University of Connecticut

Aptima®
Human - Centered Engineering

www.aptima.com

NetSTAR: Identification of Network Structure, Tasks, Activities, and Roles from Communications

Georgiy Levchuk[1], georgiy@aptima.com
Kari Chopra[1], kchopra@aptima.com
Krishna Pattipati[2], krishna@engr.uconn.edu

[1]Aptima, Inc.
[2]University of Connecticut

10-th ICCRTS Mac Lean, VA, June, 2005
Track 1: *C2 Modeling and Simulation*

© 2005, Aptima, Inc.

A UNIQUE FOCUS ON HUMAN-CENTERED ENGINEERING

Overview

- The problem: notional scenario
- The need: design problem
- NetSTAR system process
- HMM-based activity modeling
- Previous work
- Next steps
- Example

Aptima®
Human - Centered Engineering

Notional Scenario

- **Mission:** US SOF assist the army of Urbanistan (AOU) in their spring offensive against the territories held by the militant rebel coalition called True Sons of Urbanistan (TSU).
- **Situation:** TSU irregulars are well concealed in towns and mountains of their Liberated Zone. Extensive system of tunnels and caves. Porous borders with neighboring countries.
- **Friendly intel capabilities:** US multi-INT capabilities plus Urbani Intelligence Service's extensive HUMINT.
- **Enemy Command and Control:** TSU is led by a network of several disparate organizations, ranging from informal cells to military structure.
- **Plan of the offensive:** AOU forces penetrate the Liberated Zone along 4 avenues of approach. NLT H+72 seal the borders. Defeat larger units of TSU with the help of US air assets and AOU armor. NLT H+240 force TSU fighters into several base towns. Isolate and conduct clean-up operations.

- **Current info on Enemy C2:**

#136: .....

#137: Abbadirov – commander of the Lions Brigade. Former Soviet Spetsnaz officer. Style of command decision-making: influenced by traditional Soviet.

#138: Lions Brigade Staff: 10-12 people, some with FSU military training.

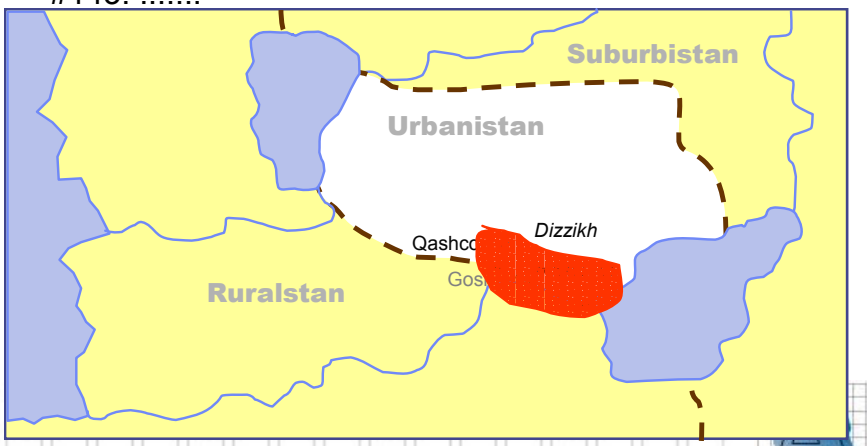
#139: Commander, Mountain Martyrs Detachment (name unknown). Uses cell system. Supported by an influential deputy and 2-3 senior advisers.

#140: Bobbimov: manages a logistics cell of 5-10 "brain" people in Gosh across the Ruralstan border. Supplies the Lion Brigade and sometimes the Mountain Martyrs.

#141: Qashcow Tribal Council: 10-15 people, control up to 200 local fighters. Report to Abbadirov but often stays neutral.

#142: Gollyadov: Field Commander of semi-independent formation. Staff of 4-7 competent personnel. Coordinates with Mountain Martyrs.

#143: .....



®

Aptima®
Human - Centered Engineering

Notional Scenario: Threats and Opportunities

Threats to the AOU Offensive Plan:

- Massive exfiltration of TSU into the Dizzikh region
- Rapid concentration in well-defended town of Eddiren
- Cross-border instigation of uprising in Ruralstan's town of Gosh
- .....

Feasible AOU Actions to Impact TSU C2:

- Feint advance toward the Qashcow tribal center.
- Precision elimination of Abdykadirov's Deputy
- Temporary disruption of comms between Gollyadov and Qashcow
- Disinformation about defection of Bobbimov to Government
- .... And about 50 other possibilities

Questions:

1. What combination and timing of actions would yield best observables to improve our knowledge of the TSU C2 structure?
2. What combination and timing of actions will best reduce the effectiveness of TSU C2 and minimize the threats to AOU plans?

The Need

- Need to **disrupt activities of the enemy**
- Consider enemy military with **significant** Command and Control (C2) organization
- TO **act** against enemy effectively, need to know:
  - What the enemy **IS**?
    - → Enemy C2 **structure**, roles, actors, resources
  - What the enemy **WANTS TO DO**?
    - → Enemy **goals/objectives**
  - What the enemy **DOES**?
    - → Enemy **actions**
- Need: **System Identification-like Models**
  - Focus on **what organization is** rather than ***how it can be changed***

How it is done today?

- What is available:
  - Manual procedures for analyzing enemy C2 decision-makers, processes, impacts
  - Commercial tools for data collection and visualization
  - Static networks topology metrics tools
  - Targeting heuristics (centrality, in-between-ness, etc.)

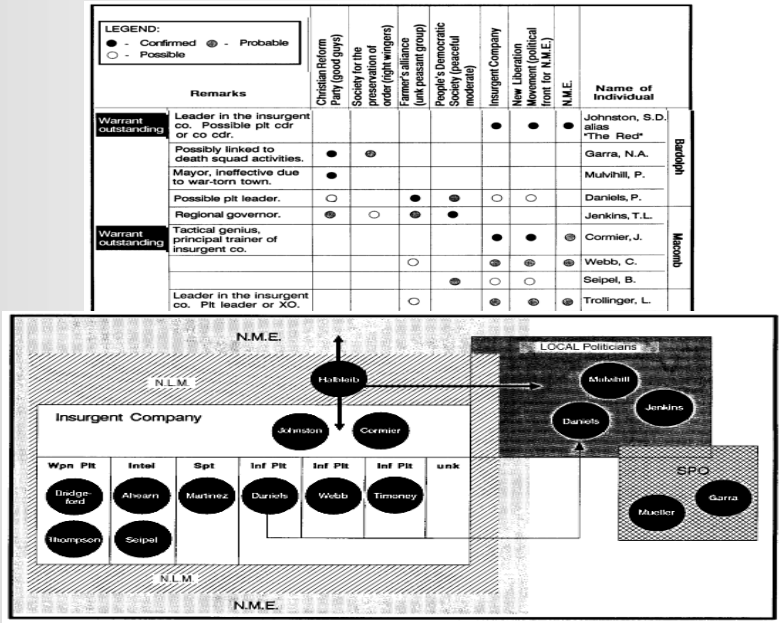


Figure 3-3-10. Link diagram.

Army FM34-130

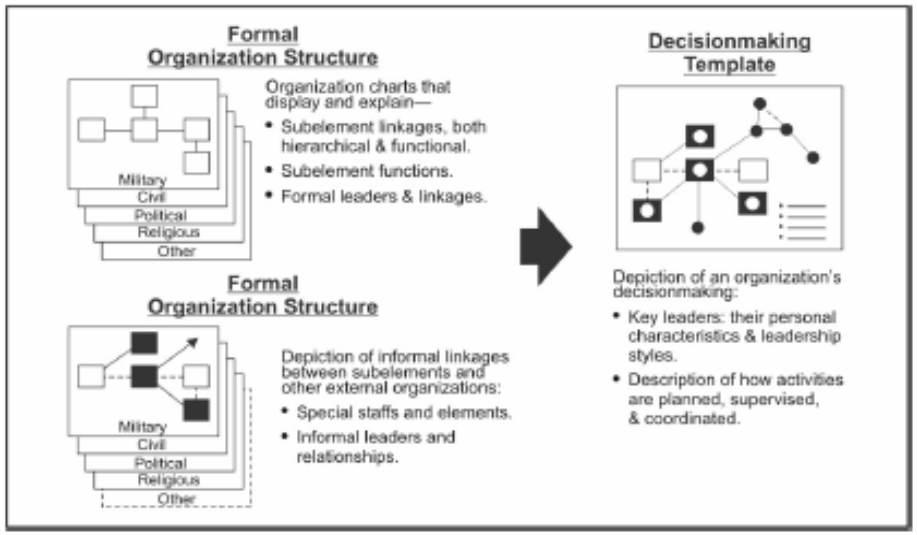
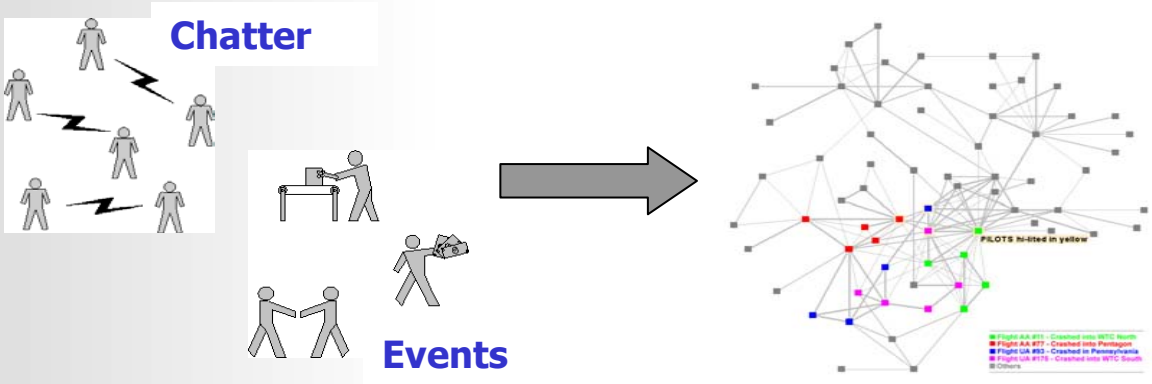


Figure 5-3. Sample Information Operations Doctrinal Template

Army FM 3-13, Information Ops

Aptima®
Human - Centered Engineering

Problem Identification



Question:

Given what we can observe about an enemy, can we determine its underlying structure and activities?

Answer:

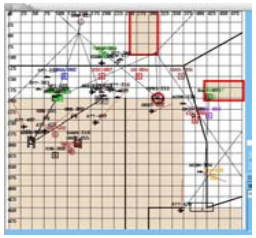
NetStar system for identification of Network Structure, Activity and Roles
Leverages models, algorithms, and test data from A2C2 program

Basis: A2C2 Experiments

Organization Library

Mission Library

Military Team: Process/Activity Models



Human-in-the-loop simulations: Distributed Dynamic Decision-making (DDD) Simulator

Activity Log

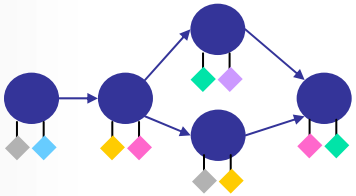
Agent	Start	End	Action
PARK	1401.10	1410.43	Clear mines
GARCIA	1405.07	1412.32	Blow bridge

Communications Transcript

Sender	Receiver	Start	End	Content
KLEIN	PARK	1400.03	1400.07	"Can you clear out those mines?"
PARK	KLEIN	1400.10	1400.12	"I'm on it."

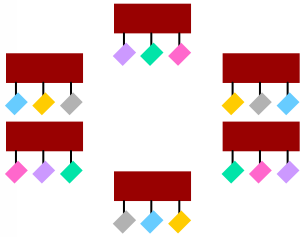
Idea

Mission



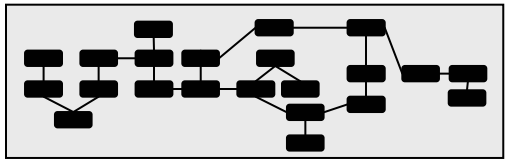
X

C2 Organization



=

Activity Pattern

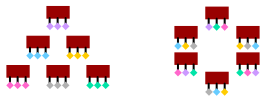


Aptima®
Human - Centered Engineering

NetSTAR Workflow

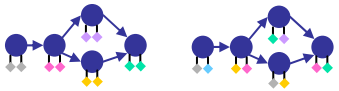
Previous A2C2 Research

Organization Library



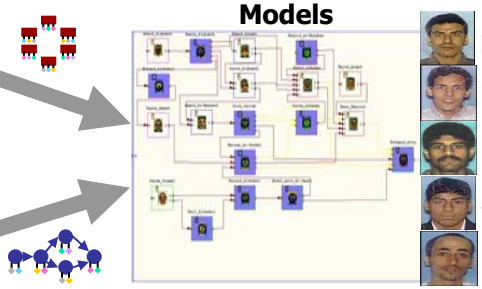
Functional Divisional

Mission Library



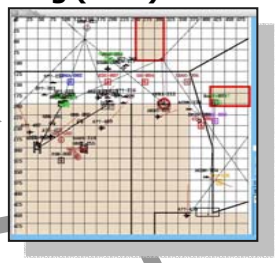
Single Asset Multi Asset

RED Military Team: Process/Activity Models



Khalid Almihdhar
Majed Moqed
Nawaf Alhazmi
Salem Alhazmi
Hani Hanjour

Human-in-the-loop simulations: Distributed Dynamic Decision-making (DDD) Simulator



Activity Log

Agent	Start	End	Action
Khalid	1401.10	1410.43	Explosives Acquisition
Majed	1405.07	1412.32	VBIED Attack

Communications Transcript

Sender	Receiver	Start	End	Content
Khalid	Majed	1400.03	1400.07	"Prepare Explosives"
Majed	Khalid	1400.10	1400.12	"I'm on it."

Proposed NetSTAR Research: Reverse Engineering

COMPARE

COMPARE

Uncertainty of Observations

Observed Events

Agent	Start	End	Action
Khalid	1401.10	1410.43	Explosives Acquisition
---	---	---	---

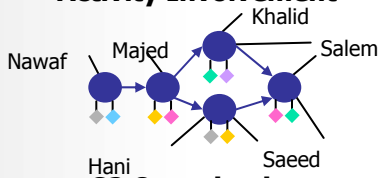
Chatter Levels

Sender	Receiver	Start	End
Khalid	Majed	1400.03	1400.07
Majed	Khalid	1400.10	1400.12

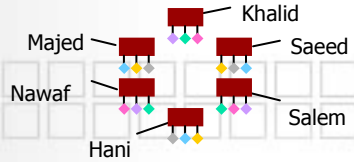
Message Decoding

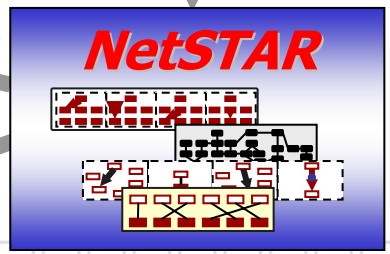
Content
…"explosives"…

Activity Involvement



C2 Organization



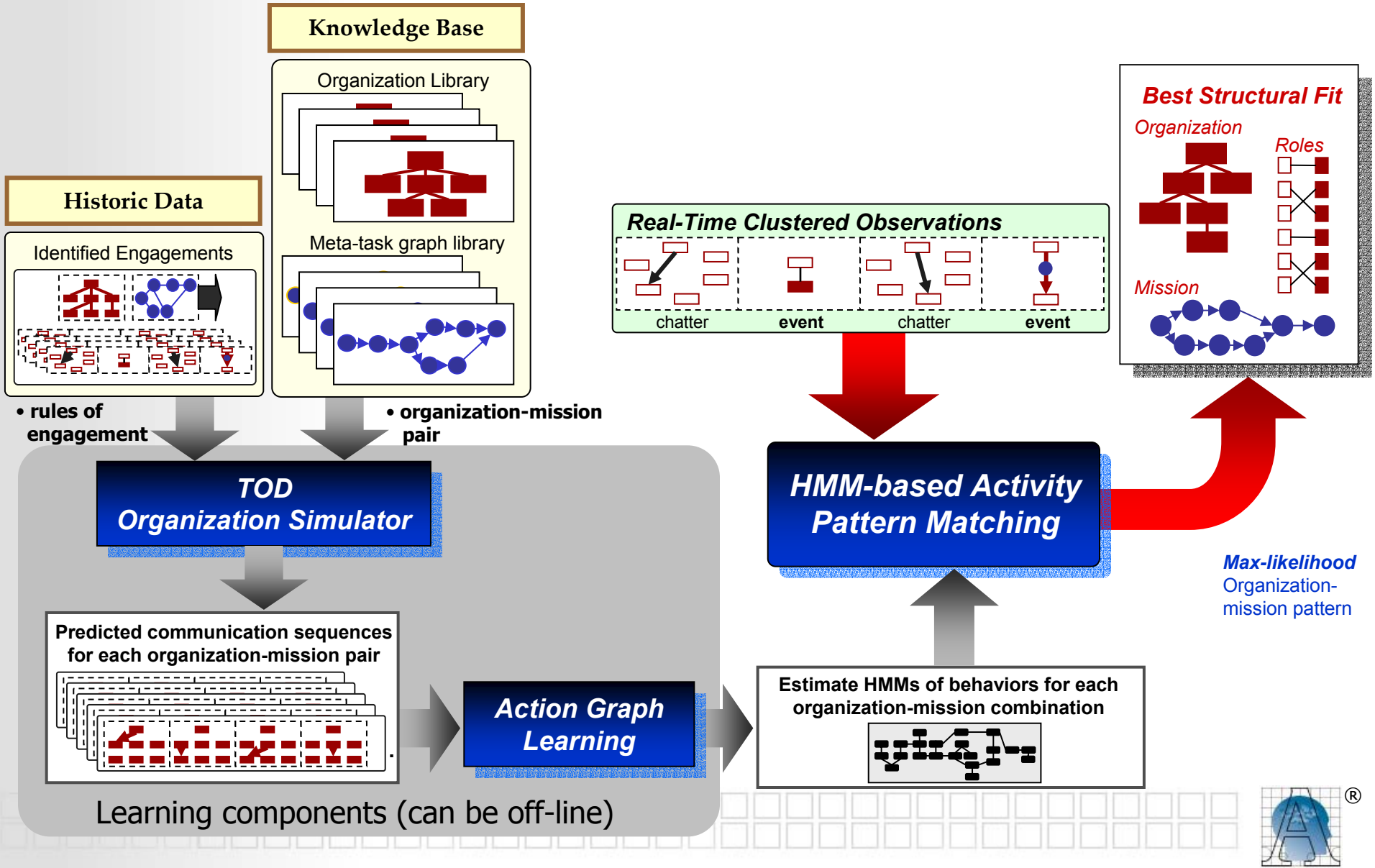


Reconstruct the mission, organization and roles

®

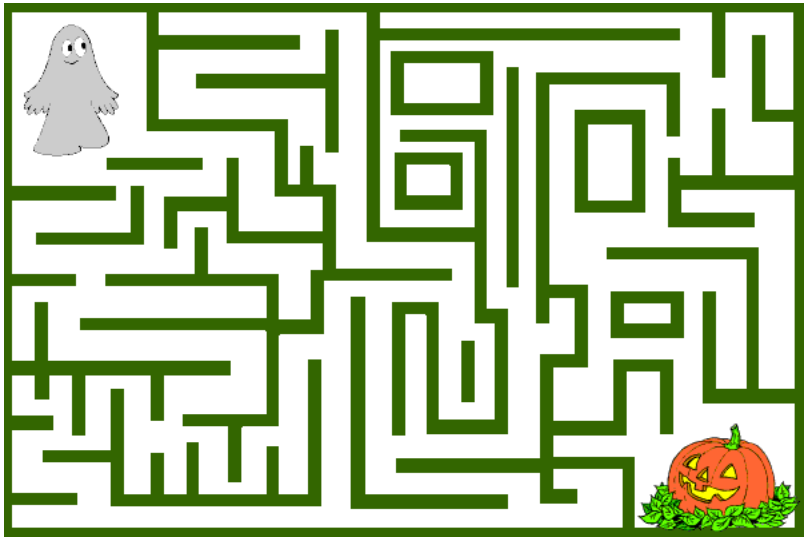
Aptima®
Human - Centered Engineering

NetSTAR Process



Can Activities be Modeled? Are there Distinguishable Patterns?

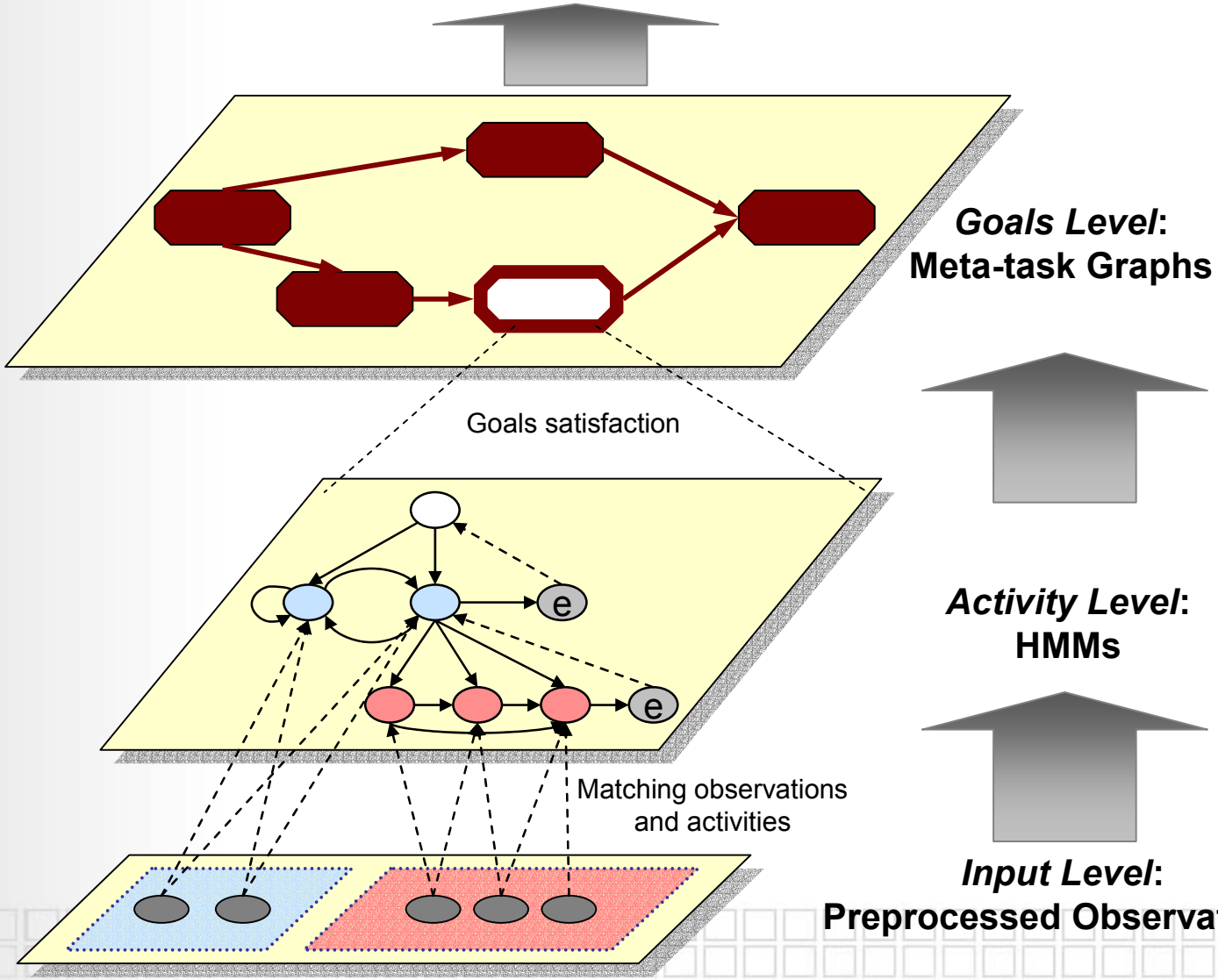
- Yes!!!
- Why?:
  - Patterns/templates of “how to achieve a purpose”
  - Sub-activities depend on one another
    - Precedence
    - Parallelism
    - Geo-dependence
    - Timed dependence
    - Input-output (influence)
    - …
  - People follow patterns in their daily routines
  - C2 organization MUST FOLLOW PATTERNS due to its design – constraints on
    - Who can do what
    - Who communicates to whom
    - Who owns what
    - Who supports whom
    - Who has authority over whom



Aptima®
Human - Centered Engineering

Activity Structure Modeling

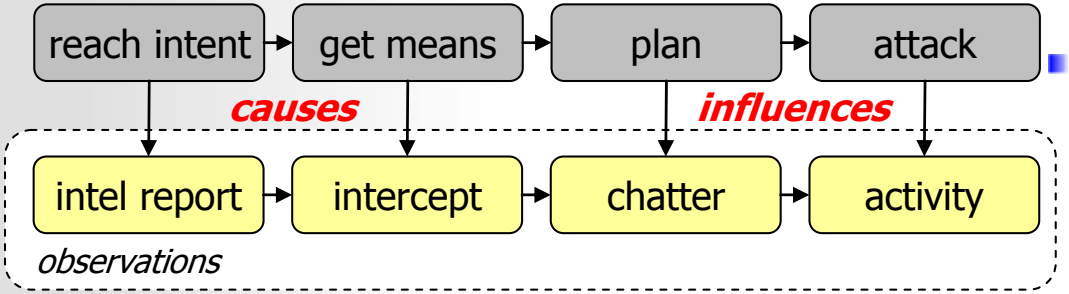
Global Intention & Behavior Matching



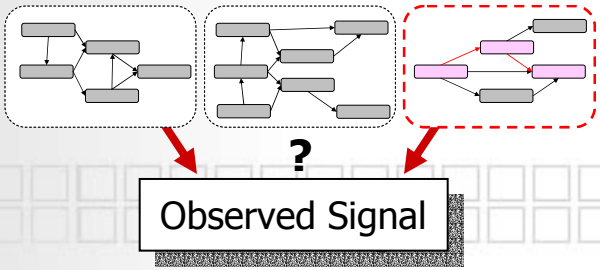
Aptima®
Human - Centered Engineering

Why Hidden Markov Models?

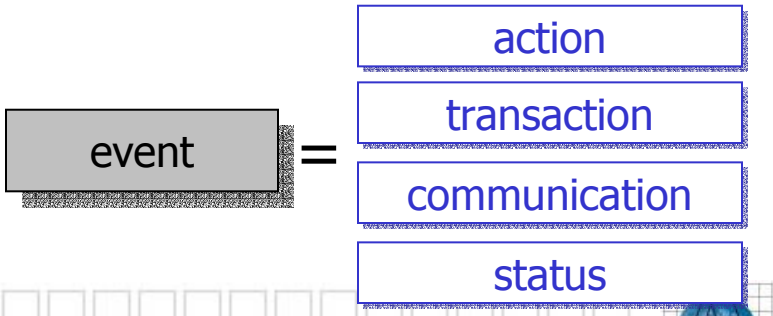
- Model relationships between
  - **Hidden events**
  - **Hidden** true **patterns** of events (event structure)
  - **Observations** which are uncertain representations of true events



- Question:
  - Can I know what is true from what I see?
- Rephrase:
  - What model explains my observations better?
  - What actually happended in that model?

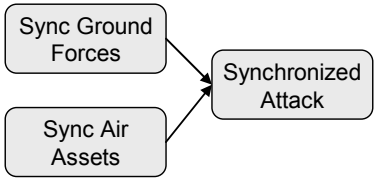


- HMMs can
  - Identify most likely **event pattern that produced observations**
  - Identify the most likely set of **true** (hidden) **events that occurred**
  - **Learn the pattern** structure and parameters given multiple realizations (event/obseravtion sequences)
- Specific Uses
  - Voice/speech recognition
  - Image (e.g. handwriting, faces, etc.) recognition
  - Signal detection
  - Activity detection, environment evolution
  - Control systems
  - Segmentation of DNA sequences and gene recognition
  - Stock data analysis

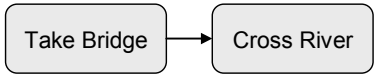


Issues in Activity Modeling (continued)

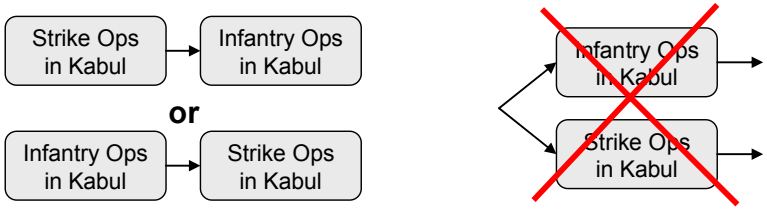
- HMMs can model
  - Time dependence (duration)
  - Absence of observations
  - Multiple observations
  - Observation from possibly multiple sources
  - Influence between events
  - Alternative events
  - Parallel, sequential events
  - Constraints in time, geography, etc. resulting in changed sequencing of events



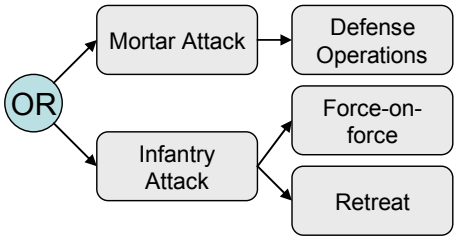
(a) Temporal constraints



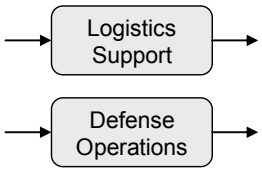
(b) Sequential implementation



(c) Spatial constraints

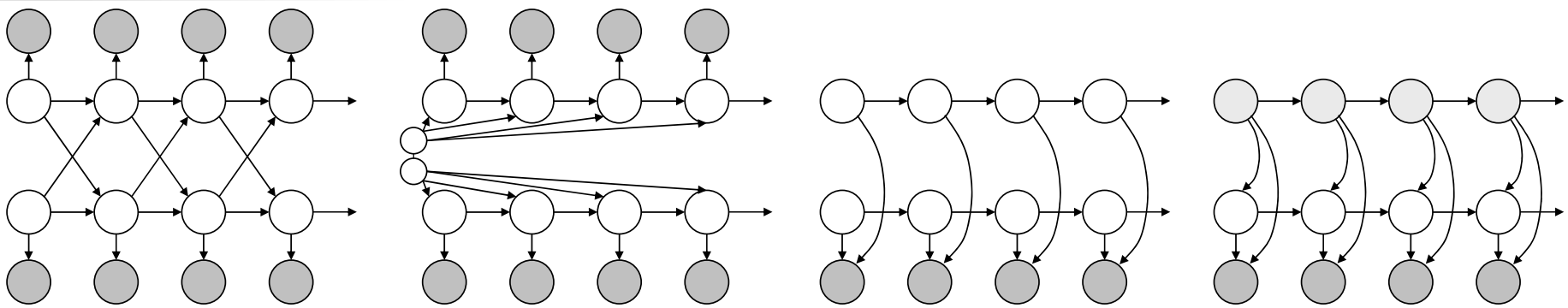


(d) Influence & alternatives

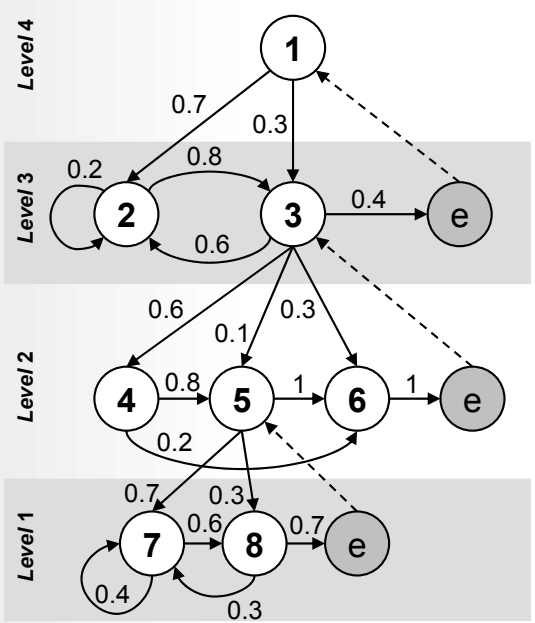


(e) Parallel

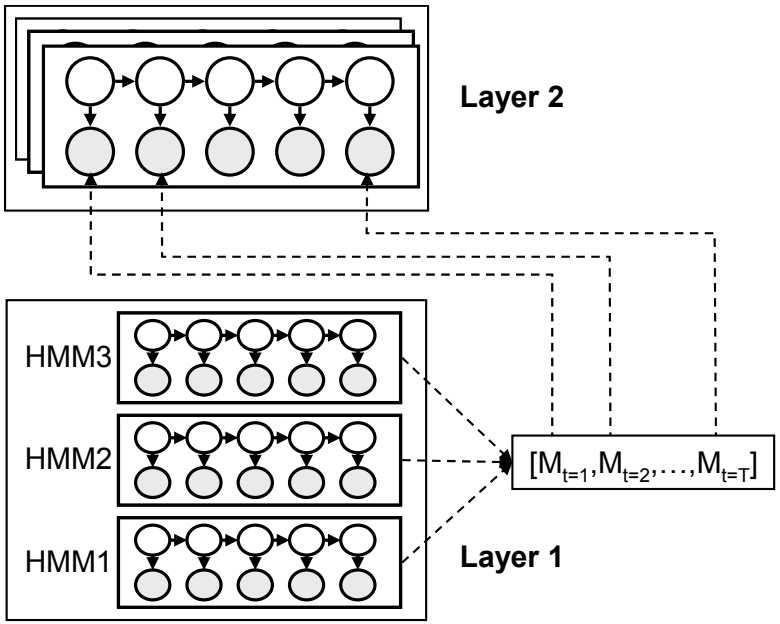
Modeling Methodology: Coupled, Hierarchical & Layered HMMs



(a) Fully-coupled HMM (b) Event-coupled HMM (c) Factorial HMM (d) Input-output HMM



(a) Hierarchical HMM

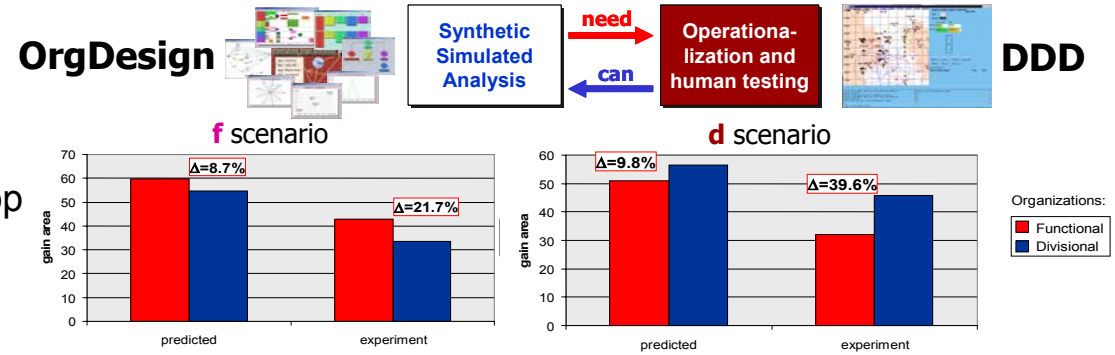


(b) Layered HMM

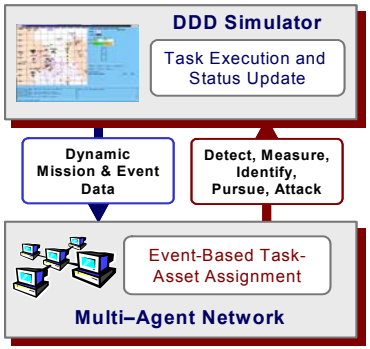
Aptima®
Human - Centered Engineering

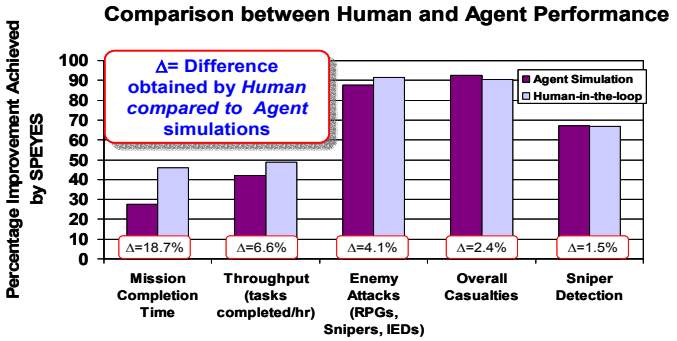
Previous Work (Aptima/UConn)

- A2C2 Experiments
  - Reverse-engineered missions and organizations to test congruence concepts
  - Conducted multiple human-in-the-loop experiments
  - Simulated models predicted the patterns of human performance

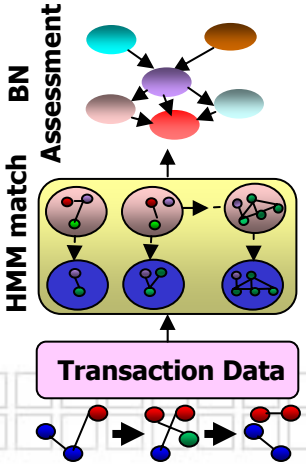


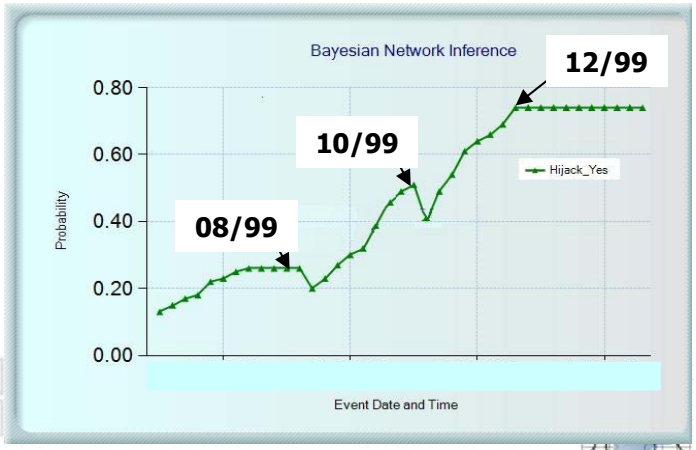
- Synthetic agent development & calibration
  - Integrated OrgDesign synthetic agent with DDD
  - Obtained comparable results for human-in-the-loop and agent runs





- NEMESIS-ASAM (Adaptive Safety Analysis and Monitoring)
  - Predict possible existence & evolution of the terrorist activities from noisy transactions data
  - Identify threats (via ASAM detection schema) & suspicious persons (via feature-aided tracking)
  - Develop models based on real world events or open source information
    - **Indian Airlines Hijacking Model**
    - **Greece Olympics Threat Model**

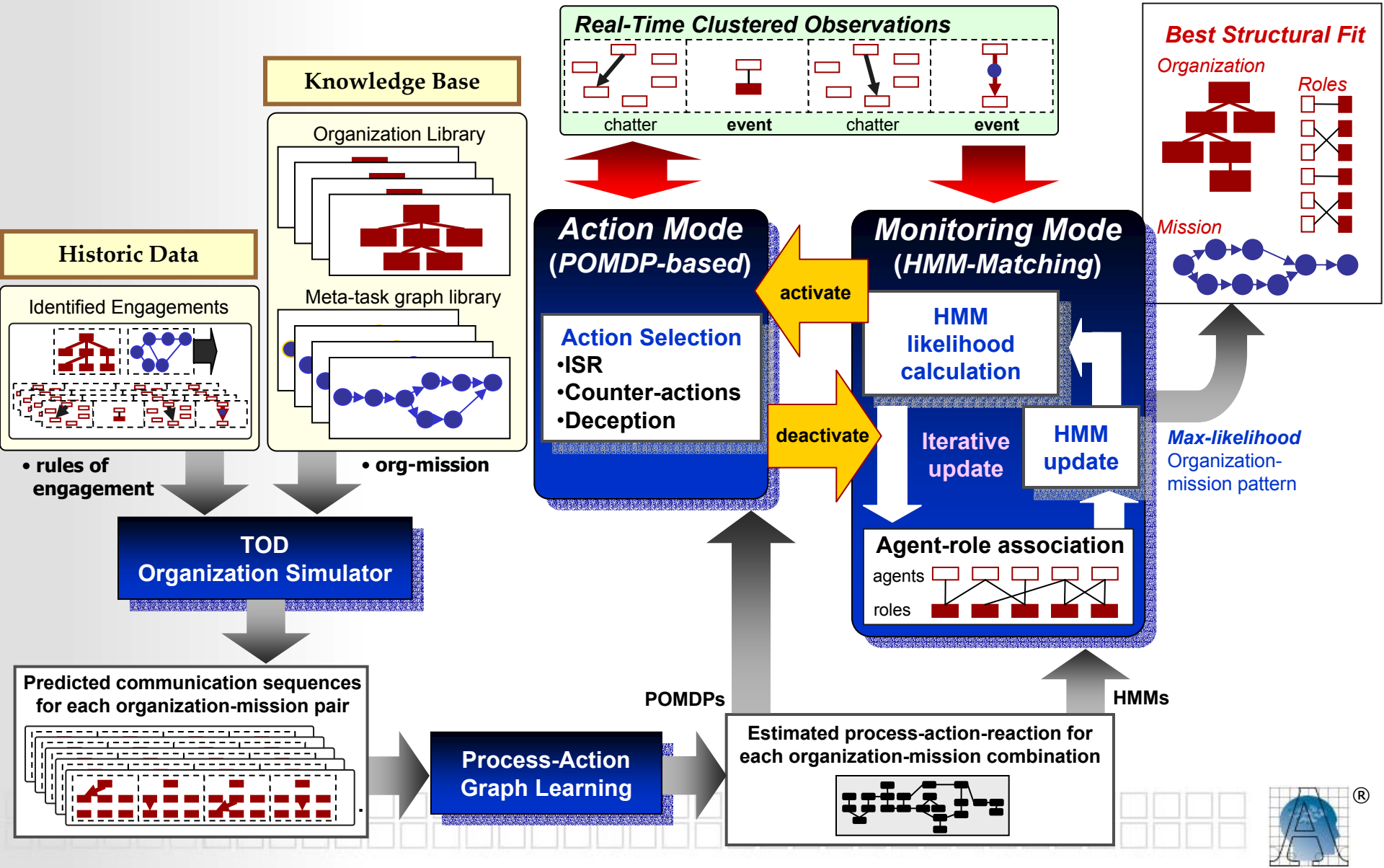




®

Aptima®
Human - Centered Engineering

Next Steps: NetSTAR Monitoring-Action Integration



Aptima®
Human - Centered Engineering

Example: Problem Setup

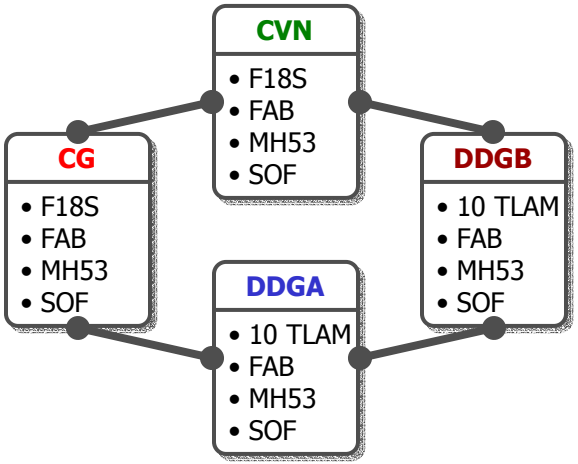
Two Organizations

Command Network and Resource Control Structure

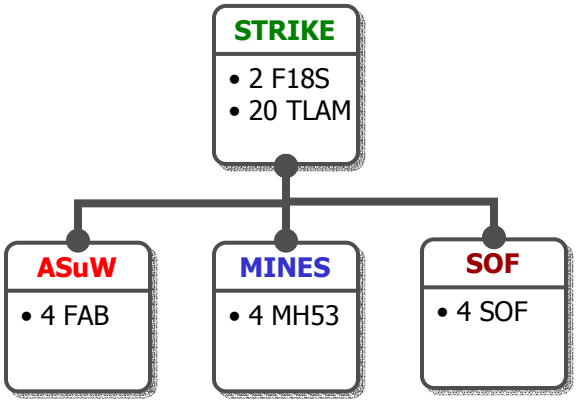
Resources (JTF platforms)

Name	Description	Mines	ASuW	Strike	SOF
F18S	Strike aircraft	0	0	2	0
MH53	Mine clearing helo	1	0	0	0
FAB	Fast attack boat	0	1	0	0
SOF	Special Ops unit	0	0	0	1
TLAM	Tomahawk missile	0	0	1	0

DIVISIONAL Organization

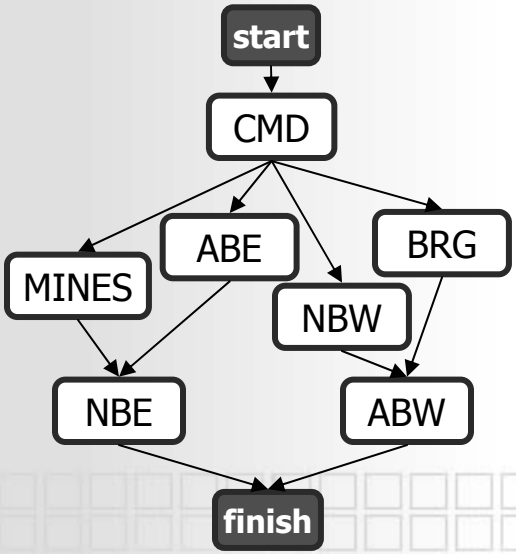


FUNCTIONAL Organization



Two Missions

Task Decomposition

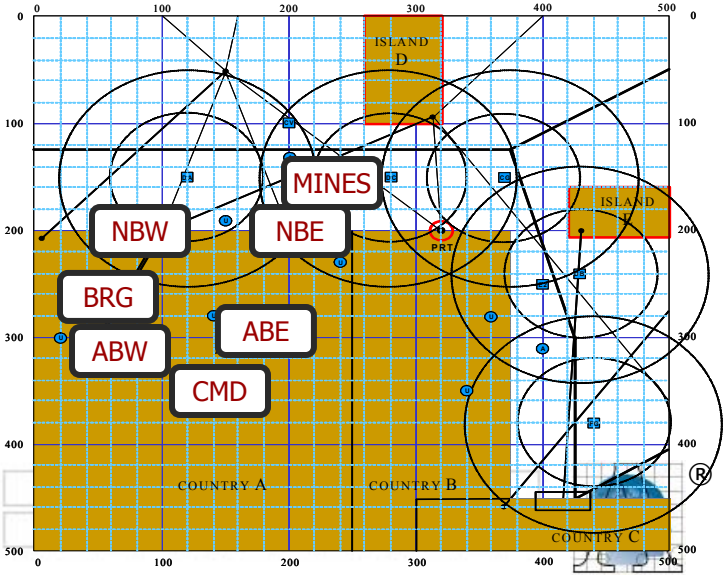


Task Resource Requirements

d scenario

Name	Description	Mines	ASuW	Strike	SOF
CMD	Command Center	0	0	1	1
BRG	Blow Bridge	0	0	1	1
NBE	Naval Base-East	0	1	1	0
NBW	Naval Base-West	1	0	3	1
ABE	Air Base-East	0	0	0	3
ABW	Air Base-West	0	0	2	1
MINE	Clear Mines	1	1	0	0

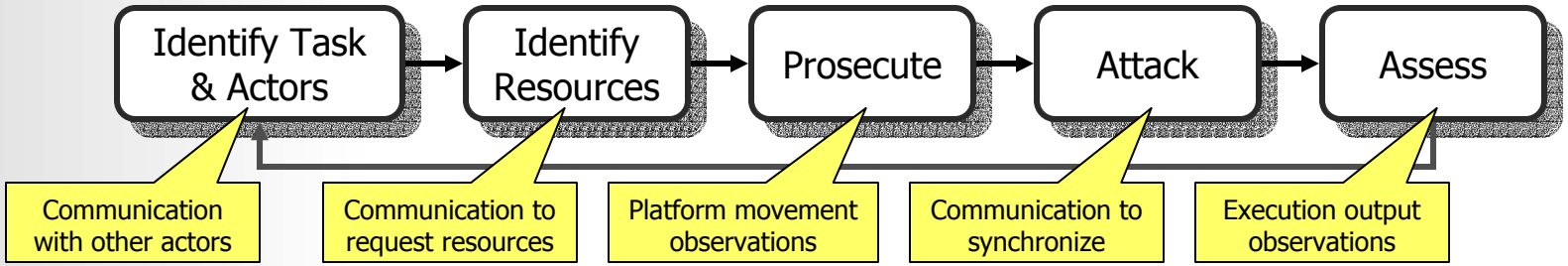
Geographic Layout



Aptima®
Human - Centered Engineering

Example: Task-Activity Generated for "NBW" task

Bases: Decision-Action-Assessment Process Loop of C2 Organization



DIVISIONAL Organization

Primary Commander: **CVN**
Secondary Commander(s): **DDGB** or **CG & DDGA**

- CVN communicates activity initiation to DDGB & CG
- CVN requests commitment from DDGB
- F18S is moved into vicinity
- Attack sequence is initiated from CVN to DDGB
- TLAMs launched from DDGB
- Synchronized attack
- Target destroyed 100%
- Assess

- CVN communicates activity initiation to DDGB & CG
- CVN requests commitment from CG, DDGA
- 2 F18S's are moved into vicinity
- TLAMs launched from DDGA
- Unsynchronized attack
- Target destroyed 50%
- Assess

FUNCTIONAL Organization

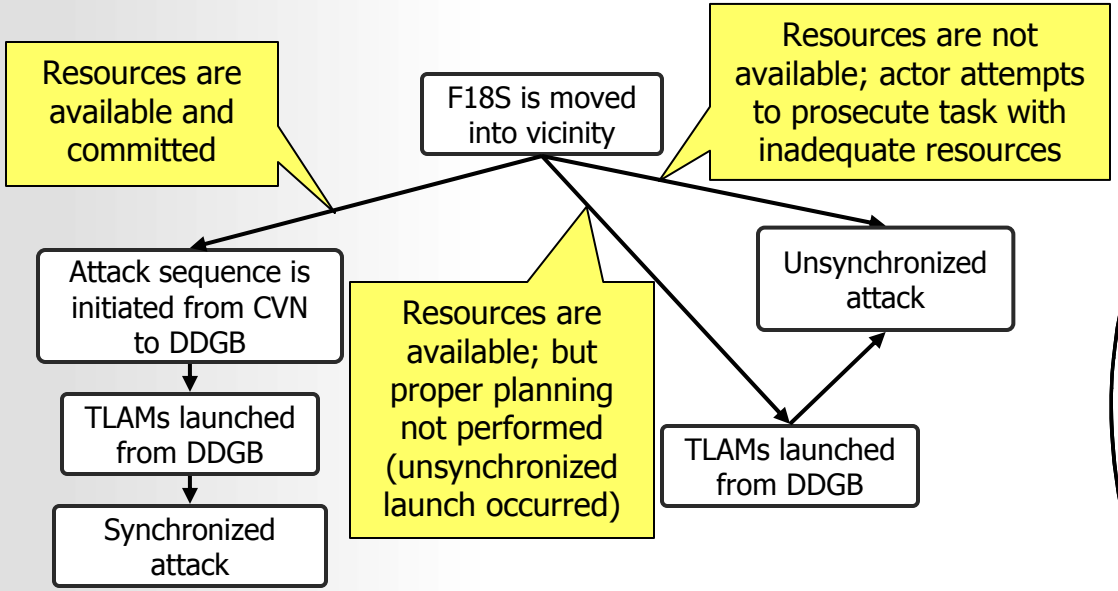
Primary Commander: **STRIKE**
Secondary Commander(s): none

- STRIKE communicates activity init to ASuW & SOF
- F18S is moved into vicinity
- Unsynchronized attack
- Target destroyed 50%
- Assess

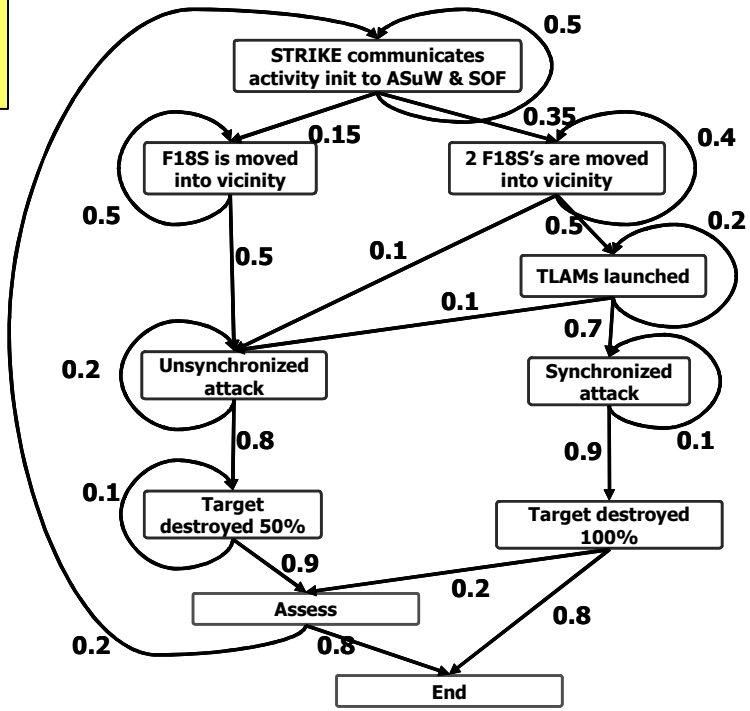
- STRIKE communicates activity init to ASuW & SOF
- 2 F18S's are moved into vicinity
- TLAMs launched
- Synchronized attack
- Target destroyed 100%
- Assess

Aptima®
Human - Centered Engineering

Example: NBW Task Activity Planning Modeling

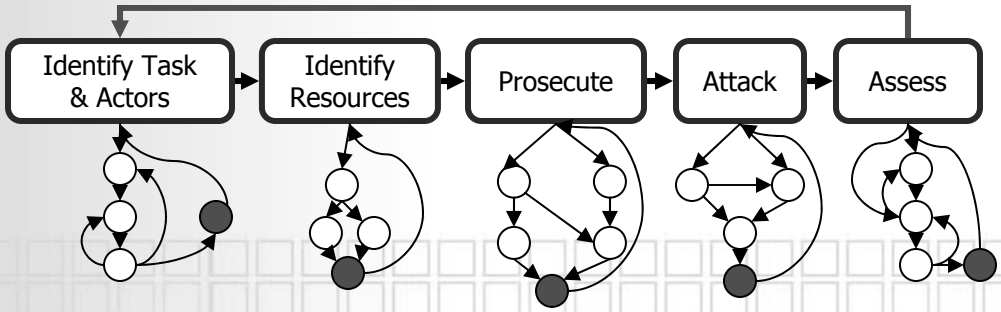


Single-Level HMM Modeling

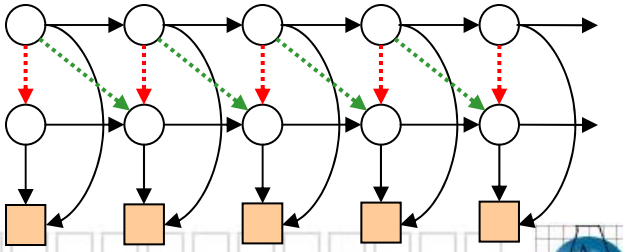


Modeling to Explore Structure and Dependencies among Meta-Tasks

Hierarchical (Layered) HMM Modeling



Factorial HMM Modeling



Aptima®
Human - Centered Engineering

Example: Observations

Time	Observations	Matching Processes/Activities for **DIVISIONAL** Organization		
00:05	Agent 1 communicates to Agent 2	CVN communicates activity initiation to DDGB & CG	CVN requests commitment from CG, DDGA	CVN requests commitment from DDGB
00:10	Agent 1 communicates to Agent 2, 3	CVN communicates activity initiation to DDGB & CG	CVN requests commitment from CG, DDGA	
00:25	Asset F18S-1 is launched	F18S is moved into vicinity	2 F18S's are moved into vicinity	
00:30	Asset F18S-2 is launched	F18S is moved into vicinity	2 F18S's are moved into vicinity	
00:55	Assets F18S-1 & F18S-2 are converging	2 F18S's are moved into vicinity		
01:05	Attack message intercepted to 2,3	Attack sequence is initiated from CVN to CG & DDGA		
01:15	3 TLAM launches observed	TLAMs launched from DDGB	TLAMs launched from DDGA	
01:30	3 TLAMs close on area NW	Synchronized attack	Unsynchronized attack	
01:32	Agent 2 communicates to agent 1	Synchronized attack	Unsynchronized attack	
01:44	NW area heavy explosions observed	Target destroyed 100%	Target destroyed 50%	

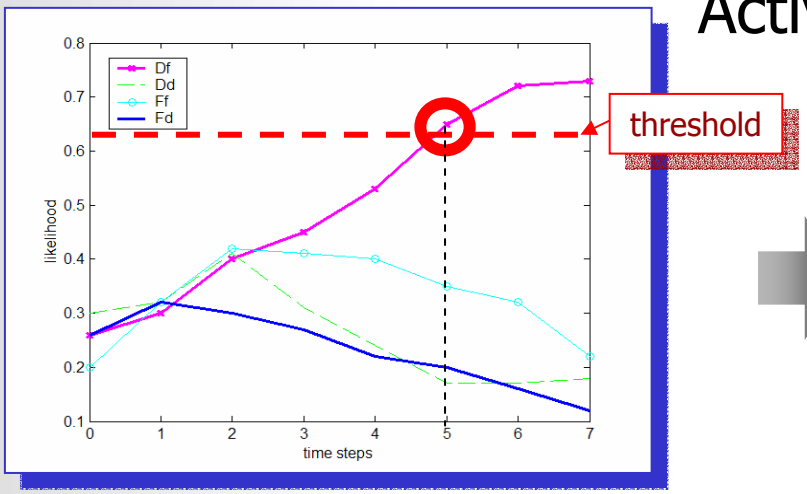
Observations:

- Communication between actors
  - Initiators
  - Content (asset request; activity initiation; report; asset transfer)
  - Duration
  - Roles/identities are not known
- Launch and/or movement of platforms
  - Duration
- Engagement
  - Initiation
  - Resource discrepancies
  - Duration
- Task execution success
- Null (no observations)

Aptima®
Human - Centered Engineering

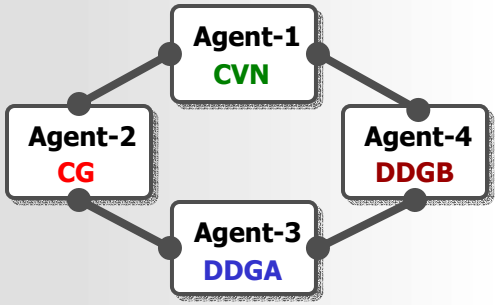
Example: Results

Active Monitoring



Organization	Mission	Likelihood
DIVISIONAL	f	0.65
DIVISIONAL	d	0.18
FUNCTIONAL	f	0.22
FUNCTIONAL	d	0.12

Agent Network

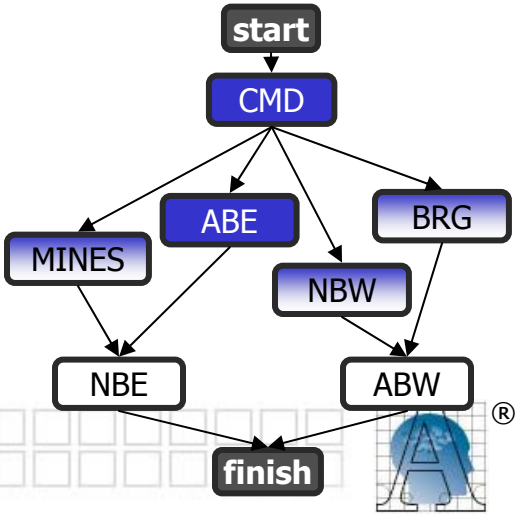


Agent Assignments

Monitored Agents	Roles	Primary Tasks	Supported Tasks	Tasks in Progress
Agent-1	CVN			NBW, BRG
Agent-2	CG		ABE	MINES, NBW
Agent-3	DDGA	ABE	CMD	MINES
Agent-4	DDGB	CMD	ABE	NBW

Monitored Agents	Roles	Asset/Resource Control			
Agent-1	CVN	F18S	FAB	MH53	SOF
Agent-2	CG	F18S	FAB	MH53	SOF
Agent-3	DDGA	10 TLAM	FAB	MH53	SOF
Agent-4	DDGB	10 TLAM	FAB	MH53	SOF

Mission Progress



®

Conclusions

- Proposed methodology to identify the organization structure and mission
- Based on activity matching
- Activities are modeled using Hidden Markov Models
- Future steps: integration with action component using Partially Observable Markov Decision Problem representation

THANK YOU!

Backups

Aptima®
Human - Centered Engineering

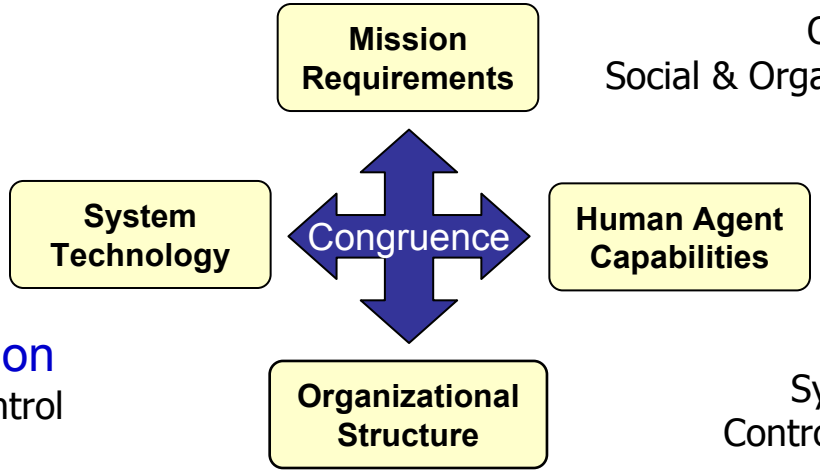
Aptima, Inc.

- Inter-disciplinary Small R&D Business
  - 80+ staff members (>80% advanced degrees)
  - Among the leading Human Engineering firms in the US
  - Supported by 100+ corporate and academic partners
  - Wide range of repeat clients in government and industry

Focus: **Human Centered Engineering**

Areas of Expertise
Human Factors
Organizational Psychology
Cognitive Science
C2 Operations
Mathematical Modeling
Software Engineering

Domains of Application
Military Command and Control
Intelligence Analysis
Aerospace Systems
Medical Systems
Business & Consumer Software Products



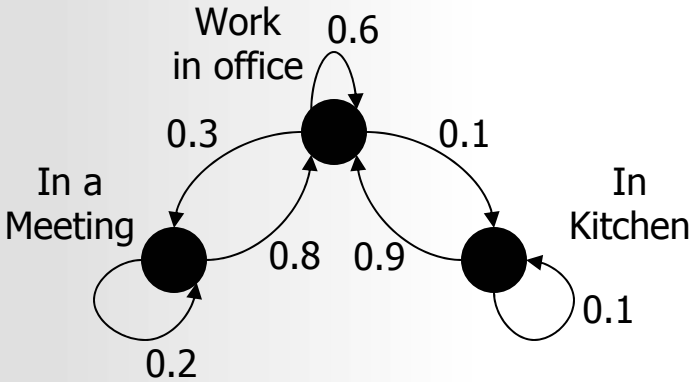
Products and Services
Organizational Design Tools
Social & Organizational Behavior Models
HSI Design and Evaluation
Cognitive Analysis
Training Systems
Performance Assessment
Competency Analysis
Intelligent Agents
Synthetic Task Environments
Controlled and Field Experiments
Decision Support Systems

Aptima®
Human - Centered Engineering

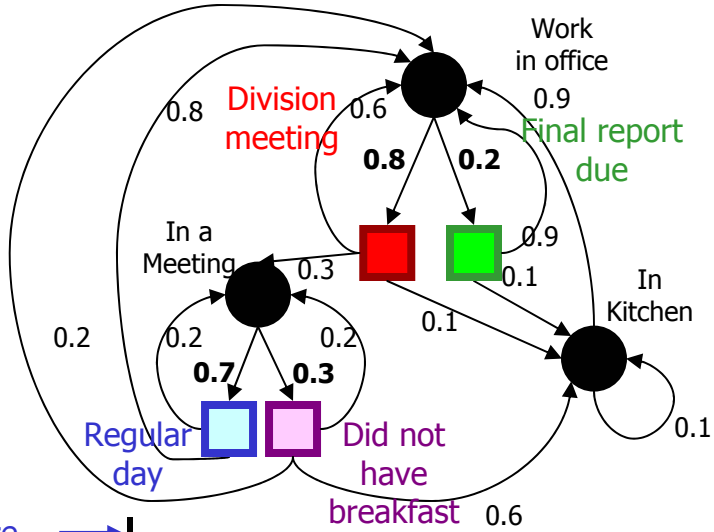
Next Steps:

- From **Identification** to **Action**
- ⇒ from **HMM** to **POMDP**
- Action policies in POMDP create different HMMs

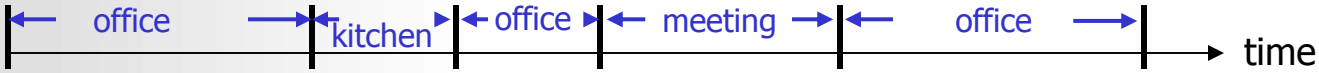
HMM Pattern/Model:



POMDP: effect of actions/decisions

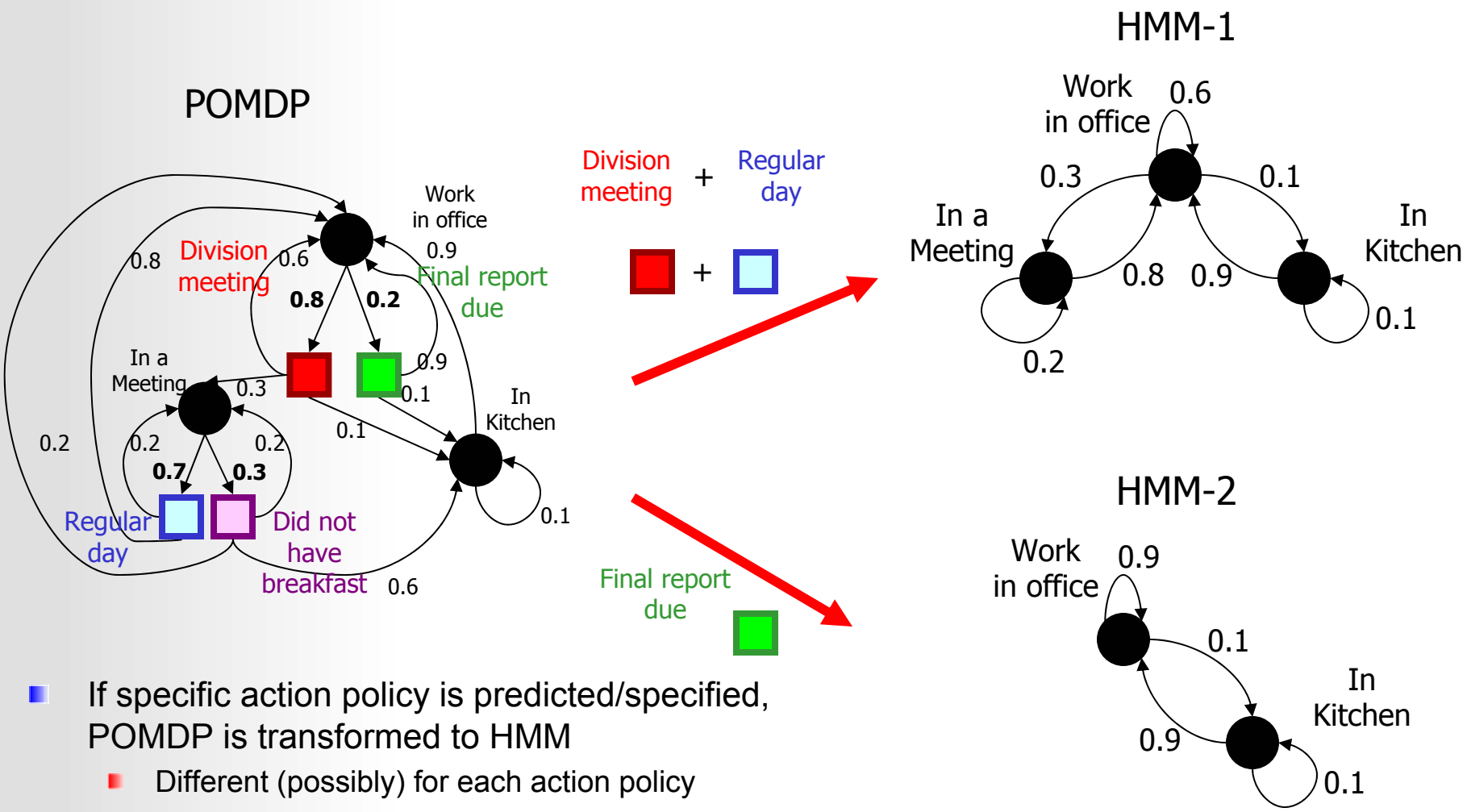


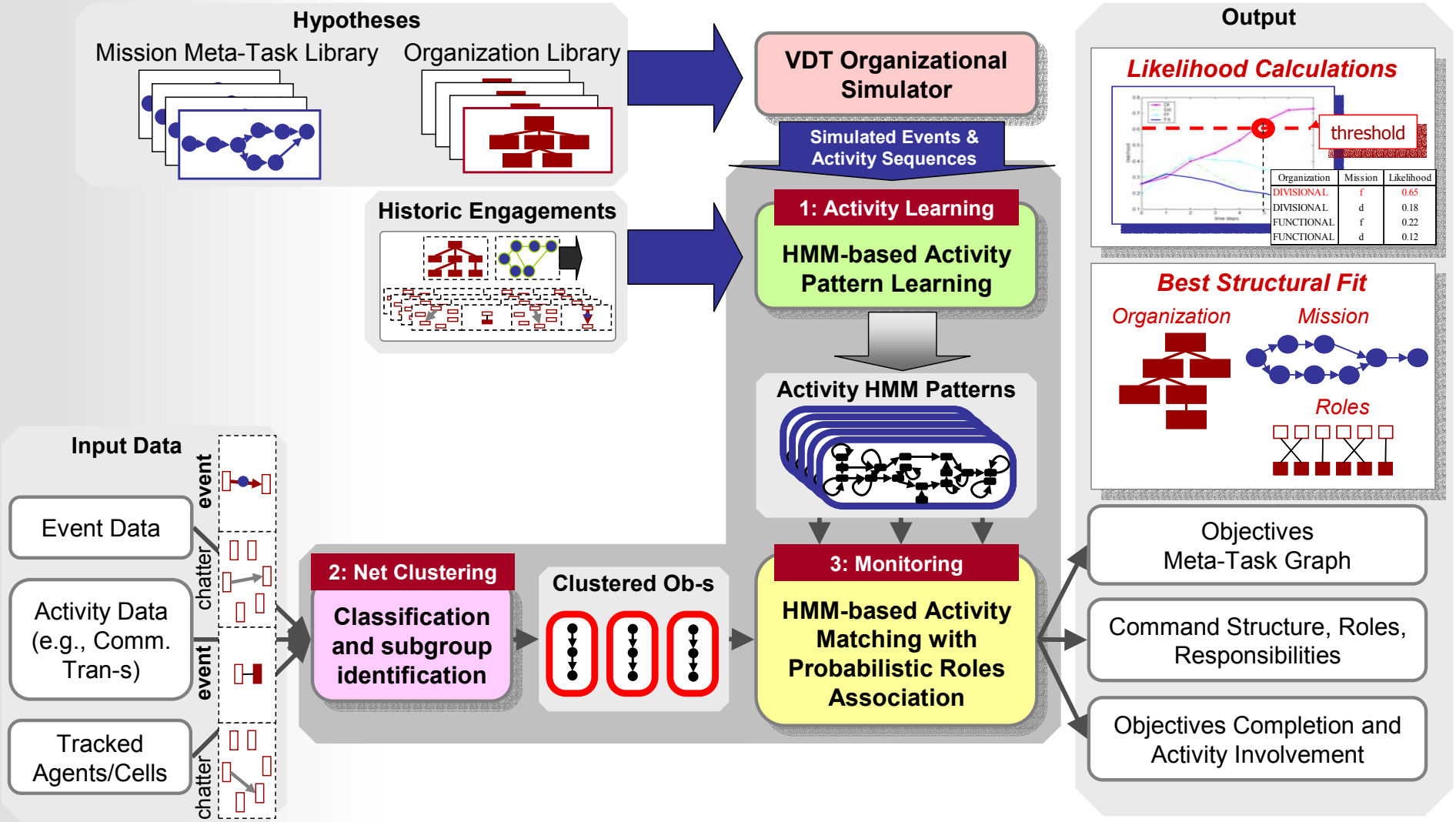
True activity sequence:



Observations:

Transition from POMDP to HMM



- If specific action policy is predicted/specified, POMDP is transformed to HMM
  - Different (possibly) for each action policy
  - Differ in pattern/structure
  - Differ in transition/observation probabilities

Aptima®
Human - Centered Engineering