

APTIMA®
HUMAN-CENTERED ENGINEERING

Identification of Adversarial Activities:

Profiling Latent Uses of Facilities from Structural Data and Real-time Intelligence

Darby E. Grande, Aptima, Inc.

Georgiy M. Levchuk, Aptima, Inc.

E. Webb Stacy, Aptima, Inc.

Martin Kruger, Office of Naval Research

13th ICCRTS-2008

www.aptima.com
Boston • DC • Dayton



Problem & Challenges

The Problem

- Repetitive crimes are supported by an “invisible” supply chain that occupies physical locations
 - IED manufacturing
 - Nuclear power materials
 - Storage facilities
 - Hideaways
 - Meeting places, etc
- How can we **profile facilities** and decide where to focus concerted efforts to **disrupt** the adversary’s ability to perform its actions?

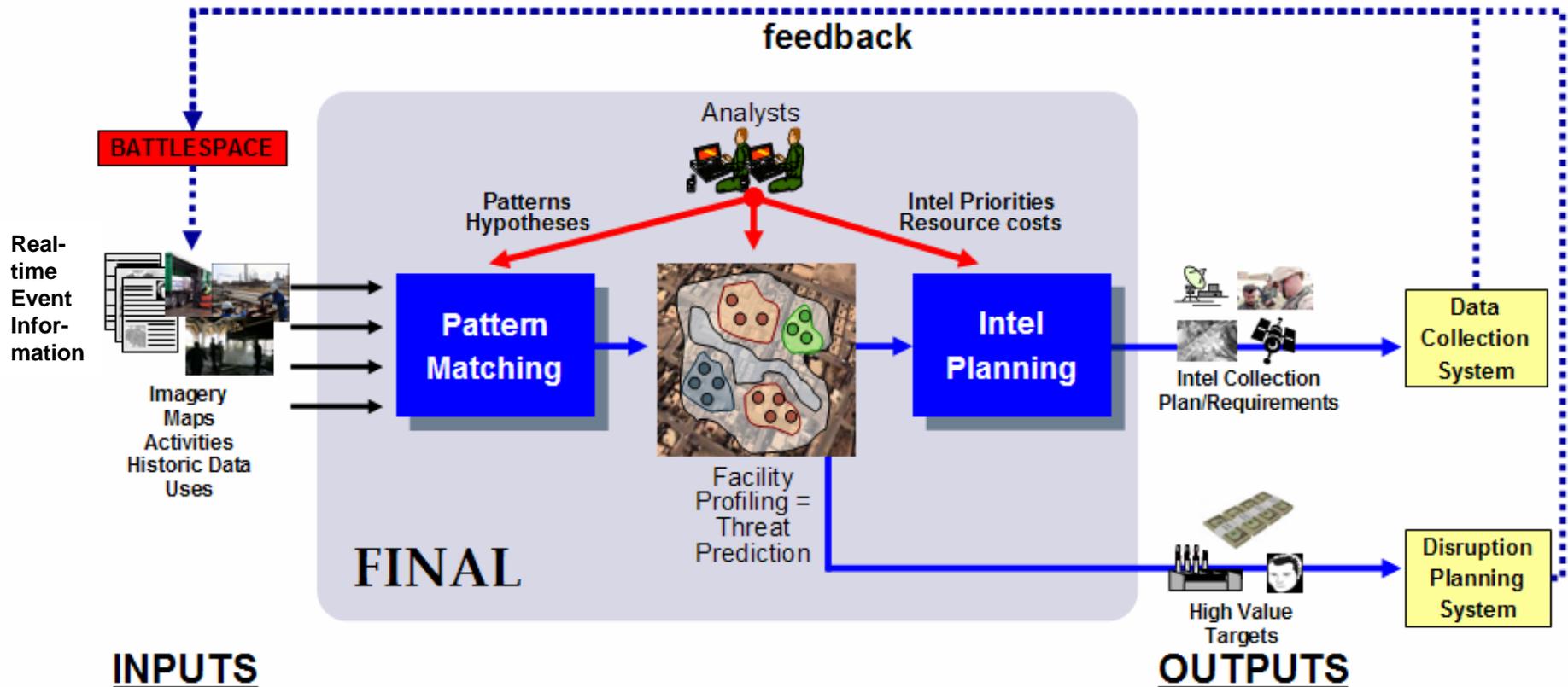


The Challenges

- Facilities’ normal use overlaps with nefarious use
 - Lots of irrelevant positives
- How can we predict use of facilities based on their features?
 - Many **features**, some cannot be directly observed; which to use?
 - Past uses of facilities matter (enablers)
 - Facility use follows a **pattern** (esp. with repeated use), with use of one facility depending on other activities and facilities
 - Normal and unusual
- Data quality
 - Multi-source data – overlapping and contradictory
 - Lots of noise (missing data, incorrect classification/detection, irrelevant data, deceptions)
 - Limited sensors (humans are “best sensors”!)
- Enemy is adapting
 - Change a pattern of facility use
- Large data complexity



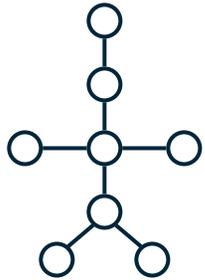
Conceptual Overview



Develop decision support tool for intelligence analysts and planners: find and disrupt facilities supporting criminal acts

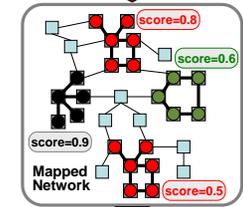
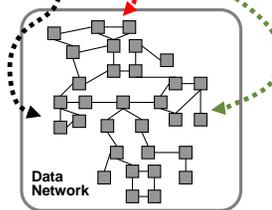
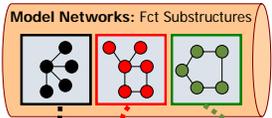
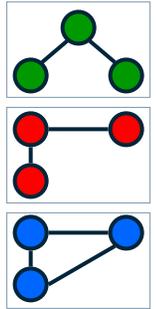


Pattern-matching Workflow

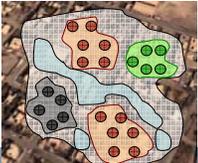


Data Networks
Facilities, Capabilities
and Connections

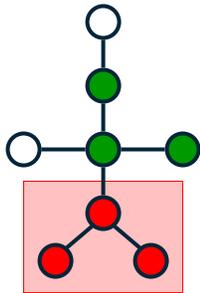
Model Networks
Functions, Patterns
and Activities



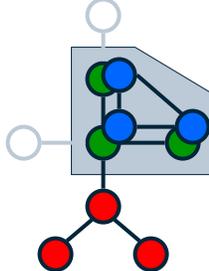
Threat Map



Matching
Map Functions on
Facilities = Threats



Searching
Matching Uncertainty
Reduction

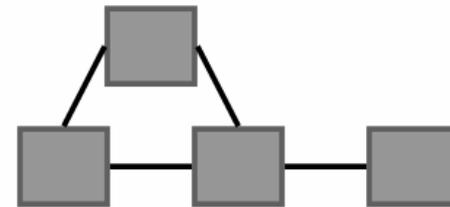
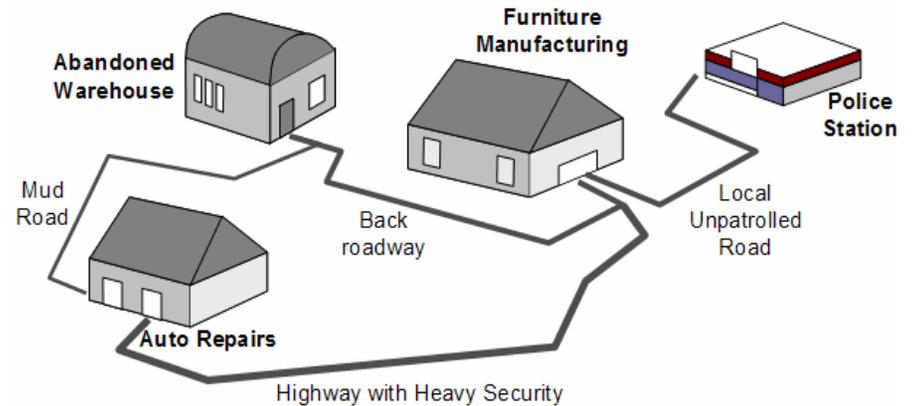




Facilities = OBSERVATIONS

Facilities are related in a pattern

- Info: geo-spatial & attributes information
- Nodes & links:
 - Capabilities = enablers
 - size of a building, the number of floors, the number and size of building entrances, and the height of the ceiling, etc.
 - Uses = attractors/generators
 - storage, gov/police use, educational, entertainment, commercial, residential, etc.

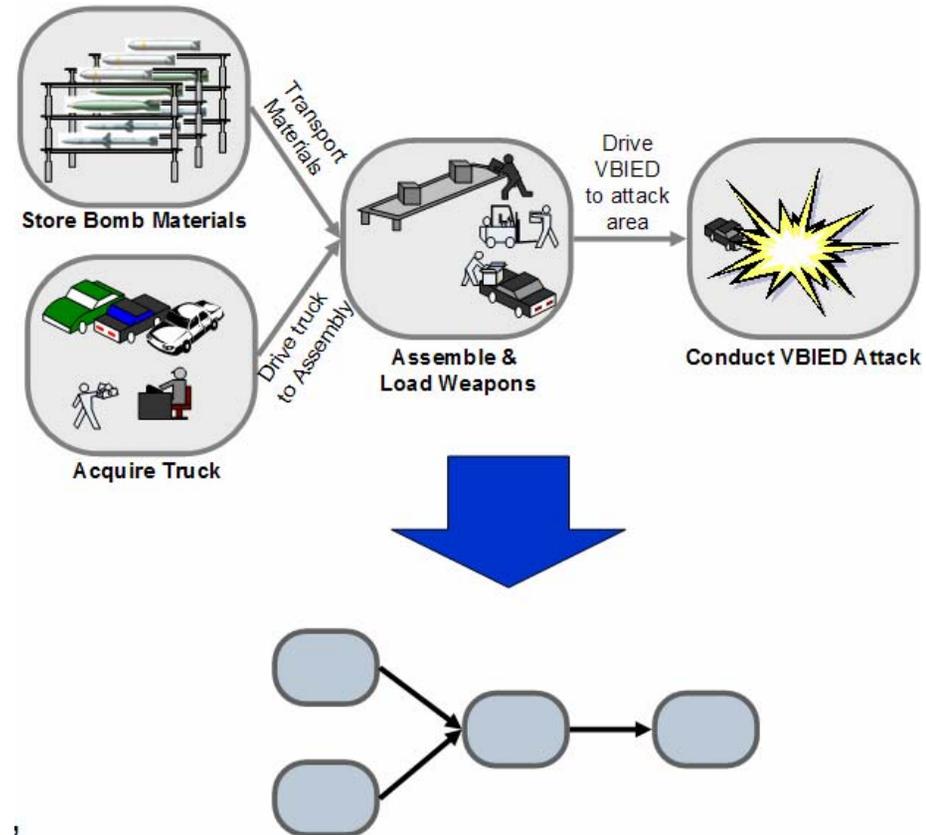


Patterns = **networks** with attributes on nodes & links



Actions occur in a pattern = RED Mission

- Info: historic data, expert hypotheses
 - patterns of potential RED activities
 - patterns of specific facilities utilization
- Nodes & links:
 - **Actions** or **functions** that RED wants to perform
 - weapons assembly, drug storing, hide-away, training ground, financial transaction, etc.
- Will comprise “hypotheses library”



Patterns = **networks** with attributes on nodes & links

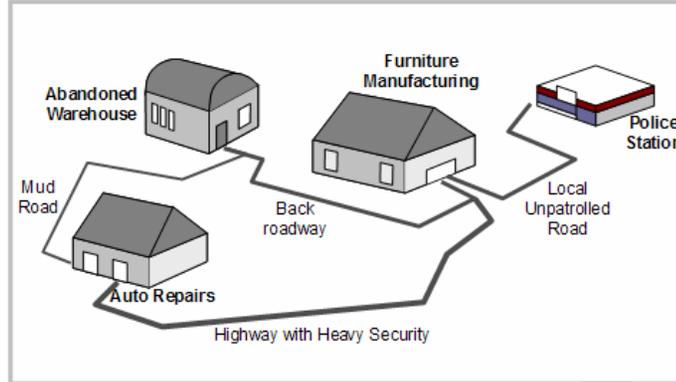


Mapping Actions on Facilities

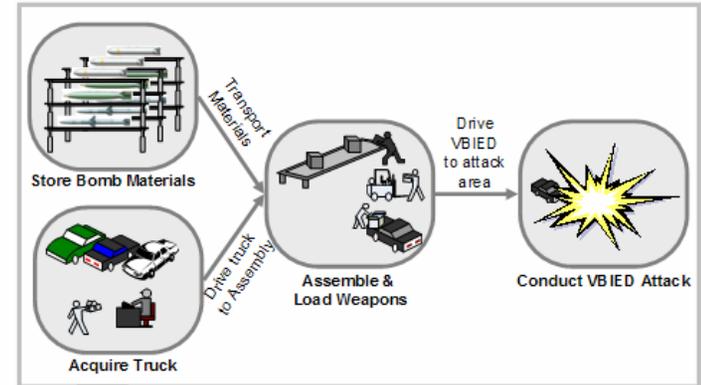
Node-to-node & link-to-link mapping:

- Structural network consistency
- Function-capability/use match

Data Network: Facilities, Capabilities, Connections

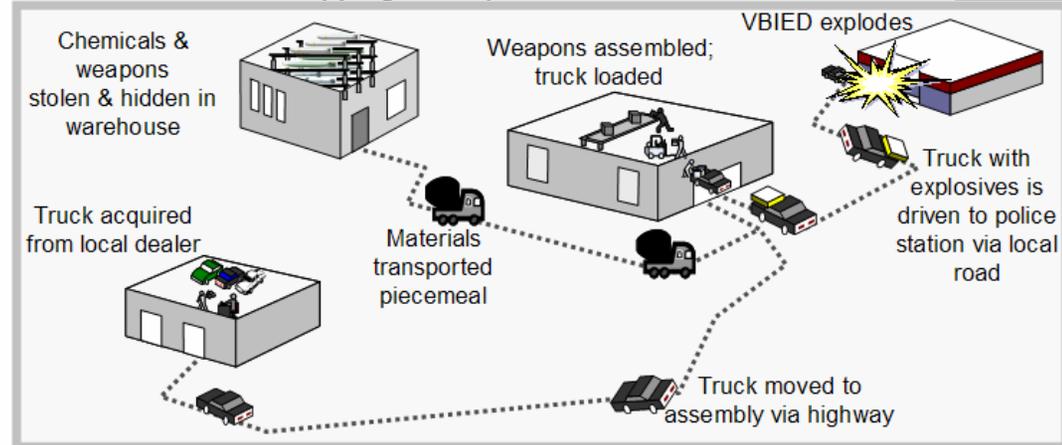


Model Network: Actions



Network Mapping

Mapping: Activity Conduct & Facilities Use



Need to know:

- Node (facility, function) and link (roads, transportation requirements) attributes
- Hypothetical function/activity patterns (models)

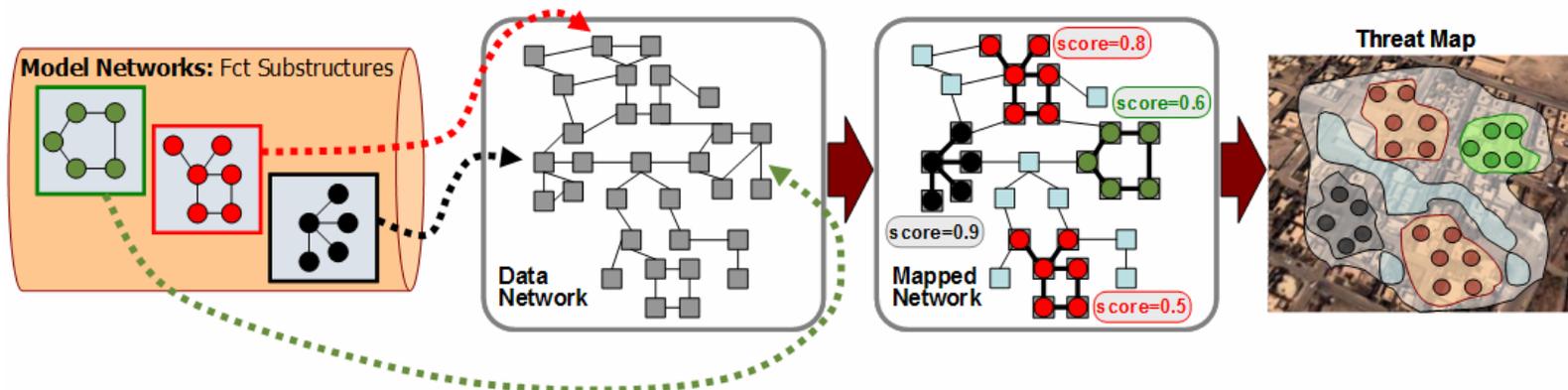


Summary Technical Approach: Action-Facility Mapping

GOAL: Develop algorithms to match activity patterns with facility structures

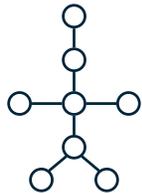
Approach: Pattern matching

- Map actions to facilities
- Score mapping using node-link match
- Rank-order threat activity patterns based on mapping scores
- Generate terrain threat map based on matched activities and mapped actions



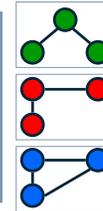


Mapping Formulation & Notations: Solving Quadratic Assignment Problem



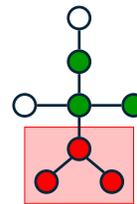
Data Networks
Facilities, Capabilities
and Connections

Model Networks
Functions, Patterns
and Activities



Map from “model” to “data”
▪ Allow multiple actions to
single facility mapping

Matching
Map Functions on
Facilities = Threats



$$S^* = \arg \max_S P(A_D | A_m, S)$$

$$\approx \arg \min_S \sum_{km;ij} S_{ki} S_{mj} \cdot C_{ki,mj} + \sum_{ki} S_{ki} \cdot C_{ki}$$

Link
mismatch

Node
mismatch

- Attributes:
 - A_M (model = action/function network)
 - A_D (data = facility network)

- **Outcome:** assignment matrix S

$$s_{ij} = \begin{cases} 1, \text{action } i \text{ allocated to facility } j \\ 0, \text{otherwise} \end{cases}$$

- **Objective:** Match between action model and facility node/link attributes

- **Solution:** Graduated assignment with stochastic soft-max approximation



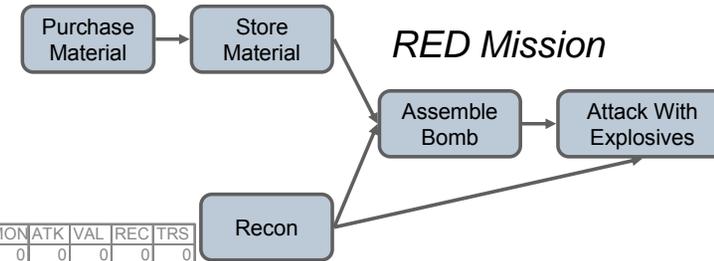
FINAL Constructive Simulation

Simulations inputs:

- RED, BLUE, GREEN (facilities), etc. organizations & actors
 - Locations, movement abilities, resource capabilities
- RED and BLUE missions
 - Tasks, precedence/transportation constraints, resource requirements and facility requirements, geo-spatial constraints, etc.
- Terrain
 - Roads, obstacles, etc.

Simulation dynamics:

- Actors move in environment and perform tasks from their missions in the precedence order
- Tasks are selected based on value & mission duration impact



RED Actors

Capability (what it CAN do)

	SZ	SEC	STR	MAT	TEC	KNW	MON	ATK	VAL	REC	TRS
BombMaker	0	0	0	0	0	1	0	0	0	0	0
Financier	0	0	0	0	0	0	1	0	0	0	0
Transportation	0	0	0	0	0	0	0	0	0	0	1
Recon	0	0	0	0	0	0	0	0	0	1	0

Mission Tasks

	Resource Requirements											Facility Requirements											
	SZ	SEC	STR	MAT	TEC	KNW	MON	ATK	VAL	REC	TRS	SZ	SEC	STR	MAT	TEC	KNW	MON	ATK	VAL	REC	TRS	
Purchase	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Store	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0
Recon	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	2	0	0
Assemble	0	0	0	1	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0
Attack	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	2	0	0	0

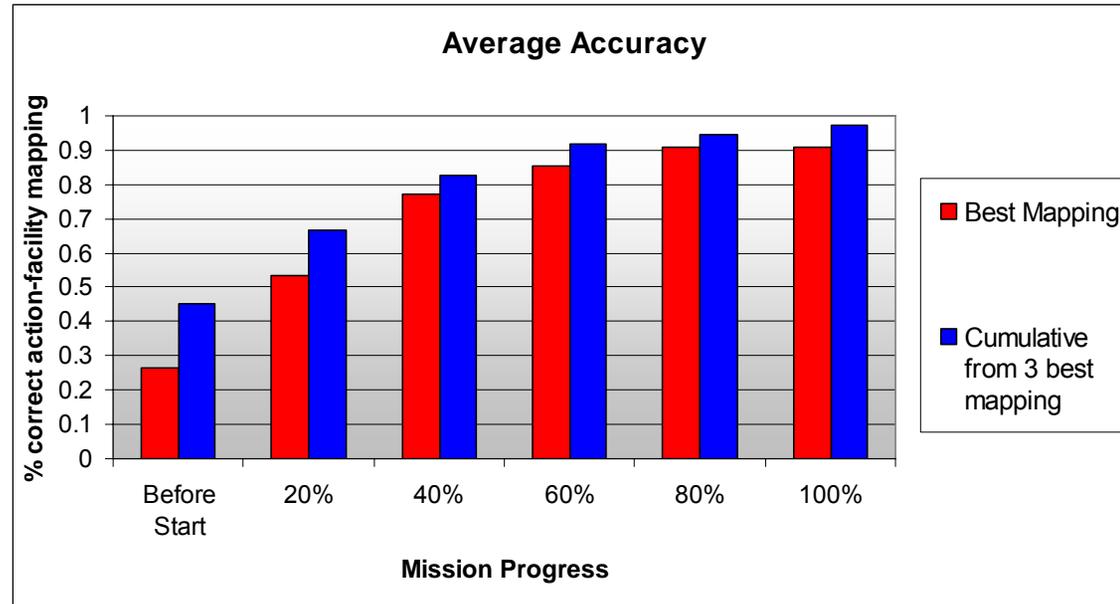
Facilities

	Capability (what it CAN do)											Vulnerability (what can be done TO it)											
	SZ	SEC	STR	MAT	TEC	KNW	MON	ATK	VAL	REC	TRS	SZ	SEC	STR	MAT	TEC	KNW	MON	ATK	VAL	REC	TRS	
BioLab	1	2	0	2	1	0	0	1	0	0	0	0	0	0	1	0	1	2	1	0	1	1	1
Mall	2	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	1	1	1
Airport	3	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	1	3	0	1	1	1
Park	3	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1
Residential	1	3	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	0	1
Commercial	1	0	1	0	1	0	0	1	0	0	0	0	0	0	1	0	1	2	1	0	1	0	1
Farm	3	3	3	1	0	0	0	0	0	0	0	0	0	0	2	0	0	1	0	0	1	1	1
Government	1	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	2	0	0	1	0
PublTrnsp	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	1	0	1
Hospital	2	1	0	3	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	1
Construction	2	2	1	0	2	0	0	1	0	0	0	0	0	0	2	0	1	0	1	0	1	1	1
Temple	2	4	2	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	1	0	1	0	1
Mansion	1	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1
School	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1
Bank	0	0	0	0	0	0	2	0	1	0	0	0	0	0	0	0	0	1	1	0	1	0	1
Car dealership	1	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0



Example of Sensitivity Analysis: Effect of Missing Intelligence Data

- Performed probabilistic classification over time based on prior knowledge & incoming intel
- Developed best 3 solutions, compared to ground truth
- Measured accuracy of detecting **correct action-to-facility allocation** over time in the mission
 - %Mission progress = 100 – %Missing Intelligence Data
 - Equivalent to judging impact of missing data

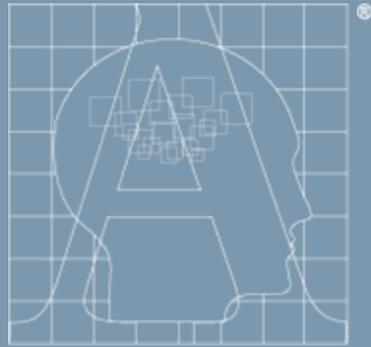


Conclusions:

- Can have high recognition even if limited intel collection has been possible

Results:

- Accuracy $\approx 66\%$ under 80% missing event data
- Multiple alternative solutions provide largest benefit under high missing data



APTIMA[®]
HUMAN-CENTERED
ENGINEERING