APTIMA
HUMAN-CENTERED
ENGINEERING

Identifying Command, Control and Communication Networks from Interactions and Activities

Georgiy Levchuk, Ph.D., Aptima Inc.
Yuri Levchuk, Ph.D., Aptima Inc.

CCRTS, 2006

© 2006, Aptima, Inc.

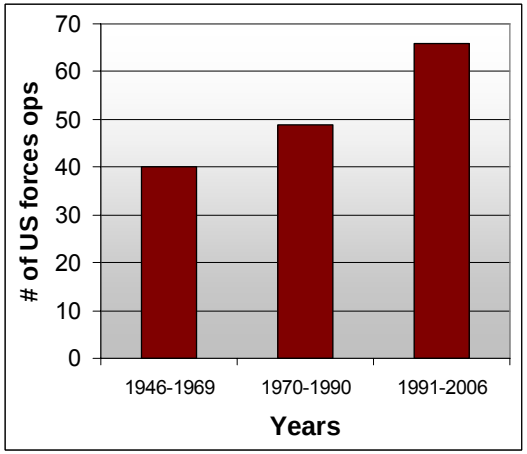
Agenda

- Challenges of tactical operations
- Proposed integrated solution concept
- Focus of this research: adversary organization identification
- Technical approach
- Results and conclusions

© 2006, Aptima, Inc.

3 Major Challenges of Tactical Operations

Conflicts Trends

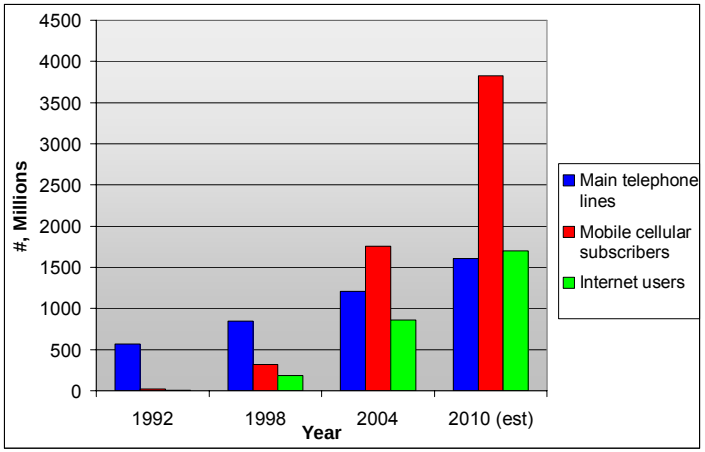


Past
- Slow-time conflict
- Numbered engagements

Current
- Asymmetric threats and changing missions

Future: Increased # of Ops
- Fast-paced engagements
- Larger number of and higher time criticality

Technology/Information Trends



Past
- Mainly hard-line communications

Current
- Internet traffic doubles/year
- 630,000 phone lines installed/week
- 50,000 new wireless users/day
- 650M SIGINT cables generated (~0.001% to products)
- 34M voice mail messages/day
- 7.7M e-mails sent/min

Future: Data Explosion
- Data impossible to analyze manually

Adversary's Trends

Past
- Large-size forces of well-known organizational forms

Current
- Small- to moderate-size militia forces taking many less organized forms

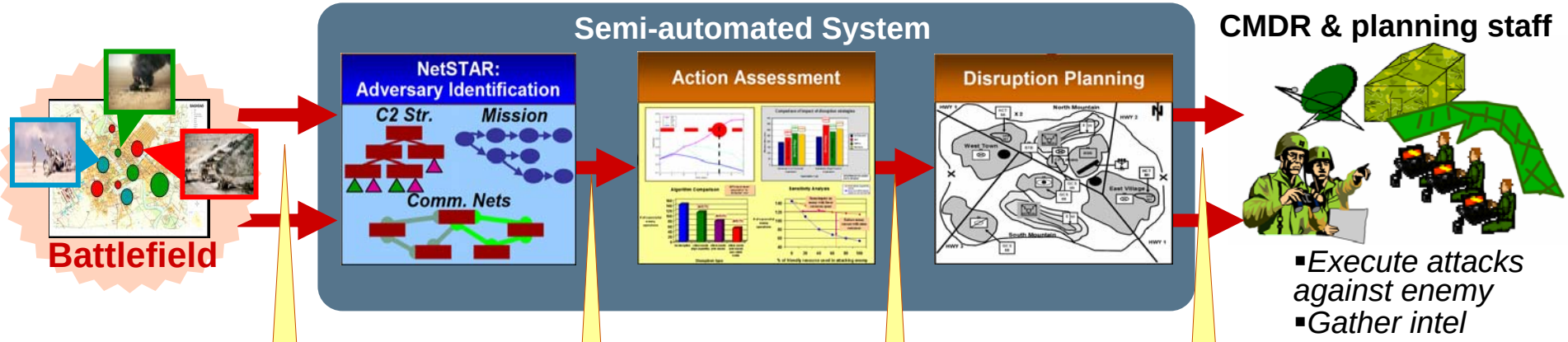
Future: Adaptive Enemy
- Almost unrestricted ability to connect and coordinate
- Can change size and adapt structure

Tactical Planning Issues
- High manpower needs
- Takes long time
- High info gaps, complexity, overload
- Biases of human decisions

© 2006, Aptima, Inc.

Solution:

A System to Aid Battlefield CMDR to Design Effective Counteractions against Tactical Adversary



INPUT

- comm. intercepts
- events
- actions

predicted enemy C2 structure, CMDR roles, & intent

vulnerabilities & counter-action impact assessment

PRODUCT

counteractions, disruptions & probes plan

Outcome: enemy's performance degrades
- –incorrect actions
- –delayed commands
- –missed critical information and engagements

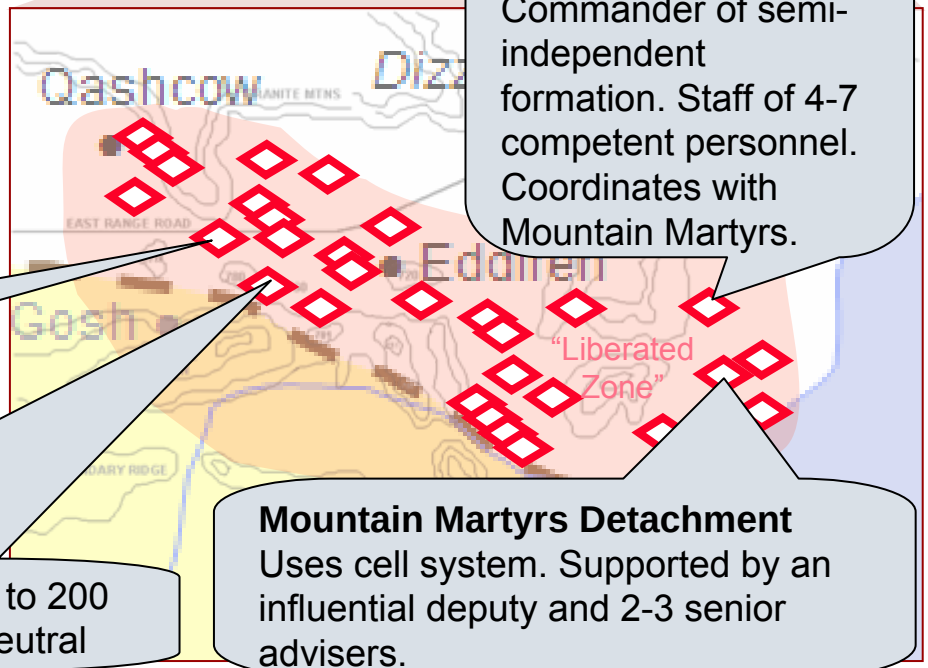
Challenges
- **Complexity:** large data amounts & solution space to explore
- **Criticality:** limited time for decision
- **Uncertainty:** large data gaps

© 2006, Aptima, Inc.

Notional Scenario:

Support Spring Offensive of Urbanistan Government

- **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.
- **Enemy Command** and Control: TSU is led by a network of several disparate organizations, ranging from informal cells to military structure.



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

Lions Brigade : 10-12 people, some with FSU military training. **CMDR Abbadirov** – Former Soviet Spetsnaz officer.

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

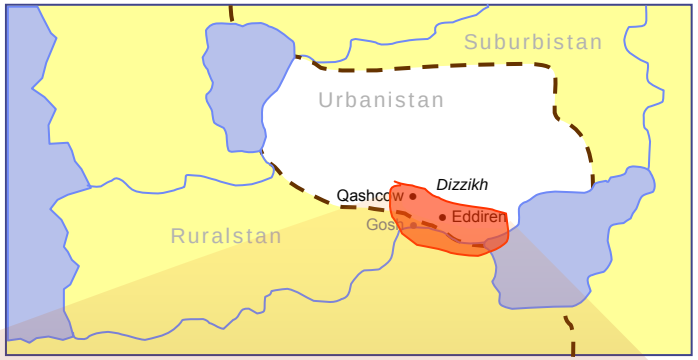
Mountain Martyrs Detachment Uses cell system. Supported by an influential deputy and 2-3 senior advisers.

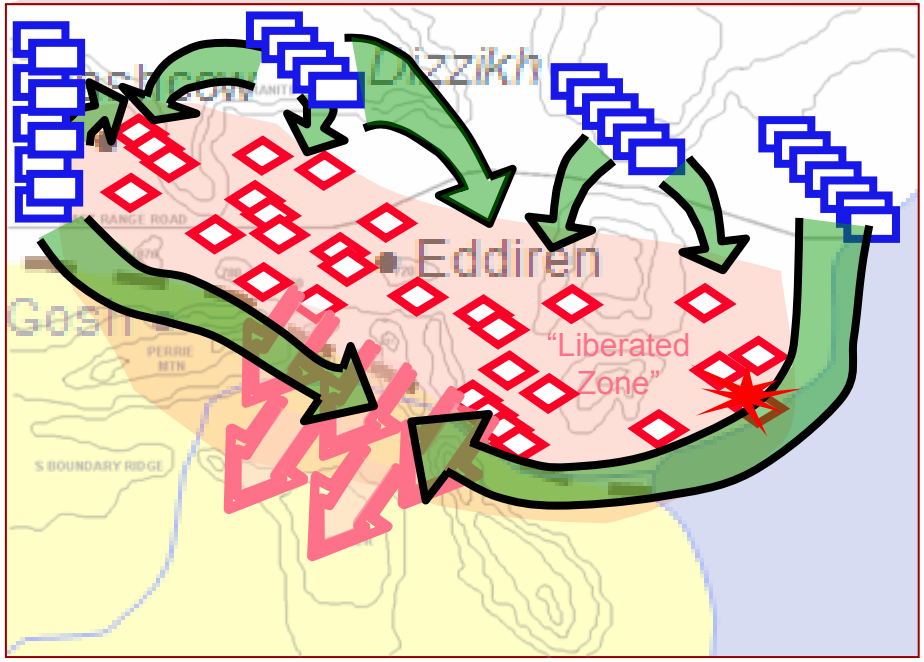
© 2006, Aptima, Inc.

Notional Scenario:

Support Spring Offensive of Urbanistan Government

- **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.
- **Enemy Command** and Control: TSU is led by a network of several disparate organizations, ranging from informal cells to military structure.
- **Original Plan of the offensive**: AOU forces penetrate the Liberated Zone along 4 avenues of approach. NLT H+72 seal the borders.



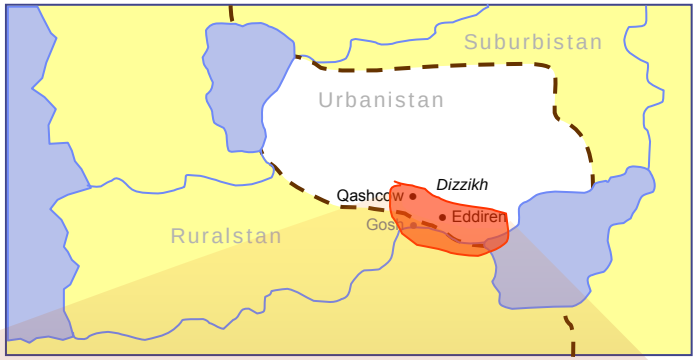


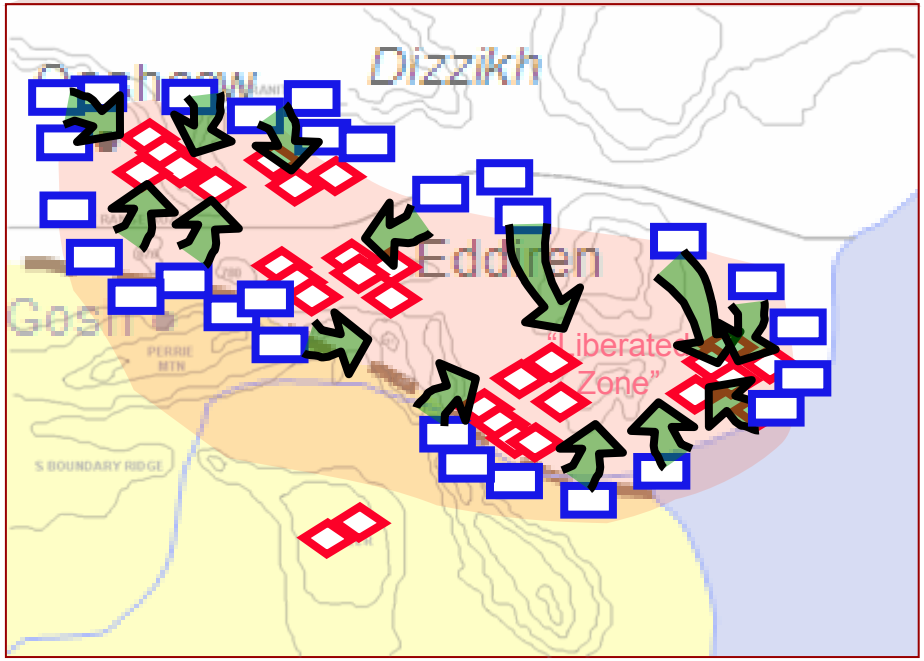
© 2006, Aptima, Inc.

Notional Scenario:

Support Spring Offensive of Urbanistan Government

- **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.
- **Enemy Command** and Control: TSU is led by a network of several disparate organizations, ranging from informal cells to military structure.
- **Original 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.



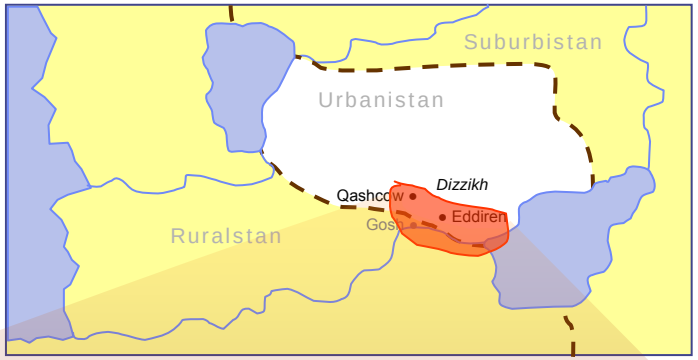


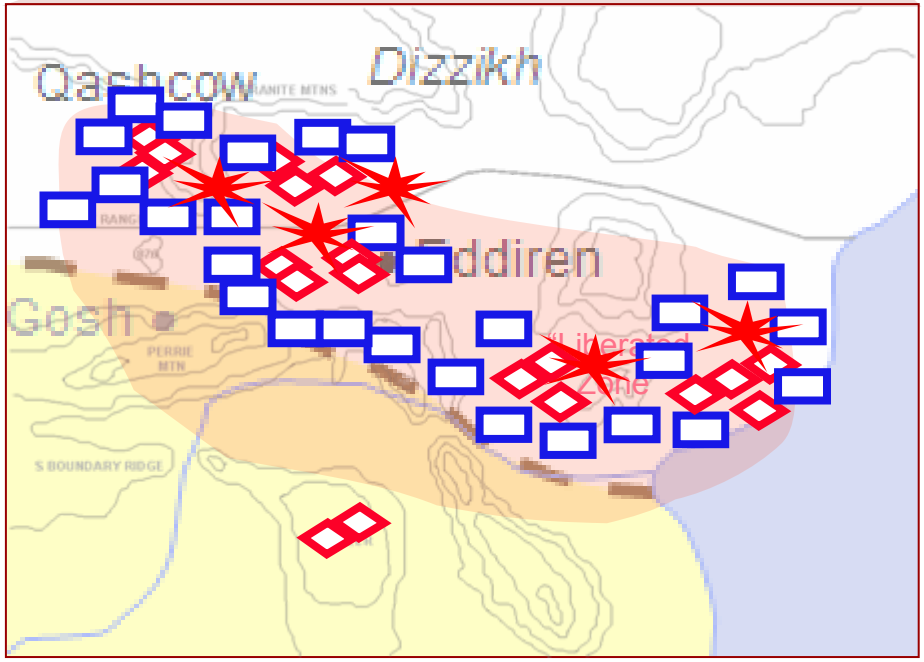
© 2006, Aptima, Inc.

Notional Scenario:

Support Spring Offensive of Urbanistan Government

- **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.
- **Enemy Command** and Control: TSU is led by a network of several disparate organizations, ranging from informal cells to military structure.
- **Original 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..





© 2006, Aptima, Inc.

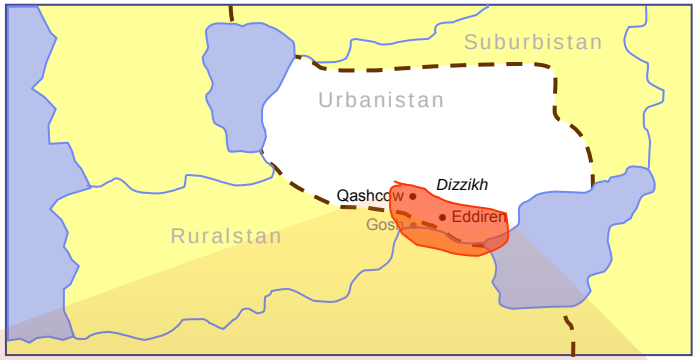
Notional Scenario:

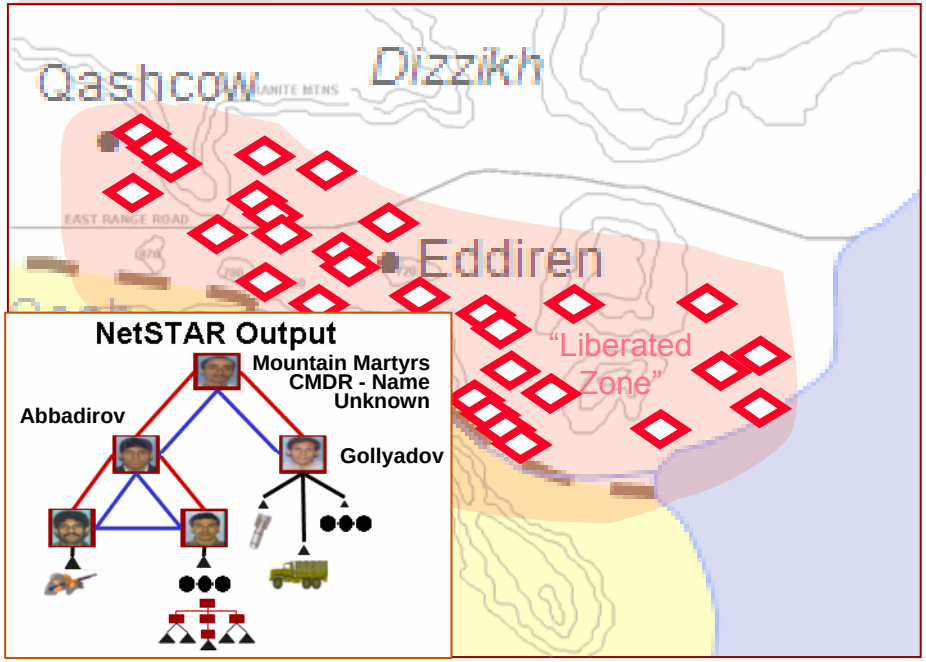
Support Spring Offensive of Urbanistan Government

- **Original 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..

- **Uncertainties in the Original Plan**:
  - Movement of the enemy units (and rapid concentration of forces in well protected areas)
  - Attempted points of massive exfiltration of TSU into the Dizzikh region and/or across the border
  - Events that may influence the outcome (e.g., cross-border instigation of uprising in Ruralstan's town of Gosh)
- **Info to Help Reduce Uncertainty** :
  - Structure of the enemy C2
  - Locations of the enemy leadership
  - Ties between TSU and groups in Ruralstan's town of Gosh
- **NetSTAR:** Utilize friendly intel capabilities (US multi-INT capabilities plus Urbani IntService's HUMINT) to **fill in the blanks** in the Info





Notional Scenario:

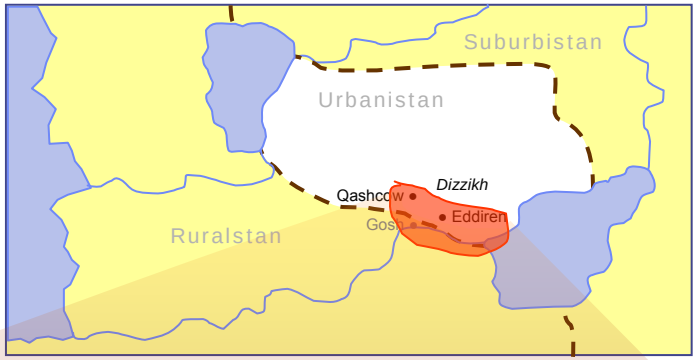
Support Spring Offensive of Urbanistan Government

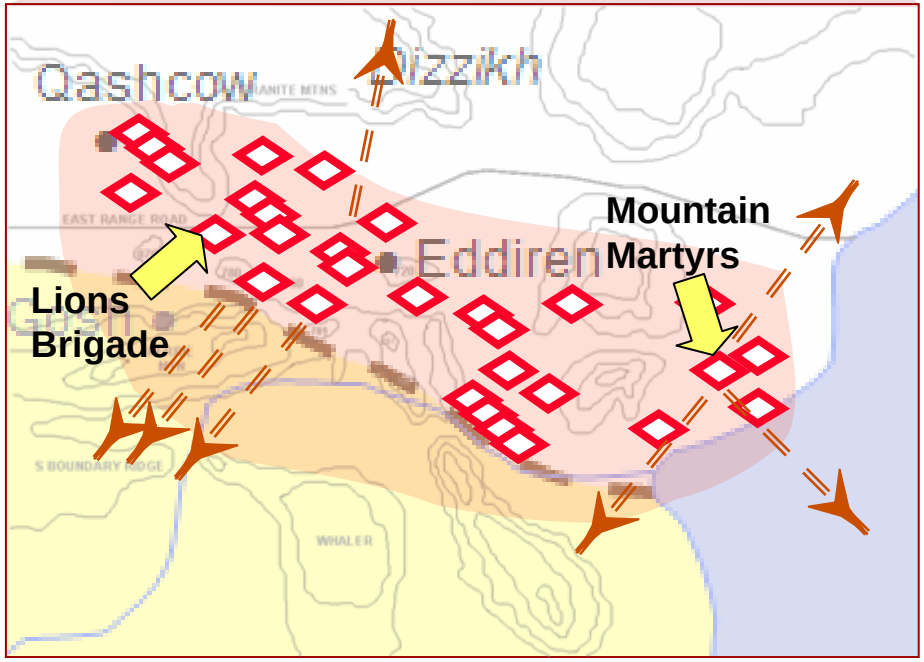
- **Original Plan of the offensive**: AOU forces penetrate the Liberated Zone along 4 avenues of approach. NLT H+72 seal the borders.

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..

- **Summary of NetSTAR findings** and follow-up analysis:
  - Chief Leadership is located at Mountain Martyrs Cell
    - attempt to exfiltrate in/out/by sea is likely
    - area is likely well protected;
    - rapid concentration of forces if assaulted is likely
  - Secondary echelon of operational command is with Lions Brigade (CMDR Abbadirov)
    - may conduct a massive exfiltration of TSU into the Dizzikh region or across the border
    - likely to initiate distraction maneuvers to divert attention from Chief Leadership

- **Projected enemy strategy**:
  - Two main exfiltration brake-through efforts with possible rapid concentration of forces at Mountain Martyrs area of operations





Notional Scenario:

Support Spring Offensive of Urbanistan Government

- **NetSTAR-aided Plan of the offensive**:

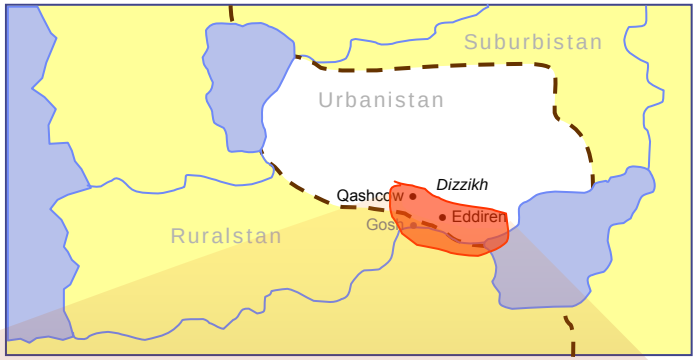
  - AOU forces penetrate the Liberated Zone along 4 avenues of approach. NLT H+72 seal the borders. Concentrate own forces to block movement of enemy forces towards Mountain Martyrs. Block sea access. Set up ambush groups.

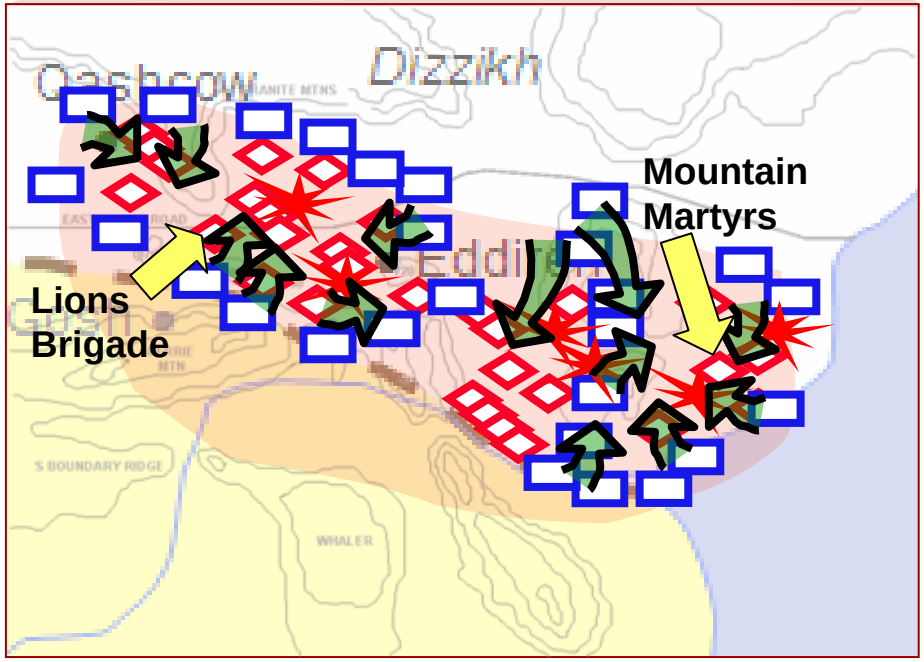
  - Massive air strikes at Mountain Martyrs and Lions Brigade positions

  - 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.

NetSTAR-driven plan modifications





© 2006, Aptima, Inc.

Desired Capability
Identify Enemy C2 Structure and Likely Strategy

Outcome of applying modified Plan:

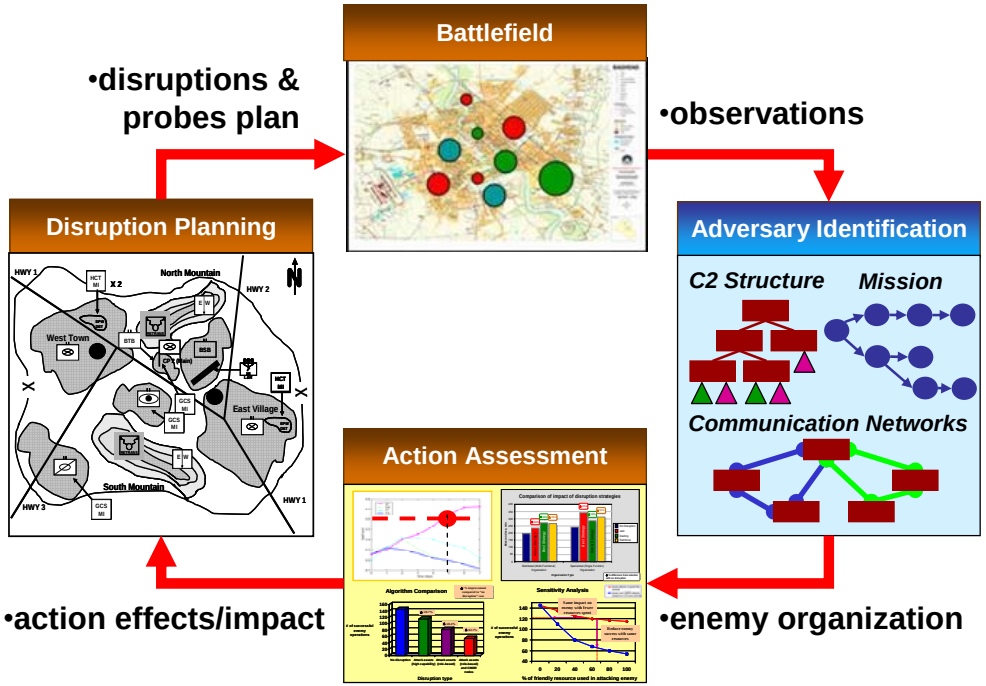
Enemy force concentration prevented, escape routs blocked; Enemy leadership captured/ annihilated; Enemy forces defeated

NetSTAR-driven COA recommendations:

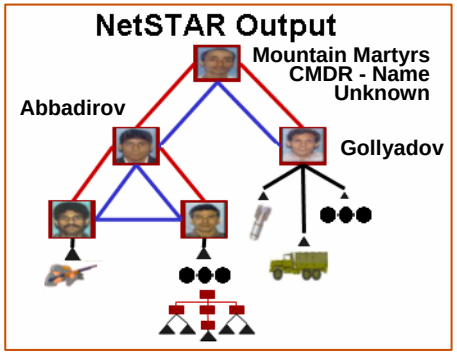
Augment original plan by concentrating own forces to block likely enemy movement.

Block sea access. Set up ambush groups.

Conduct massive air strikes at Mountain Martyrs and Lions Brigade positions



Projected Enemy Structure:

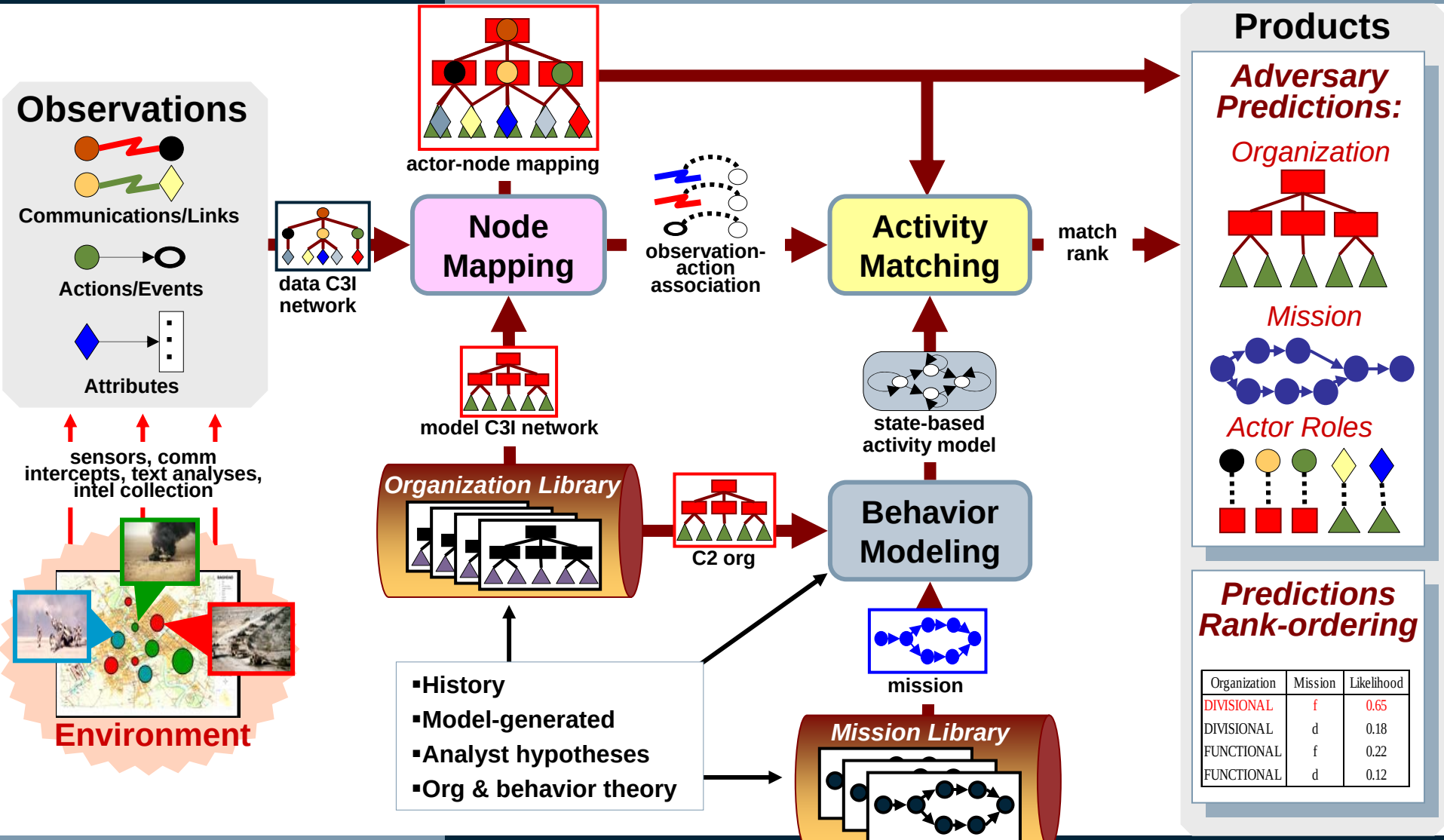


Projected Enemy Strategy:

Two main exfiltration brake-through efforts; Rapid concentration of forces at Mountain Martyrs area of operations if needed

© 2006, Aptima, Inc.

NetSTAR
Adversary Identification Process



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

© 2006, Aptima, Inc.

NetSTAR Sample Outputs

Inputs

- Hypothesized candidate C2 networks
- Observed resources and activities/events
- Observed (categorized) communications
  - Actor-to-actor
  - Actor-to-resource (i.e., to field unit commander)

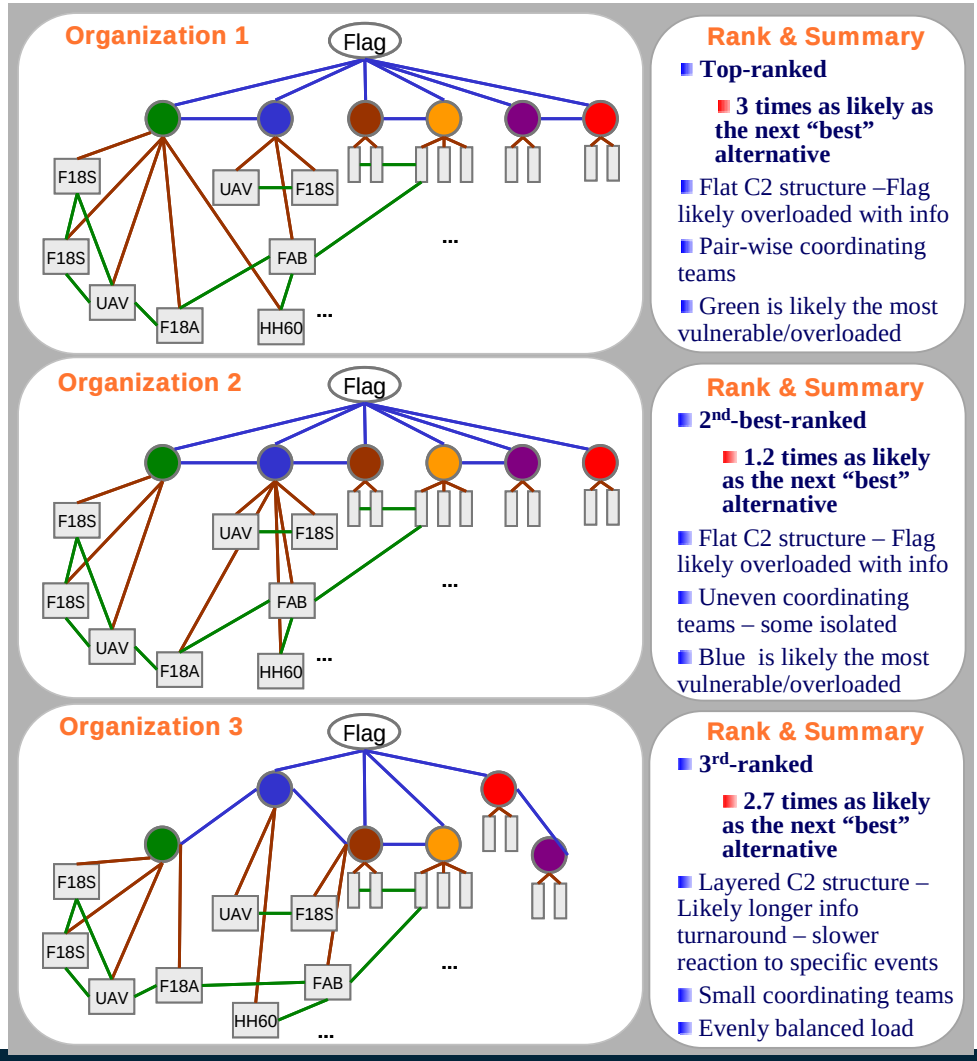
Assumptions

- Assume known number of actors and resources (need to determine relationships)

Outputs

- Command, control, & communication structure
  - C2 superior-subordinate hierarchy
  - Peer-to-peer coordination/ synchronization relationships
  - Communication network(s)
  - Resource/unit control allocation of adversary commanders
- Roles of adversary actors in C2 network
- Joint resource utilization relationships

Output Illustration

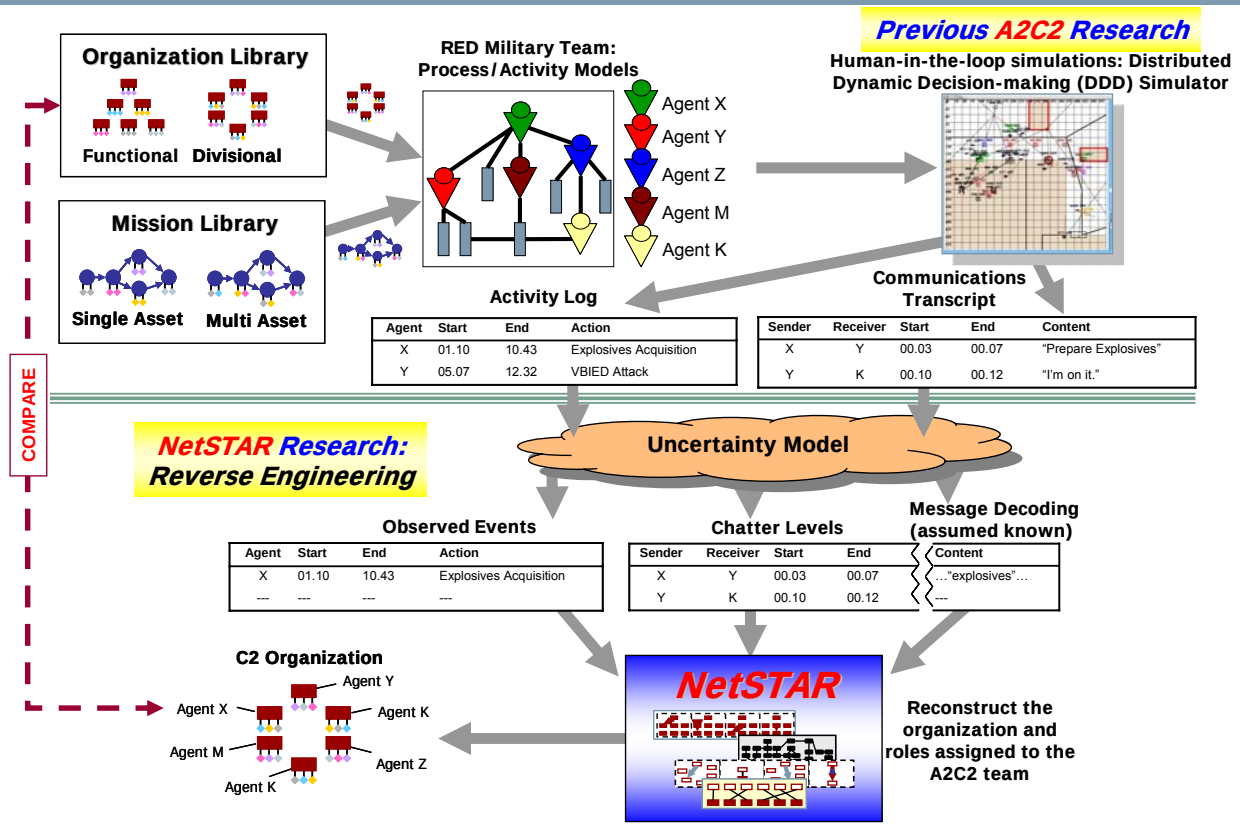


© 2006, Aptima, Inc.

NetSTAR Experimental Validation

Focus of the Analyses

- Reuse readily available data – A2C2 Experiments
- Detection focus:
  - Identification of nodes: actor-node mapping
  - Identification of resource allocation: control structure
- Use "uncertainty model" to introduce noise to data:
  - **Communications** filtered according to **security of channel** (probability of observing communication)
  - **Activities** filtered according to **class of tasks** (probability of observing the involvement in the task)

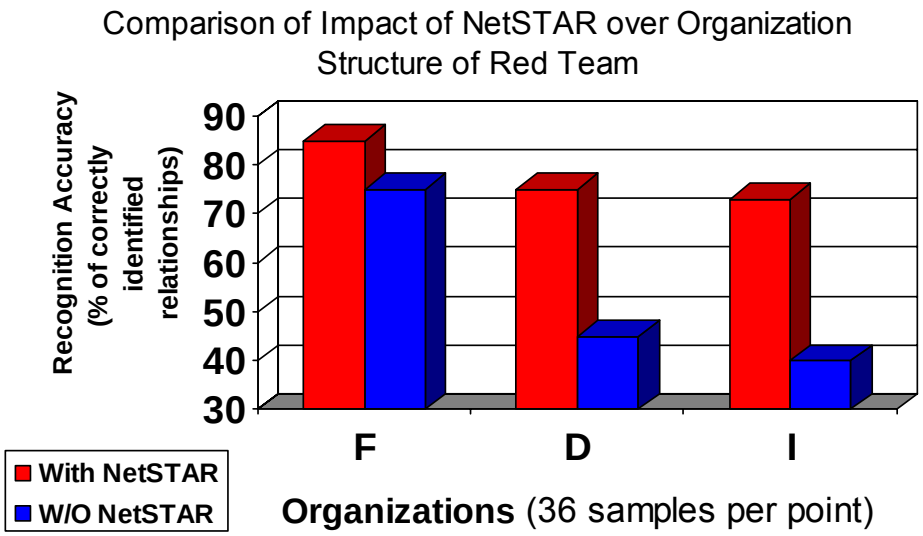


A2C2 data

- Missions executed by joint task force organizations
- Communications manually coded
- Number of human-in-loop experimental logs: 40

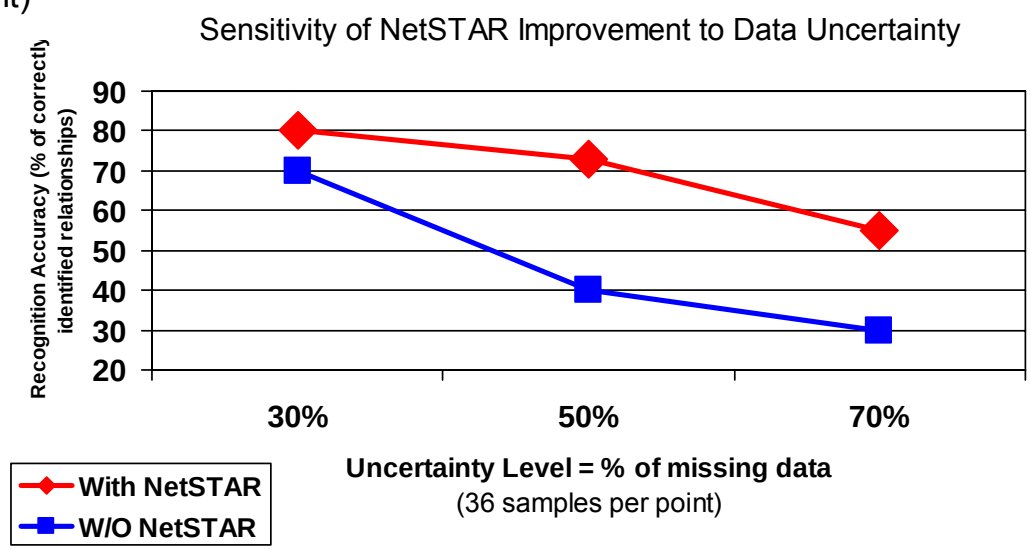
© 2006, Aptima, Inc.

NetSTAR
Anticipated Benefits



- Impact of NetSTAR increases with increased organizational complexity

- Curvilinear impact of NetSTAR with increased uncertainty in source data

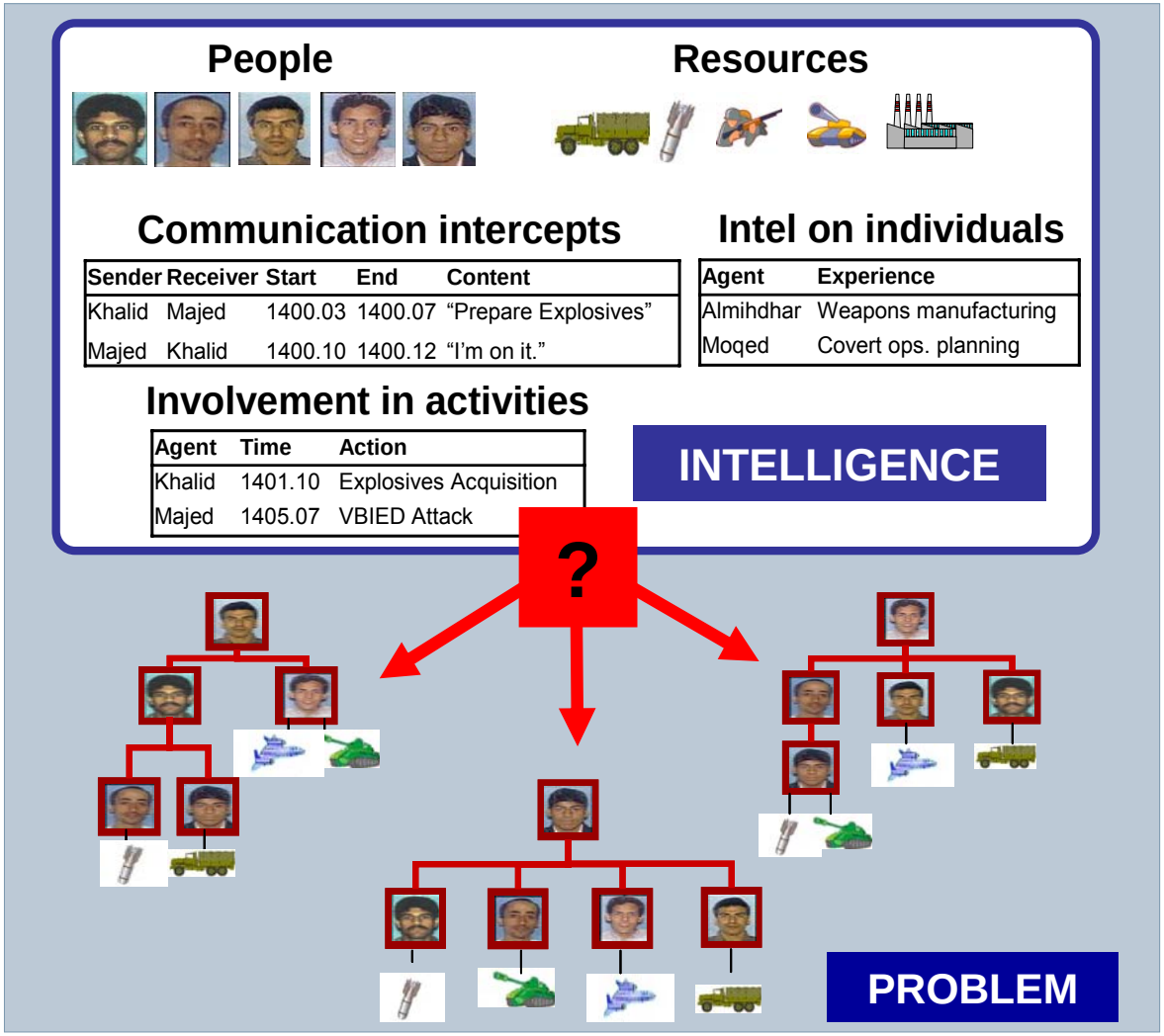


© 2006, Aptima, Inc.

Problem Formalization

How can we recognize the **enemy C3I organization** given uncertain observations

- *Actors*
- *Resources*
- *Communication intercepts*
- *Involvement in activities*
- *Intel on individual actors & resources*



© 2006, Aptima, Inc.

Organization Identification Conceptual Solution

Objectives

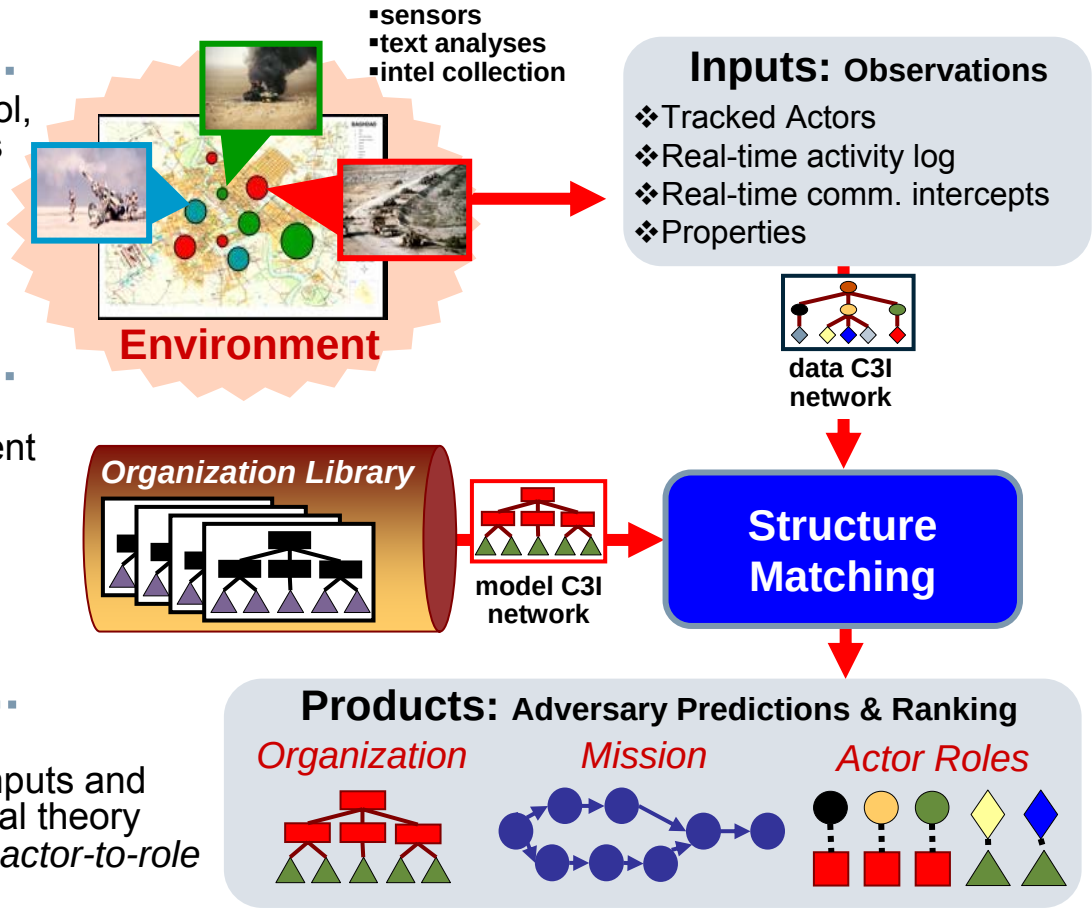
- Automatically identify enemy Command, Control, and Communication networks and CMDR roles from events observations and communication intercepts

Benefits

- Speed-up & improve accuracy of analysts' decisions by automating hypotheses assessment
- Handle large complexity of data and high uncertainty

Technical Approach

- Real-time hypotheses testing
- Hypotheses generated manually from users' inputs and automatically from historic data & organizational theory
- *Attributed relational graph matching model for actor-to-role mapping – **network pattern recognition***



© 2006, Aptima, Inc.

Summary

- NetSTAR model supports intelligence analyses by focusing the adversary organization identification on the *small number of most relevant hypotheses* about the enemy C2 structure
- NetSTAR finds the **rank-ordering** of the hypothesized command, control, communication, and task structures of the adversary and the **roles** of their decision makers and resource nodes
- NetSTAR algorithms are based on finding the **structural match** between observed network of interactions of adversary actors and resources
  - The model uses the notions of structural consistency and maximizes the likelihood that the observed interaction network between the enemy actors and resources has been generated by a specific hypothetical C2 organization
  - NetSTAR algorithm uses the information about actors/resources' involvement in actions to improve the identification of their roles in the organization
  - NetSTAR model works with missing and erroneous data, deceptions from the adversary, and can handle a large complexity of the C2 networks

© 2006, Aptima, Inc.

- Backup

© 2006, Aptima, Inc.

"Know Thy Enemy"

- Cannot effectively predict enemy's COAs w/o knowing **enemy C2 organization**
- Cannot develop effective enemy HVTs & counteractions w/o knowing **enemy C2 organization**
- Might entail unintended consequences if the action is taken w/o full realization of the C2 structure and roles of individuals

Past

Event
- US Civil War, 1861-1865

Action
- Death of Confederate cmdr Stonewall Jackson, 05/1863

Impact
- Argued by many historians, was a blow to Army of Northern Virginia and contributed to its eventual loss

Reason
- Provoked a reorganization of the command from which the army never fully recovered
  - Resulted in the division of the army into three infantry corps
  - Two new corps commanders would prove to be poor choices

Present

Event
- Israel-Palestinian Conflict, 1948-today

Action
- Elimination of HAMAS founder Sheikh Ahmed Yassin and his successor Abdel Aziz Rantisi, 01/2004

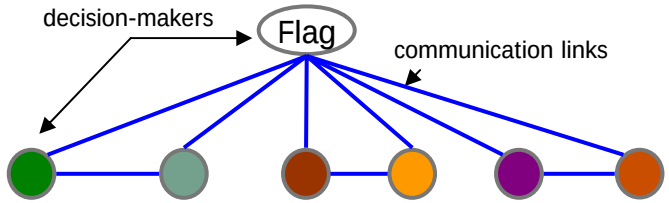
Impact
- Huge protests
- HAMAS enters political process through municipal elections, 2005
- HAMAS wins Palestinian parliamentary elections 01/2006

Reason
- HAMAS reorganized and solidified, gaining more strength and people's support

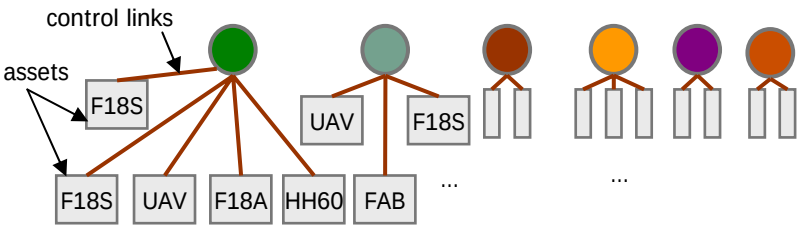
© 2006, Aptima, Inc.

Organization Network Elements: Key enemy leaders and relationships

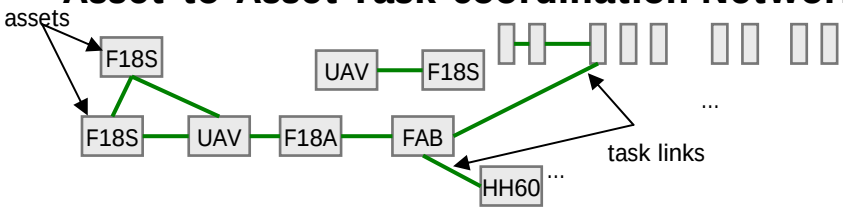
Communication and Command Network



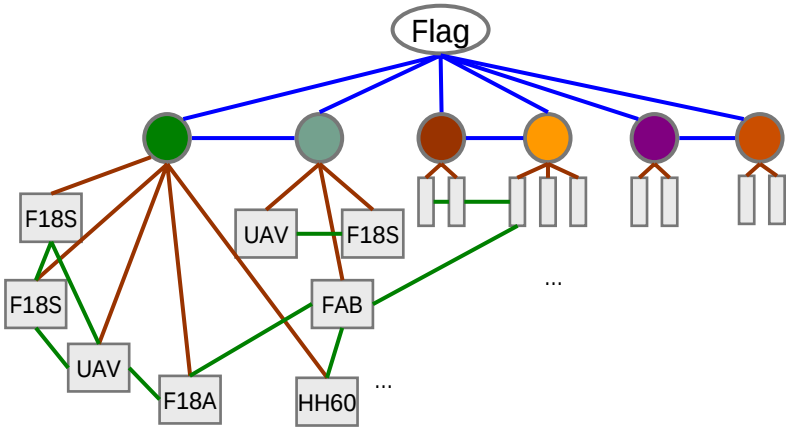
CMDR-to-Asset Control Network



Asset-to-Asset Task-coordination Network



Overall Organizational Structure



Uncertainty in *communication messages*, *CMDR-asset commands*, *asset-asset task execution*

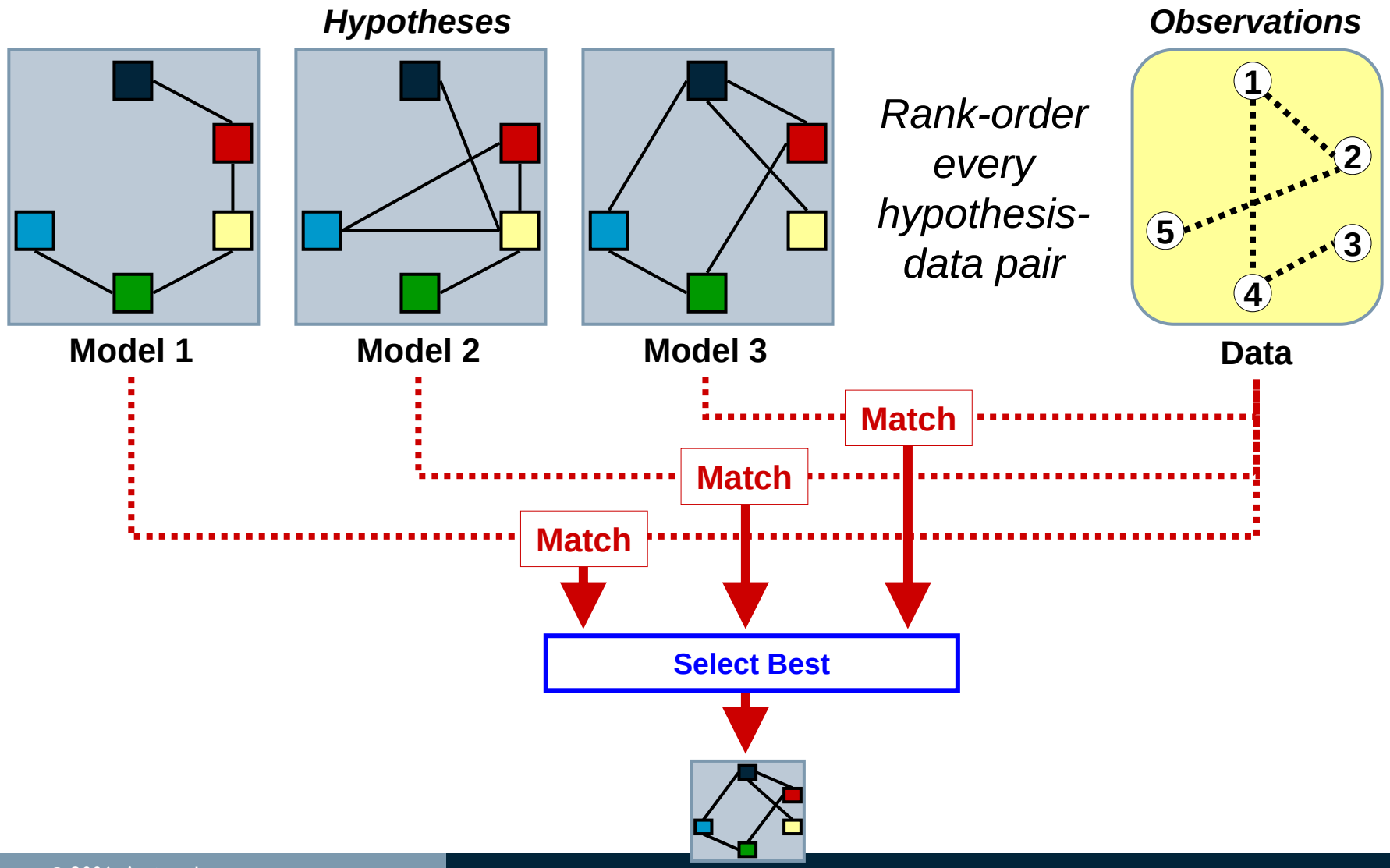
Missing data: unobserved transactions (modeled with miss probability)

Noisy data: wrongly observed transactions (modeled with false alarm probability)

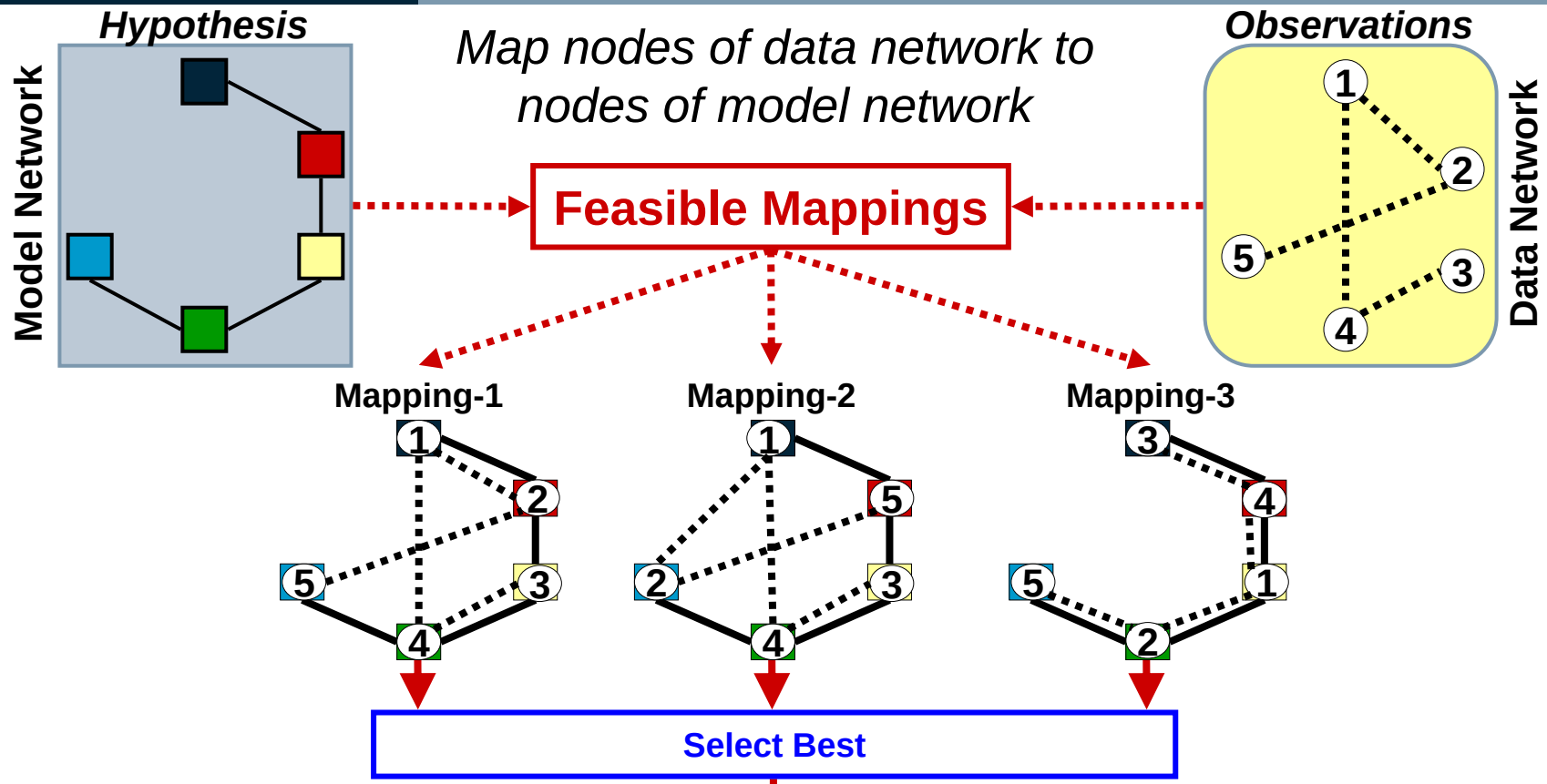
Object	Meaning	Attributes	Observations (real world equivalent)
Communication Link	Who talks to whom about what	Classes of messages	Message between actors and its association
Control Link	What agents control what resources	"Attack" commands	Commands sent from CMDR to asset
Task Link	What assets synchronize	Classes of tasks	Task execution by multiple assets
Nodes	Agents & Assets	Geographic area, functions	Task execution by actor or asset (attacks, recon)

© 2006, Aptima, Inc.

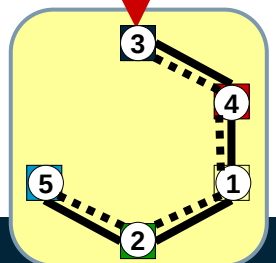
Solution:
Structure Matching via Node Mapping



Solution:
Structure Matching via Node Mapping



- **Objective:** Likelihood or A-Posteriori Function



- Max Structural Consistency
- Max Observed Links
- Min False Observations and Miss

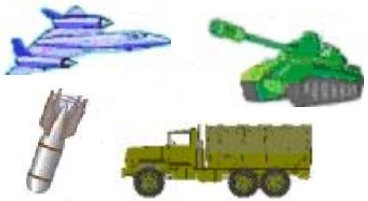
© 2006, Aptima, Inc.

How to Create Data Network

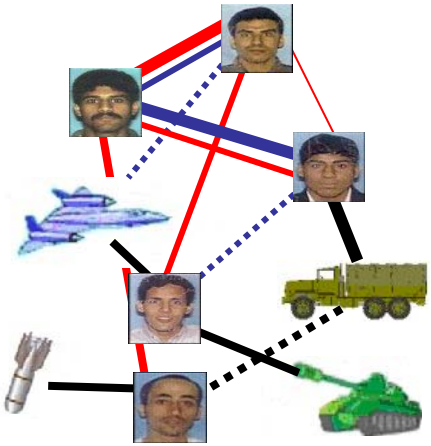
Tracked Actors

Enemy commanders

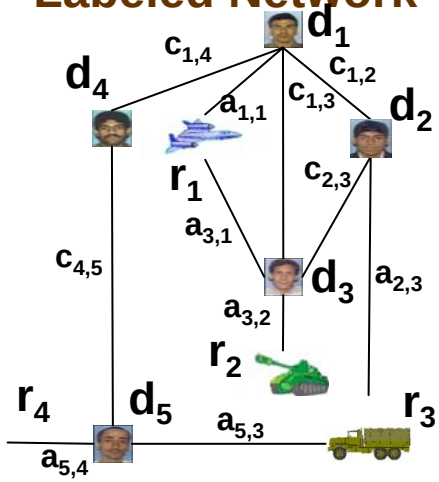
Units/Assets



Observed Interactions



Labeled Network



Labels

- Vector of values for quantitatively representing multiple relationship types
- Value weighs the relationship

Node labels

- **Source:** area of responsibility, performed functions/tasks, expertise
- **Example:** sniper ops; sales of weapons; money laundering

Link labels

- **Source:** types of messages
- **Example:** transfer of information; action request; synchronization; etc.

Hypotheses Networks

- Link labels correspond to expected volume of messages

© 2006, Aptima, Inc.

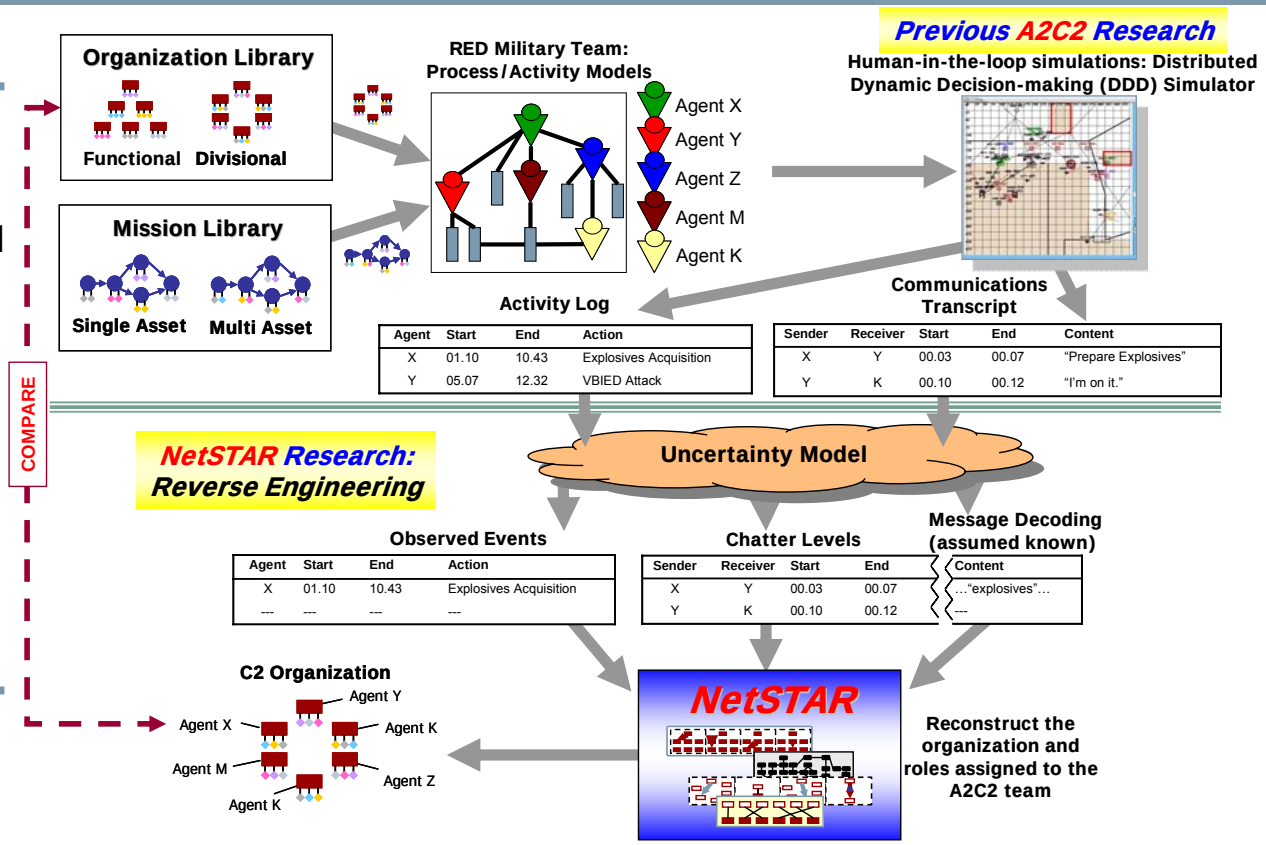
Research Process

Data

- Reuse readily available data from human-in-loop A2C2 Experiments
  - JTF operations; 42 data samples
  - Communications manually coded
  - Events logged in
- Complexity
  - Number of commanders = 6, number of assets = 137
  - Number of events, comms = 1000-4000
- Data uncertainty model based on probability of miss, deception, & error

Detection Focus

- Identification of nodes: **actor-node mapping**
- Identification of resource allocation: **control structure**



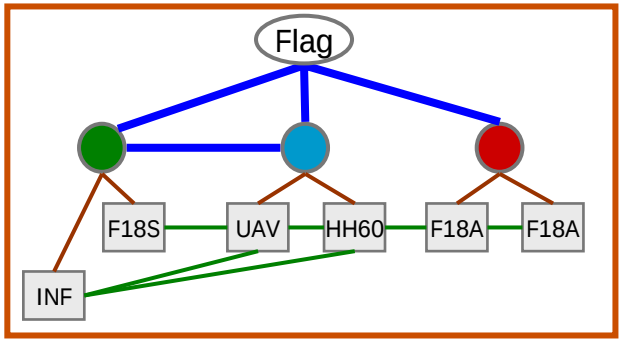
Experimental Comparisons

- Compare results of detecting adversarial organizations as produced by human **2-person test team** in 1 hour vs **algorithm**
- Calculate the impact of information uncertainty on prediction accuracy

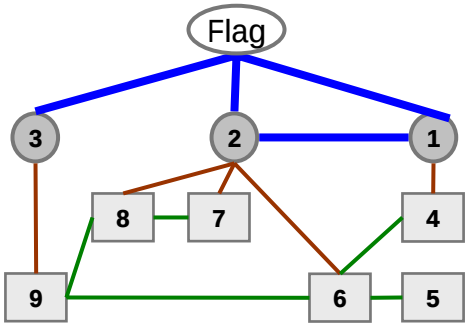
© 2006, Aptima, Inc.

Example Analysis (Simplified)

Structure Hypotheses (true)



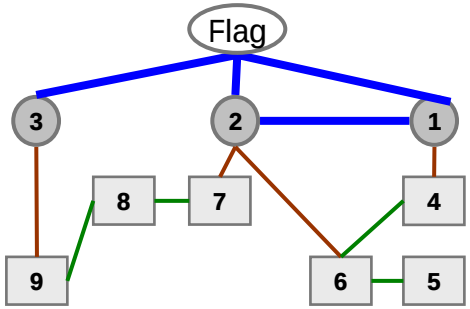
Actual Observations



Correct Map:

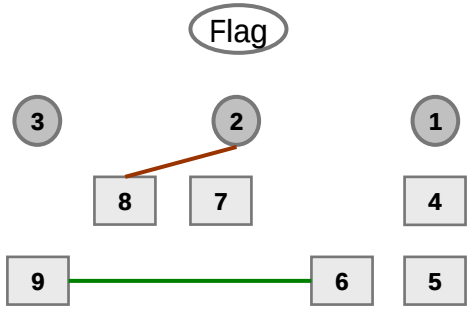
1=GREEN	5=INF
2=BLUE	6=UAV
3=RED	7=HH60
4=F18S	8=F18A
	9=F18A

Correctly Identified Relationships



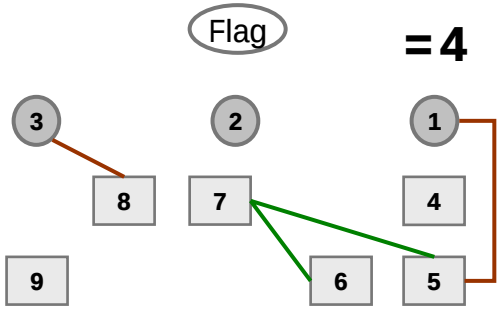
=12

Misidentified Observations (noise)



=2

Undetected Relationships



=4

# of Random Mappings (permutations for actor-agent X resource-asset groups) = 3!*6! = **4320**

# of Random Mappings for Actual Experiment-8 data =6!*126!≈10^{237} (w/o asset class info) or ≈10^{100} (with asset class info)

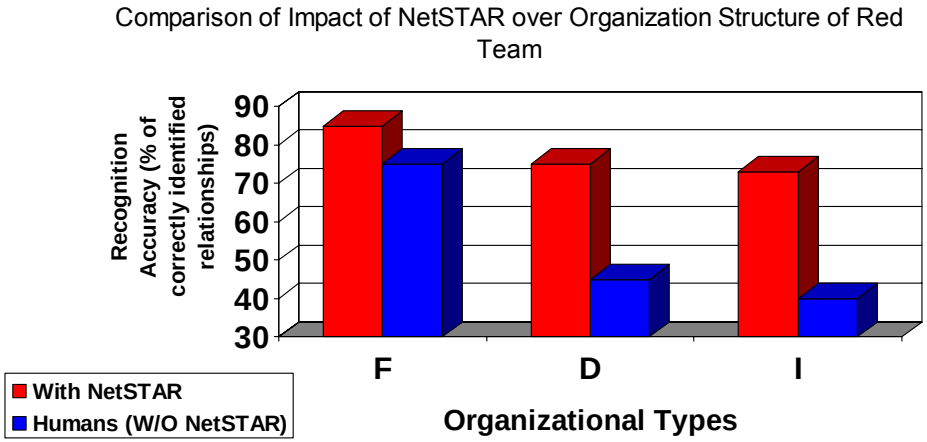
Other Mapping that looks "similar":
1=RED, 2=BLUE, 3=GREEN, 4=F18A, 5=F18A, 6=HH60, 7=F18S, 8=UAV, 9=INF

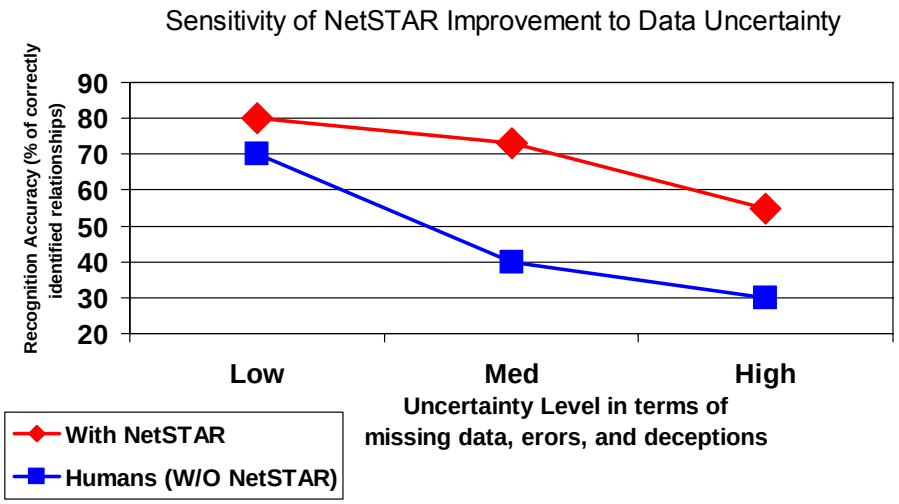
If this mapping was correct:
correct relationships = 12
misidentified relationships = 3
undetected relationships = 5

Truth: # correct node associations by this mapping=1

© 2006, Aptima, Inc.

Anticipated Results





- *Improvement of NetSTAR grows with increased organizational complexity*
- *Curvilinear improvement of NetSTAR with increased uncertainty in source data*

© 2006, Aptima, Inc.

Conclusions

Empirical Observations of Human Team Experiment:

- Humans had difficulty handling the **large volumes of data** – did not use all available information
- Humans exhibited **confirmatory biases** – used first decision and tried to validate it instead of considering other possible solutions
- Humans exhibited **decision biases** – used prior knowledge in their decisions, while it did not apply
- Humans found the problem very **complex** – did not finish solving all parts of the problem

Algorithm

- Automated algorithm is less sensitive to information complexity and data uncertainty
- Initial results suggest significant improvement in recognition accuracy

Next Steps

- Integrate node mapping and temporal behavior pattern recognition

© 2006, Aptima, Inc.

Backups

© 2006, Aptima, Inc.

Experimental Work

Focus

- Compare results of detecting adversarial organizations as produced by
  - Human analysts team alone
  - Automated algorithms

Impact of Uncertainty & Organization Type

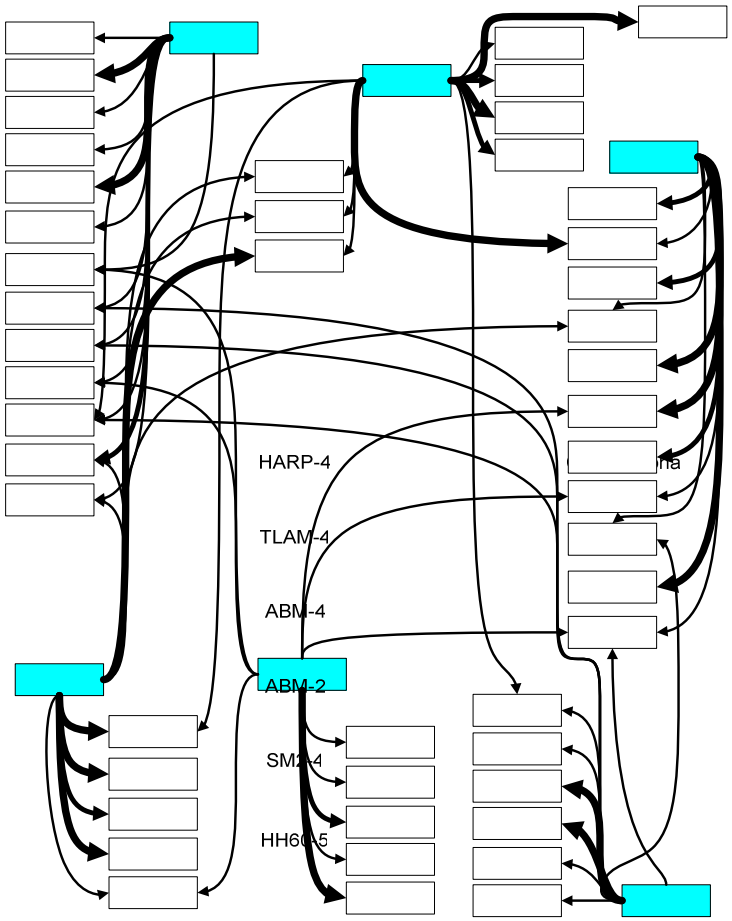
- Calculate the impact of information uncertainty on prediction accuracy
- Calculate the impact of organization type (problem complexity) on prediction accuracy

Recognition Accuracy

- **High-level:** Assess correctness of recognizing operating organization (type)
- **Mid-level:** Assess correctness of mapping tracked actors to adversarial decision-making nodes
- **Low-level:** Assess accuracy of identifying relationships (resource control, communications, command, task coordination)

© 2006, Aptima, Inc.

Human Experiment Design



Input Example: Network of Intercepted Control Messages from CMDRs to units/assets

(Data Sample: Divisional Org)

Procedure

- Teams were given observed data and tasked with matching it to 1 of 7 hypothetic C2 structures
- At the end of each trial, teams developed two products
  - Surveys measuring:
    - Self-reported workload
    - Selection confidence
    - Perceived Fogging Level
    - Perceived Complexity
  - Mapping between Commanders, Leaders, & Assets

		Observed					
	Commanders Mapping	CMDR Alpha	CMDR Bravo	CMDR Charlie	CMDR Delta	CMDR Echo	CMDR Foxtrot
Hypotheses	Green	x					
	Blue			x			
	Purple						x
	Red		x				
	Orange				x		
	Brown					x	

Output Example: Mapping between Observed and Hypothesis CMDRs

Experiment: Effects of Organization Type

Original hypothesis

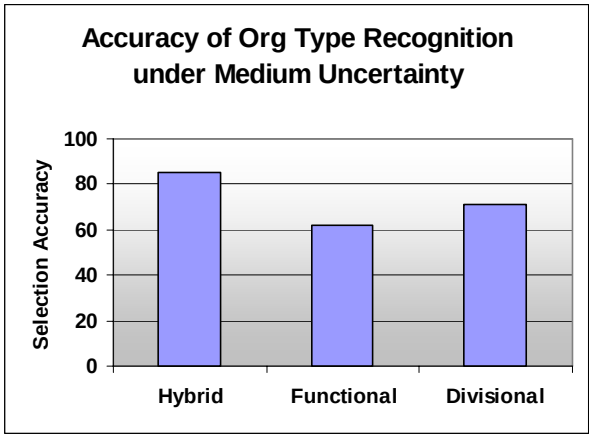
- "Functional" org. (CMDRs controlling assets of the same type) would be easier to recognize by human analysts due to distinction between CMDRs

Experiment results

- Showed that in fact it was more difficult to recognize this organization type

Reasons

- All data was fogged – hence no "clear-cut" picture
- The affecting feature was not a complexity of the baseline but a closeness of other hypotheses
  - Among 7 hypotheses, 3 lied closely to Functional org.



© 2006, Aptima, Inc.

Experiment: Effects of Organization Type

Original hypothesis

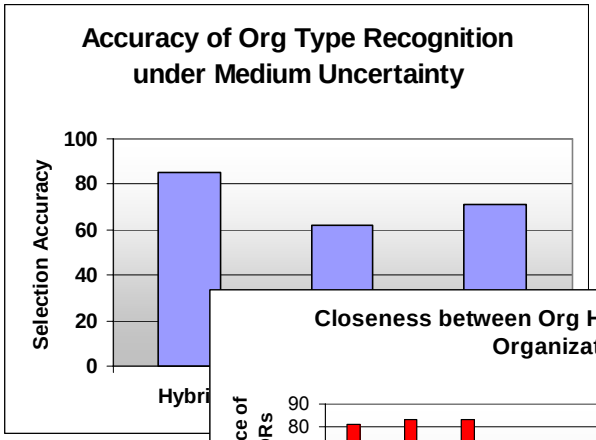
- "Functional" org. (CMDRs controlling assets of the same type) would be easier to recognize by human analysts due to distinction between CMDRs

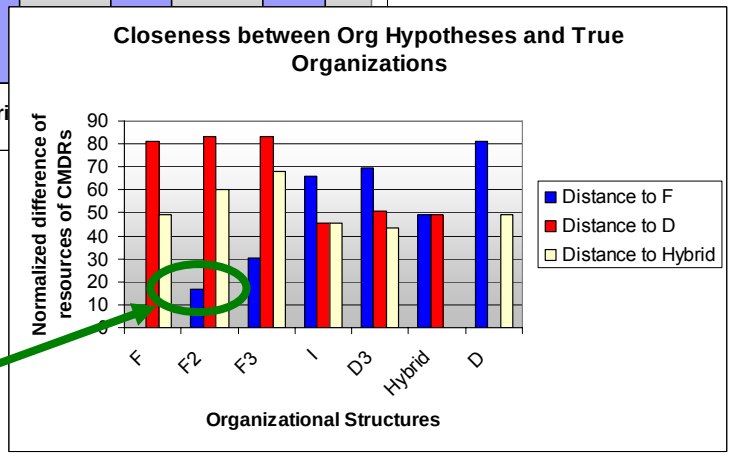
Experiment results

- Showed that in fact it was more difficult to recognize this organization type

Reasons

- All data was fogged – hence no "clear-cut" picture
- The affecting feature was not a complexity of the baseline but a closeness of other hypotheses
  - Among 7 hypotheses, 3 lied closely to Functional org.





Problem: Incorrect hypothesis too close to baseline

Corrective Action:

- Recognizing the org type is not main objective
- Give partial credit for correctly mapping CMDRs' asset control

© 2006, Aptima, Inc.

Experiment: Effects of Organization Type

Original hypothesis

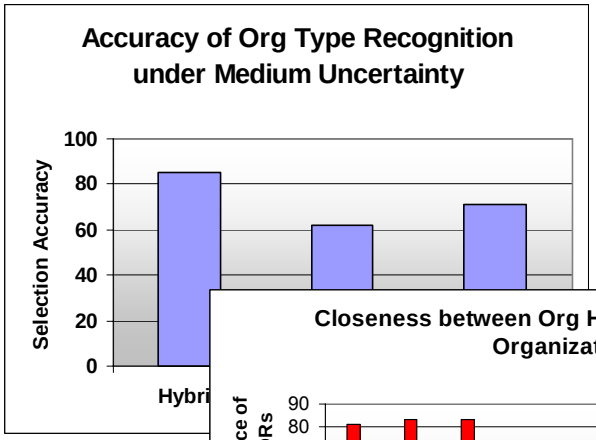
- "Functional" org. (CMDRs controlling assets of the same type) would be easier to recognize by human analysts due to distinction between CMDRs

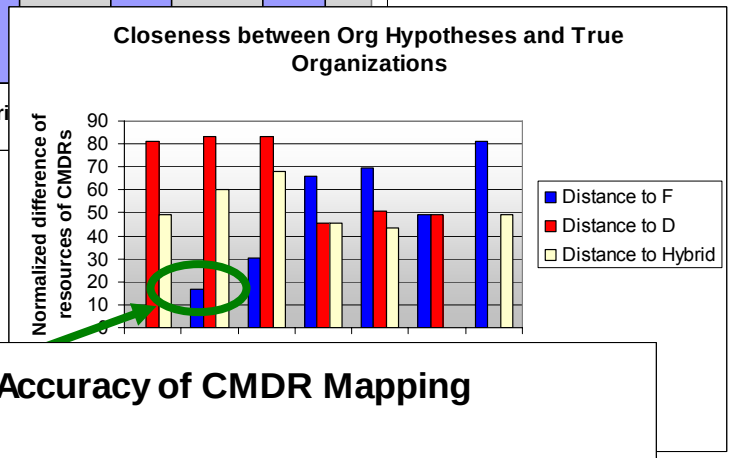
Experiment results

- Showed that in fact it was more difficult to recognize this organization type

Reasons

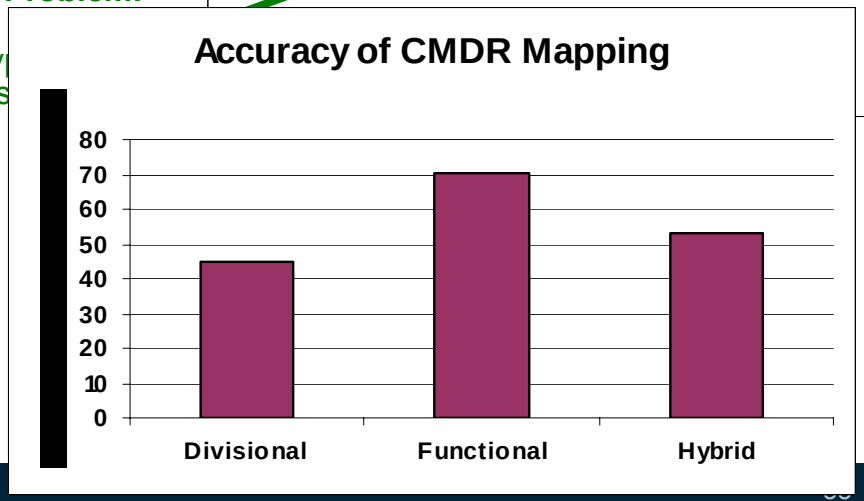
- All data was fogged – hence no "clear-cut" picture
- The affecting feature was not a complexity of the baseline but a closeness of other hypotheses
  - Among 7 hypotheses, 3 lied closely to Functional org.





Problem:

hy
clos



© 2006, Aptima, Inc.

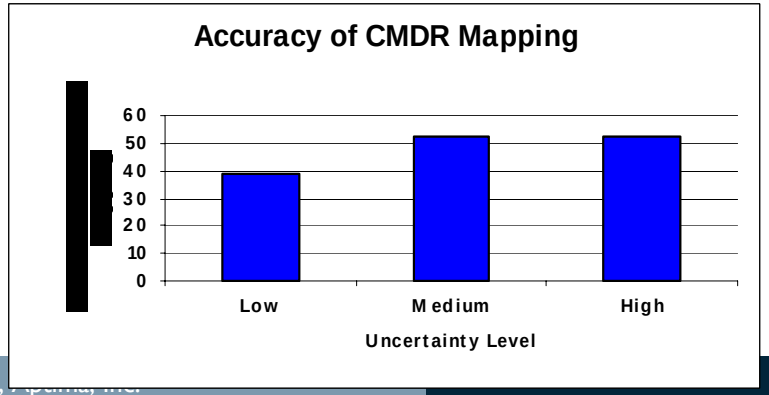
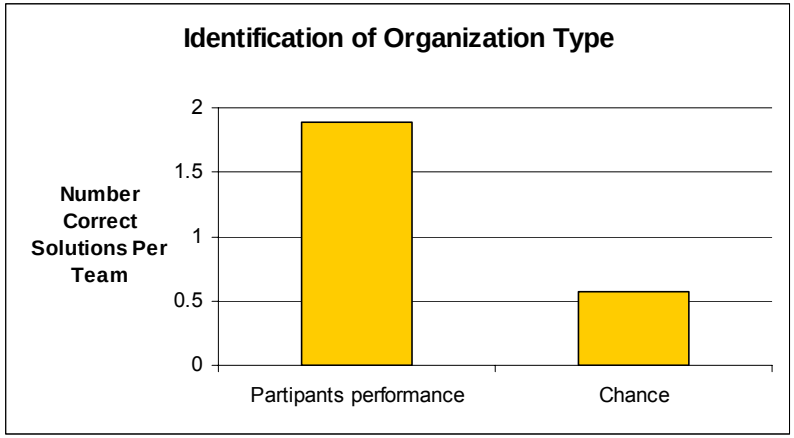
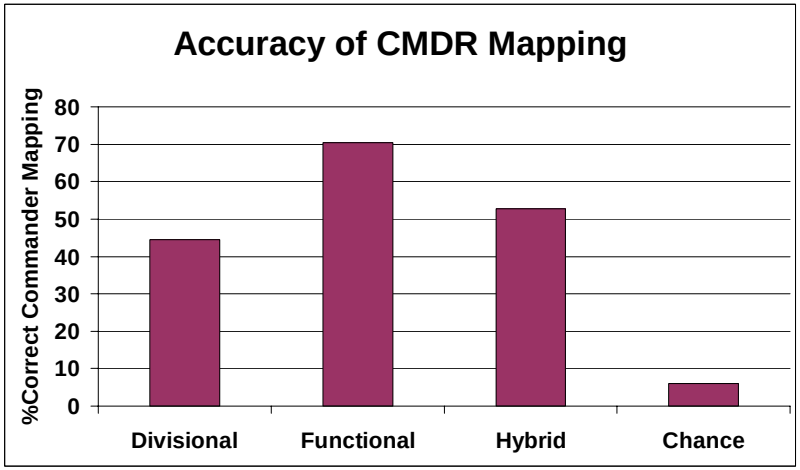
Experiment: Recognition Accuracy

Original hypothesis

- Human analysts achieve higher accuracy than random choice
- Performance degrades with increase in solution complexity & uncertainty

Experiment results

- Showed that in fact human performance was higher than random choice
- The uncertainty results were not conclusive

Reasons

- Between-team testing