

Executive Summary: Decision Support for Counter-Terrorism Strategy (TRANSEC™)

Challenges for Counter-Terrorism Strategy

Improved intelligence sharing is helping Homeland Security authorities identify terrorist threats more effectively. However, this progress accentuates key “downstream” problems for leaders:

- Modeling and assessing credible but imprecisely defined threats
- Formulating cost-effective strategies to prevent, recover from, and respond to terrorist attacks
- War gaming strategies to better understand their consequences
- Adapting strategies as the security landscape evolves over time

Conventional decision support tools lack the horsepower required to address these needs effectively. Spreadsheets and simulation engines excel at manipulating numerical data, projecting quantitative trends, and the like. However, they fall short in modeling and reasoning about qualitative factors; complex relationships; uncertain information; and disruptive events. Thus, capturing and leveraging expert knowledge about terrorist behavior patterns and domestic vulnerabilities in traditional software is problematic.

DecisionPath has partnered with Teledyne-Brown Engineering, a leading government contractor and systems engineering company, to develop TRANSEC™, an advanced decision support tool for defining and validating counter-terrorism strategies.

Background - Homeland Security for National Transportation Networks

TRANSEC addresses two categories of terrorist threats against national 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.

Homeland Security efforts today focus primarily on the first category – threats of direct attack. The formula $\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$ drives standard risk modeling approaches. 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 port or hijacking a commercial airplane. Vulnerability is estimated in terms of physical accessibility and security defenses in place. Consequence hinges on estimated economic impacts (e.g., deaths, injuries, property damage, costs of disruption and replacement), symbolic significance and preparedness measures in place to mitigate those effects.

Terrorist transfer threats are more 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 not known yet. However, transfer threats cannot be ignored or dismissed simply because they are difficult to analyze. In addition, making 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.

Counter-terror security measures include developing new technologies, systems, and processes; hiring personnel; and training programs. The critical challenge is to identify and assemble security measures that address the components of terrorist threats – diverse targets and attack modes, vulnerabilities, consequences, and transfer risks – into a strategic “portfolio” that (1) delivers cost effective protection; and (2) is robust in the face of evolving security conditions, including terrorist groups adapting their strategies and tactics to try to defeat our defenses.



Executive Summary: Decision Support for Counter-Terrorism Strategy (TRANSEC™)

Technical Approach: ForeTell® and TRANSEC™

DecisionPath developed ForeTell® to address urgent decision support problems such as counter-terrorism. ForeTell combines a methodology based on scenario planning with powerful “what-if” simulation-based modeling and analysis software. ForeTell enables organizations to systematically explore and compare the likely outcomes of alternate decisions in a low-risk virtual environment, much as consumers test-drive cars before buying them. This approach allows authorities to practice strategies and learn from simulated rather than real mistakes.

DecisionPath partnered with Teledyne Brown to develop TRANSEC, which models counter-terror strategies for both transfer and direct attack threats. Primary inputs to TRANSEC include:

- Estimated effectiveness of system security by actors such as national governments; owners and operators of aircraft, vessels, ports, and airports; and local law enforcement agencies
- Intelligence about terrorist capabilities and intent to transfer personnel and materiel from foreign countries and to carry out attacks in emplaced (on-board/on-site) or standoff mode
- Candidate counter-terrorism measures, which are modeled in terms of projected schedules, costs, and most importantly anticipated impacts. That is, if measure X is implemented, how is it likely to affect TRANSEC’s security effectiveness metrics over time. Example measures include passenger screening systems and transportation worker identity credential programs
- Assumptions about social, political, economic forces and events that drive alternate futures.

ForeTell incorporates an advanced “what-if” simulation engine that processes these TRANSEC inputs to project the likely outcomes of counter-terror strategies across alternate scenarios. Key outputs are projected costs and values of security effectiveness metrics and risks. For transfer threats, TRANSEC projects probabilities of interdicting terrorists and materiel and net transfer threat risks at domestic debarkation points. For direct threats, TRANSEC projects Threat, Vulnerability, Consequence, and Risk for terrorist attacks from emplaced and standoff positions.

ForeTell provides powerful analytic tools such as summary reports and graphic plots to reduce TRANSEC simulation data. These tools help analysts quickly compare projected outcomes to isolate the relative strengths and weaknesses of alternate strategies across diverse scenarios. Users can then refine their decisions to incorporate the best features of competing counter-terrorism strategies. The resulting strategies are robust in that they leave the country well-protected despite our inherent uncertainty as to how the future will actually play out.

DecisionPath and Teledyne Brown are applying TRANSEC to assist the United States Coast Guard in extending their current risk management capabilities. We have also modeled aviation security strategies for the Joint Counter-Terrorism Centre of the Government of Singapore.

Bottom Line

TRANSEC increases the speed, quality, depth, and scope of critical decision-making processes. Its scenario-based “what-if” simulation capabilities can help Homeland Security authorities increase confidence and consistency and reduce risk in key counter-terrorism strategies.

For further information, please contact:

Dr. Richard Adler
President,
DecisionPath, Inc.
(617) 794-9036
rich@decpath.com

Mr. Jeff Fuller
Director of Homeland Security Services
Teledyne Brown Engineering, Inc.
(703) 731-2093
jeff.fuller@tbe.com

