SANDIA REPORT
SAND2006-1484
Unlimited Release
Printed March 2006

Extended Defense Systems: I. Adversary-Defender Modeling Grammar for Vulnerability Analysis and Threat Assessment

Peter B. Merkle

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831
Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161
Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2006-1484
Unlimited Release
Printed March 2006

Extended Defense Systems: I. Adversary-Defender Modeling Grammar for Vulnerability Analysis and Threat Assessment

Peter B. Merkle, Ph.D., P.E.
Systems and Vulnerability Analysis
Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-0757

Abstract

Vulnerability analysis and threat assessment require systematic treatments of adversary and defender characteristics. This work addresses the need for a formal grammar for the modeling and analysis of adversary and defender engagements of interest to the National Nuclear Security Administration (NNSA). Analytical methods treating both linguistic and numerical information should ensure that neither aspect has disproportionate influence on assessment outcomes. The adversary-defender modeling (ADM) grammar employs classical set theory and notation. It is designed to incorporate contributions from subject matter experts in all relevant disciplines, without bias. The *Attack Scenario Space* $\mathbf{U_S}$ is the set universe of all scenarios possible under physical laws. An attack scenario is a postulated event consisting of the active engagement of at least one adversary with at least one defended target. *Target Information Space* $\mathbf{I_S}$ is the universe of information about targets and defenders. Adversary and defender groups are described by their respective *Character* super-sets, $\{A\}_{\mathbf{P}}$ and $\{D\}_{\mathbf{F}}$. Each super-set contains six elements: *Objectives*, *Knowledge, Veracity*, *Plans*, *Resources*, and *Skills*. The *Objectives* are the desired end-state outcomes. *Knowledge* is comprised of empirical and theoretical *a priori* knowledge and emergent knowledge (learned during an attack), while *Veracity* is the correspondence of *Knowledge* with fact or outcome. *Plans* are ordered activity-task sequences (tuples) with logical contingencies. Resources are the *a priori* and opportunistic physical assets and intangible attributes applied to the execution of associated *Plans* elements. *Skills* for both adversary and defender include the assumed general and task competencies for the associated plan set, the realized value of competence in execution or exercise, and the opponent's planning assumption of the task competence.

This page intentionally left blank

CONTENTS

ACRONYMS/KEYWORDS 7

1. EXECUTIVE SUMMARY 9

2. INTRODUCTION 10
The Need for Comprehensive Adversary-Defender Modeling (ADM) 10

3. THE ADVERSARY-DEFENDER MODELING GRAMMAR 11
Assumptions and Definitions 11
Common Notation and Definitions 11
Adversary, Defender, and Neutral Agents: Permissible States and Transition Rules 11
Examples of Agent States and Transitions 14
Adversary Notation and Definitions 15
Adversary Objectives, $\{ O_{i,j} \}$ 15
Adversary Target Knowledge, $\{ K_{k,j} \}$ and Veracity, $\{ V_{k,j} \}$ 15
Regarding Targets and Facilities 16
Adversary Attack Execution Plans, $\{ E_i \}$ 16
Adversary Resources, $\{ R_{k,j} \}$ 17
Adversary Skills, $\{ S_{k,j} \}$ 17
Defender Notation and Definitions 18
Defender Objectives, $\{ O_T \}$ 18
Defender's Adversary Knowledge, $\{ K_A \}$ and Veracity $\{ V \}_T$ 19
Defender's Operations Plans, $\{ E_T \}$ 19
Defender's Resources, $\{ R_T \}$ 20
Defender Skills, $\{ S_T \}$ 20

4. SCENARIO ANALYSIS USING ADM GRAMMAR 22
Extended Detection and Defense for a Fixed Site and Targets 22
Fictional Scenario: "Lights, Camera, Terror!" 22
Scenario Analysis 24
Scenario Commentary: The Value of Extended Detection and Defense 26

5. SUMMARY 28

6. REFERENCES 31

DISTRIBUTION 32

This page intentionally left blank

ACRONYMS/KEYWORDS

ADM	Adversary-Defender Modeling
DBT	Design Basis Threat
EM	Electromagnetic
GPS	Global Positioning System
IED	Improvised Explosive Device
JLB	Jihado Liberation Brigade
NNSA	National Nuclear Security Administration
PIDAS	Perimeter Intrusion Detection and Assessment System
VBIED	Vehicle-borne Improvised Explosive Device

This page intentionally left blank

1. EXECUTIVE SUMMARY

This work presents a formal grammar for the modeling and analysis of adversary and defender engagements of interest to the National Nuclear Security Administration (NNSA). Vulnerability analysis and threat assessment programs require systematic treatments of adversary and defender force capabilities for a variety of threats and defended targets. Attack detection and timeline analyses, tactical simulations, and scenario-based field exercises rely upon many assumptions about adversary and defender characteristics. Rigorous consistency throughout the analytical process is necessary, since unidentified or implicit assumptions and prior judgments may be influential. Analytical methods treating both linguistic and numerical information may ensure that neither aspect has disproportionate influence on assessment outcomes. The adversary-defender modeling (ADM) grammar employs classical set theory and notation. It is designed to incorporate contributions from subject matter experts in all relevant disciplines, without bias. The *Attack Scenario Space* $\mathbf{U_S}$ is the set universe of all scenarios possible under physical laws. An attack scenario is a postulated event consisting of the active engagement of at least one adversary with at least one defended target. *Target Information Space* $\mathbf{I_S}$ is the universe of information about adversaries, targets, and defenders. Adversary and defender groups are described by their respective *Character* super-sets, $\{A\}_P$ and $\{D\}_F$.

Adversary Character $\{ \mathbf{A} \}_\mathbf{P} = \mathbf{\{}\ \{ O_{i,j} \} \cup \{ K_{k,j} \} \cup \{ V_{k,j} \} \cup \{ E_i \} \cup \{ R_{k,j} \} \cup \{ S_{k,j} \}\ \mathbf{\}_P}$

Objectives Set = $\{ O_{i,j} \}$
Target Knowledge Set = $\{ K_{k,j} \}$
Veracity Set = $\{ V_{k,j} \}$
Attack Execution Plans Set = $\{ E_i \}$
Resources Set = $\{ R_{k,j} \}$
Skills Set = $\{ S_{k,j} \}$

Defender Character $\{ \mathbf{D} \}_\mathbf{F} = \mathbf{\{}\ \{ O_T \} \cup \{ K_A \} \cup \{ V_T \} \cup \{ E_T \} \cup \{ R_T \} \cup \{ S_T \}\ \mathbf{\}_F}$

Objectives Set = $\{ O_T \}$
Defender's Adversary Knowledge Set = $\{ K_A \}$
Veracity Set = $\{V_T\}$
Defender's Operations Plans Set = $\{ E_T \}$
Resources Set = $\{ R_T \}$
Skills Set = $\{ S_T \}$

Objectives are desired end-state outcomes. *Knowledge* is comprised of empirical and theoretical *a priori* knowledge and emergent knowledge (learned during an attack). *Plans* are ordered activity-task sequences with logical contingencies. Resources are *a priori* and opportunistic physical assets and intangible attributes applied to execution of associated *Plans* elements. *Skills* for adversary and defender include assumed general and task competencies for the *Plans* set, the realized value of task competence, and the opponent's planning assumption of the task competence. Subscript *k* denotes a specific target, and subscript *T* denotes a defender's threat assumptions for a given facility and target, such as a DBT statement.

2. INTRODUCTION

The Need for Comprehensive Adversary-Defender Modeling (ADM)

This work develops a structured grammar for the modeling and analysis of adversary and defender engagements in the context of extended defense systems. Such systems encompass extended detection capabilities in association with particular targets, as well as target-independent intelligence and warning. The ADM grammar accommodates explicit treatment of adversary and defender insider and defector elements.

The consequences of failing to secure critical strategic assets can be catastrophic (GAO, 2005). Extreme care in the planning and evaluation of security systems is indicated for this special class of targets; a formal and comprehensive grammar for adversary-defender engagements is warranted. While strategic assets have been successfully protected to date, the evolution of adversary threats requires constant innovation in security assessment technology and special care in treatment of novel threat capabilities. The grammar developed in this work is intended to serve as a universal framework for analysis of high security facility protection systems. It is designed to accommodate the diversity of subject matter expertise necessary for comprehensive assessment.

Vulnerability analysis and threat assessment programs require systematic treatments of adversary and defender force capabilities. Attack detection and timeline analyses, tactical simulations, and scenario-based field exercises rely upon many assumptions about adversary and defender characteristics. Rigorous consistency throughout the analytical process is necessary, since unidentified or implicit assumptions and prior judgments may be influential. Analytical methods treating both linguistic and numerical information should ensure that neither aspect has disproportionate influence on assessment outcomes. The adversary-defender modeling (ADM) grammar employs classical set theory and notation. It is designed to incorporate contributions from subject matter experts in all relevant disciplines, without bias. The grammar is scale-independent, and can treat adversary-defender engagements at any level of complexity. Scenarios, tabletop exercise scripts, tactical simulations, and field exercises are amenable to description by the ADM grammar.

3. THE ADVERSARY-DEFENDER MODELING GRAMMAR

Assumptions and Definitions

Common Notation and Definitions

Attack Scenario Space $\mathbf{U_S}$ is the universe of all possible attack scenarios $\varepsilon_{i=1,n}$ allowed under physical laws and logical constraints.

Target Information Space $\mathbf{I_S}$ is the universe of information (adversaries, targets, defenders).

1. An attack scenario ε_i is a unique sequence of postulated events requiring the active engagement of at least one adversary with at least one target.
2. Any attack scenario ε_i may become a realized attack event e_1.
3. Attack event e_1 is a unique attack undertaken by a specified adversary.
4. Attack event e_1 concerns a specified unique target ("target").
5. A target may or may not be defended.
6. Attack event e_1 may occur at least once in the lifetime of a defended target.
7. Attack event e_1 begins when an adversary with motivation and intent initiates information collection activity for a target or class of targets.
8. The attack event e_1 consists of two distinct activity phases:
    a. Adversary attack phase 1 (p_1): target selection, study, terminal attack planning
    b. Adversary attack phase 2 (p_2): initiation of the terminal attack sequence.
9. The defender of a target operates in two distinct activity phases:
    a. Defender phase 1 (d_1): defensive readiness and awareness for a target
    b. Defender phase 2 (d_2): terminal defense sequence (once an attack is assessed)

Adversary, Defender, and Neutral Agents: Permissible States and Transition Rules

An agent may be assigned to only one of the following states: adversary, defender, or neutral.

The neutral state (n_0) is defined as the condition in which one or more agents have no motivation or intent to attack or defend any target of interest to an adversary or defender, respectively.

An adversary (symbol "p" for perpetrator) must exist in at least one state. Motivation and intent state (p_0) is defined as the condition in which one or more agents have the desire and will to undertake an attack against an undetermined target of value to at least one adversary or defender.[1] No specific categories or particular targets may be known to the adversary in this state.

Attack state phase 1 (p_1) exists when an adversary in motivation and intent state p_0 initiates any information collection activity for at least one target or category of targets. This phase includes target selection, study, and terminal attack planning. Current motivation and intent p_0 are

[1] See reference cited, Center for Nonproliferation Studies (2004) for a more comprehensive treatment of adversary motivation and intent.

required for the p_1 state to persist. Within phase p_1, an adversary agent may become an insider within a defender group (Ins_{p1}), or withdraw to p_0 or n_0. Adversary defeat state p_{X1} exists when an adversary or adversary insider in phase p_1 is prevented from accomplishing a particular set of p_1 attack plan objectives. This may occur as a result of externalities, adversary incompetence, target-independent defender capabilities or the defender in direct physical association with the target defensive system itself.

Attack state phase 2 (p_2) is defined to begin with the initiation of the terminal attack sequence, in which an attack plan to achieve all final adversary objectives for the target is attempted. Current motivation and intent p_0 and prior p_1 state are required for p_2. An adversary may defect (Def_{p2}) to a defender group during p_2 (as p_0 becomes d_0) and become a d_2 agent in effect. Attack phase p_2 concludes when adversary objectives are accomplished (p_W), or the adversary withdraws (n_0), or is defeated. Adversary defeat state p_{X2} exists when an adversary, or defender defector, in phase p_2 is prevented from accomplishing a particular set of p_2 attack plan objectives, as a result of externalities, incompetence, engagement with target-independent defender capabilities or the defender in direct physical association with the target defensive system itself.

A defender (symbol "d") must exist in at least one state. Motivation and intent state (d_0) is defined as the condition in which one or more agents have the desire and will to defend at least one unspecified target of perceived value to at least one adversary or defender.

Defense state phase 1 (d_1) is defined as the condition in which a defender with motivation and intent maintains defensive readiness and awareness for at least one specified target. Current motivation and intent d_0 are required for the d_1 state. Within phase d_1, a defender agent may withdraw to p_0 or n_0, or become an insider within at least one attacking adversary group. Defeat state p_{X1} exists when a defender or defender insider in phase d_1 is prevented from accomplishing a particular set of d_1 defense plan objectives, as a result of externalities, incompetence, engagement with target-independent adversary capabilities or the adversary in direct physical association with the target defensive system itself.

Defense state phase 2 (d_2) is defined to begin with the assessment that a terminal attack is in progress. Current motivation and intent d_0 and prior d_1 state are required for d_2. A defender may defect (Def_{d2}) to an adversary group during d_2 (as d_0 becomes p_0) and become a p_2 agent in effect. Defense phase d_2 (the terminal defense sequence) concludes when defender objectives are accomplished (d_W), or the defender withdraws (n_0) or is defeated. Defender defeat state d_{X2} exists when a defender or adversary defector in phase p_2 is prevented from accomplishing a particular set of d_2 defense plan objectives as a result of externalities, incompetence, engagement with target-independent adversary capabilities or the adversary coming into direct physical association with the target defensive system itself. Adversary state p_2 does not require a d_2 defender state.

State d_1 does not require the existence of an adversary. State d_2 requires the presence of a real adversary in state p_2. Defender state d_2 activities in response to non-adversary phenomena are formally considered to pertain to state d_1. States d_w and p_w may exist simultaneously: both sides may "win". The attack objectives of an adversary may be accomplished while the defender also accomplishes its defense objectives. States d_{X2} and p_{X2} may exist simultaneously as well: both sides may "lose". An adversary may fail to accomplish its attack objectives, but in the process, the defense plan objectives may be denied to the defender. This grammar assumes that

accomplishment of any single attack or defense plan objective is a binary outcome of success or failure. Also, the global outcomes d_w and p_w are binary outcomes, in that a minimal set of plan objectives are accomplished to define a "win". Alternative "fuzzy set" descriptors of adversary or defender success or failure (and agent state) are possible and likely of value in further analysis, but are not treated here.

The special case of insider defection in d_1 and p_1 is permitted, with the agent permitted to become an opponent insider in their former group, or withdrawing to neutrality. An adversary in p_2 or defender in d_2 may not withdraw to p_1 or d_1 respectively: the attack objectives for each side must be resolved for the engaged agents associated with the target. Observers in either group during attack phases p_2 or d_2 are considered engaged. Other logical transitions are permitted, as depicted in Figure 1. Although these are not treated in this work, all other logically consistent transitions are allowed; agent transitions after attack resolution are not portrayed for simplicity.

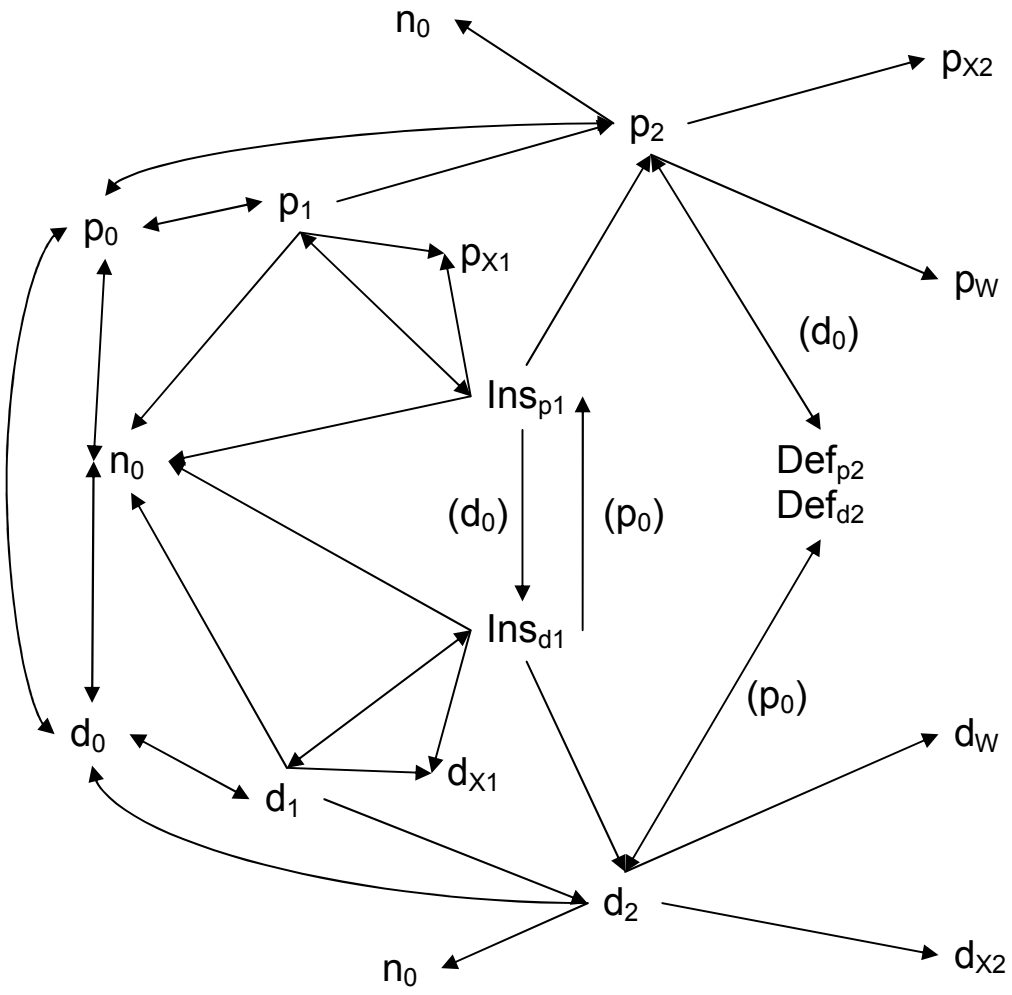

Figure 1. Permissible states and transitions for adversary, defender, and neutral groups.

Examples of Agent States and Transitions

The ADM grammar enables formal description of a wide variety of scenarios, illustrated in the following examples.

Scenario A: Cell Disruption

1. Ted, an immigrant to the U.S., becomes a citizen: $n_0 \rightarrow d_0$
2. Ted enlists in the U.S. Air Force and becomes a security guard: $d_0 \rightarrow d_1$
3. Ted takes a night class at the local university once a week: d_1
4. Bill is a foreign student in the U.S., and is influenced by radical clergy: $n_0 \rightarrow p_0$
5. Bill forms a cell to undertake violent acts of terrorism in the U.S.: p_0
6. The cell meets and selects a local U.S. Air Force base as a target: $p_0 \rightarrow p_1$
7. The cell membership grows at first, but some members drop out: $p_1 \rightarrow p_0$, n_0
8. The cell begins to research the Internet for information on the target: p_1.
9. Sally joins the cell. She knows Ted, and romances him to get information: $n_0 \rightarrow p_0 \rightarrow p_1$
10. Ted is suspicious of Sally, and reports to his security officer: d_1
11. Ted is asked by counterintelligence and police to help defeat the cell, and he agrees: d_1
12. Ted pretends to "fall in love", and gives her false information as a setup: p_1, d_1
13. On a bad tip from Sally, Bill conducts target surveillance and is arrested: $p_1 \rightarrow p_{X1}$
14. Sally is followed, and some cell members are arrested at their next meeting. $p_1 \rightarrow p_{X1}$
15. The cell falls apart as members scatter, some join other cells, some quit: $p_1 \rightarrow p_0$, n_0

Scenario B: Cell Penetration and Network Disruption

11. Ted is asked to penetrate the cell over a period of several months: d_1
12. Ted "quits" the Air Force. He is "radicalized" by Sally's influence: d_1
13. Ted is asked to join the cell eventually. $d_1 \rightarrow Ins_{d1}$
14. Ted helps the cell plan a major attack, providing false information: p_1 , Ins_{d1}
15. Ted is able to identify Bill's contact in the terror network. He tells the FBI: d_0, Ins_{d1}
16. The cell attacks at night, approaching the base on foot from the forest: $p_1 \rightarrow p_2$, $d_1 \rightarrow d_2$
17. The attackers are surprised in an ambush and arrested for interrogation: $p_2 \rightarrow p_{X2}$, $d_2 \rightarrow d_W$
18. The police round up several cells at other universities: $d_0 \rightarrow d_1$, $p_1 \rightarrow p_{X1}$

Scenario C: Adversary Defection

11. Ted never reports his suspicions about Sally: $d_1 \rightarrow d_{X1}$
12. Sally plants a keystroke logger on Ted's home computer: $d_1 \rightarrow d_{X1}$
13. With the stolen password, the cell obtains the base defense plan and other data: p_1
14. Bill orders Sally to break up with Ted. She has real feelings for him. Months pass: p_1
15. Suspicious vehicles painted like Air Force trucks approach the base: $p_1 \rightarrow p_2$, $d_1 \rightarrow d_2$
16. Sally is hidden in the woods, operating the remote control for the truck bombs. Looking through binoculars, she recognizes Ted in the guard station at the secure perimeter: p_2, d_2
17. Sally cannot harm Ted, and she detonates the bombs early: $p_2 \rightarrow Def_{p2}$
18. The attack force is killed. The guards are unhurt. Sally flees: $p_2 \rightarrow p_{X2}$, $p_2 \rightarrow n_0$, $d_2 \rightarrow d_W$

Adversary Notation and Definitions

The adversary is completely described by the Adversary Character Superset, $\{\mathbf{A}\}_{\mathbf{P}}$. This is a five element set containing all adversary attributes. Subscript P ("perpetrator) is a unique adversary identifier.

$$\{\ \mathbf{A}\ \}_{\mathbf{P}} = \{\ \{O_{i,j}\} \cup \{K_{k,j}\} \cup \{V_{k,j}\} \cup \{E_i\} \cup \{R_{k,j}\} \cup \{S_{k,j}\}\ \}_{\mathbf{P}} \qquad (1)$$

$\{O_{i,j}\}$ = Objective set for adversary attack event i

$\{K_{k,j}\}$ = Target knowledge for attack upon target k

$\{V_{k,j}\}$ = Veracity of adversary knowledge for attack upon target k

$\{E_i\}$ = Attack execution plan for attack event i

$\{R_{k,j}\}$ = Adversary resources for attack upon target k

$\{S_{k,j}\}$ = Adversary skills for attack upon target k

Adversary Objectives, { $O_{i,j}$ }

The adversary objectives set $\{O_{i,j}\}$ describes the intended end-state outcomes of a single attack event. The attack event may have multiple objectives and must have at least one. Rationality, feasibility, or potential for success from the defender perspective are not required for validity to the adversary.

Examples of adversary objectives for event e_1 for j = 1 to 4 are:

O_{11} = "Bring down the government"

O_{12} = "Humiliate the enemy in their homeland"

O_{13} = "Steal the Declaration of Independence without detection"

O_{14} = "Free the hostages by blackmail"

Adversary Target Knowledge, { $K_{k,j}$ } and Veracity, { $V_{k,j}$ }

The target knowledge set $\{K_{k,j=1,2,3}\}$ is a superset that describes the totality of knowledge about the target k at the command of the adversary.

$$\{K_{1,j=1,2,3}\} = \{\ \{K_{11}\}\ ,\ \{K_{12}\}\ ,\ \{K_{13}\}\ \} \qquad (2)$$

For j=1, $\{K_{11}\}$ is the empirical knowledge *a priori* phase p_2, concerning target 1, acquired by the adversary in attack phase p_1. The adversary forms empirical knowledge from access to

information within Information Space, $\mathbf{I_S}$. Photographs, maps, blueprints, and intercepted communications are examples of information sources that support the formation of empirical knowledge. Note that this category of knowledge does not necessarily require veracity as an attribute of set membership. For example, a blueprint obtained by theft may have been deliberately edited so that critical information is not included, or misinformation might have been substituted for the as-built design.

For j=2, $\{K_{12}\}$ is the theoretical knowledge *a priori* concerning target 1, developed in p_1. For example, an assumption about lighting conditions inside a facility, without particular objective information, is *a priori* theoretical knowledge: "There is adequate light inside the facility." Veracity is not a requirement for theoretical knowledge.

For j=3, $\{K_{13}\}$ is the emergent knowledge concerning target 1, acquired in p_2. Once the p_2 attack sequence begins, the adversary will learn information from target engagement, and develop empirical target knowledge or relevant theories. For example, an attacker may be fired upon from a hardened firing position not discovered during p_1, and assume it may be destroyed with a grenade. The knowledge of this position may be communicated to other attackers. Veracity (truth in fact or outcome) is not required for emergent knowledge. An associated veracity descriptor $\{V_{k,j}\}$ may be assigned to each element of $\{K_{k,j}\}$. Values for $\{V_{k,j}\}$ may be quantitative or linguistic. An adversary may assume a lock is "easy", when in fact it is "very difficult".

Regarding Targets and Facilities

The word "target" in the ADM grammar has both inclusive and specific meanings, depending on context. It may refer to all possible targets that exist in *Attack Scenario Space*, $\mathbf{U_S}$, or to classes of targets: physical objects, engineered system integrity and function, persons, or information. It may refer to a specific unique target: that parked car is a target for an auto thief, the River Bridge is the target of a terrorist, the database of XYZ credit card company is the target of an identity-theft ring. The target must be carefully distinguished from associated defensive systems or features of the target's proximal environment. The latter are termed *facilities*, defined as the integral surroundings and necessary associated systems where targets reside. A defender force is always associated with at least one target and a facility. Special cases exist: the defender force may be the target, the target may be the function of one or more facilities, or the defender force may be the "facility" in association with an otherwise unaccompanied target. For typical NNSA applications, one or more targets are located within a single defended facility.

Adversary Attack Execution Plans, $\{E_i\}$

The adversary attack execution plans set $\{E_i\}$ is comprised of elements that are nested activity-task sequences. A single plan developed during p_1 is initiated at the start of p_2, the terminal attack sequence, and may be altered within p_2. The plan may include logical contingency dynamics to accommodate conditional findings or outcomes during p_2. For attack event e_1, using plan E_1, the following simple plan illustrates the grammar.

$$\{E_1\} = \text{tuple, activities } W_{1n} = < W_{11}, W_{12}, \ldots W_{1n} > \quad (3)$$

$$\text{activity } W_{11} = \text{tuple, tasks } T_{11n} = < T_{111}, T_{112} \text{ or } T_{113} > \quad (4)$$

$$\text{activity } W_{12} = < T_{121} > = T_A^* = \text{critical adversary task} \quad (5)$$

The success of attack event e_1 is described in relation to the accomplishment of specific objectives concerning the target k =1. The competent execution of critical adversary task T_A^* achieves attack success. An activity consists of at least one task.[2]

Adversary Resources, { $R_{k,j}$ }

The adversary resources superset consists of physical assets and intangible adversary attributes applied to the execution of adversary plan $\{E_i\}$ on target k.

$$\{R_{k,j=1,2}\} = \{ \{R_{11}\} , \{R_{12}\} \} \quad (6)$$

For j =1, $\{R_{11}\}$ is the set of *a priori* adversary assets and attributes existing during attack phase p_1. These resource elements are subject to change during attack phase p_2 due to defender actions and adversary interactions with the target and facility. This set includes customary items such as vehicles, firearms, and passwords. Motivation, ideology, leadership, improvisation ability, health, intellect, and general knowledge are also included as intangible resources.

For j =2, $\{R_{12}\}$ is the set of emergent or opportunistic resources, including vantage point, cover and concealment, found objects, and improvised objects available in phase p_2. Commandeered vehicles or weapons are found objects that are opportunistic tangible resources. Adversary confidence resulting from successful accomplishment of intermediate attack plan tasks is an example of an emergent intangible resource.

Adversary Skills, { $S_{k,j}$ }

The adversary skills superset consists of the competency portfolio for tasks required in execution of the original attack plan and any contingency plan. The superset $\{ S_{1,j} \}$, for target k =1, is comprised of two sets:

$$\{S_{1,1}\} = \text{superset, requisite task competence for elements of attack execution plan } \{E_1\} \quad (7)$$

$$\{S_{1,2}\} = \text{superset, general competencies of universal utility} \quad (8)$$

The superset $\{S_{1,1}\}$ has three subsets:

$$\{S_{1,1}\} = \{ \{C_{TP}\} , \{C_{TR}\} , \{C_{TD}\} \} \quad (9)$$

[2] Once defined by ADM grammar, an adversary plan may be evaluated for internal consistency by vulnerability analysts and subject matter experts. Plan competence is distinct from plan definition. A given plan may be illogical or internally inconsistent. For a robust plan, task and outcome precedence must be respected and simultaneity of tasks must be considered. For example, an attack squad cannot storm a facility until after the perimeter fence is penetrated by their truck bomb. The implicit and explict contingencies and assumptions of a plan require evaluation as well. A large truck waiting outside a fence may be approached by police if noticed. Even though a second team may succeed in cutting power to the building, the truck is detained and neutralized. The adversary plan did not account for the contingency of discovery, making an implicit assumption that interdiction would not take place.

$$\{C_{TP}\} = \text{task competence assumed by adversary for } \{E_1\} \quad (10)$$

For each task T_{1nn} , there is at least one C_{TP} assumed by the adversary plan, based on the $\{K_{k,j}\}$, $\{R_{k,j}\}$, and other $\{S_{k,j}\}$ of the adversary characteristics.

$$\{C_{TR}\} = \text{the realized value of } C_{TP} \quad (11)$$

For each task T_{1nn} , there is at least one C_{TP} value including null if the task was omitted. Since the tasks are executed in a conflict environment that is imperfectly known by the adversary, tasks may not be executed successfully even if no defensive capability is met.

$$\{C_{TD}\} = \text{the defender's planning assumption of adversary task competence} \quad (12)$$

For each task T_{1nn} , there is at least one C_{TD} value including null if the task was not anticipated by the defender. Note that the defender may explicitly estimate the competence of an adversary in the design and operation of a defensive system. For example, a defender may assume that a computer firewall security system will detect all attempts at outside compromise, so that no outside adversary is assigned competence in the task of acquiring system administrator privileges without being detected. Alternatively, the defender may not anticipate the possibility of an adversary gaining the confidence of an insider, leading to a corresponding null value for C_{TD}.

Defender Notation and Definitions

The defender is completely described by the Defender Character Superset, $\mathbf{\{D\}_F}$. This is a five element set containing all defender attributes for facility F, and for all associated targets.

$$\mathbf{\{\ D\ \}_F} = \mathbf{\{}\ \{\ O_T\ \} \cup \{\ K_A\ \} \cup \{V_T\} \cup \{\ E_T\ \} \cup \{\ R_T\} \cup \{\ S_T\ \}\ \mathbf{\}_F} \quad (13)$$

$\{\ O_T\ \}$ = Defender objectives for target under assumed threat capability T

$\{\ K_A\ \}$ = Defender's adversary knowledge set

$\{\ V_T\}$ = Veracity of defender's knowledge

$\{\ E_T\ \}$ = Defender's operations plans set for target under assumed threat capability T

$\{\ R_T\ \}$ = Resources set available to defender under assumed threat capability T

$\{\ S_T\ \}$ = Skills set of defender under assumed threat capability T

Defender Objectives, { O_T }

The defender objective superset $\{O_T\}$ describes the intended end-state outcomes of defensive operations during any attack upon target k. Objectives are strategic and tactical. The defender may have multiple objectives in each subset, and must have at least one.

$$\{O_T\} = \{ \{O_{k,1}\}, \{O_{k,2}\} \} \quad (14)$$

$$\{O_{k,1}\} = \text{Strategic defender objectives, target k} \quad (15)$$

$$\{O_{k,2}\} = \text{Tactical defender objectives, target k} \quad (16)$$

Strategic defender objectives can include goals such as "deny access to the gold vault" or "recover the stolen gold if the vault is opened ". These objectives must be developed and deployed as operational guidelines before or during defensive phase d_1, prior to the initiation of the terminal attack sequence. Examples of tactical defender objectives are "hold position in the guard house until assistance arrives" and "cover all exits with suppressing fire". These objectives may be developed and adopted at any time during d_1 and d_2.

Defender's Adversary Knowledge, $\{K_A\}$ and Veracity $\{V\}_T$

The superset $\{K_A\}$ of the defender's knowledge of adversaries is comprised particular and general types, such that:

$$\{K_A\} = \{ \{K_j\}, \{K_P\} \} \quad (17)$$

$$\{K_j\} = \text{General adversary knowledge} \quad (18)$$

$$\{K_P\} = \text{Specific knowledge for adversary P} \quad (19)$$

For the defender, general adversary knowledge includes elements such as awareness of historical adversary characteristics and generic adversary scenarios. *Knowledge* of a particular adversary group includes elements such as identities, unique tactics and weapons. The defender forms empirical knowledge from access to information within $\mathbf{I_S}$. For each element of $\{K_A\}$, there is a corresponding *Veracity* descriptor set $\{V\}_T$ that may be quantitative or linguistic.

Defender's Operations Plans, $\{E_T\}$

A defender deploys systems and agents under an assumed threat, T, and develops defensive plans for normal and contingency operations. For j =1, $\{E_{k,1}\}$ is the set of *a priori* defender operations plans concerning target k that are developed during defense phase d_1. These encompass all tactics, techniques, and procedures for defender systems and agents. For j =2, $\{E_{k,2}\}$ is the set of emergent plans, devised in phase d_2.

$$\{E_T\} = \{ \{E_{k,1}\}, \{E_{k,2}\} \} \quad (20)$$

$$\{E_{k,1}\} = \text{a priori operations plans, phase } d_1 \quad (21)$$

$$\{E_{k,2}\} = \text{emergent operations plans, phase } d_2 \quad (22)$$

The defender plans set $\{E_{k,j}\}$ is comprised of elements that are nested activity-task sequences. A single defense plan is initiated at the start of d_2, the terminal defense sequence. The plan may include logical contingency dynamics to accommodate any conditional findings and outcomes emerging during defense phase d_2.

$$\{E_{k,j}\} = \text{tuple, activities } W_{1n} = < W_{11}, W_{12}, \ldots W_{1n} > \quad (23)$$

$$\text{activity } W_{11} = \text{tuple, tasks } T_{11n} = < T_{111}, T_{112} \text{ or } T_{113} > \quad (24)$$

$$\text{activity } W_{12} = < T_{121} > = T_D^* = \text{critical defender task} \quad (25)$$

The defender's success in defeating the p_2 phase of event e_1 is described in relation to the accomplishment of the specific objectives $\{O_T\}$ concerning the target k =1. The competent execution of critical defender task T_D^* achieves defender success. An activity consists of at least one task.

Defender's Resources, { R_T }

The defender resources superset consists of physical assets and intangible defender attributes applied to the execution of defender plan $\{E_T\}$ for target k, under assumed threat T.

$$\{R_T\} = \{ \{R_{k,1}\}, \{R_{k,2}\} \} \quad (26)$$

$$\{R_{k,j=1}\} = \text{a priori resources} \quad (27)$$

$$\{R_{k,j=2}\} = \text{opportunistic resources} \quad (28)$$

For j =1, $\{R_{11}\}$ is the set of *a priori* defender assets and attributes existing during defense phase d_1 for target k=1. These resource elements are subject to change during defender phase d_2 due to adversary actions and interactions with the target and facility. This set includes customary items such as vehicles, firearms, and site defensive systems. Ideology, leadership, improvisation ability, health, intellect, and general knowledge are considered intangible resources.

For j =2, $\{R_{12}\}$ is the set of emergent or opportunistic resources, including vantage point, cover and concealment, found objects, and improvised objects available in phase d_2 for target k=1. Opportunistic tangible resources may include items such as captured adversary weapons or ammunition. Defender confidence resulting from successful accomplishment of intermediate tasks is an example of an emergent intangible resource.

Defender Skills, { S_T }

The defender skills superset consists of the competency portfolio for tasks required in execution of the *a priori* defense plan $\{E_{k,1}\}$ and any contingency plan elements within $\{E_{k,2}\}$.

$$\{S_T\} = \{ \{S_{k,1,T}\}, \{S_{k,2,T}\} \} \quad (29)$$

The superset $\{ S_{1,j,T} \}$, for target k =1 and threat T, is comprised of two sets:

$\{S_{1,1,T}\}$ = superset, requisite competence for tasks in defense execution plan $\{E_{k,j}\}$ (30)

$\{S_{1,2,T}\}$ = superset, general competencies of universal utility (31)

The superset $\{S_{1,1,T}\}$ has three subsets:

$$\{S_{1,1,T}\} = \{ \{C_{DP}\} , \{C_{DR}\} , \{C_{DD}\} \} \quad (32)$$

$\{C_{DP}\}$ = task competence assumed by defender for elements of $\{E_{k,j}\}$ (33)

For each defender task T_{1nn} , there is at least one C_{DP} assumed by the defender plan, based on the $\{K_A\}$, $\{R_T\}$, and other $\{S_T\}$ of the assumed defender characteristics.

$\{C_{DR}\}$ = the realized value of C_{DP} (34)

For each defender task T_{1nn}, there is at least one C_{DR} value including null if the task was omitted. Since the tasks are executed in a conflict environment, defender tasks may not be executed successfully.

$\{C_{DD}\}$ = the adversary planning assumption of defender task competence (35)

For each defender task T_{1nn} , there is at least one C_{DD} value including null if the task was not anticipated by the adversary. Note that the adversary may explicitly estimate the competence of a defender in the design and operation of a defensive system. For example, an adversary may assume that a computer firewall security system will be easily and undetectably compromises, so that no competence is assigned to the defender task of protecting system administration access. Alternatively, the adversary may not anticipate the possibility of a defender placing an insider in a terror cell, leading to a corresponding null value for C_{DD}.

4. SCENARIO ANALYSIS USING ADM GRAMMAR

Extended Detection and Defense for a Fixed Site and Targets

Fictional Scenario: "Lights, Camera, Terror!"

"Dinero" is a high-security facility, located on a sprawling military installation in the desert of the southwestern U.S. The defense force personnel at Dinero are all U.S. Special Forces combat veterans. Selection, training, and periodic qualification standards are rigorous. Each member of the force is annually screened for physical and psychological health. A guard may only work 4 days a week in overlapping 10 hour shifts, with 6 hours on patrol, and 4 hours set aside for training, preparation, and reserve response duty. This restriction guarantees that an alert and capable protection force of at least 8 officers is on duty at all times, with 16 on standby alert when off duty. They are supplied with the best weapons and protective equipment ensembles available. Regular field exercises keep the defense force operating at peak effectiveness. The surrounding military base has a perimeter fence, a security police vehicle patrol, and guarded gates for entry by authorized personnel with vehicle permit stickers and base badges. Only 15 personnel are assigned to perform the critical mission functions at Dinero, they maintain 24-hour coverage in three-person teams.

Almost all members of the defense force live in or near Starville, a town of 10,000 people about 30 minutes east of the airfield. The nearest major city to Dinero is Jihado, 150 km north on the interstate. Operational security at Dinero is airtight. No one really knows what goes on there, but rumor has it that the U.S. Special Forces Command uses the site for critical mission planning and rehearsal. Some new large satellite dishes visible on public satellite photos have fueled Internet speculation that Dinero is much more than meets the eye. The local paper did a "what is it?" story last year that was widely picked up by the news wire services. The story described some new extended detection and weapons systems a local defense contractor had developed, and suggested these might be in use at Dinero.

A few klicks toward the scrub-covered hills on the main base road, a lone guard station marks a checkpoint entrance to the Dinero range area. Two base security police man the station 12 hours a day. During off-hours, the access road gate can be opened with a coded key and badge reader. By the time the police arrived every day at 0600, the duty and guard shifts at Dinero had already arrived at 0430, working on east coast time. Past the guard station, the paved access road continues for 500m to the crest of Heartbreak Ridge, overlooking an imposing structure in a large clearing. At Dinero itself, perimeter security features include exterior lighting and the latest Perimeter Intrusion Detection and Assessment System (PIDAS) technology with several remotely-operated machine gun emplacements. Planned additions to the facility include long-range radar and intelligent video detection and assessment systems.

Unknown to the Dinero defense force, they are being watched. Last year's news story caught the attention of Sally, a terrorist cell leader in Jihado. She became obsessed with Dinero, and organized a meticulous target analysis and reconnaissance effort. Her small group, the Jihado Liberation Brigade (JLB), swept the Internet and combed library archives for information on the

base and Dinero. Armed with topo maps and a GPS unit, two cell members were tasked to find a safe access route to Heartbreak Ridge. Posing as mountain bikers, they rode onto adjacent US Forest Service land and altered a section of the outer base fence to open easily while appearing intact. The pair subtly marked a path through dense scrub to a set of large boulders, a vantage point on the ridge, with lines of sight to both Dinero and the outer guard station on the base road. Their hide site was only 100m from where the access road began a gentle descent to the Dinero front gate, 200m away.

Sally's plan was to become a player, put her cell on the map, and strike a blow for the cause. Bill and Ted had no previous criminal backgrounds. Using false identities, they would rent an apartment in Starville and get access to the base. The base newspaper had lots of classified ads for unskilled part-time labor. With the job came a base vehicle permit and ID. Sally purchased two fairly decrepit-looking pickup trucks for her yard maintenance business, but made sure the engines and tires were sound, and added camper tops. Bill and Ted began commuting to the airfield in separate vehicles. They arrived as early as possible to the base gate every day, which opened at 0530, but never within 10 minutes of each other.

A tree at the hide site was outfitted with a gadget Ted devised. Two USB cameras, a wireless PDA, and a solar-powered recharger were placed in what looked like a squirrel nest. One camera watched the road, and the other watched DINERO. Sally was able to learn the patterns of activity 24 hours a day on her cable modem connection. She could see cameras and microwave dishes, and some other equipment on poles and the roof that was unidentifiable, but looked like some kinds of sensors. Bill and Ted made one last trip to the hide site to bury the parts of two improvised explosive devices (IEDS), made from stolen quarry dynamite and blasting caps. The final attack plan began just after dawn. Sally had camped out the night before, and carefully hiked into the hide site before sunrise. She assembled the IEDs; each weighed about 20 pounds. She had been lifting weights, just to make sure. Bill and Ted had filled 20 gasoline cans over the last few weeks, and loaded the back of each pickup with 50 gallons, in addition to the full tanks. On a cell phone text message signal from Sally, Bill and Ted timed their arrival at the outer guard station for 3 minutes after the first guard opened up, just after he swung the gate open. The second guard was almost always about 15 minutes late on Tuesdays, as he had to drop his kids off at daycare. Sally sent the all-clear signal: no vehicles were in the area. Smiling broadly, Ted waved the right color badge as the lone guard approached. He fell as Ted shot him twice in the face with a silenced pistol. Bill was already out of his truck and moving to drag the body into the station house. Both trucks then drove at normal speed up the access road.

At the spot where the access road entered the dense scrub, they turned off to the side before they would become visible to any high-tech Dinero sensor systems. Sally ran up with the IEDs and placed one in the back of each truck, arming them for remote detonation. She ran back to the boulders and grabbed her video camera and trigger remotes. Bill and Ted drove back onto the road and reached the crest just where Dinero came into view. Bill was first: he jammed the accelerator with a lever and jumped out as his truck began to speed down the hill toward the guard station. Ted waited 20 seconds and did the same. The first truck hit the fence about 10m from the guard station as Sally triggered the VBIED: a guard was killed. The second truck rolled toward the entrance. The gate had blown off in the first blast, and the second truck would hit the command center head on if it kept rolling. The alert remote machine gun operator began to direct

fire from all weapons at the truck, and the second VBIED detonated prematurely well outside the perimeter. Sally captured all the action on her video camera. Just in case, it also was being transmitted in real time from the "squirrel nest" back to her cell in Jihado. They had orders to rebroadcast it immediately via anonymous remailer and disband, sanitizing everything. The victorious trio ran as fast as they could back to the campsite, where they hopped into Sally's truck. Bill and Ted were arrested at a vehicle checkpoint near Starville later that day. Sally appears regularly on the popular TV show "America's Most Wanted" as the FBI's top fugitive.

Scenario Analysis

The adversary and defender character sets may be populated in summary form (but not exhaustively) using the scenario narrative.

$$\{\,\mathbf{A}\,\}_{\mathbf{P}} = \{\,\{O_{i,j}\} \cup \{K_{k,j}\} \cup \{V_{k,j}\} \cup \{E_i\} \cup \{R_{k,j}\} \cup \{S_{k,j}\}\,\}_{\mathbf{P}} \qquad (1)$$

$$\{\,\mathbf{D}\,\}_{\mathbf{F}} = \{\,\{O_T\} \cup \{K_A\} \cup \{V_T\} \cup \{E_T\} \cup \{R_T\} \cup \{S_T\}\,\}_{\mathbf{F}} \qquad (13)$$

The adversary succeeded in their attack objectives against the target, the Dinero facility (p_W).

$\{O_{i,j}\}$: O_{11} = cause spectacular explosions at the facility itself, with some fatalities
O_{12} = make a video of the attack for Internet broadcast with claim of responsibility

The defender force achieved their objectives for protecting the facility against threats (d_W).

$\{O_T\}$: O_1 = maintain 24-hour integrity of mission functions at Dinero facility
O_2 = prevent significant damage to critical systems
O_3 = prevent compromise of national security information
O_4 = prevent capture and transport of mission-critical personnel by adversaries

The adversary knowledge of the target and the facility was extensive, but incomplete.

$\{K_{k,j}\}$: K_{11} = video and visual surveillance data
K_{12} = patterns of activity and access procedures at Dinero, outer guard station, base gate
K_{13} = patterns of life activity for outer guard police force
K_{14} = public satellite imagery, terrain maps, facility and base maps
K_{15} = identification of Dinero as a target of value
K_{16} = defender weapons (machine gun installation was not known)

The defender knowledge of potential adversary threats was substantial, but incomplete.

$\{K_A\}$: K_1 = daily law enforcement and intelligence updates on threat conditions
K_2 = annual security training and in-depth threat assessment activities
K_3 = regular liaison activities with law enforcement and intelligence agencies
K_4 = adversary group profiles, tactics, techniques, and procedures (JLB cell not known)

The veracity of the adversary knowledge set was "very accurate" except for defender weapons.

$\{V_{k,i}\}$: $V_{1,1\text{-}5}$ = very accurate knowledge sufficient for confident planning and execution
$V_{1,6}$ = missing/inaccurate knowledge insufficient for confident planning and execution

The veracity of the defender knowledge was lacking in content on the JLB cell.

$\{V_T\}$: $V_{1,2}$ = very accurate knowledge sufficient for confident planning and execution
$V_{3,4}$ = missing knowledge of viable potential threat in facility area

The adversary terminal attack sequence plan was fairly simple.

$\{E_i\}$: E_1 = Sally arrive at hide site at 0500 and assemble IEDs, check batteries in "squirrel nest"
E_2 = Bill and Ted drive onto base at 0530 and 0540, respectively, link up near Dinero
E_3 = Sally call Ted when first guard arrives
E_4 = Bill and Ted drive up within 3 minutes
E_5 = All-clear signal from Sally: go or no go
If no go:
E_{51} = Ted expresses confusion, back trucks out, report to work as normal.
E_{52} = Sally returns to camp and drives away.
E_{53} = revise attack plan
If go:
E_6 = Ted kills guard.
E_7 = Bill hides body in station.
E_8 = Drive at normal speed and rendezvous with Sally in screened position
E_9 = Sally places IEDs in camper shells of each truck and runs to hide site to make video
E_{10} = Bill drives and directs truck toward Dinero from crest of ridge, jumps out
E_{11} = Ted waits 20 seconds
E_{12} = Ted drives and directs truck toward Dinero from crest of ridge, jumps out
E_{13} = Sally detonates first VBIED while taking video
E_{14} = Sally detonates second VBIED while taking video
E_{15} = Trio runs back to truck and escapes to fight another day

Some relevant elements of the defender's extensive operations plans were not executed competently.

$\{E_T\}$: $E_{1,1}$ = maintain two guards on duty at all times when outside gate is open
$E_{1,2}$ = one guard assists vehicle while one guard stands ready for intervention
$E_{1,3}$ = maintain video surveillance of outside gate from Dinero command post

Adversary critical resources were sufficient for success in phases p_1 and p_2:

$\{R_{k,j}\}$: $R_{1,1}$ = secure operations planning and communications site (Sally's business)
$R_{1,2}$ = physically-fit, motivated personnel
$R_{1,3}$ = improvised surveillance equipment using commercial components
$R_{1,4}$ = vehicles, IEDs, base passes

Given the threat assumption T, defender critical resources were sufficient for success in achieving defender objectives, but insufficent to prevent adversary success.

$\{ R_T \}$: R_1 = Outer guard station and personnel, PIDAS
R_2 = machine gun installations

Adversary skills were lacking only in the lack of command detonation for the second VBIED, and in the escape and evasion of Bill and Ted.

$\{S_{1,1}\} = \{ \{C_{TP}\} , \{C_{TR}\} , \{C_{TD}\} \}$

$\{C_{TP}\}$ = task competence assumed by adversary for all E_i = "high"
$\{C_{TR}\}$ = the realized value of C_{TP} = "low" for $E_{14, 15}$. "high" for all E_i ($i \neq 14, 15$)
$\{C_{TD}\}$ = the defender's planning assumption of adversary task competence = "low" for all E_i

$\{S_{1,2}\}$ = adversary general task competence = "high" for all E_i

The defender skills were lacking in key respects, enabling adversary success, p_W.

$\{S_T\} = \{ \{C_{DP}\}, \{C_{DR}\}, \{C_{DD}\}, \{S_{k,j=2,T}\}\}$

$\{C_{DP}\}$ = task competence assumed by defender for all $E_{k,j}$ = "high"
$\{C_{DR}\}$ = the realized value of C_{DP} = "low" for all $E_{k,i}$
$\{C_{DD}\}$ = the adversary planning assumption of defender task competence = "low" for all $E_{k,i}$

$\{S_{k,2,T}\}$ = general competencies of universal utility

For analysis of an actual site, greater detail is both possible and desirable, requiring full access to site facility, target, defense force, and threat information.

Scenario Commentary: The Value of Extended Detection and Defense

The design of the defender security systems at Dinero was deeply flawed. The standard PIDAS configuration was intended to detect and delay an adversary approaching by stealth, not an adversary arriving with speed and violence. The response force was intended to neutralize such an attacking force to protect the identified targets. The terrain around Dinero was not well-suited for a facility of its critical importance, as it permitted unrestricted and largely undetectable close access for surveillance. The location of outer guard station required perfect vigilance by the interior video assessment operator to detect the kind of attack used. On the morning of the attack, the operator was distracted for 30 seconds while the guard was shot. This unfortunate lapse allowed an adversary with two VBIEDs to approach within 200m of the facility undetected. An intelligent video detection system looking out from the perimeter and at the surrounding terrain was not yet operational. This could have detected the anomalous vehicles well before they reached the outer guard station. The smart camera system could have recognized the unusual posture of the guard who had been shot and the resulting alarm could have alerted the response

force to deploy or adopt a higher state of readiness. This alone could have deterred Sally from detonating the VBIEDs, as the JLB was not motivated to conduct martyrdom operations. Only the alert response of the machine gun operator reduced security force casualties and protected the target from significant damage.

Ideally, the JLB attackers should never have been able to approach Dinero and establish a vantage point and cache site. The ridgeline approach from the US Forest Service land could have been monitored with intrusion detection or deterrence systems, foiling the adversary in the attack planning stage p_1. Electromagnetic (EM) spectrum monitoring was not used at Dinero, as the site itself generated a large EM signature from its own communications. The outer guard post location was too close given the masked approach to the ridge crest, where a backup post would be prudent as well, given the terrain.

The adversary was competent, but somewhat fortunate. They were not aware of the machine gun installation or the cameras at the outer guard station. If they had not been very careful, they could have been spotted at any time while operating on the ridge. The distraction of the video assessment monitor at a critical time was simply lucky. The adversary attack objectives were unusual from the defender's perspective, although the VBIED attack means had been anticipated in the Dinero threat assessment and operations planning process. The site had not yet been fully re-engineered to deal with an evolving threat. In the attack scenario space $\mathbf{U_S}$ understood by the defender, the adversary was not deemed credible, or simply overlooked. The adversary perspective should have been adopted in scenario screening. Base security measures should have been more closely integrated with the Dinero site defense requirement. The lack of prior activity by the JLB in the area made law enforcement detection and warning practically impossible. A random vehicle check at the base gate could have discovered a gasoline payload.

The defender failed to understand the extent of their information footprint in the public domain. The information space $\mathbf{I_S}$ was a richly-detailed field of data. More importantly, the base and Dinero security architecture allowed the adversary to expand $\mathbf{I_S}$, by permitting undetected close access.

5. SUMMARY

Attack Scenario Space $\mathbf{U_S}$ is the universe of all possible attack scenarios $\varepsilon_{i=1,n}$ allowed under physical laws and logical constraints.
Target Information Space $\mathbf{I_S}$ is the universe of information (adversaries, targets, defenders).

1. An attack scenario ε_i is a unique sequence of postulated events requiring the active engagement of at least one adversary with at least one target.
2. Any attack scenario ε_i may become a realized attack event e_1.
3. Attack event e_1 is a unique attack undertaken by a specified adversary.
4. Attack event e_1 concerns a specified unique target ("target").
5. A target may or may not be defended.
6. Attack event e_1 may occur at least once in the lifetime of a defended target.
7. Attack event e_1 begins when an adversary with motivation and intent initiates information collection activity for a target or class of targets.
8. The attack event e_1 consists of four distinct activity phases:
    a. Adversary attack phase 1 (p_1): target selection, study, terminal attack planning
    b. Adversary attack phase 2 (p_2): initiation of the terminal attack sequence.
9. The defender of a target operates in two distinct activity phases:
    a. Defender phase 1 (d_1): defensive readiness and awareness for a target
    b. Defender phase 2 (d_2): terminal defense sequence (once an attack is assessed)
10. An agent may be assigned to only one of the following states: adversary, defender, or neutral.
11. A defender force is always associated with at least one target and a facility.
12. Transitions among states are specified in Figure 1 of this work. All other logical transitions are permitted.
13. The Adversary P Characteristic Superset is:

$$\mathbf{\{\ A\ \}_P} = \mathbf{\{}\ \{O_{i,j}\} \cup \{K_{k,j}\} \cup \{V_{k,j}\} \cup \{E_i\} \cup \{R_{k,j}\} \cup \{S_{k,j}\}\ \mathbf{\}_P}$$

$\{O_{i,j}\}$ = Objective set for adversary attack event i

$\{K_{k,j}\}$ = Target knowledge for attack upon target k

$\{V_{k,j}\}$ = Veracity of adversary knowledge for attack upon target k

$\{E_i\}$ = Attack execution plan for attack event i

$\{R_{k,j}\}$ = Adversary resources for attack upon target k

$\{S_{k,j}\}$ = Adversary skills for attack upon target k

Example: $\{E_1\}$ = tuple, activities $W_{1n} = < W_{11}, W_{12}, \ldots W_{1n} >$
activity W_{11} = tuple, tasks $T_{11n} = < T_{111}, T_{112}$ or $T_{113} >$
activity $W_{12} = < T_{121} > = T_A^*$

T_A^* = critical adversary task

$\{S_{k,1}\}$ = superset, requisite task competence for elements of attack execution plan $\{E_i\}$
$\{S_{k,1}\} = \{ \{C_{TP}\} , \{C_{TR}\} , \{C_{TD}\} \}$

$\{C_{TP}\}$ = task competence assumed by adversary for $\{E_i\}$
$\{C_{TR}\}$ = the realized value of C_{TP}
$\{C_{TD}\}$ = the defender's planning assumption of adversary task competence

$\{S_{k,2}\}$ = superset, general competencies of universal utility

14. The Defender F Characteristic Superset is:

$$\{ \mathbf{D} \}_{\mathbf{F}} = \{ \{ O_T \} \cup \{ K_A \} \cup \{ V_T \} \cup \{ E_T \} \cup \{ R_T \} \cup \{ S_T \} \}_{\mathbf{F}} \quad (13)$$

$\{ O_T \}$ = Defender objectives for target under assumed threat capability T
$\{ K_A \}$ = Defender's adversary knowledge set, $\{ V_T \}$ defender's veracity of $\{ K_A \}$
$\{ E_T \}$ = Defender's operations plans set for target under assumed threat capability T
$\{ R_T \}$ = Resources set available to defender under assumed threat capability T
$\{ S_T \}$ = Skills set of defender under assumed threat capability T

$\{O_T\} = \{ \{O_{k,1}\}, \{O_{k,2}\} \}$
$\{O_{k,1}\}$ = Strategic defender objectives, target k
$\{O_{k,2}\}$ = Tactical defender objectives, target k

$\{K_A\} = \{ \{K_j\}, \{K_P\} \}$, $\{V_T\}$ elements correspond to $\{K_A\}$
$\{K_j\}$ = General adversary knowledge
$\{K_P\}$ = Specific knowledge for adversary P

$\{E_T\} = \{ \{E_{k,1}\}, \{E_{k,2}\} \}$
$\{E_{k,1}\}$ = a priori operations plans, phase d_1
$\{E_{k,2}\}$ = emergent operations plans, phase d_2 Critical defender task = T_D^*
$\{R_T\} = \{ \{R_{k,1}\}, \{R_{k,2}\} \}$
$\{R_{k,j=1}\}$ = a priori resources, phase d_1
$\{R_{k,j=2}\}$ = opportunistic resources, phase d_2

$\{S_T\} = \{ \{S_{k,j=1,T}\}, \{S_{k,j=2,T}\} \}$

$\{S_{k,1,T}\}$ = superset, requisite competence for tasks in defense execution plan $\{E_{k,j}\}$

$\{C_{DP}\}$ = task competence assumed by defender for elements of $\{E_{k,j}\}$
$\{C_{DR}\}$ = the realized value of C_{DP}
$\{C_{DD}\}$ = the adversary planning assumption of defender task competence

$\{S_{k,2,T}\}$ = superset, general competencies of universal utility

6. REFERENCES

Center for Nonproliferation Studies (2004). "Assessing Terrorist Motivations for Attacking Critical Infrastructure." Monterey, CA.

U.S. Government Accountability Office (2005) Preventing Nuclear Smuggling, GAO-05-375, Washington, D.C.

DISTRIBUTION

2	MS9018	Central Technical Files, 8945-1
2	MS0899	Technical Library, 4536
1	MS0757	Peter Merkle, 6442
1	MS0757	Mark Snell, 6442

This page intentionally left blank