Optimal mix of history and intelligence for antiterrorism analysis

M. M. Łatek, S. M. M. Rizi and T. A. Alsheddi
Point of contact: mlatek@gmail.com

13 November 2011

Fancy Quotes

Whoever wishes to foresee the future must consult the past; for human events ever resemble those of preceding times. This arises from the fact that they are produced by men who ever have been, and ever shall be, animated by the same passions, and thus they necessarily have the same results.

Niccolò Machiavelli

Fancy Quotes

Whoever wishes to foresee the future must consult the past; for human events ever resemble those of preceding times. This arises from the fact that they are produced by men who ever have been, and ever shall be, animated by the same passions, and thus they necessarily have the same results.

Niccolò Machiavelli

History teaches everything, even the future.

Alphonse de Lamartine

Fancy Quotes

Whoever wishes to foresee the future must consult the past; for human events ever resemble those of preceding times. This arises from the fact that they are produced by men who ever have been, and ever shall be, animated by the same passions, and thus they necessarily have the same results.

Niccolò Machiavelli

History teaches everything, even the future.

Alphonse de Lamartine

Any philosophy that asserts human experience repeats itself is ineffective.

Jacques Ellul

Fancy Quotes

Whoever wishes to foresee the future must consult the past; for human events ever resemble those of preceding times. This arises from the fact that they are produced by men who ever have been, and ever shall be, animated by the same passions, and thus they necessarily have the same results.

Niccolò Machiavelli

History teaches everything, even the future.

Alphonse de Lamartine

Any philosophy that asserts human experience repeats itself is ineffective.

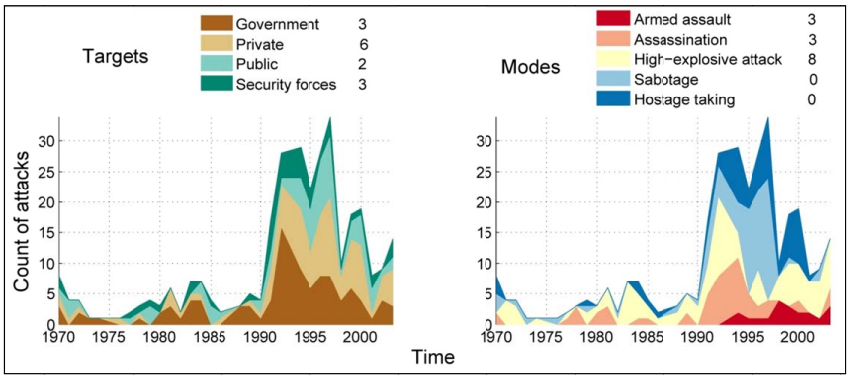
Jacques Ellul

History never repeats itself; at best it sometimes rhymes.

Mark Twain

The Problem in Vignettes

History of Attacks till 2003



Yearly attack counts in the region of interest in 1970-2003. Numbers next to the legend refer to attacks, their modes and targets in 2003.

Counts of attacks in 2000-2003, tabulated by type and mode

Attack mode	Government	Private	Public	Security
Armed assault	1	3	2	2
Assassination	3	1	0	1
High-explosive attack	7	9	5	3
Sabotage	0	2	0	0
Hostage taking	1	4	5	0

Total 4 year counts of attacks: 50

Intelligence Brief

Organizations

At least four major terrorist organizations of different sizes, age and history are believed to operate in the region:

Name	Size	Total attacks	Success rate	Fatalities per attack	Time since last attack	Mode of last attack
X_1	50	6	100%	7	0	Raid
X_2	20	2	10%	10	2	Assassination
X_3	200	8	40%	0.5	1	Sabotage
X_4	20	4	100%	20	0	Car bomb
Multiple unknown	n/a	14	62%	2	0	Trash bomb

Latest intelligence obtained

1. Intercepted message by an X_2 operative left for a prominent financier:

   We will soon teach the American lapdogs and their masters a lesson they won't forget.
2. Radio scanners, annotated maps and light weapons were found a week ago in a deserted safe house possibly belonging to an X_2 cell.
3. Comment by a known X_2 recruiter in a discussion thread on a Jihadist forum about their attitude towards civilian fatalities caused by a terror attack:

   Weren't the people working at the WTC helping the enemy occupy our brothers' land? Any sane man would say yes. They were doing what American soldiers are doing in Iraq, only in suits.
4. A known X_1 sympathizer left his job ten days ago and has not been seen since.
5. An X_1 explosives guru has travelled to Dubai several times in the past six months.

Atmospherics

A video of a successful car bomb attack by X_2 that killed 34 U.S. servicemen has gone viral among male cell phone users in the country.

A recent survey in the region shows that 79% of male respondents are satisfied with government crackdowns on terrorist activity.

The Problem in Words

Antiterrorists who face adaptive and intelligent adversaries need to construct the most likely and effective terrorist courses of action (COAs) to devise optimal countermeasures

- History is one source of terrorists' COAs. But organizations evolve and terrorists *do* learn not to repeat the same mistakes.
- Another way to predict terrorists' COAs is to deduce them from current intelligence on their preferences, organizational behavior and structure. Intelligence is necessarily incomplete and noisy; deduction is difficult.

The Problem in Words

Antiterrorists who face adaptive and intelligent adversaries need to construct the most likely and effective terrorist courses of action (COAs) to devise optimal countermeasures

- History is one source of terrorists' COAs. But organizations evolve and terrorists *do* learn not to repeat the same mistakes.
- Another way to predict terrorists' COAs is to deduce them from current intelligence on their preferences, organizational behavior and structure. Intelligence is necessarily incomplete and noisy; deduction is difficult.

Can data on past terrorist operations be optimally blended with forward-looking analysis?

Agenda

i **History and intelligence in antiterrorism analysis**

- Red and Blue courses of action;
- Notion of analytical mix.

ii **Case study: Vinnell corporation car bomb attack in 1995**

- Data requirements of the model;
- Agents: (*a*) recursive strategists; (*b*) beliefs and behaviors for operatives;
- Environments.

iii **Simulation results**

iv **Conclusions**

Red Courses of Action

The Red *strategist* uses his partial knowledge of

1. The environment;
2. Current Blue strategy and
3. His own organization and behavioral heuristics of *operatives*

to design a course of action as a set of triplets

$$\langle \textbf{target}, \textbf{attack mode}, \textbf{agent} \rangle$$

The Red *strategist* must

1. Account for the stochasticity of the environment;
2. Be able to achieve diversion by making temporal tradeoffs among courses of action with similar short-term payoffs;
3. Be able to handle failure by replanning, and planning to replan.

Blue Courses of Action

The Blue *strategist* uses his partial knowledge of

1. The environment;
2. History of interactions between Blue and Red and
3. Intelligence on Red organization

to design a course of action as a vector of budget items

$$\begin{bmatrix} \boldsymbol{s}_1 & \boldsymbol{s}_2 & \cdots & \boldsymbol{s}_N & \boldsymbol{m} \end{bmatrix}$$

where N is the number of targets and $\boldsymbol{m}$ is the mobile defense not tied to any specific target.

The Blue *strategist* must

1. Account for the stochasticity of the environment;
2. Be able to tackle "strategic uncertainty" when Red can launch multiple operations it is indifferent to.

Interactions between COAs

After Red sets its COA, we simulate which operations will be sucessfully organized. This process generates a stream of triplets

$$\langle \textbf{target}, \textbf{attack mode}, \textbf{time} \rangle$$

A prepared attack at target i with hardness of h_i is foiled by security forces with probability

$$\frac{1}{1 + \exp\left[h_i \left(\boldsymbol{s}_i + \gamma \boldsymbol{m}\right)\right]}$$

After an attack, m is depleted and slowly recovers afterwards. Blue gains information when a Red attack gets past the production stage. Blue also intercepts portion of communication between Red agents regardless.

Analytical Mix

Blue *strategist* needs to obtain a set of stream of triplets to design his defensive allocation:

$$\langle \textbf{target}, \textbf{attack mode}, \textbf{time} \rangle$$

This information comes from (*a*) history and (*b*) from running simulations initialized with the fused current intelligence Blue has on the Red organization.

An **analytical mix** is a tuple $\langle \kappa, \tau \rangle$ where κ denotes the number of sets of $\langle$target, attack mode, time$\rangle$ triplets taken from history; τ the number of those sampled from by the oracle.
$\tau + \kappa$ sets of triplets $\langle$target, attack mode, time$\rangle$ can indicate that Red will launch

1. No attack at all;
2. Single set of $\langle$target, attack mode$\rangle$ multiple times or
3. Multiple combinations of $\langle\langle$target, attack mode$\rangle\rangle$.

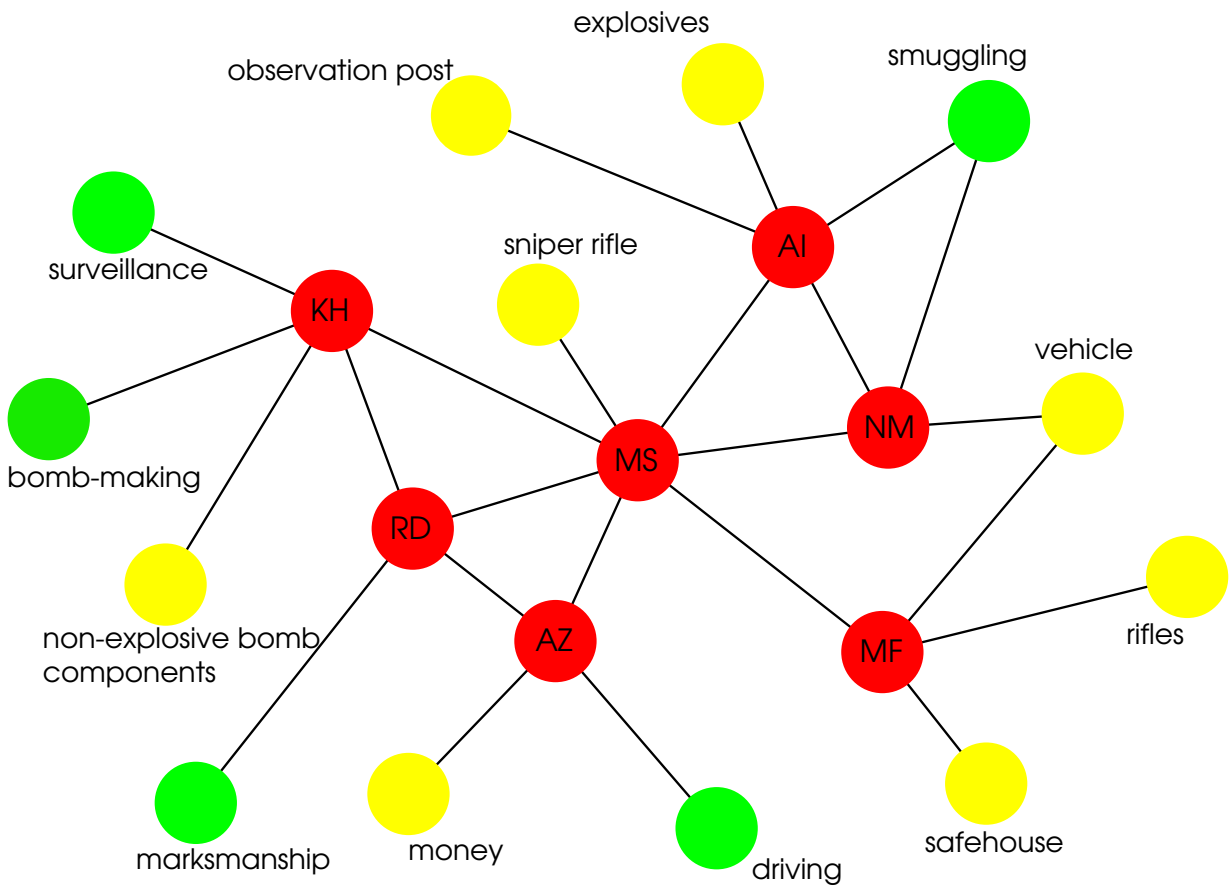
Initial Network of Agents, Resources and Skills

AZ is the strategist for Red organization.

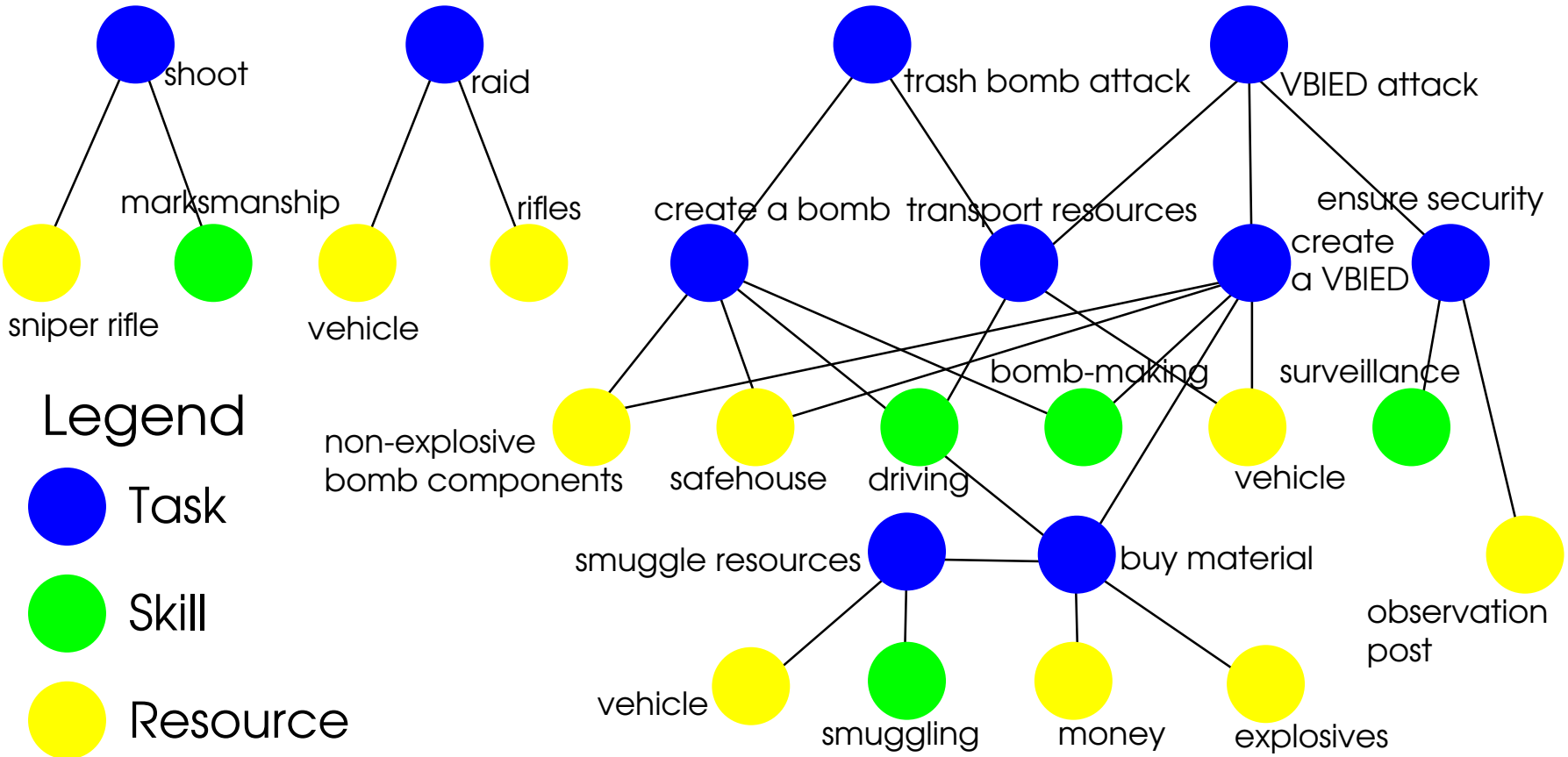
Neither Red nor Blue agents do not *necessarily* have access to this picture.

Legend

- Agents
- Resources
- Skills



Tasks, Resources and Skills



Red and Blue Payoffs

Target	Mode of attack				Hardness
	VBIED	Sniping	Bombing	Raiding	
VC	$\begin{pmatrix} 10 & -10 \\ -3 & 1 \end{pmatrix}$	*	$\begin{pmatrix} 2 & -2 \\ -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 3 & -3 \\ -4 & 1 \end{pmatrix}$	1
MOM	$\begin{pmatrix} 20 & -10 \\ -3 & 1 \end{pmatrix}$	*	$\begin{pmatrix} 2 & -2 \\ -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 6 & -6 \\ -4 & 1 \end{pmatrix}$	2
MOD	*	$\begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix}$	*	*	5
AE	$\begin{pmatrix} 40 & -40 \\ -3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix}$	*	*	4
TIU	*	$\begin{pmatrix} 2 & -1 \\ -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 3 & -3 \\ -2 & 1 \end{pmatrix}$	*	3

In $\left(\begin{smallmatrix} a & b \\ d & c \end{smallmatrix}\right)$, a and b are Red and Blue payoffs respectively if an attack succeeds; c and d are payoffs if an attack is foiled by Blue. * means that the operation is not applicable.

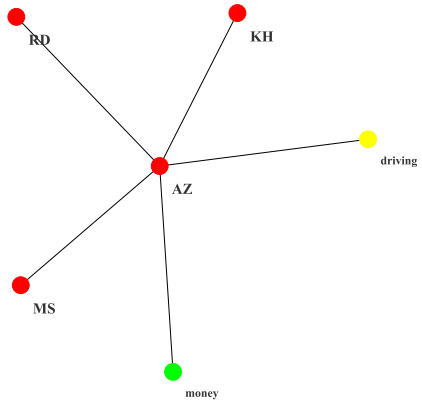
Sample Event Trace

-1 Strategist AZ remains inactive.
15 Strategist AZ remains inactive.
31 Strategist AZ remains inactive.
47 Strategist AZ plans to raid MOM, delegates the task to KH.
48 KH: Task raid and dependencies received.
48 KH: Obtaining a vehicle delegated to MS.
49 MS: Obtaining a vehicle delegated to MF.
50 MF: Vehicle is ready and delivered to MS.
51 MS: Vehicle is ready and delivered to KH.
52 KH: Vehicle delivered back by MS.
70 KH: Obtaining rifles delegated to MS.
71 MS: Obtaining rifles delegated to MF.
72 MF: Rifles are obtained.
73 MS: Rifles delivered by MF.
73 AZ has waited since time 47 for feedback from KH and decides to go for time-out.
74 Strategist AZ plans to execute a trash bomb attack on VC, delegated to KH and a raid on MOM delegated to RD.

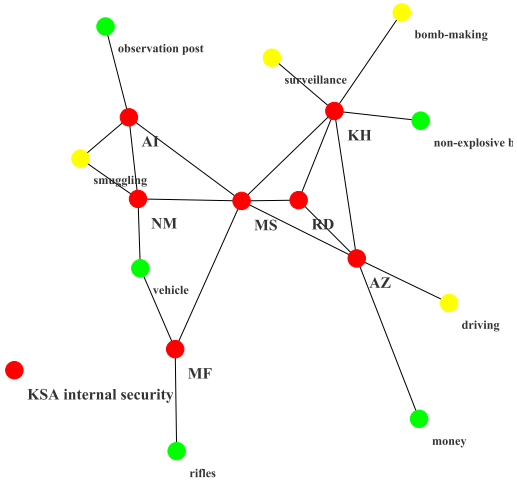
•
•
•

699 Strategist AZ plans to execute a VBIED attack on AE, delegated to RD and sniping TIU, delegated to MS.
699 RD: Task VBIED attack received.
699 RD: Finding an observation post delegated to MS.
700 MS: Task sniping received.
700 MS: Searching for an observation post delegated to AI.
701 AI: Observation post is found.
702 MS: Finding observation post is reported back by AI.
702 MS: RD is denoted marksman.
704 RD: Target surveillance for the VBIED attack delegated to KH.
704 MS: Sniper rifle is available.
706 RD: Surveillance results reported by KH.
706 RD: Operation security ensured.
706 AZ: Readiness to shoot reported by MS.
707 RD: Driving delegated to AI.
707 Operation sniping aimed at TIU foiled by security forces.
708 AZ: Scrapping the rest of the operation.

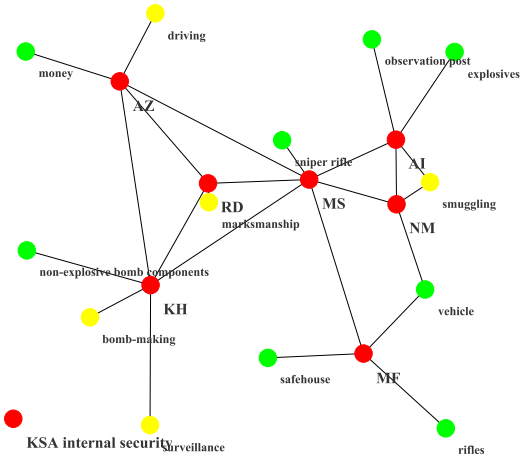
Evolution of Blue and Red Beliefs



(c) AZ, $T = 0$

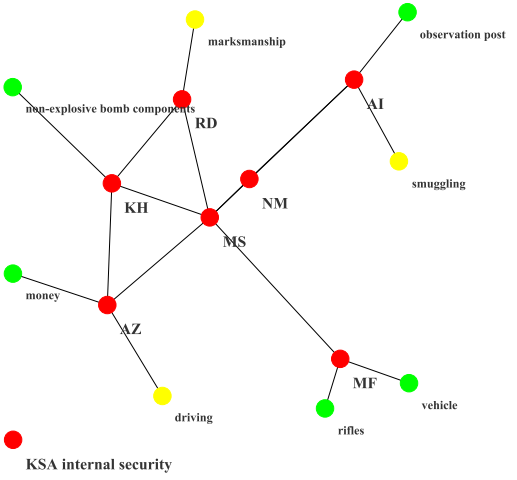


(d) AZ, $T = 200$

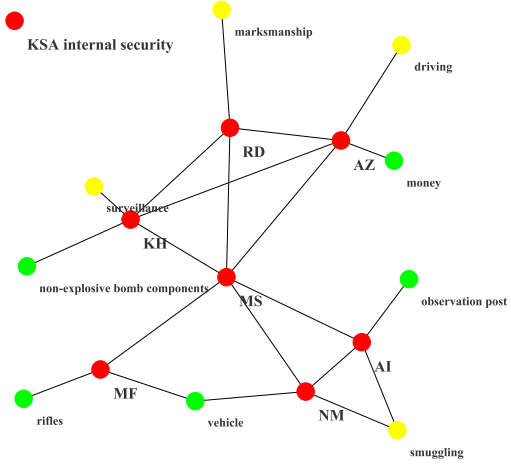


(e) AZ, $T = 600$

(f) KSA, $T = 0$

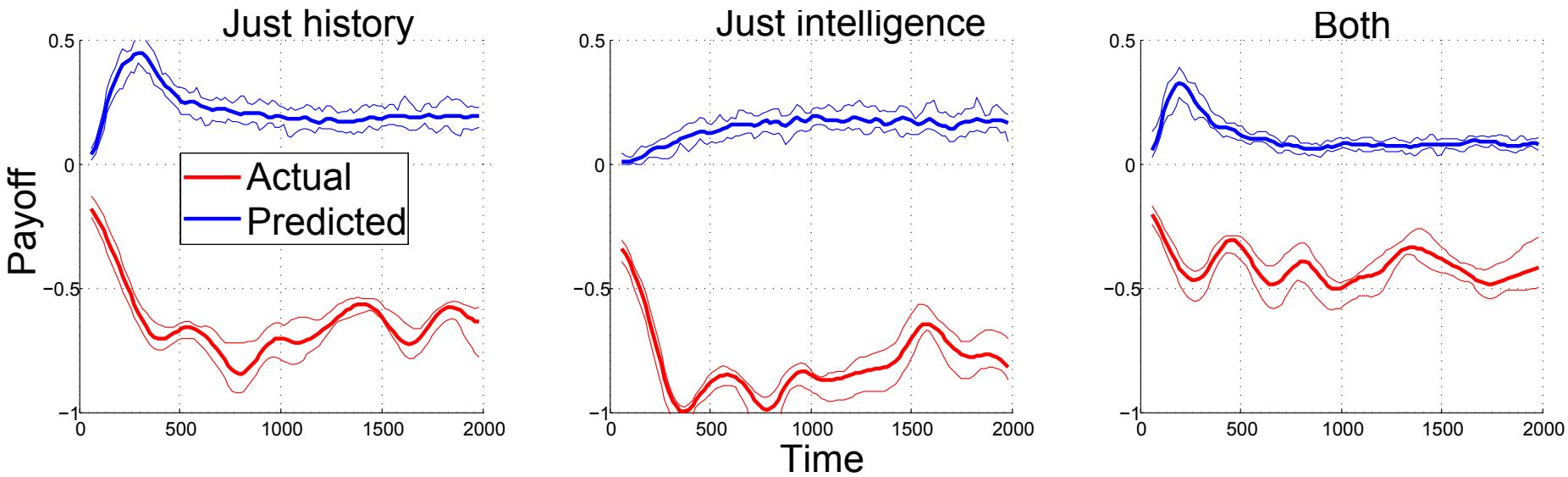


(g) KSA, $T = 200$



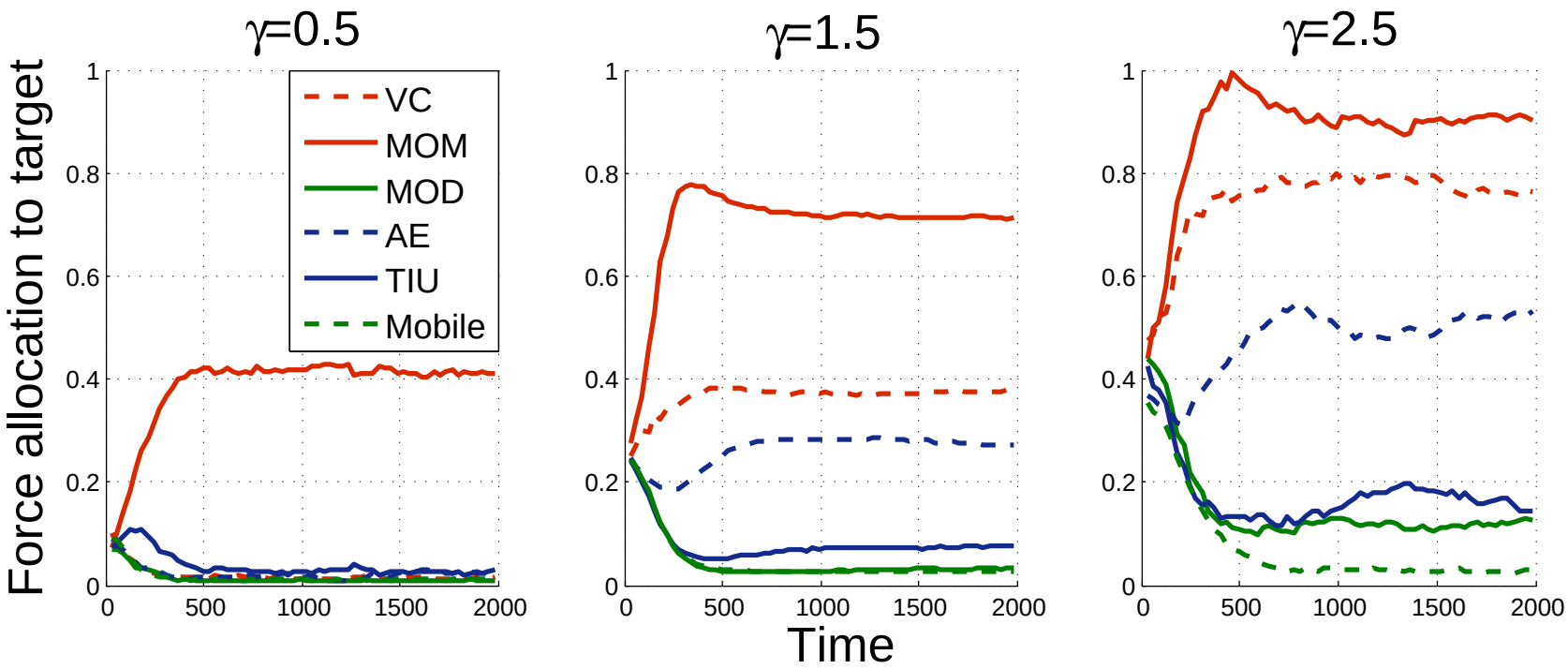
(h) KSA, $T = 600$

Optimal Analytical Mix



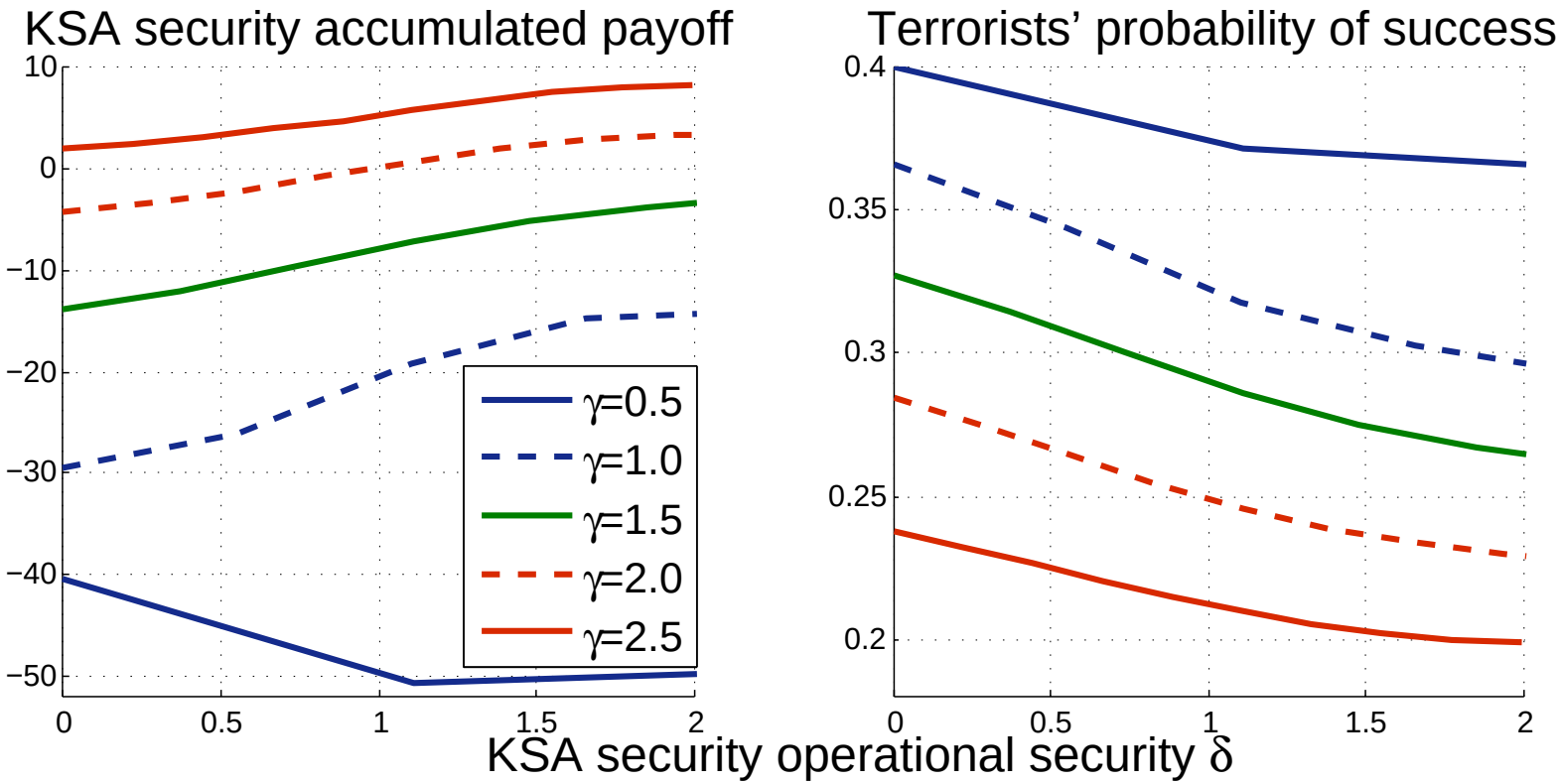
Predicted versus actual payoffs for different analytical mixes. When Blue only optimizes against historical patterns of attack by the terrorist organization we set $\langle \tau_B, \kappa_B \rangle = \langle 0, 10 \rangle$; when it disregards such patterns and relies on anticipation alone we set $\langle \tau_B, \kappa_B \rangle = \langle 10, 0 \rangle$ and when it emphasizes history and anticipation equally, we set $\langle \tau_B, \kappa_B \rangle = \langle 5, 5 \rangle$. Blue used budget of 1.5.

Blue Courses of Action for Different Budgets



Optimal Blue courses of action for budgets of 0.5, 1.5, and 2.5, averaged over 10 runs and plotted as a function of time in absolute and relative terms.

Effectivness of Blue Operational Security



Influence of Blue operational security on Blue loss and Red probability of sucess for different budget levels under optimal analytical mixes.

Comments

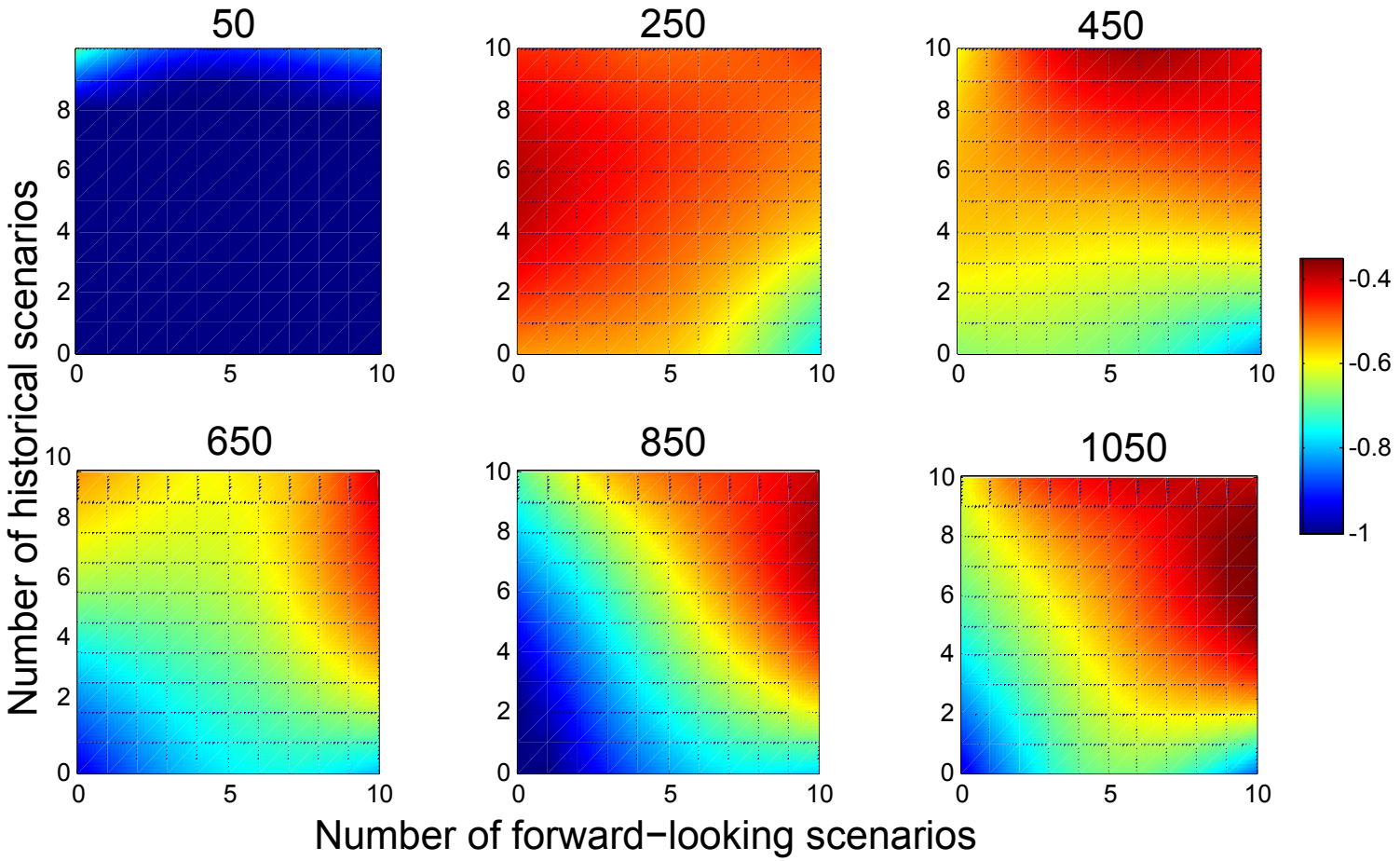
- Our anticipatory agents tackle strategic uncertainty, replanning contingencies, deception and diversion;
- The cognitive architecture has few parameters and can self-calibrate terrorists' and antiterrorists' levels of "sophistication" to the complexity of the environment they operate in;
- The approach does not require elicitation of probabilities, but rather of CONOPS and reasoning heuristics of leaders and operatives.

Thank you!

Parameters of Simulation Experiments

Parameter	Value	Meaning
$d_R, h_R, \tau_R, \kappa_R, K_R$	$1, 50, 1, 0, 10$	AZ's rationality order, planning horizon, numbers of forward-looking, historical and stochastic samples.
d_B, h_B, K_B	$2, 50, 10$	Blue rationality order, planning horizon and number of stochastic samples.
$\langle \tau_B, \kappa_B \rangle$	$\in (0, 10) \times (0, 10)$	KSA security analytical mixture.
Blue budget	$\in \{0.5, 1.5, 2.5\}$	KSA security budget.
y	1.0	KSA mobile defense contribution to site security.
α	0.25	KSA mobile defense damage in a terrorist attack.
Intercept	0.005	Probability that KSA security intercept terrorists' messages.

Optimal Analytical Mix



KSA security payoffs on days 50, 250, 450, 650, 850 and 1050 as a function of analytical mix, with KSA security budget of 1.5. The Y-axis is the size of a set of historical scenarios κ_B; the X-axis is the number of forward looking samples τ_B.

Nature of Oracle

The environment

- Defines all COAs available to terrorists and antiterrorists and allows to replay all of their possible combinations against one another.
- Contains a history of terrorist operations and antiterrorist measures against each operation. If actual information is not available, this history is either empty or filled with COAs designed by experts.
- Codes terrorists' and antiterrorists' payoffs for the outcome of all COAs.

The environment also defines oracle: a minimally sufficient model of organizational behavior for terrorists in which terrorist operatives decompose the operations they are assigned, into tasks and negotiate task delegation and execution among themselves.