Terrorist Decision Making (TDM™) - A New Paradigm in Aviation Security

Abstract

Terrorists have proven that they are highly adaptable, particularly as they search for new potential targets.

"Red Teaming", today's main method for detecting vulnerabilities, is a fine technique, but it is not up to the challenges in the fight against threats to the aviation sector.

In its search to improve aviation security, TAL Global developed Terrorist Decision Making (TDM™) – a method designed to "turn an organization against itself", in an effort to challenge aviation security layers, by teaching defenders to look at themselves through the eyes of the "bad guys".

The on-going Challenge of Protecting the Aviation Sector

Recent terror incidents in Brussels, Istanbul and the loss of Metrojet 9286 in Egypt, have demonstrated that terrorists have the capacity to adapt to compromise layers of security countermeasures. Unfortunately, in our zeal to protect ourselves from the next attack, the current emphasis on technological countermeasures focuses on yesterday's threat and usually does not give enough attention to "the human element" which evolves rapidly, creating ever-changing threat profiles.

"Red teaming" is today's main operational vulnerability-detecting mechanism. It not new by any means. Law enforcement agencies and infrastructure operators challenge the integrity and functionality of access control systems, security personnel and technologies used to detect a variety of threats. The purpose of a red team is to analyze the capabilities and expose vulnerabilities of people and/or systems by challenging their operation in real-time and real-life, while employing multiple attack vectors (e.g., people & technology).

Yet, red teams tend to focus on challenging existing vulnerabilities, such as physical access barriers, screening technologies and personnel. Red teams are not trained to look at existing vulnerabilities in the way a terrorist does.

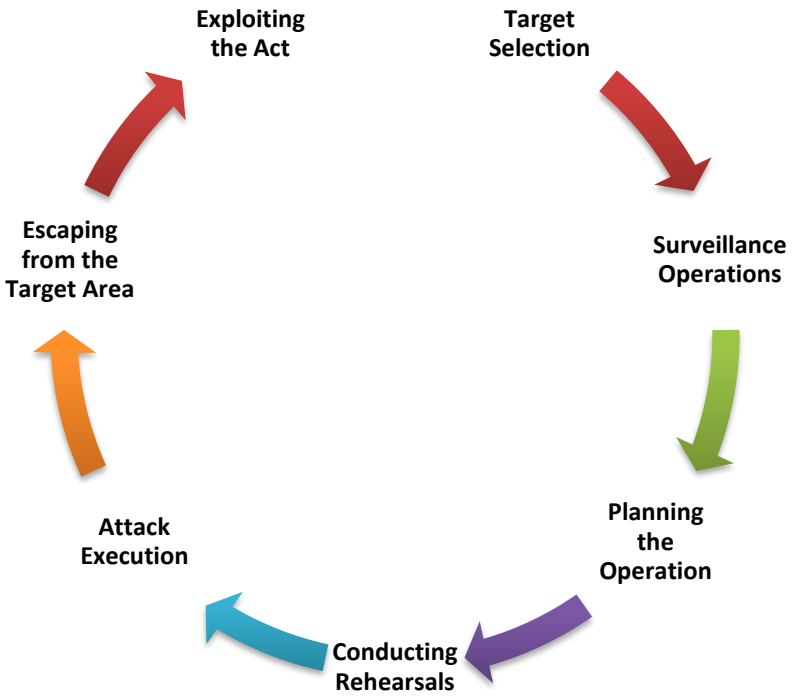
This is what Terrorist Decision Making (TDM™) methodology provides. TDM™ delivers an additional layer of proactive, counter-terrorism aviation security analysis and concrete security recommendations, designed to "turn an organization against itself", thereby challenging aviation security layers by looking at them through the eyes of the attacking "bad guys" instead of through the eyes of defenders.

Mitigating Risk by Thinking Like the "Bad Guys"

We know that a terrorist's target attack cycle looks something like this:

- ✓ Target Selection
- ✓ Surveillance and Reconnaissance Operations
- ✓ Planning the Operation
- ✓ Conducting Rehearsals
- ✓ Attack Execution
- ✓ Escaping from the Target Area (unless a suicide mission)
- ✓ Exploiting the Act

Figure 1: Terrorists' Attack Cycle



TAL Global believes that to counteract this sophisticated cycle requires a major rethinking and re-engineering of traditional approaches to aviation security. We need to shift the emphasis to thinking like the enemy. Under TDM™ we constantly ask ourselves: "What is the best way to attack to achieve our goals?" and "Are we doing all we can to reduce the risk of an attack? If not, what is missing?"

As part of its implementation, TDM™ employs specialized 'cells', each designed to emulate a terrorist's specific behavior, act or philosophy. For example, there is a "Shura Council", which imitates the terrorists' command organization, and is responsible for several actions, such as determining attack objectives and selecting targets.

TDM™ **Target Analysis Cell** will devote itself to the following tasks:

- ✓ All-source intelligence
- ✓ Characterization of the target's mission and objectives
- ✓ Determining economic vitality
- ✓ Considering population
- ✓ Determining local and global infrastructure importance
- ✓ Analyzing the perceived level of protection

TDM™ **Operations Cell** will promote the following agendas:

- ✓ Bringing in foreign assets
- ✓ Performing OSINT analysis
- ✓ Determining target viability
- ✓ Carrying out buffer zone considerations

Other Cells will perform additional tasks designed to bring the analytic power of TDM™ as close as possible to the target goal of emulating the thinking and actions of the "bad guys", thus being able to effectively address the vulnerabilities that may attract them to a specific target.

Together, these and other TDM™ Cells collect, analyze and refine the knowledge necessary to provide greater insight into the ways terrorists may look at vulnerabilities that could attract them to a specific target over another.

What Do You Get From TDM™?

Essentially, TDM™ provides better understanding of our adversaries and is a radical departure from security strategies that place all of our attackers into the single, one-size-fits-all, undifferentiated category of "terrorists".

For example, when it comes to aviation, TDM™ 's focus extends far beyond the physical area of the airport. This does so by taking into account all activities and facilities associated with the life cycle of passenger and cargo movement: transportation to and from the airport and associated facilities (e.g., tourist attractions, hotels, stadiums, convention centers) is part of one continuous chain of related elements, and therefore requires a holistic assessment of protection efforts from an intelligence, operations and logistics perspective – all taken from the adversary's view point.

This new perspective on critical infrastructure security means that key personnel must be familiar with the broader aspects of risk assessment methods, associated security technology, intelligence analysis, vulnerability and threat assessment procedures, emergency response and emergency recovery. These elements all come into play within a multi-layered, interagency environment, supported by a complex command, control and communications (C^3I) infrastructure. Meeting these demanding requirements requires the realization that early preparation and strenuous training are vital.

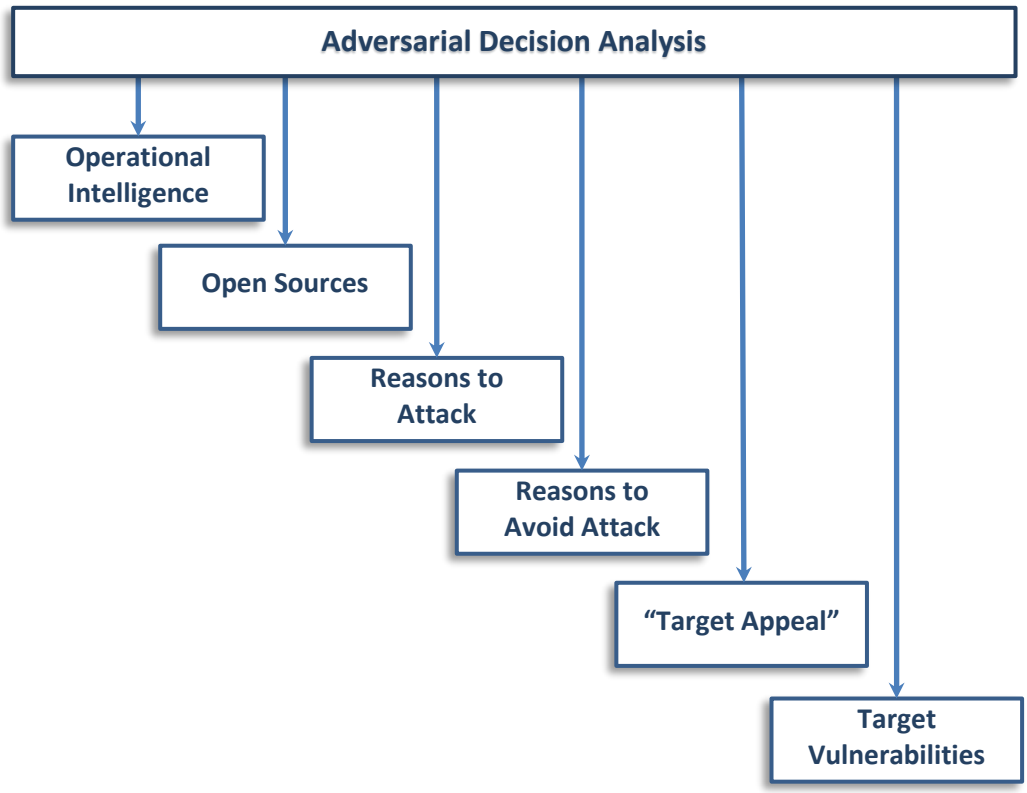
TDM™ – Deliverables

Naturally, TDM™ deliverables are unique to each client. The descriptions below are but a sample of a wide set of outcomes that flow from TDM™:

Adversarial Decision Analysis Outcomes:

- ✓ Identifying the level and content of operational intelligence the terrorist team can collect on the target(s) from open sources and with passive methodology.
- ✓ Learning *why* the terrorist team would/would not be reluctant to attack the target(s).
- ✓ Understanding what the terrorists might find appealing to attack at the target(s), and the vulnerabilities associated with those sites.

Figure 2: Adversarial Decision Analysis



Target Vulnerability Assessment Outcomes:

- ✓ The TDM™ Analysis will examine the efficacy and adequacy of countermeasures currently deployed in the target environment by understanding the reaction and response of the terrorists to these measures.
- ✓ Inasmuch as Islamic Jihadi terror groups demonstrate a propensity for simultaneous attacks, TDM™ would examine what other infrastructure sites would be attractive if attacked in concert with the target(s).

Beyond analysis and recommendations, TDM™ also delivers concrete and actionable products and services designed to continuously optimize the deterrent and defensive capabilities of the serviced site. This holistic suite of processes includes but is not limited to:

- ✓ Performing the necessary risk assessment for each specific venue and surrounding rings of relevance (transportation, residence, entertainment)
- ✓ Determining and acquiring the security workforce needed for the specific threat profile
- ✓ Establishing the required, secure communications topology and determining optimal communication technology
- ✓ Designing optimized access control policies, including screening and physical security
- ✓ Organizing the required intelligence and counter-intelligence infrastructure
- ✓ Supervising security aspects of the administrative and logistics support system
- ✓ Determining coordination needs with the necessary fire, EMS, medical and public health facilities
- ✓ Determining tactical support and crisis management needs and networks
- ✓ A thorough examination of potential vulnerabilities, threats and potential impacts on the relevant cyber environment

TDM™ in Action

TDM™ was developed by a multi-disciplinary team of seasoned experts in counter terrorism, aviation security, risk assessment and cyber security.

Dr. Erroll Southers, TAL Global's TDM™ leader, is the firm's Managing Director of Counter-Terrorism and Infrastructure Protection. Dr. Southers is former head of Homeland Security and Intelligence for the four Los Angeles World Airports' locations, as well as former Critical Infrastructure Protection Deputy Director for Homeland Security to California Governor Arnold Schwarzenegger.

Mr. Johnathan Tal, TAL Global's President and CEO brings with him a rich history of international aviation security work, investigations, and preventive operations.

Mr. Lawrence Dietz, COL (Retired), US Army, JD, and TAL Global's General Counsel and Managing Director of Information Security, is an authority on cyber security, psychological warfare, intelligence and legal analysis.

Mr. Lucien G. Canton, TAL Global's Managing Director of Emergency Preparedness and former Director for Emergency Services for the City & County of San Francisco, has over 30 years of experience in hazard and risk analysis, loss mitigation and emergency planning.

Together, the TDM™ team stresses that one-size-fits-all strategies are insufficient, and may fail to respond to the complex nature of potential threats. Their combined experiences brought them to the conclusion that an additional "game changer" element is needed in aviation security, and they are convinced that the TDM™ continuum provides an innovative way to examine terrorists' threats. It is designed to help defenders understand "why" a target is selected, in addition to the "traditional" questions of how a target may be attacked. Thus, interdisciplinary efforts are central to the development of more holistic notions of security and understanding of our enemy. TDM™ is a process that promotes rapid adaptation, as well as considerable savings of precious financial and operational resources.

Beyond TDM™

TDM™ is only one element of TAL Global's comprehensive transportation and critical infrastructure security solution. Additional comprehensive transportation and critical infrastructure security strategies include:

- ✓ The development and implementation of a unique Vulnerabilities Due Diligence Process, designed to identify and characterize operational and systemic vulnerabilities, which may expose the facility to increased risk from a terrorist attack.
- ✓ The planning and initiation of a collection of interdisciplinary countermeasures designed to blend passive and active counter measures aimed at mitigating threats to the airport environment using a combination of procedures, technologies and special training tools.
- ✓ Providing necessary testing, exercise, simulation and modeling tools required to probe and challenge the system constantly, evaluate its performance at the individual and system levels, identify weak links and take action to remedy and improve.

At TAL Global, we believe that our proactive approach is what airports and other aviation venues should take if they want to reduce the chance of a failure similar to the one that resulted in the downing last October of a Russian MetroJet flight 9268 from Sharm el-Sheikh, Egypt.