters, making them harder to attack with vehicles carrying bombs. Similarly, adding security patrols or sensor systems reduces vulnerability by

increasing the likelihood of deterring or interdicting terrorists before they can carry out their threatened attacks.

Second, assuming that attacks are successful, risk can be managed by improving response and recovery capabilities thereby minimizing or containing consequences. For example, improving communication systems and coordination capabilities of local law enforcement, other first responders, and relevant commercial or government property owners enhances response capabilities and mitigation consequences. These interventions can also reduce vulnerability by improving detect/decide/engage/defeat functions of system security.

Systems designed to analyze risk can often be extended to manage risk, at least at a basic level. First, one applies the given model to analyze risk at the present time based on inputs that describe the current security conditions (e.g., threats, vulnerabilities, and consequences). Next, one computes risk based on inputs that are altered to reflect one or more proposed security measures. Finally, comparing current risk to the risk projected for projected new security programs yields a differential analysis of risk management strategies. MSRAM, for example, provides this kind of "before-after" capability.

Additional Risk Mitigation Factors

We contend that methods for assessing risk mitigation strategies must reflect four additional critical factors in order to be truly effective. These factors relate to financial and dynamic temporal aspects of risk and risk reduction.

First, reducing risk (by improving security effectiveness) is not a discrete action undertaken at a single instant, but rather an extended *process* that is executed over time. In particular, security measures require months to years to develop, deploy, and perfect. They cannot simply be "switched on." And their success in achieving their objectives is by no means guaranteed: programs may be deficient in design or execution or they may not yield the anticipated effects. In short, managing risk involves a more granular approach than simply measuring risk exposure or reduction via "snapshot" measurements or extrapolations at discrete points in time.

Second, the risk "landscape" will inevitably evolve continually over the periods it takes to implement new security strategies: socio-political and economic conditions shift, technologies advance, and so on. Equally important, terrorist groups detect and respond to changes in their envi-

Decision Support for Countering Terrorist Threats against Transportation Networks

ronment, adapting their objectives, capabilities, tactics, and strategies accordingly. This includes working to circumvent announced security measures underway and/or shifting to other targets and methods. Risk management methods must explicitly anticipate the potential impact of these exogenous factors in designing and executing risk reduction strategies.

Third, from a policy standpoint, risk management strategies cannot be decoupled from their financial "footprints:" decisions to adopt new strategies must explicitly estimate the anticipated costs of competing approaches and weigh them against projected benefits. Cost-benefit tradeoffs (over time) are particularly critical to portfolio-based approaches to minimizing risk across threats and geographical locales.

Finally, focusing on cost and (change over) time materially affects the structuring of risk strategies. Currently, security programs tend to be designed monolithically, to achieve a specific level of risk reduction at some target point in the future. Real options theory suggests a more fine-grained approach.⁵ Originally developed for designing financial derivatives, options theory is increasingly used in high-risk, high-cost decisions involving drug research and development and manufacturing capacity. The core idea is to segment programs into smaller pieces with several checkpoints in the future where go/no-go decisions can be made based on the situation and value of the investment at those points in time. For example, factories can be designed in a modular manner to provide an initial expansion short-term, with options to expand incrementally (and cost effectively) if future product demand warrants it.

Security programs can be structured more flexibly through options to achieve escalating levels of protection that can be adopted to reflect risk exposure as it evolves over time. Terrorism is an economically asymmetric threat: our adversaries seek to provoke us to invest in ruinously costly national-scale countermeasures by carrying out (or merely threatening to stage) single attacks via new modes (e.g., chemical weapons, recruiting indigenous vs. foreign suicide bombers). A more adaptive approach that accommodates staging security programs to achieve deterrence before moving onto prevention is an essential enhancement in our thinking about counter-terrorism.

In short, analyzing risk tends to be a static activity anchored to specific points in time. However, risk evolves continually, driven by changes in the world at large. Correspondingly, managing risk is an inherently dynamic and, ideally, adaptive process: authorities must anticipate both the evolution of risks and extended program deployment cycles in devising new

security strategies, track risk reduction performance and changes in risk landscapes over time, and adjust strategies as appropriate.

The remainder of this article describes TRANSEC, a decision support tool that addresses these core aspects of managing terrorism risk. TRANSEC is implemented using advanced scenario-based "what-if" dynamic simulation and analysis software called ForeTell.⁶ The system helps authorities evaluate risk reduction strategies by projecting the consequences of proposed security measures and comparing their capabilities (and costs) to reduce risk from terrorist threats over time *and* across alternate future conditions.

Background—Terrorism Threats Involving Transportation Networks

TRANSEC addresses two categories of terrorist threats against transportation systems:

- Interdicting direct terrorist attacks against international transports such as vessels and aircraft and debarkation points such as ports and airports;
- Interdicting attempts to transfer individual terrorists or materiel into our country for purposes of carrying out attacks later.⁷

Domestic homeland security efforts today focus primarily on the first category ? threats of direct attack. As noted earlier, the canonical risk analysis construct is:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}.$$

Numerous challenges arise in estimating these three factors uniformly and accurately, but the basic framework is relatively clear.⁸

The *terror transfer threat* consists of the movement of terrorists and materiel (including components of weapons of mass destruction) into our country via independent transport modes from multiple countries and shipping points. Once inside our borders, terrorists and materiel can be moved via domestic transport modes and assembled to perpetrate attacks elsewhere.

Terrorist transfer threats are open-ended in nature because they involve the staging of resources into our country *prior to* attacks. The standard Risk construct does not apply because specific targets and attack modes are generally not known at this stage.

However, transfer threats cannot be ignored or dismissed simply because they are complex and challenging to model and analyze. On the contrary, we contend that the risks are too great *not* to attempt a systematic analytic approach, despite the inherent difficulties. In particular, we argue that making any progress on blocking transfer threats will reduce the scope of the "downstream" problem of interdicting terrorists as they attempt to launch direct attacks from within our borders. Hence, interdicting such piecemeal transfer threats *before* they penetrate our borders is a critical security priority.

TRANSEC—Decision Support for Managing Terrorism Risks in Transportation⁹

TRANSEC models risk assessments for both (or either) terrorist transfer and transportation system attack threats. It then models and helps refine and validate strategies for mitigating those risks. TRANSEC utilizes open source intelligence,¹⁰ expert judgments of security analysts, and inputs produced by other risk analysis tools such as MSRAM.

TRANSEC employs a dynamic multi-tiered decision model that abstracts terrorist threats into a network. The nodes of this network consist of the following entity types: Terrorist Groups, Countries of Origin, Points of Embarkation, International Transport Modes, Country of Destination, and associated Points of Debarkation. Figure 1 depicts this network model from a stylized geospatial perspective.

For transfer threats, TRANSEC breaks out two categories of risk—transfers of individuals and material from foreign countries to our borders. Examples of materiel include conventional and chemical, biological, radiological, or nuclear (CBRN) weapons (or weapon components).

For direct attack threats, TRANSEC focuses on two types of targets—Debarkation Points and International Transports. To minimize input requirements, the current version clusters attack modes into three categories: Emplaced, Standoff, and Hijack. Emplaced means that terrorists launch attacks aboard vessels, planes, trains, etc., while Standoff means

that attacks are staged from Debarkation Point perimeters. Hijack mode only applies to Transports and assumes that the terrorists use the plane or vessel as a weapon.

Figure 1: TRANSEC Transfer Threat Network Model

Following MSRAM's model for analyzing Risk elements, TRANSEC posits three distinct categories of *actors* with capabilities to detect and/or interdict terrorist personnel and materiel: national governments, local law enforcement agencies (LEAs), and owner/operators (OOs) of transport modes and supporting facilities. Each category of security actor has a distinct scope of authority, responsibilities, and operations; resources; and local presence.

For example, in maritime security scenarios, OOs are assumed to be commercial or civil entities that operate passenger or cargo vessels and terminal facilities at seaports. The lead domestic national authority for maritime security is the U.S. Coast Guard. LEAs in the United States include state and city police departments and emergency management agencies. Collaboration among security players to leverage complementary detection, deterrence, and engagement capabilities is critical for effective interdiction.

Decision Support for Countering Terrorist Threats against Transportation Networks

TRANSEC defines a set of quantitative performance measures, called System Security Effectiveness (SE) metrics. SE metrics are defined for each class of security actor and represent their capabilities to interdict transfer threats at Embarkation, Transit, and Debarkation points and to interdict attack threats at Transit and Debarkation points. These metrics are assigned values from 0 to 100 and can be annotated with comments. Table 1 summarizes TRANSEC's primary performance data elements. Data elements for direct attack threats are shown in *italics*; all other data support transfer threat modeling.

Table 1: TRANSEC Security Metrics

TRANSEC Entity	Security Metric/Datum	Metric Usage
Point of Embarkation	Security effectiveness of Owner/Operators, Local Law Enforcement Agencies, and National Government in Port vs. Transfer Threat of Terrorists and Materiel	Update
	Probability of Interdicting Terrorists and Materiel	Output
International Transport (by mode/category)	Security effectiveness of Owner/Operators, and National Government in Port vs. Transfer Threat of Terrorists and Materiel	Update
	<i>Security effectiveness vs. Standoff and Emplaced/Hijacked attack modes</i>	Output
	Probability of Interdicting Terrorists and Materiel	
	<i>Threat, Vulnerability, Consequence, and Risk of Attack via Standoff and Emplaced/Hijacked attack modes</i>	

Table 1: TRANSEC Security Metrics

TRANSEC Entity	Security Metric/Datum	Metric Usage
Point of Debarkation	Security effectiveness of Owner/ Operators, Local Law Enforcement Agencies, and National Government in Port vs. Transfer Threat of Terrorists and Materiel	Update
	<i>Security effectiveness vs. Standoff and Emplaced attack modes</i>	Output
	Probability of Interdicting Terrorists and Materiel Aggregate Transfer Threat of Terrorist and Materiel (broken out by Point of Embarkation and Intl. Transport)	
	<i>Threat, Vulnerability, Consequence, and Risk of Attack via Standoff and Emplaced attack modes</i>	

Decision Support for Countering Terrorist Threats against Transportation Networks

Additional inputs include:

- Estimated capability and intent of terrorist groups to initiate transfer threats of Terrorists and Materiel from specific countries¹¹
- Estimated capability and intent of terrorist group to carry out attacks against Transport and Debarkation Point nodes in Emplaced/Hijack and Standoff modes
- Factors contributing to Vulnerability and Consequence of attack modes relating to International Transport or Debarkation Point nodes (e.g., vessels, aircraft, ports)
- Assumptions about social, political, and economic forces; trends; and disruptive events that might take place over the duration of the security strategy¹²

Finally, TRANSEC models counter-terrorism strategies via sets of *security measures*. Each such measure specifies an allocation of existing resources and prospective investments to improve capabilities to interdict terrorist personnel and/or materiel prior to or upon arrival at our borders. Security measures are characterized in terms of three types of behavioral content:

1. Projected schedules to acquire or develop and deploy the given measure, depicted as start date and duration (in months);
2. Projected costs, expressed in terms of estimated capital expenditures (for start-up) and annual outlays for ongoing operations, maintenance, and support;
3. Expert assessments as to how the measures will likely impact particular SE metrics over time.¹³ TRANSEC's "what-if" capabilities allow analysts to explore the impacts of alternate assumptions about how benefits will occur or fail to materialize. The latter type of analysis is critical for assessing the potential impacts of delays, implementation errors, technology failures, and other types of programmatic risks on security effectiveness.

Table 2 lists several example Security Measures and their anticipated impacts. Generally, individual Security Measures impact only one or several of the SE metrics tied to risk from transfer or attack threats.

Table 2: Example Security Measures (and Strategies)

Index	Threat Type	Security Measure/ Strategy	Expected (Causal) Impact
1	Direct Attack	Security Training Program for aircraft crew	Reduce vulnerability to emplaced attack on aircraft
2	Direct Attack	Passenger Scanning Program for airport	Reduce vulnerability to emplaced attack on airport
3	Direct Attack	Procurement Program to develop Emergency Medical Services capability	Reduce consequence of attack on airport
4	Direct Attack	Combine Measures 1, 2, and 3	Combine impacts 1,2, 3
5	Transfer	Transportation Worker Identity Credential (TWIC) program	Reduce transfer threat at Debarkation Points by controlling individual access
6	Transfer	Overseas Port Security Program to coordinate with and certify security practices of foreign ports and authorities	Reduce transfer threat at Embarkation Points by controlling individual access and materiel
7	Transfer	Intl Maritime Org. (IMO) Shipper Security program to coordinate with and certify security practices of owner/operators of vessels	Reduce transfer threat at Intl Transport nodes by controlling individual access and materiel
8	Transfer	Combine Measures 5, 6, and 7	Combine impacts 6,7,8

These inputs—transportation network nodes, security strategies and measures, environmental assumptions and events—collectively define a TRANSEC *Scenario*. Figure 2 depicts the taxonomy of entity types used to build TRANSEC Scenarios.¹⁴

Decision Support for Countering Terrorist Threats against Transportation Networks

Figure 2: Entity Taxonomy for TRANSEC

The TRANSEC software system incorporates a "what-if" simulation engine that dynamically projects the likely impacts of Security Measures and environmental influences to generate the following outputs, in monthly increments:

- Updates to SE metrics at all nodes in the security network.
- Probabilities of interdicting terrorists and material at Embarkation, Transit, and Debarkation points.
- Net transfer threat risks of personnel and materiel at specific Points of Debarkation.
- These projected values are broken out by specific combinations of Terrorist Groups, Points of Embarkation and International Transport modes. For example, what is the risk of Transferring Personnel at the Port of Miami from al-Qaeda operating out of the Port of Athens via a break bulk cargo vessel?
- Updated estimates of Threat, Vulnerability, and Consequence and aggregate Risk for direct attacks, by mode, at International Transport and Point of Debarkation nodes.

For direct attack threats, TRANSEC employs the standard Threat, Vulnerability, and Consequence construct to compute Risk. For transfer threats, TRANSEC employs a probabilistic computation using SE metrics adapted from standard failure models used by system reliability engineers. TRANSEC employs various other simulation techniques to model environmental dynamics.¹⁵

TRANSEC's overall data processing architecture is summarized in Figure 3. Inputs are indicated in green, while outputs are labeled in blue. The upper half of the diagram addresses threat from direct attack, while the lower portion focuses on transfer threats.

TRANSEC provides powerful analytic tools such as summary reports and graphic plots to reduce simulation data. These tools help analysts quickly *compare* projected outcomes to isolate the *relative* strengths and weaknesses of alternate strategies across diverse scenarios. Analysts can also drill down to determine how forces, trends, events, and security measures impacted risk or cost in particular months. Users can refine their security strategies to incorporate attractive features of competing approaches. The resulting strategies are *robust* in that they leave the country well protected despite our inherent uncertainty about the future.

A strategy, no matter how robust, must be executed effectively in order to be successful. TRANSEC supports the post-decision phase of the strategic life cycle with a monitoring mode: as time passes, programs are enacted. All the while, social, political, economic, and technological conditions change and terrorist groups evolve, adapting their capabilities, objectives, and methods in response to the evolving landscape and their analysis of our defenses.

Decision Support for Countering Terrorist Threats against Transportation Networks

Figure 3: TRANSEC decision model architecture

Analysts use TRANSEC to update their Scenarios periodically to reflect current intelligence and re-project the chosen security strategy.¹⁶ If the projected outcomes are uniformly positive, the strategy has been revalidated. If not, TRANSEC acts as an Early Warning System, alerting authorities promptly to changing conditions and emerging problems. Analysts can diagnose the problems, alter (or replace) the current security strategy, and implement those midcourse corrections to ensure continued success.

The following figures illustrate sample outputs from TRANSEC, projecting counter-terrorism strategies described in Figure 2 above. For example, Figure 4 displays comparative time series plots projecting the reduction of risk for transferring terrorists for two strategies. As the key indicates, one set of curves assumes that a transportation worker identity credential (TWIC) program is implemented, while the other set assumes a broader program that implements security measures that impact Embarkation Points, Transport Modes, and Debarcation Points.

Figure 4: Example TRANSEC Time Series Output

Each curve depicts the risk for a transportation network path starting out from a particular Embarkation Point (e.g., Port of Athens) via one Transport Mode (e.g., a cruise ship) into one Debarcation Point (e.g., Port of Miami). In this scenario, it is assumed that in month 12, Turkey joins the European Union. The analyst postulated that the impact of this event would be to increase the baseline transfer threat out of Europe (but not Libya), under the assumption that Turkey's border security is inferior to that of European Union countries, allowing freer movement of terrorists across EU country borders.

Figure 5 displays the corresponding curves for the transfer threat of materiel. The lines signify no reduction of threats from materiel transfer ascribable to the TWIC program alone (as expected), while the curves for

Decision Support for Countering Terrorist Threats against Transportation Networks

the composite strategy (number 4 referenced in Figure 2) reflect threat reduction benefits from strategies targeting foreign ports and vessel operators.

Figure 5: Example TRANSEC Time Series Output

Finally, Figure 6 displays a spider (radar) chart comparing security effectiveness metrics for Strategies 1 (TWIC only, turquoise) and 4 (Composite strategy, red) four years into the future. Comparative analytics help decision-makers isolate relative strengths and weaknesses of security strategies and identify areas for refinement.

Figure 6: Example TRANSEC Spider (Radar) Plot Output

Conclusions

Managing risk from terrorism threats is a dynamic and adaptive process. Security strategies must anticipate ongoing evolution of environmental conditions and adaptive responses by terrorists in response to these changes and our defensive initiatives.

The critical challenge is to devise a collection of complementary security measures that address the diverse components of terrorist threats—targets and transfer nodes, attack modes, vulnerability, and consequence factors. Such strategic *portfolios* must (1) deliver broad spectrum risk reduction in a cost effective manner and (2) anticipate changing risk landscapes and incomplete knowledge.

Unfortunately, no one can predict the future reliably. Equally regrettably, no closed-end (computationally tractable) equations exist to "optimize" counter-terrorism preparedness investments.

TRANSEC aims for the next best thing, which is to identify and manage *robust* counter-terrorism strategies. A robust strategy is one that appears likely to produce superior reductions of risk across a range of plausible possible futures in comparison to competing security portfolios. TRANSEC employs scenario-based "what-if" simulations to model risk landscapes and explore and compare alternate strategies. Authorities can apply the same projective methods to monitor and adjust strategies as they are executed.

TRANSEC provides a safe virtual environment for practicing counter-terrorism strategies and learning from simulated rather than real mistakes. It thereby reduces risk and improves confidence and consistency in strategic security decisions. In essence, TRANSEC allows authorities to "test drive" strategies much as consumers test drive cars before buying them to minimize costly surprises and disappointments.

TRANSEC focuses on terrorism threats relating to transportation systems. However, its underlying decision support methodology and software tools are easily generalized to address other critical homeland security decisions such as critical infrastructure and border protection.

About the Authors

Dr. Richard Adler is Founder and Chief Architect of DecisionPath, Inc. He designed and implemented the company's ForeTell software platform for critical decision support and currently directs development and delivery of ForeTell solutions for government, and for the life sciences and financial services markets. ForeTell systems provide modeling, "what-if" simulation, and analysis capabilities to help clients "test drive" complex decisions including preparedness strategies for countering terrorist threats and managing organizational change. Before that, Dr. Adler was a partner at Computer Science Corporation, holding positions as the Solutions Architect for the company's Internet marketplace practice and software component framework for transactional business applications. Dr. Adler was previously VP of R&D at Symbiotics, Inc., a middleware software startup, and was a key member of the technical staff at the MITRE Corporation. Dr. Adler has over two decades of experience developing advanced software technologies and innovative systems architectures in business applications, mission-critical operations support, decision sup-

port, process control, modeling and simulation, and knowledge management. Dr. Adler has spoken and published extensively on topics including pandemic preparedness, counter-terrorism decision support, knowledge management, component software, executable specifications, intelligent systems, and software architectures for distributed control. He holds advanced degrees in Physics and Philosophy. Dr. Adler can be reached for comment at: rich@decpath.com.

Jeff Fuller is the Director of Homeland Security Services at Teledyne Brown Engineering, Inc. He has supported the U.S. Coast Guard Port Security Assessment program since its inception. Mr. Fuller has extensive experience with antiterrorism and security assessments, planning, training, exercises and program management for protecting military forces and critical infrastructure, crisis management, mission analysis and planning for homeland security, special operations, WMD counter-proliferation, conventional and joint military operations, and command and control. He served as Project Manager and Senior Analyst for the U.S.S. COLE Commission Support Team, led mission area analysis for Joint Chiefs of Staff, Antiterrorism Force Protection Directorate (J-34) and managed the Pentagon Antiterrorism/Force Protection Plan Project. He served as a Department of Defense Representative to the Department of Homeland Security Interagency Incident Management Group and the DOD Coordination Element at DHS. He has supervised security assessment and planning support for the Pacific Air Force, analytic and technical support to the Defense Threat Reduction Agency's Enhanced Joint Integrated Vulnerability Assessment Program, and execution and update of the JCS Web-delivered Antiterrorism Awareness Training program. Mr. Fuller was a Lt. Colonel in the U.S. Army and participated in four Special Forces assignments to include three command assignments. Mr. Fuller can be reached for comment at: jeff.fuller@tbe.com.

References

- 1 P. L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: Wiley & Sons, 1996). See also: R.A. Posner, *Catastrophe: Risk and Response* (New York, Oxford University Press, 2004).
- 2 Congressional Research Service, "DHS's Risk Assessment Methodology: Evolution, Issues, and Options for Congress," February 2007, available at: <http://www.fas.org/sqp/crs/homesec/RL33858.pdf>.
- 3 B. Downs, "The Maritime Security Risk Analysis Model," *The US Coast Guard Proceedings of the Marine Safety and Security Council*, Spring 2007, available at: <http://www.uscg.mil/proceedings/>.

Decision Support for Countering Terrorist Threats against Transportation Networks

- 4 Casualty Actuarial Society, Enterprise Risk Management Committee, "Overview of Enterprise Risk Management," May 2003. See also: Y. Sheffi, *The Resilient Enterprise* (Cambridge, MA: MIT Press, 2005).
- 5 M.A. Brach, *Real Options in Practice* (Hoboken, NJ: Wiley and Sons, 2003). See also: T. Copeland and P. Tufano, "A Real-World Way to Manage Real Options," *Harvard Business Review*, (March 2004): 91–99.
- 6 R.M. Adler, "ForeTell: A Simulation-Based Modeling and Simulation Platform for Homeland Security Decision Support," *IEEE Conference on Technologies for Homeland Security*, Cambridge, MA, Spring 2003.
- 7 One can view this as a third logical type of intervention, targeting Threat rather than Vulnerability or Consequence. In essence, interdicting transfers impacts the Capability component of Threats. In practice, it is difficult to influence Intent directly, although reducing Vulnerability and Consequence presumably impacts Intent (i.e., targeting strategy). Capability might also be targeted at a general level by disrupting communications, funding, etc., but this is challenging because of the highly decentralized organization of most terrorist groups into small, largely self-directed cells and the small scale of most attacks to date.
- 8 L. Cox Jr., "Some Limitations of 'Risk + Threat x Vulnerability x Consequence' for Risk Analysis of Terrorist Attacks," *Risk Analysis* 28, no. 6, (2008). See also: "DHS Risk-Based Grant Methodology is Reasonable, But Current Version's Measure of Vulnerability is Limited," *Government Accountability Office*, GAO-08-852, June 27, 2008. Finally, see: T.G. Lewis, *Critical Infrastructure protection In Homeland Security: Defending a Networked Nation* (Hoboken, NJ, Wiley-InterScience, 2006).
- 9 TRANSEC has been applied to a pilot aviation security project for the Government of Singapore's Joint Counter-Terrorism Centre. The U.S. Coast Guard is currently evaluating TRANSEC as part of its program to extend the risk management capabilities of MSRAM.
- 10 CIA World Fact Book, available at: <https://www.cia.gov/library/publications/the-world-factbook/index.html>. See also: National Consortium for the Study of Terrorism and Responses (START), University of Maryland, available at: <http://www.start.umd.edu/start/>.
- 11 Given specific intelligence, the user can override these Country level estimates at individual Points of Embarkation.
- 12 An example of a force would be that a declining economy reduces the volume of flights (and purchases) of private aircraft, which lowers terrorist transfer and attack factors at airports servicing this type of aviation traffic. An example of an event would be if a country, such as Turkey, is admitted to the European Union and its borders are considered less secure than other European nations, then transfer threat values will increase for all European Countries of Origin.
- 13 Analyst users capture these assessments via a curve fitting process. They specify a set of points whose x coordinate represents time (in months) and y coordinate represents % change (+/-) in the SE metric anticipated by implementing the given Security measure. Different measures have different profiles and impacts on different metrics. For example, training programs can typically be initiated relatively quickly, but their benefits level off, whereas new systems may require years to

Journal of Strategic Security

develop, deploy in pilot mode, and tune operations, resulting in a more lengthy and graduated curve of improvements, before tailing off (i.e., equilibrating). The TRANSEC simulator coerces the data into a polynomial or piecewise linear curve and applies it via a causality (system dynamics) simulation model.

- 14 The underlying ForeTell modeling software allows analysts to create and save a baseline Scenario comprised of relevant nodes (relevant instances of these entity types) and their initial conditions. Analysts can then copy and adapt that Scenario by selectively changing environmental assumptions or Security Measures. This design supports rapid creation of alternate Scenarios that can be projected and compared.
- 15 The ForeTell software underlying TRANSEC supports system dynamics, Monte Carlo methods, complex adaptive systems (agent-based simulation), process- and event-based simulation techniques, as required.
- 16 This often involves abandoning Scenarios that no longer appear plausible and adding new Scenarios based on emerging trends and patterns.