Invited Lecture: CS 182
Security Games

MILIND TAMBE

AI & Multiagent Systems Research for Social Impact

Public Health

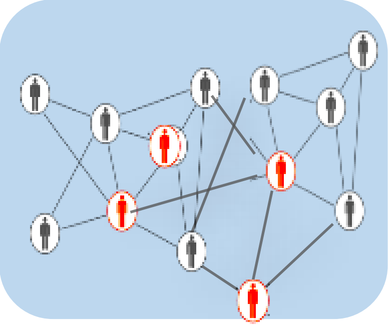
Conservation

Public Safety and Security

Key Research Challenge

Optimize Our Limited Intervention Resources

Optimizing Limited Intervention Resources



Social Networks & Bandits

Public Health

Green security games

Conservation

Stackelberg security games

Public Safety & Security

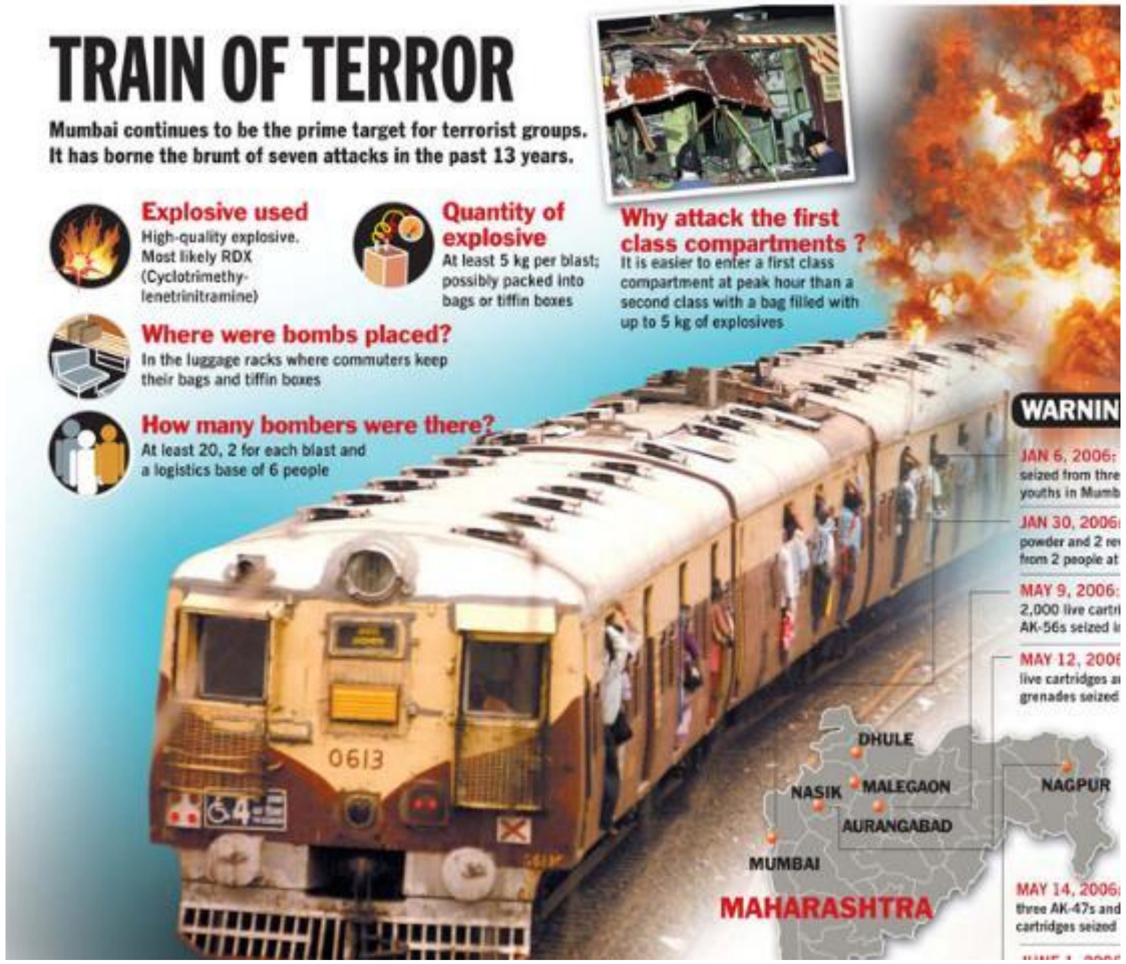
Outline

Public Safety and Security:
Stackelberg Security Games

Conservation/Wildlife Protection:
Green Security Games

20th anniversary of 9/11

11 July 2006: Mumbai



TRAIN OF TERROR

Mumbai continues to be the prime target for terrorist groups. It has borne the brunt of seven attacks in the past 13 years.

Explosive used
High-quality explosive. Most likely RDX (Cyclotrimethylenetrinitramine)

Quantity of explosive
At least 5 kg per blast; possibly packed into bags or tiffin boxes

Why attack the first class compartments ?
It is easier to enter a first class compartment at peak hour than a second class with a bag filled with up to 5 kg of explosives

Where were bombs placed?
In the luggage racks where commuters keep their bags and tiffin boxes

How many bombers were there?
At least 20, 2 for each blast and a logistics base of 6 people

WARNIN

JAN 6, 2006:
seized from thre
youths in Mumb

JAN 30, 2006:
powder and 2 re
from 2 people at

MAY 9, 2006:
2,000 live cartri
AK-56s seized i

MAY 12, 2006
live cartridges a
grenades seized

MAY 14, 2006:
three AK-47s and
cartridges seized

ARMOR Airport Security: LAX(2007)

Erroll Southers

LAX Airport, Los Angeles

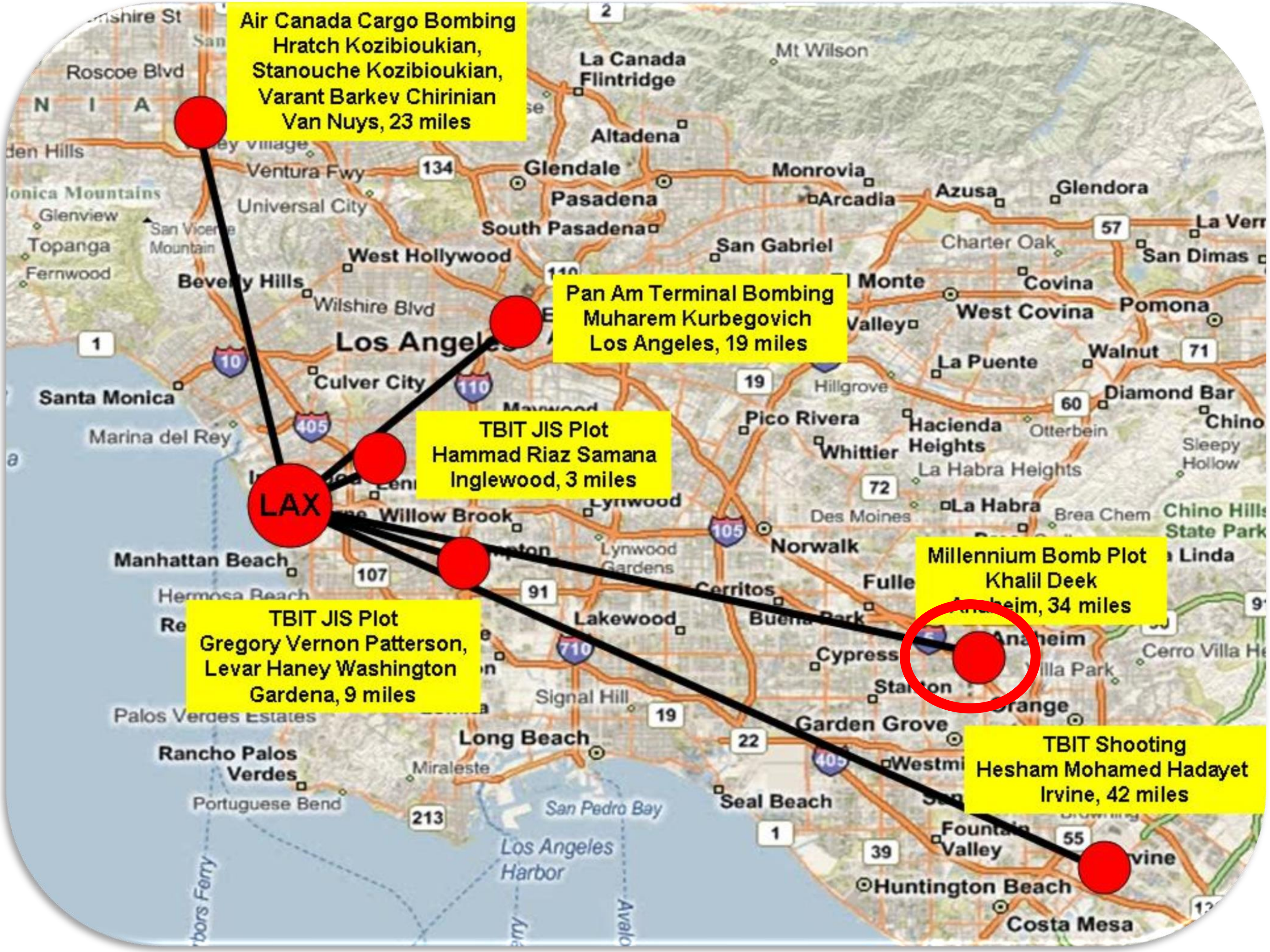
Glasgow: June 30, 2007

LAX Airport Case: Optimize Limited Security Resources

Eight Inbound Roads, Eight Terminals: Limited Staff, Canines

Can we propose game theory for security resource optimization?

Background on LAX Airport Threats:
Surveillance Opportunity



Air Canada Cargo Bombing
Hratch Kozibioukian,
Stanouche Kozibioukian,
Varant Barkev Chirinian
Van Nuys, 23 miles

Pan Am Terminal Bombing
Muharem Kurbegovich
Los Angeles, 19 miles

TBIT JIS Plot
Hammad Riaz Samana
Inglewood, 3 miles

TBIT JIS Plot
Gregory Vernon Patterson,
Levar Haney Washington
Gardena, 9 miles

Millennium Bomb Plot
Khalil Deek
Anaheim, 34 miles

TBIT Shooting
Hesham Mohamed Hadayet
Irvine, 42 miles

Game Theory for Security Resource Optimization

New Model: Stackelberg Security Games, key aspects for tractability

Set of targets, payoffs based on targets covered or not

Stackelberg Leader-Follower formulation

Adversary

Defender

	Terminal #1	Terminal #2
Terminal #1	4, -3	-1, 1
Terminal #2	-5, 5	2, -1

Game Theory for Security Resource Optimization

New Model: Stackelberg Security Games

Adversary

Defender

	Terminal #1	Terminal #2
Terminal #1	4, -3	-1, 1
Terminal #2	-5, 5	2, -1

Model: Stackelberg Security Games

Stackelberg: Defender commits to randomized strategy, adversary responds

Security optimization: Not 100% security; increase cost/uncertainty to attackers

Challenges faced: Massive scale games

Adversary

Defender

	Terminal #1	Terminal #2
Terminal #1	4, -3	-1, 1
Terminal #2	-5, 5	2, -1

ARMOR at LAX
Basic Security Game Operation [2007]

Kiekintveld

Pita

	Target #1	Target #2	Target #3
Defender #1	2, -1	-3, 4	-3, 4
Defender #2	-3, 3	3, -2	….
Defender #3	….	….	….

Mixed Integer Program

Pr (Canine patrol, 8 AM @Terminals 2,5,6) = 0.17

Canine Team Schedule, July 28

	Term 1	Term 2	Term 3	Term 4	Term 5	Term 6	Term 7	Term 8
8 AM		Team1			Team3	Team5		
9 AM			Team1	Team2				Team4
…	…	…	…	…	…	…	…	…

OK IF YOU DO NOT FOLLOW THIS SLIDE

Mixed Integer Program [2007]

Kiekintveld

Pita

j

i

	Target #1	Target #2	Target #3
Defender #1	2, -1	-3, 4	-3, 4
Defender #2	-3, 3	3, -2	….
Defender #3	….	….	….

$$\max \sum_{i\in X}\sum_{j\in Q} R_{ij} \times x_i \times q_j$$

Maximize defender expected utility

$$s.t. \quad \sum_i x_i = 1$$

Defender mixed strategy

$$\sum_{j\in Q} q_j = 1$$

Adversary response

$$0 \le (a \;\; - \sum_{i\in X} C_{ij} x_i) \le (1 - q_j) M$$

Adversary best response

We are trying to Find xi

SECURITY GAME PAYOFFS [2007]
Previous Research Provides Payoffs in Security Games

	Target #1	Target #2	Target #3
Defender #1	2, -1	-3, 4	-3, 4
Defender #2	-3, 3	3, -2	….
Defender #3	….	….	….

+ Handling Uncertainty

$$\max \sum_{i\in X}\sum_{j\in Q} R_{ij} \times x_i \times q_j$$

Maximize defender expected utility

ARMOR:
Optimizing Security Resource Allocation [2007]

First application: Computational game theory for operational security

January 2009

•January 3rd	*Loaded 9/mm pistol*
•January 9th	*16-handguns,* *1000 rounds of ammo*
•January 10th	*Two unloaded shotguns*
•January 12th	*Loaded 22/cal rifle*
•January 17th	*Loaded 9/mm pistol*
•January 22nd	*Unloaded 9/mm pistol*

ARMOR AIRPORT SECURITY: LAX [2008]
Congressional Subcommittee Hearings

Commendations
City of Los Angeles

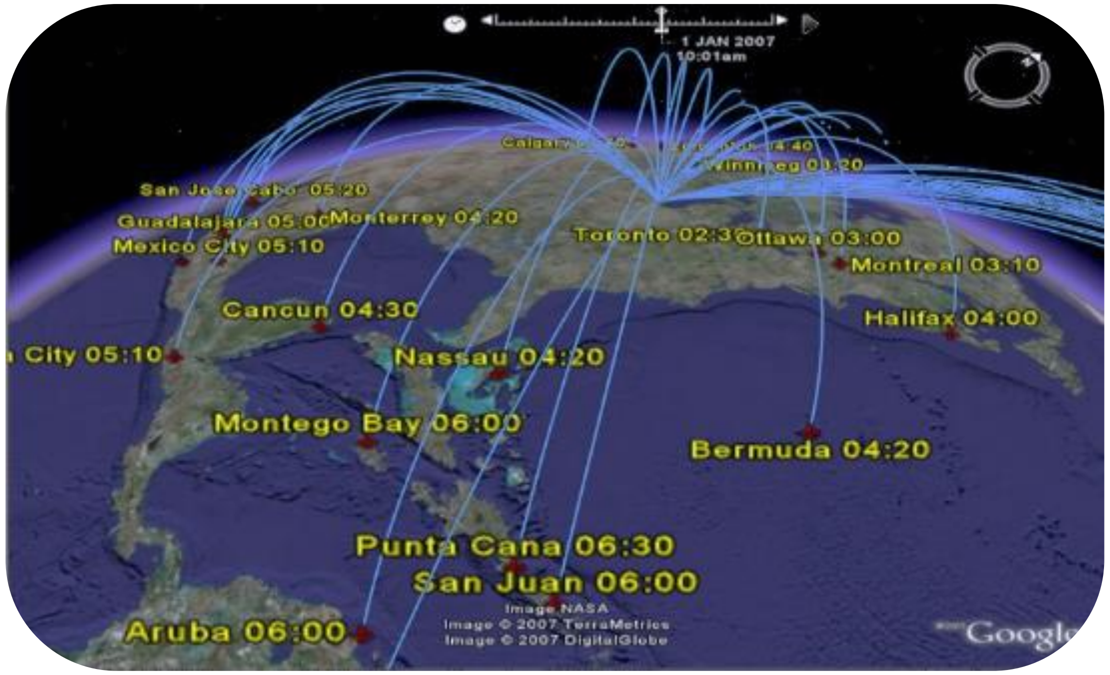
Erroll Southers testimony
Congressional subcommittee

Newsweek

ARMOR…throws a digital cloak of invisibility….

Federal Air Marshals Service [2009]

Visiting Freedom Center: Home of Federal Air Marshals Service



	Strategy 1	Strategy 2	Strategy 3	Strategy 4
Strategy 1	IRIS 1000 flights/day Actions: ~10^{41}			
Strategy 2				
Strategy 3				
Strategy 4				

Scale Up Difficulty [2009]

Kiekintveld

Jain

x_i Defender mixed strategy

1000 flights, 20 air marshals:

10^{41} combinations

$$\max_{x,q} \sum_{i\in X} \sum_{j\in Q} R_{ij} x_i q_j$$

$$s.t. \sum_{i} x_i = 1, \sum_{j\in Q} q_j = 1$$

$$0 \le (a - \sum_{i\in X} C_{ij} x_i) \le (1-q_j)M$$

	Attack 1	Attack 2	Attack …	Attack 1000
1 ,2, 3 ..	5,-10	4,-8	…	-20,9
1, 2, 4 ..	5,-10	4,-8	…	-20,9
1, 3, 5 ..	5,-10	-9,5	…	-20,9
…				
…	← 10^{41} rows			

Scale Up [2009]
Exploiting Small Support Size

Kiekintveld

Jain

Small support set size:
Most x_i variables zero

1000 flights, 20 air marshals:

10^{41} combinations

		Attack 1	Attack 2	Attack …	Attack 1000
~~X_{123} = 0.0~~	~~1 ,2, 3 ..~~	~~5,-10~~	~~4,-8~~	~~…~~	~~-20,9~~
X_{124} = 0.239	1, 2, 4 ..	5,-10	4,-8	…	-20,9
~~X_{135} = 0.0~~	~~1, 3, 5 ..~~	~~5,-10~~	~~-9,5~~	~~…~~	~~-20,9~~
X_{378} = 0.123	…				
	…	← 10^{41} rows			

New Exact Algorithm for Scale up

Kiekintveld

Jain

Incremental strategy generation: First for Stackelberg Security Games

Primary

	Attack 1	Attack 2	…	Attack 6
1,2,4	5,-10	4,-8	…	-20,9

Secondary (LP Duality Theory)

Best new pure strategy

	Attack 1	Attack 2	…	Attack 6
1,2,4	5,-10	4,-8	…	-20,9
3,7,8	-8,10			

lity Theory)

re strategy

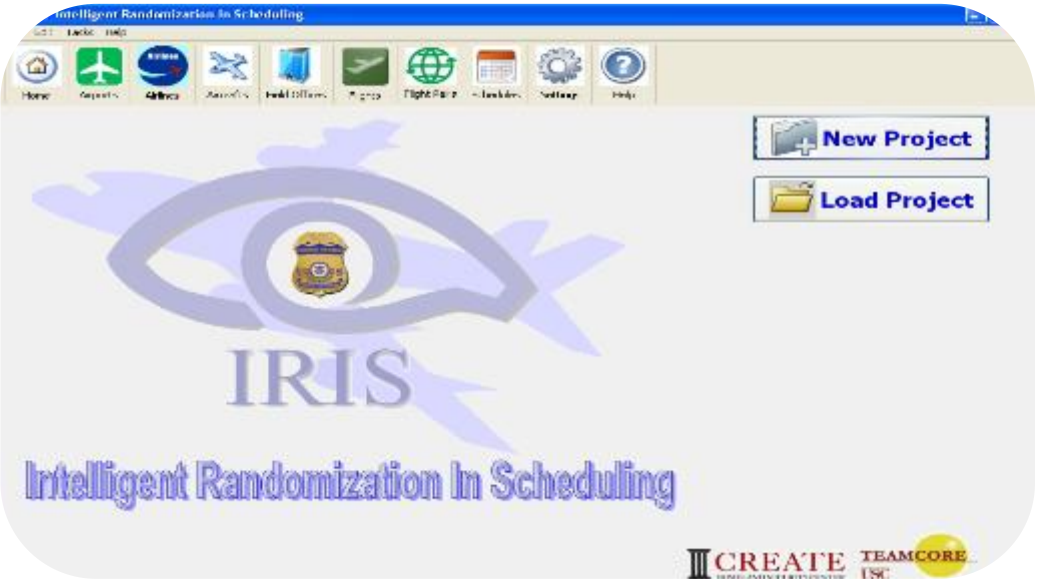
	Attack			
1,2,4	5,-10			
3,7,8	-8,10	-8,10	…	-8,-10
…	…	…	…	…

GLOBAL OPTIMAL

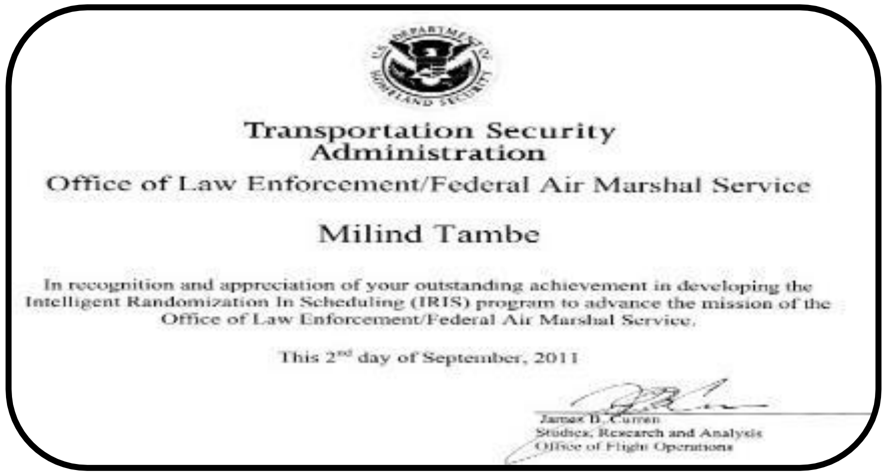
1000 defender strategies

NOT 10^{41}

IRIS: Deployed FAMS [2009-]



Significant change in FAMS operations



Transportation Security Administration

Office of Law Enforcement/Federal Air Marshal Service

Milind Tambe

In recognition and appreciation of your outstanding achievement in developing the Intelligent Randomization In Scheduling (IRIS) program to advance the mission of the Office of Law Enforcement/Federal Air Marshal Service.

This 2nd day of September, 2011

James B. Curren
Studies, Research and Analysis
Office of Flight Operations

September 2011: Certificate of Appreciation (Federal Air Marshals)

Date: 10/6/2021

Questions?

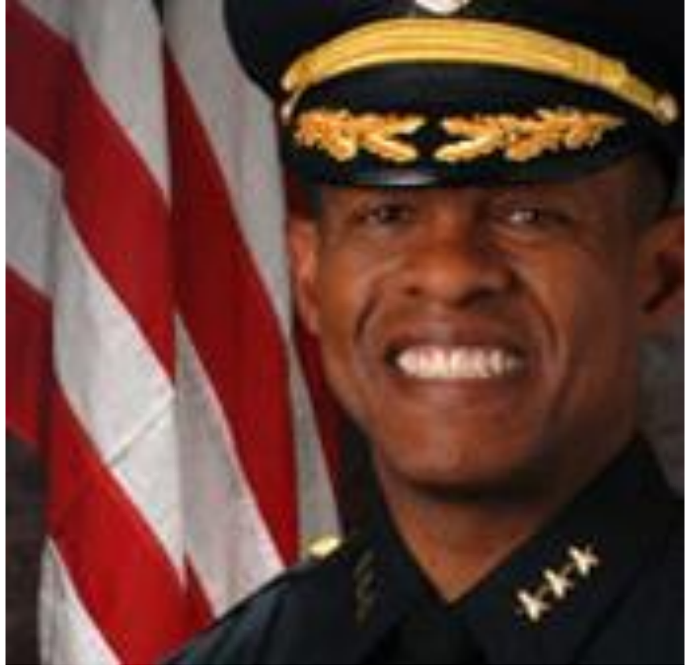
Lesson 1: Immersion & Partnership

UNITED STATES
U
S
TRANSPORTATION SECURITY ADMINISTRATION
U.S. DEPARTMENT OF HOMELAND SECURITY
FEDERAL AIR MARSHAL

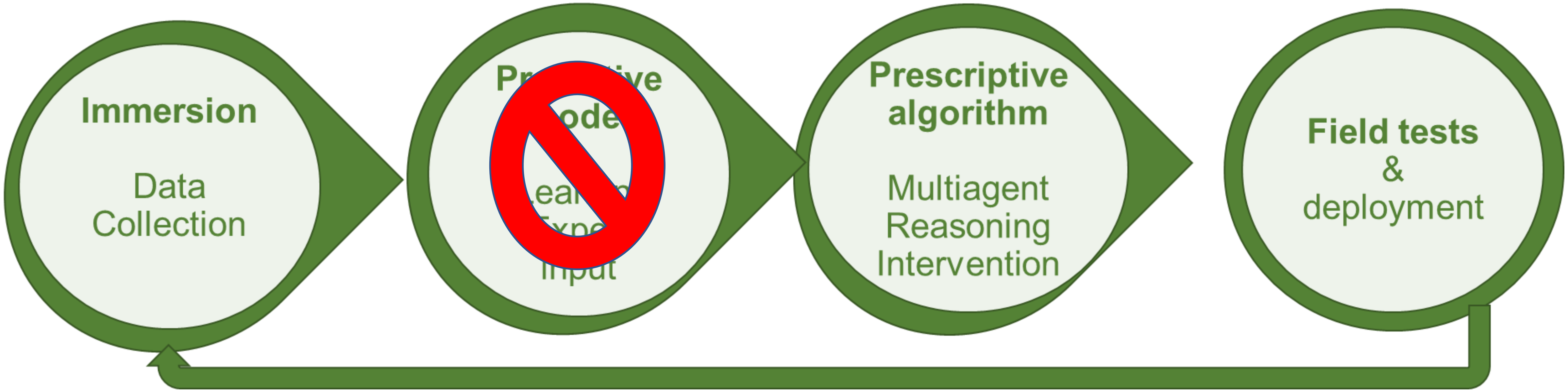
Source: GAO. | GAO-20-125

- Understanding their counter-terrorism experience

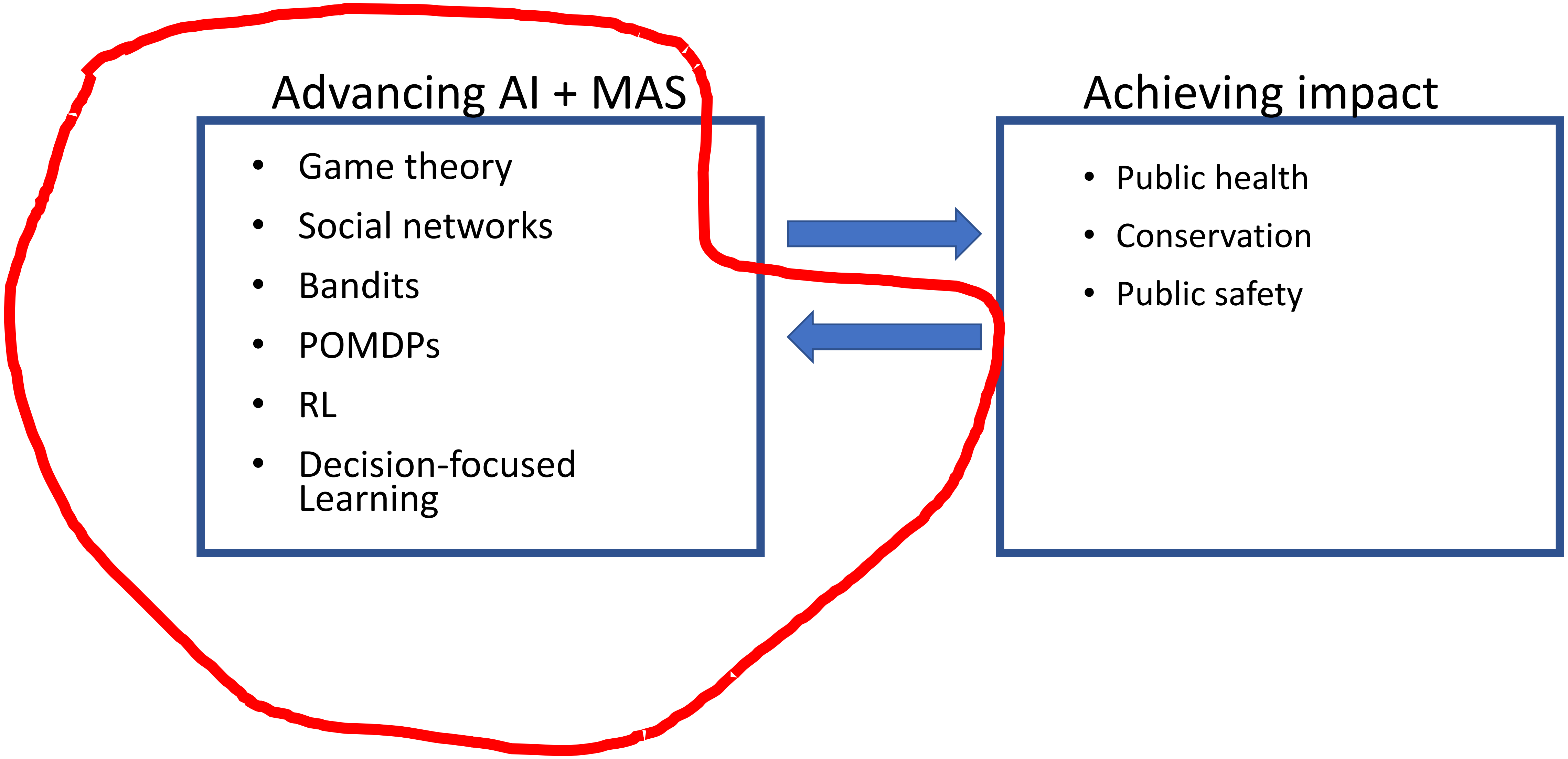
Erroll Southers



Immersion & Data to Deployment Pipeline
Partnership with Govt or non-Govt agency throughout



Lesson 2: AI Innovation & Social Impact Goes Hand-in-Hand



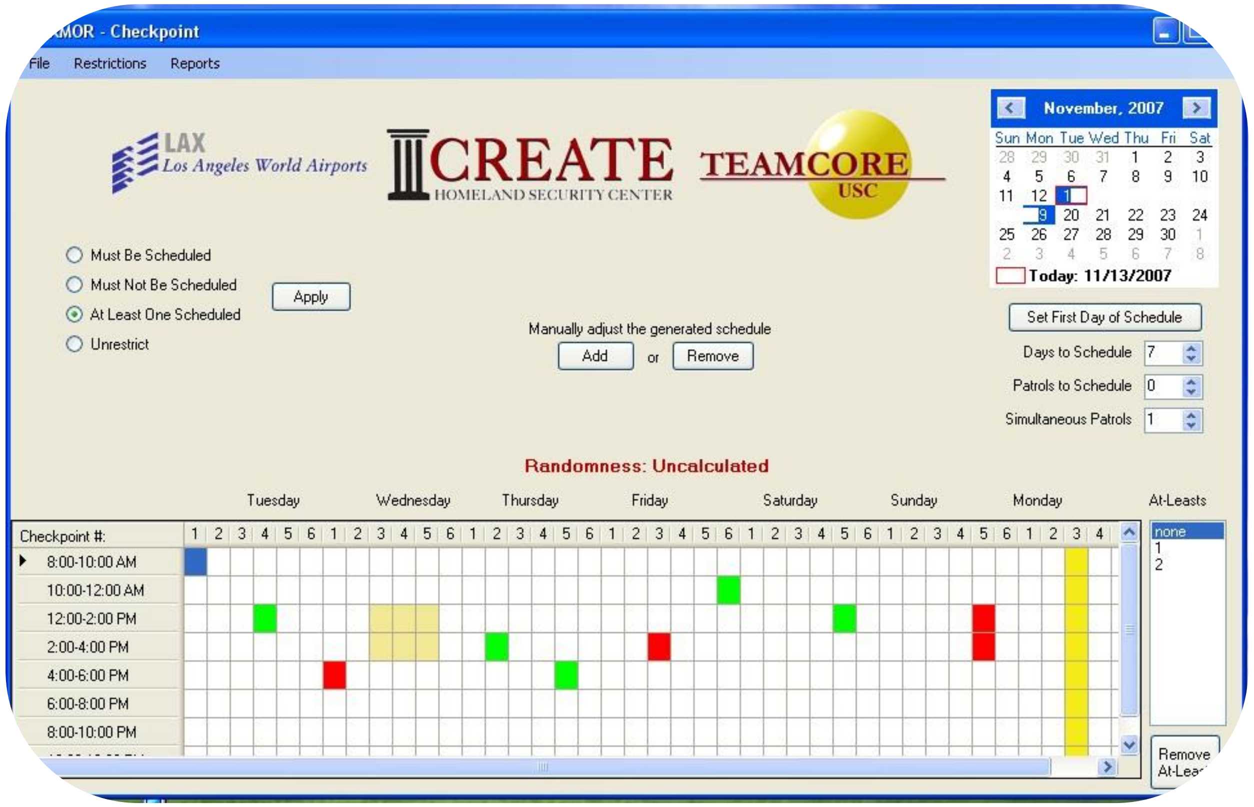
Advancing AI + MAS

- Game theory
- Social networks
- Bandits
- POMDPs
- RL
- Decision-focused Learning

Achieving impact

- Public health
- Conservation
- Public safety

Lesson 3: Need for Human Supervision? but Simplify Interaction



MOR - Checkpoint
File
Restrictions
Reports
LAX Los Angeles World Airports
CREATE HOMELAND SECURITY CENTER
TEAMCORE USC
Apply
Add
Remove
Set First Day of Schedule
Remove At-Lea

November, 2007

Today: 11/13/2007

○ Must Be Scheduled
○ Must Not Be Scheduled
● At Least One Scheduled
○ Unrestrict

Manually adjust the generated schedule Add or Remove

Days to Schedule 7

Patrols to Schedule 0

Simultaneous Patrols 1

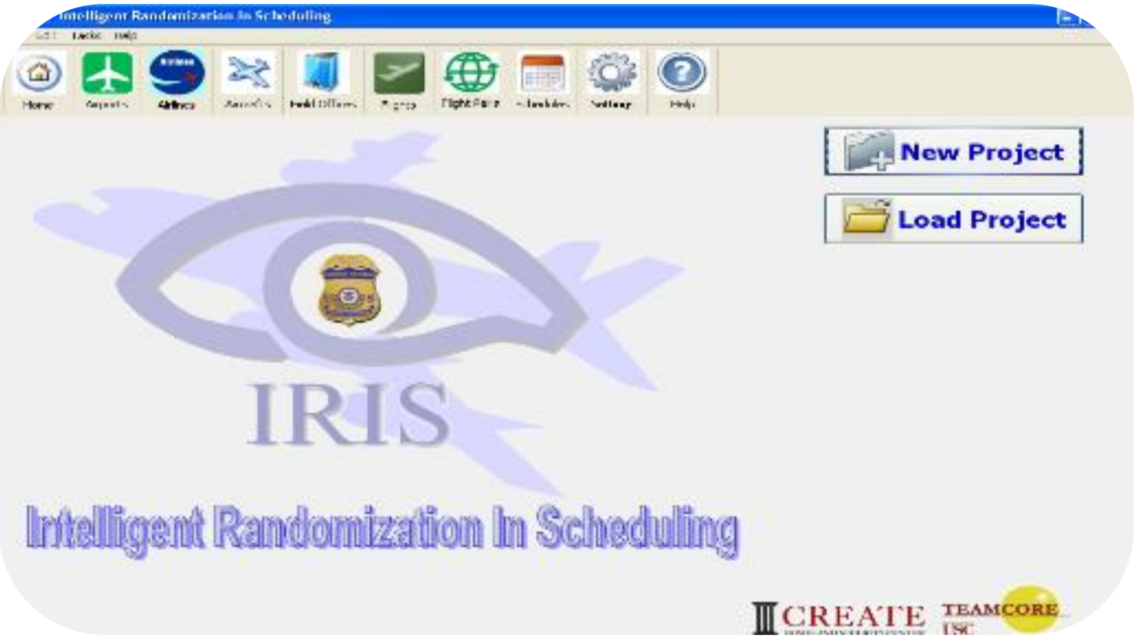
Randomness: Uncalculated

Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Monday

At-Leasts: none, 1, 2

Checkpoint #:

8:00-10:00 AM
10:00-12:00 AM
12:00-2:00 PM
2:00-4:00 PM
4:00-6:00 PM
6:00-8:00 PM
8:00-10:00 PM



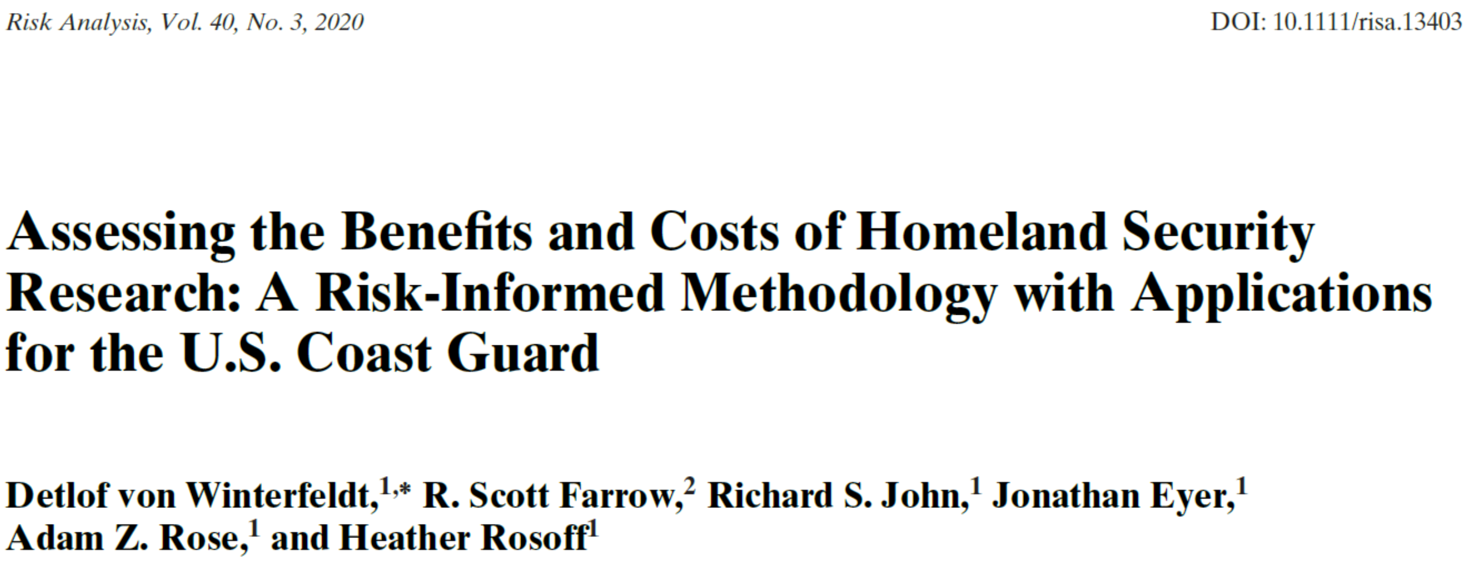
Date: 10/6/2021

ARMOR Transition

ARMOR at LAX, IRIS with FAMS: Both Needed Six Months of Evaluation

- Evaluation: Complicated, secret

Cost-benefit papers are getting published even in 2020

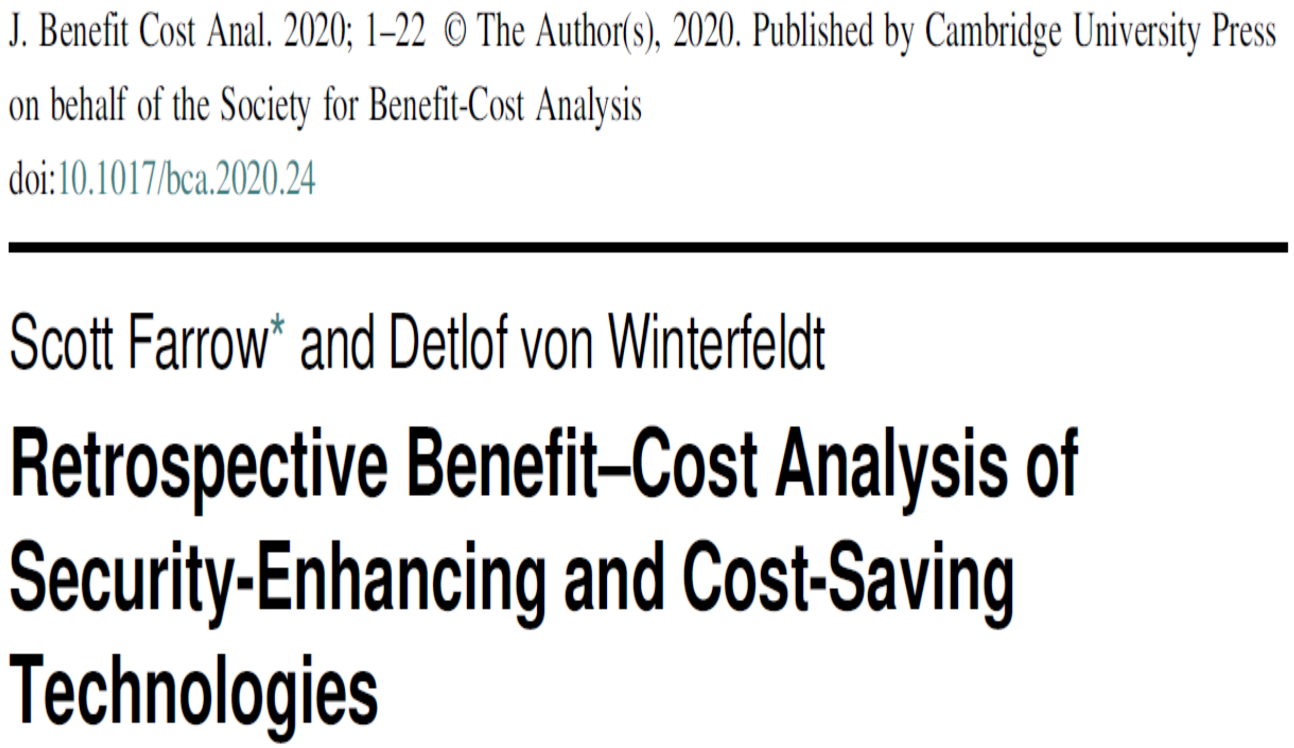


Risk Analysis, Vol. 40, No. 3, 2020

DOI: 10.1111/risa.13403

Assessing the Benefits and Costs of Homeland Security Research: A Risk-Informed Methodology with Applications for the U.S. Coast Guard

Detlof von Winterfeldt,[1,*] R. Scott Farrow,[2] Richard S. John,[1] Jonathan Eyer,[1] Adam Z. Rose,[1] and Heather Rosoff[1]



J. Benefit Cost Anal. 2020; 1–22 © The Author(s), 2020. Published by Cambridge University Press on behalf of the Society for Benefit-Cost Analysis

doi:10.1017/bca.2020.24

Scott Farrow* and Detlof von Winterfeldt

Retrospective Benefit–Cost Analysis of Security-Enhancing and Cost-Saving Technologies

Savings

- $30 Million in ARMOR
- $35 Million in PROTECT
- > benefit of IRIS

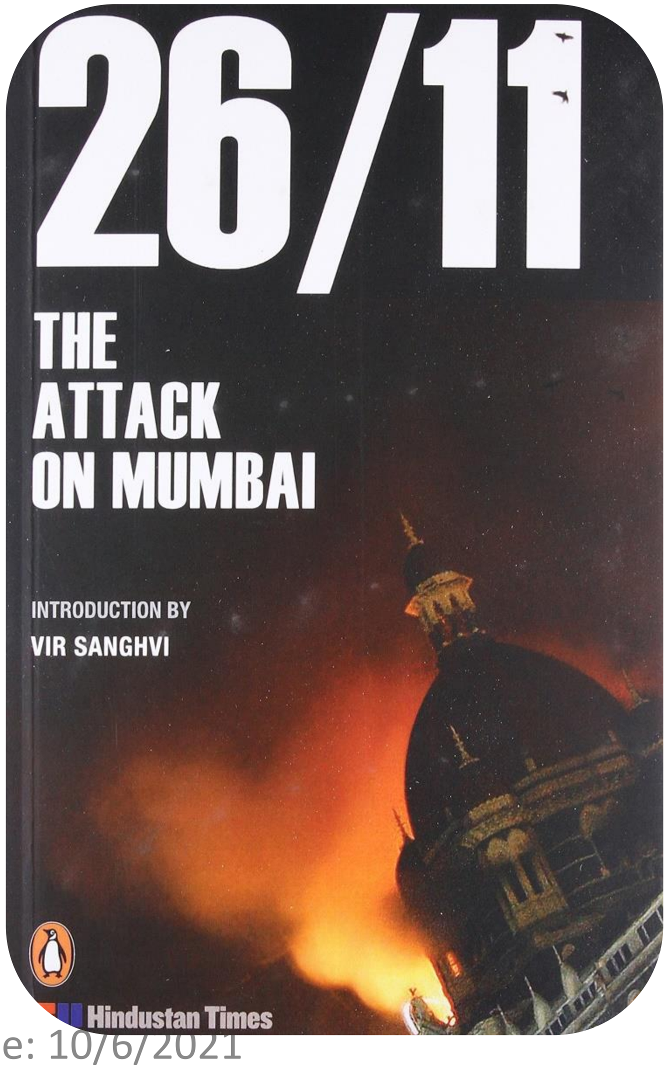
Some lessons

- Impact evaluation is complicated
- Must respect others with other areas of expertise: partnership and humility
- AI innovation and social impact often goes hand-in-hand:
  - If its not a methodological advance AI conferences did not care,
  - *Problematic for AI for social impact because impact evaluation is difficult and AI conferences at the time didn't seem to care*
- Did not set an end date! There must be an end date

Questions

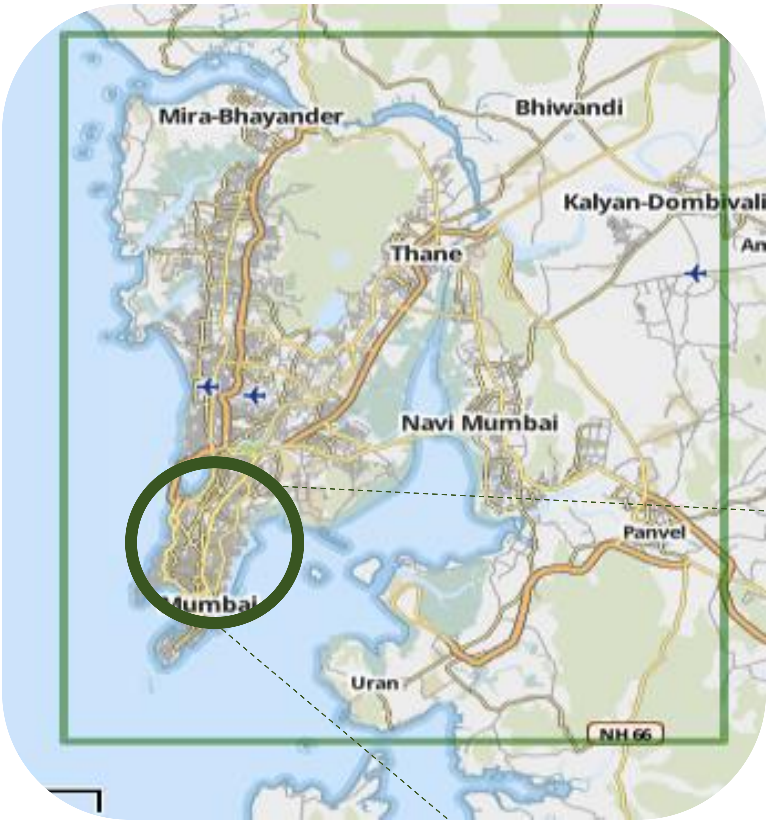
26 Nov 2008, Mumbai
Police Checkpoints: Network Security Game

Jain

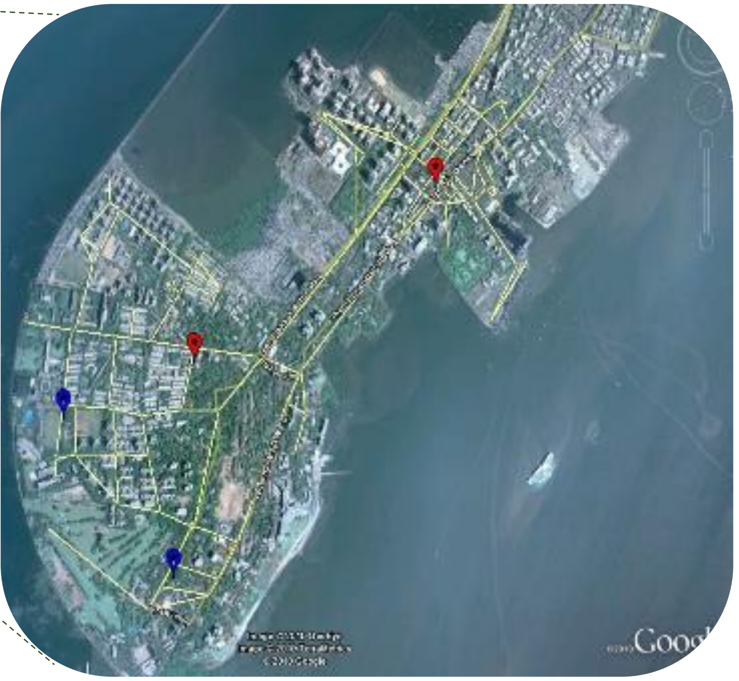


Road networks:

20,000 roads, 15 checkpoints



150 edges
2 Checkpoints
150-choose-2 strategies



Zero-Sum Network Security Game [2013]

Jain

Double oracle: New exact optimal algorithm for scale-up

	Path #1	Path #2	Path #3
Checkpoint strategy #1	5, -5	-1, 1	-2, 2
Checkpoint strategy #2	-5, 5	1, -1	-2, 2

Defender oracle

	Path #1	Path #2
Checkpoint strategy #1	5, -5	-1, 1
Checkpoint strategy #2	-5, 5	2, -1

Attacker oracle

	Path #1	Path #2	Path #3
Checkpoint strategy #1	5, -5	-1, 1	-2, 2
Checkpoint strategy #2	-5, 5	1, -1	-2, 2

Presentation at the Indian National Police Academy: Network Security Game [2016]

Road networks:

20,000 roads, 15 checkpoint:
Solved under 20 min

Mira-Bhayander
Bhiwandi
Kalyan-Dombivali
An
Thane
Navi Mumbai
Panvel
Mumbai
Uran
NH 66

Some lessons

- No “immersion” meant no ability to build up trust

PROTECT: Port and Ferry Protection Patrols [2011]

Shieh

An

Boston

Los Angeles

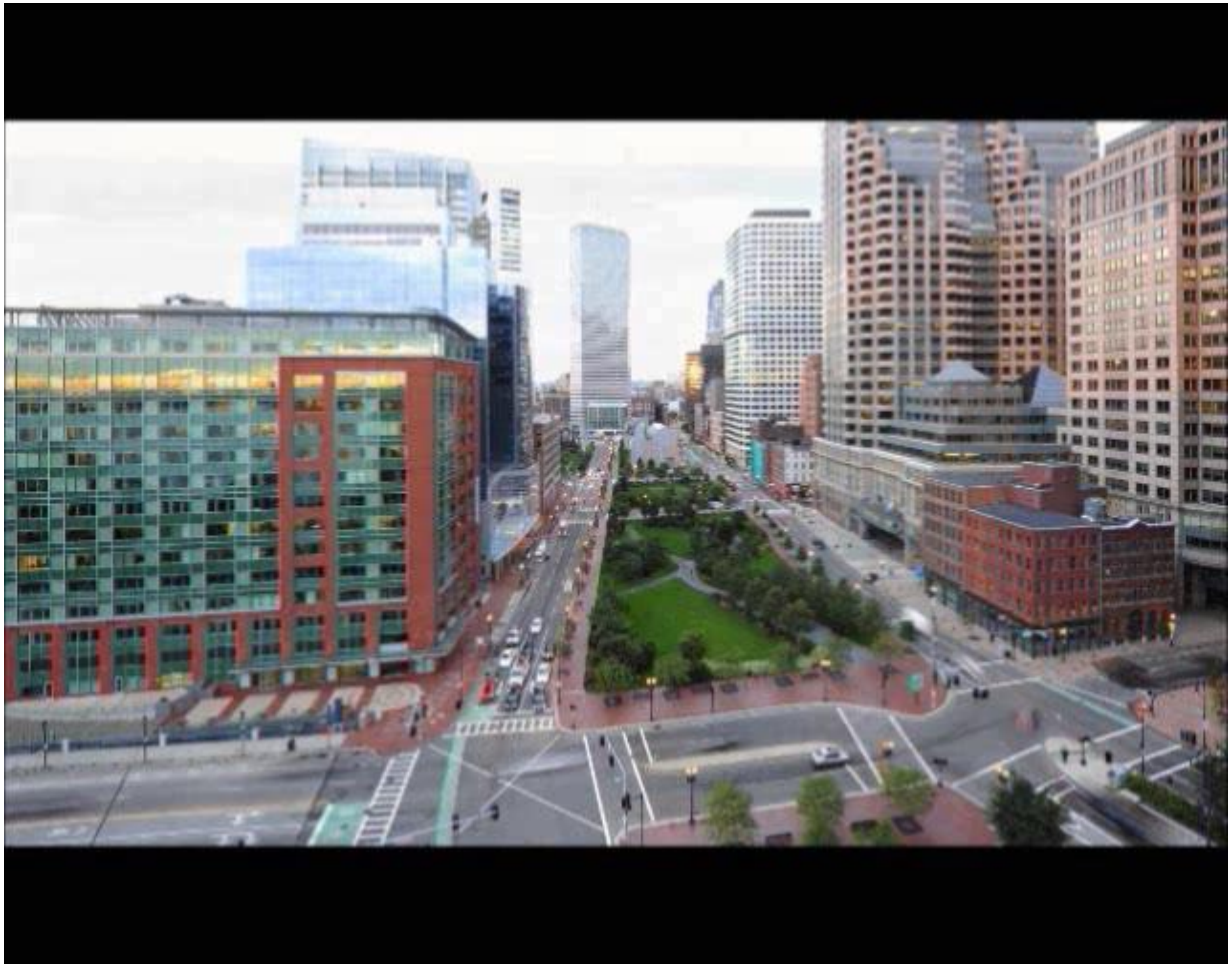
New York

Date: 10/6/2021

PROTECT: Port and Ferry Protection Patrols [2011]

Shieh

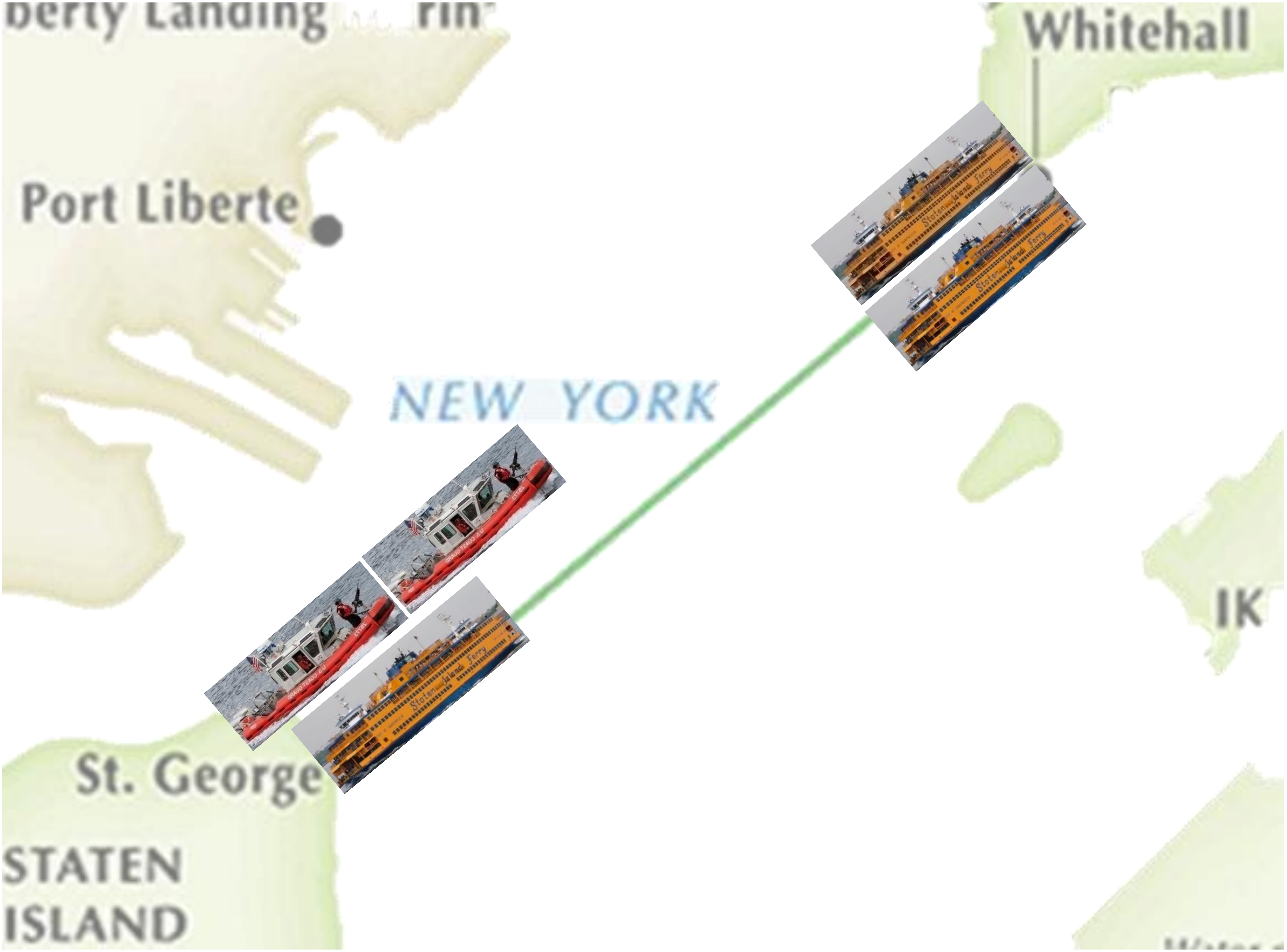
An



PROTECT: Ferry Protection Deployed [2013]

Fang

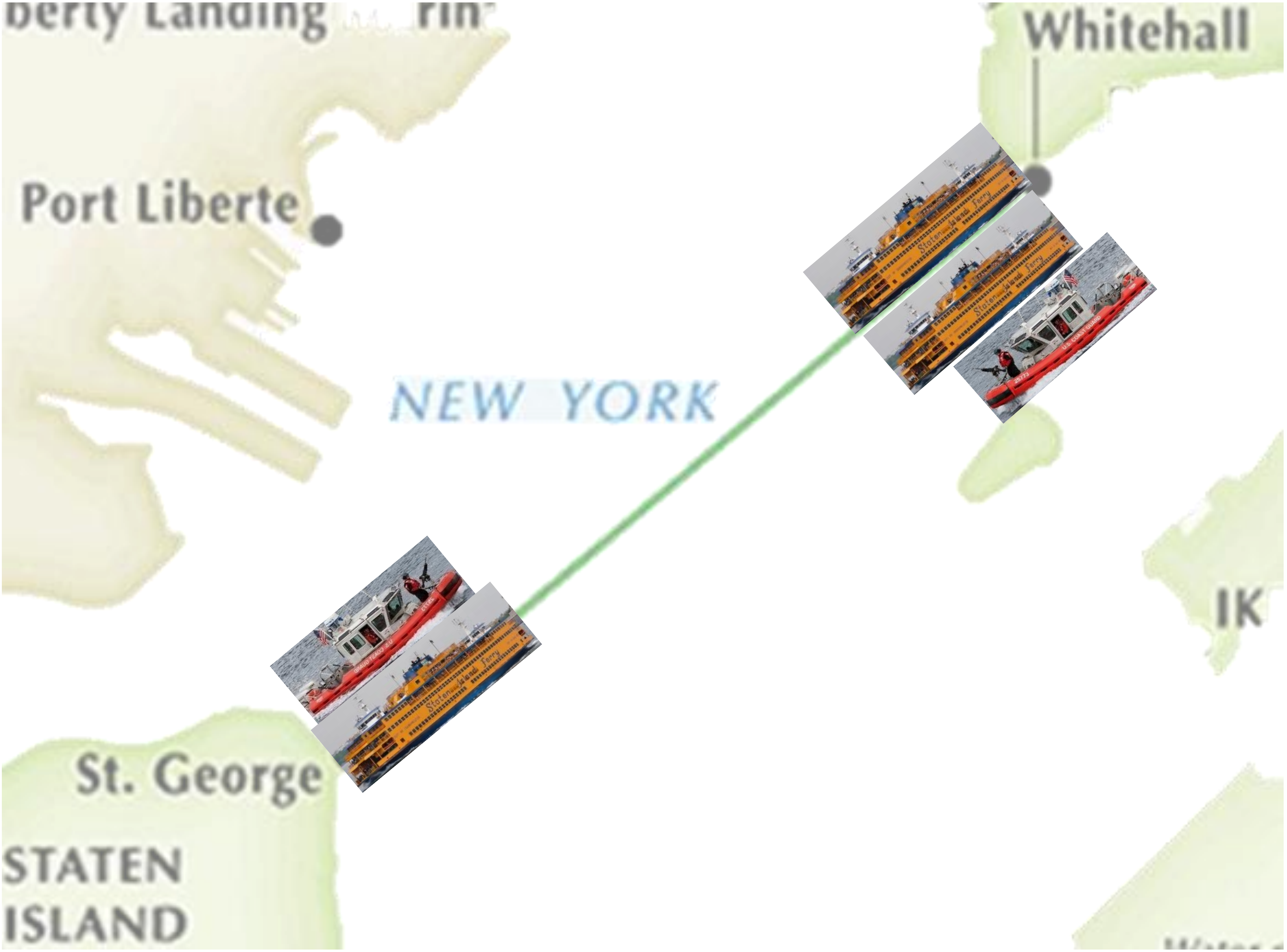
Jiang



PROTECT: Ferry Protection Deployed [2013]

Fang

Jiang



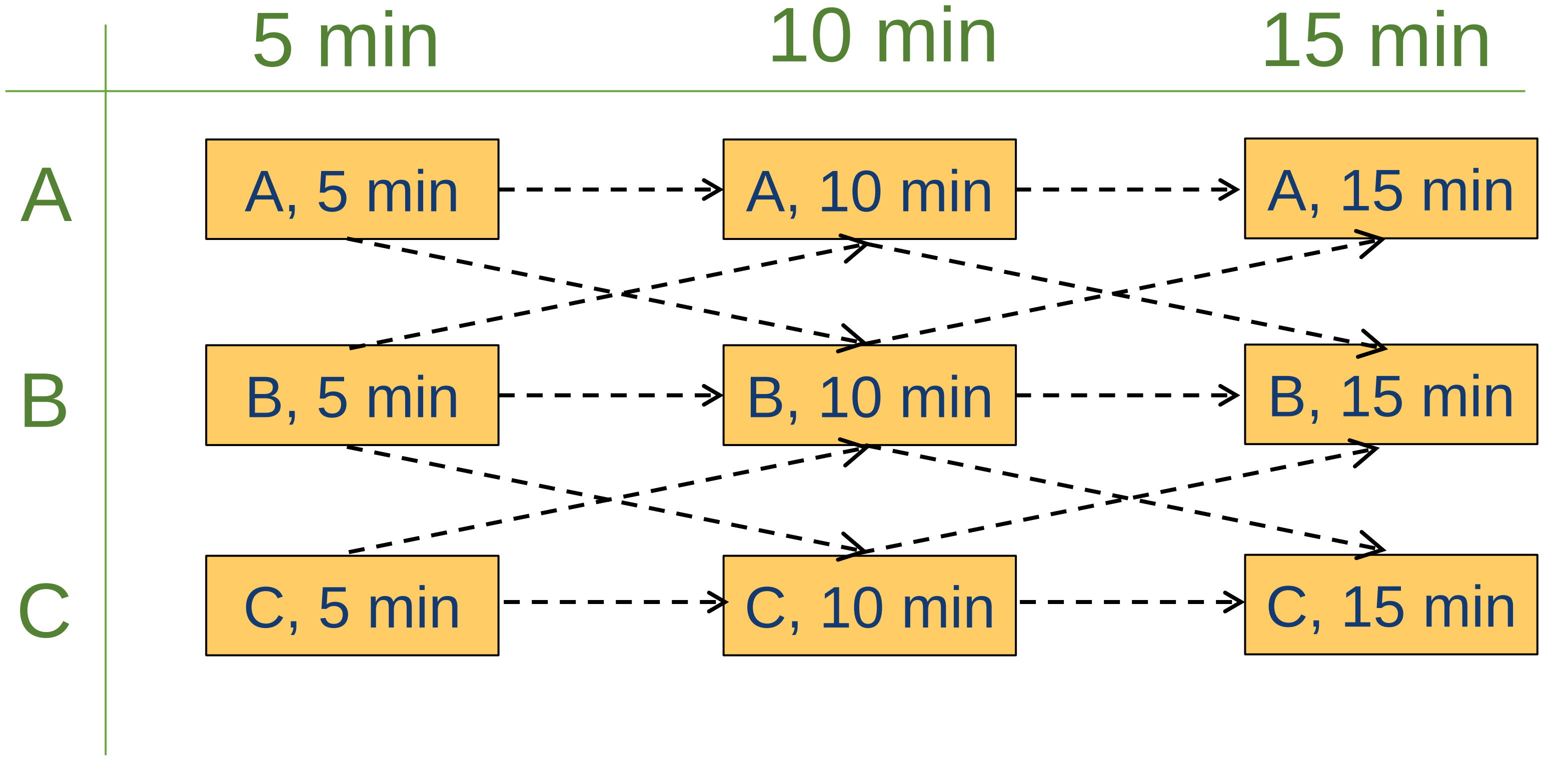
PROTECT: Ferry Protection Deployed [2013]

FERRIES: Mobile Resources & Moving Targets Transition Graph Representation

Fang

Jiang

Marginal strategy: New scale-up approach for Stackelberg Security Games

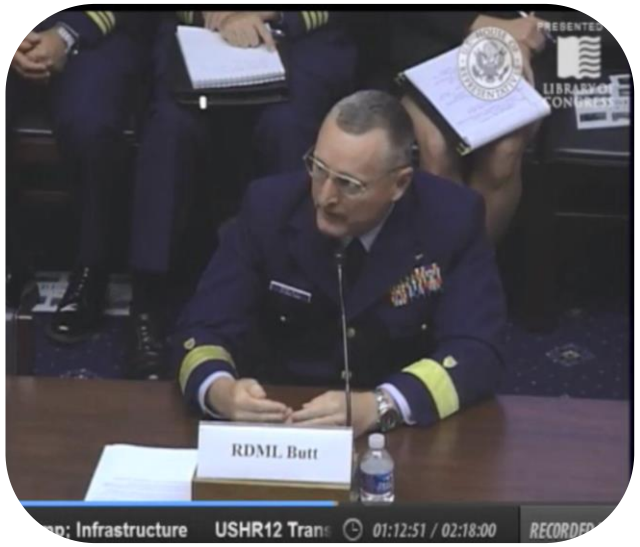


	5 min	10 min	15 min
A	A, 5 min	A, 10 min	A, 15 min
B	B, 5 min	B, 10 min	B, 15 min
C	C, 5 min	C, 10 min	C, 15 min

PROTECT: Port Protection Patrols [2013] Congressional Subcommittee Hearing

June 2013: Meritorious Team Commendation from Commandant (US Coast Guard)

July 2011: Operational Excellence Award (US Coast Guard, Boston)



US Coast Guard testimony Congressional subcommittee

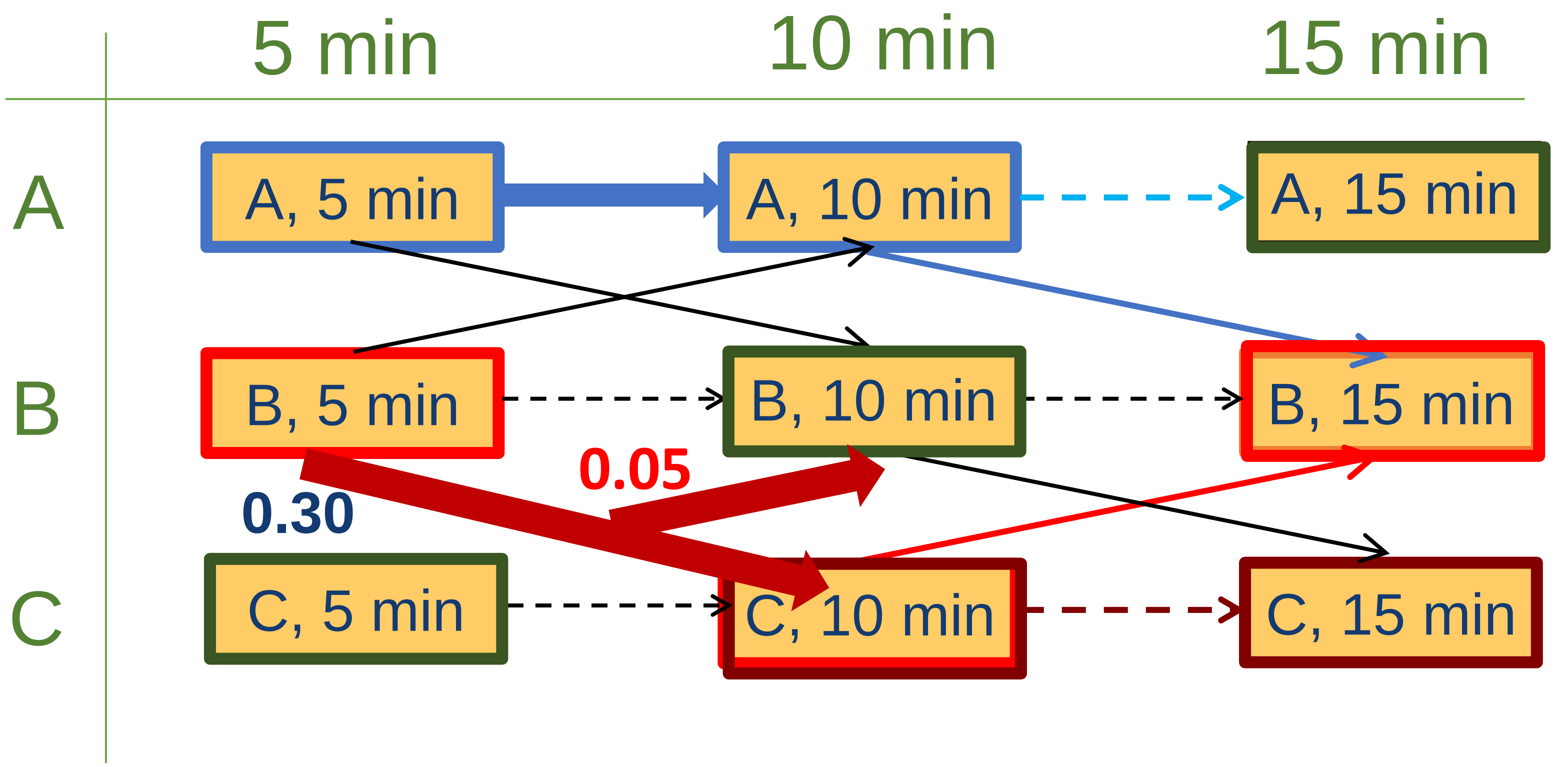
Some lessons

- PROTECT: 2011-2017

Train Patrols
Execution Uncertainty: MDPs

Jiang

Delle Fave



	5 min	10 min	15 min
A	A, 5 min	A, 10 min	A, 15 min
B	B, 5 min	B, 10 min	B, 15 min
C	C, 5 min	C, 10 min	C, 15 min

Questions

Evaluation

- “BUT DOES THIS WORK”?

Evaluating Deployed Security Systems Not Easy

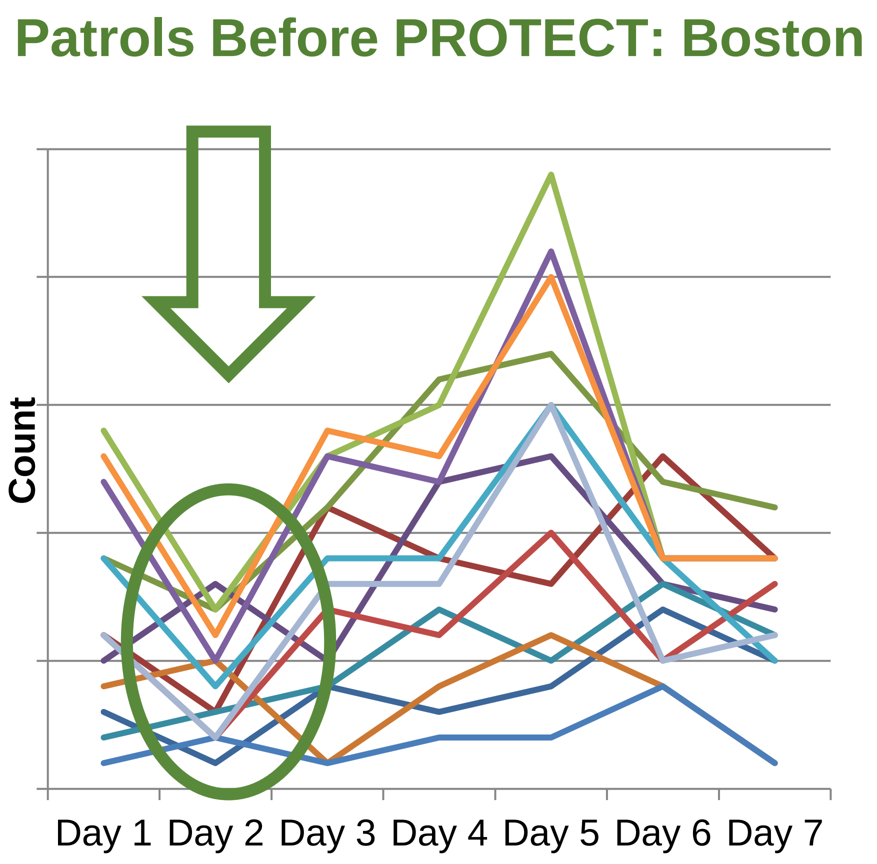
How Well Optimized Use of Limited Security Resources?

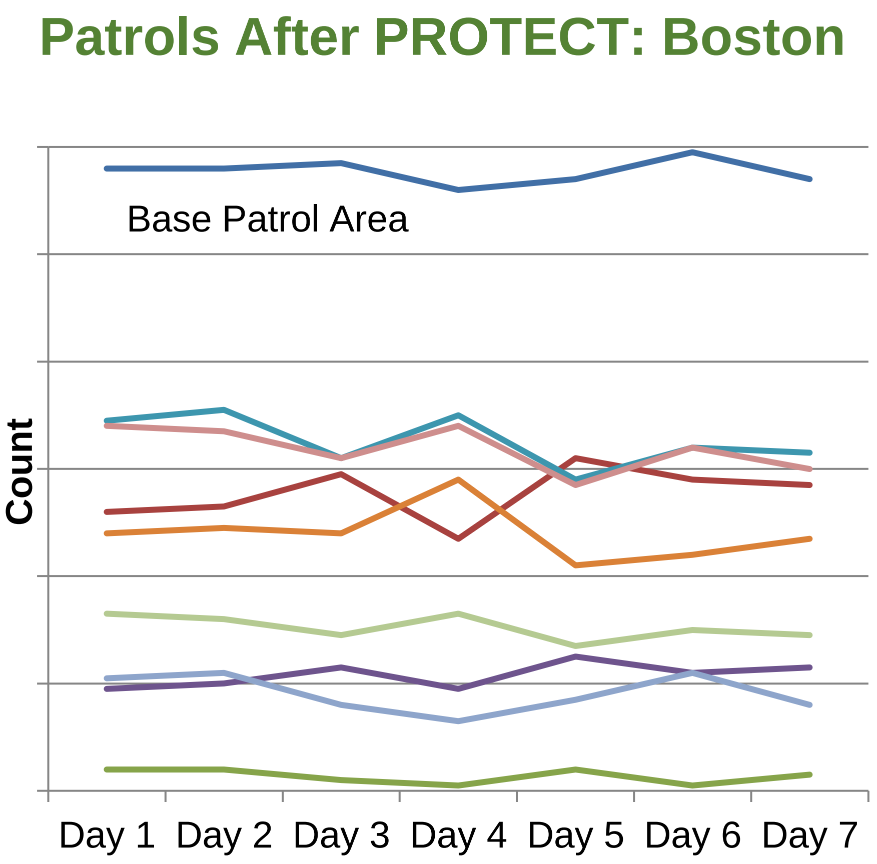
Security Games superior
vs
Human Schedulers/”simple random”

- Lab evaluation
- *Scheduling competitions: Patrol quality unpredictability? Coverage?*
- Field evaluation: Tests against real adversaries
- *Economic cost-benefit analysis*
- *…*

Field Evaluation of Schedule Quality

Improved Patrol Unpredictability & Coverage for Less Effort





350% increase in defender expected utility

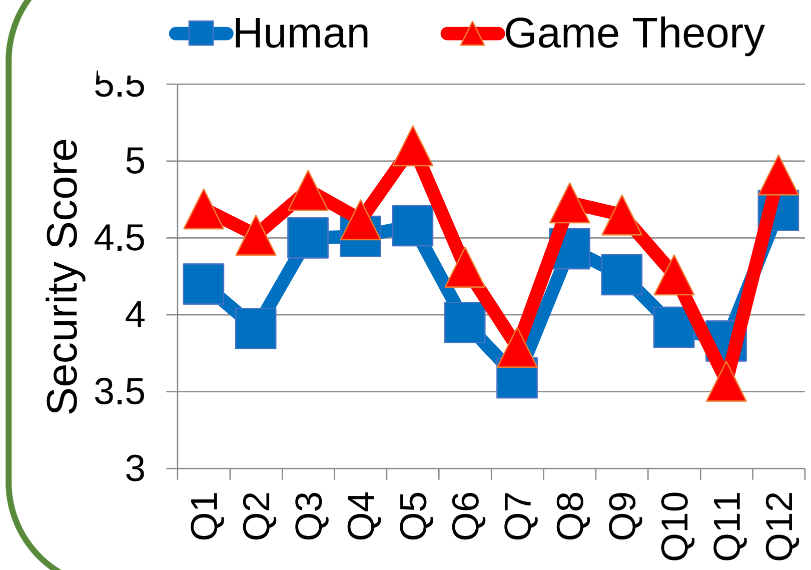
Date: 10/6/2021

Field Evaluation of Schedule Quality

Improved Patrol Unpredictability & Coverage for Less Effort

FAMS: IRIS Outperformed expert human over six months

Report:GAO-09-903T



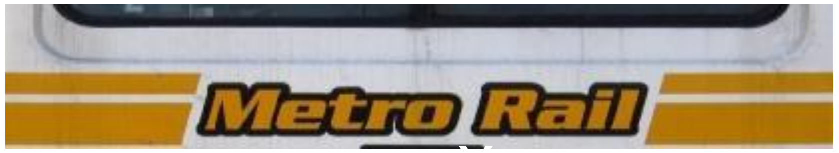
Trains: TRUSTS outperformed expert humans schedule 90 officers on LA trains

Date: 10/6/2021

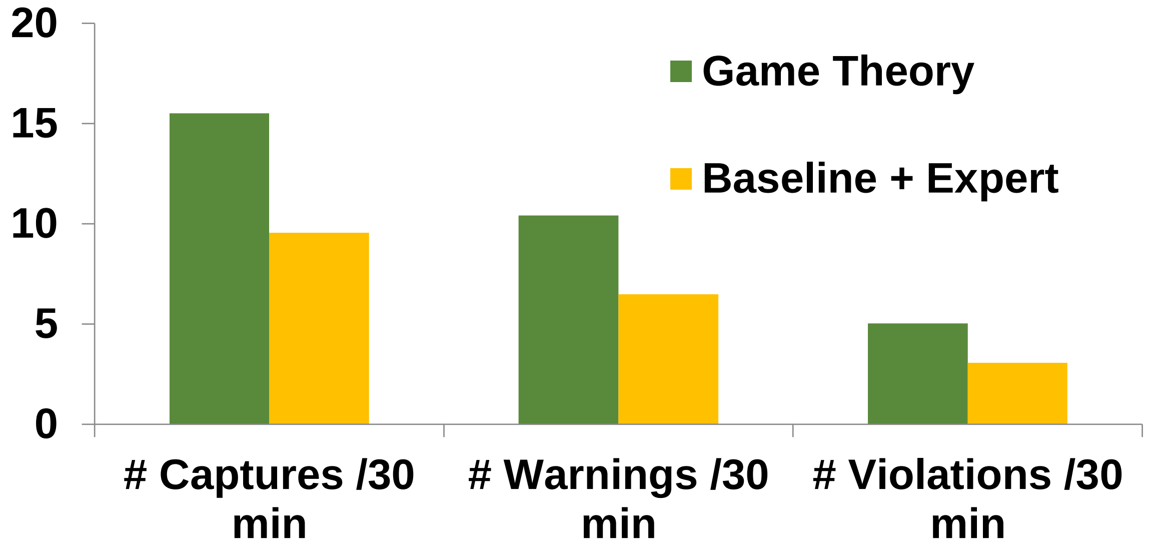
Field Tests Against Adversaries

Computational Game Theory in the Field

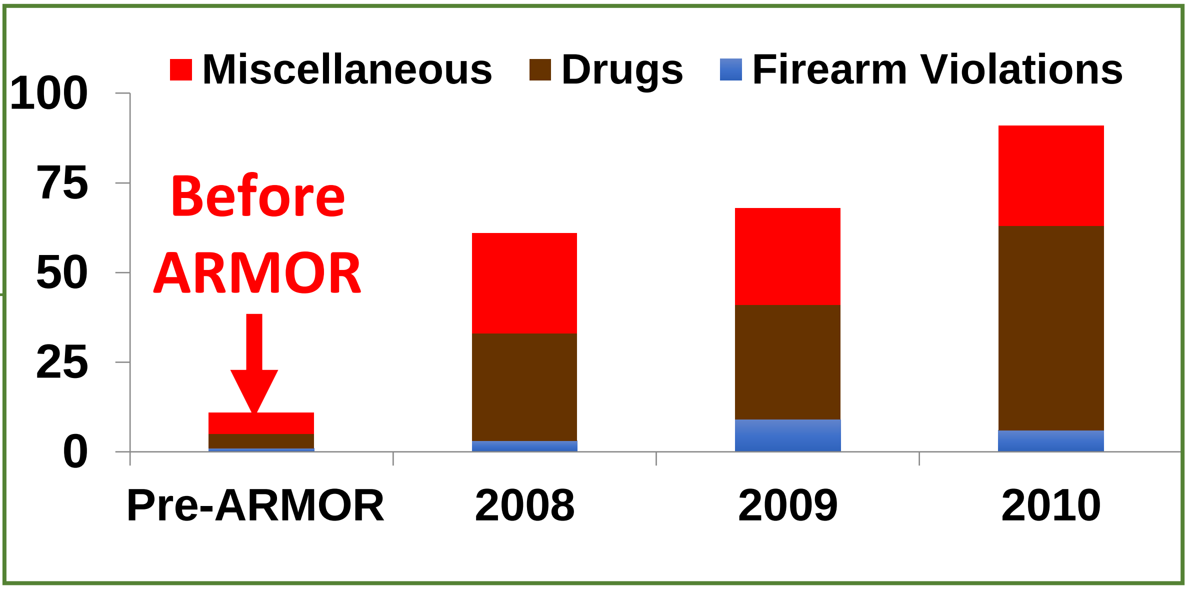
Controlled

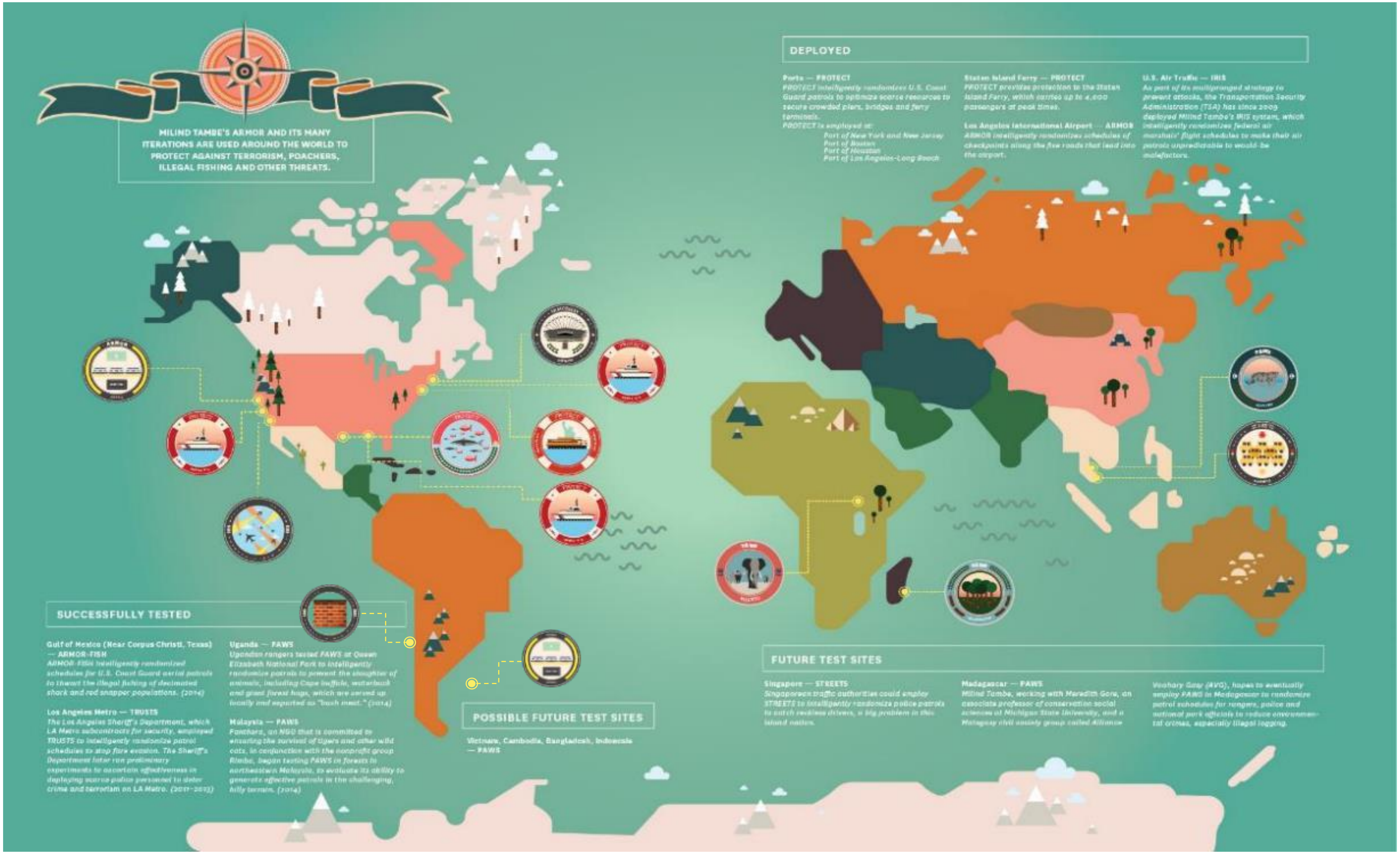


- 21 days of patrol, identical conditions
- Game theory vs Baseline+Expert



Not Controlled





MILIND TAMBE'S ARMOR AND ITS MANY ITERATIONS ARE USED AROUND THE WORLD TO PROTECT AGAINST TERRORISM, POACHERS, ILLEGAL FISHING AND OTHER THREATS.

DEPLOYED

Ports — PROTECT
PROTECT intelligently randomizes U.S. Coast Guard patrols to optimize scarce resources to secure crowded piers, bridges and ferry terminals.
PROTECT is employed at:
Port of New York and New Jersey
Port of Boston
Port of Houston
Port of Los Angeles-Long Beach

Staten Island Ferry — PROTECT
PROTECT provides protection to the Staten Island Ferry, which carries up to 4,000 passengers at peak times.

Los Angeles International Airport — ARMOR
ARMOR intelligently randomizes schedules of checkpoints along the five roads that lead into the airport.

U.S. Air Traffic — IRIS
As part of its multipronged strategy to prevent attacks, the Transportation Security Administration (TSA) has since 2009 deployed Milind Tambe's IRIS system, which intelligently randomizes federal air marshals' flight schedules to make their air patrols unpredictable to would-be malefactors.

SUCCESSFULLY TESTED

Gulf of Mexico (Near Corpus Christi, Texas) — ARMOR-FISH
ARMOR-FISH intelligently randomized schedules for U.S. Coast Guard aerial patrols to thwart the illegal fishing of decimated shark and red snapper populations. (2014)

Los Angeles Metro — TRUSTS
The Los Angeles Sheriff's Department, which LA Metro subcontracts for security, employed TRUSTS to intelligently randomize patrol schedules to stop fare evasion. The Sheriff's Department later ran preliminary experiments to ascertain effectiveness in deploying scarce police personnel to deter crime and terrorism on LA Metro. (2011–2013)

Uganda — PAWS
Ugandan rangers tested PAWS at Queen Elizabeth National Park to intelligently randomize patrols to prevent the slaughter of animals, including Cape buffalo, waterbuck and giant forest hogs, which are served up locally and exported as "bush meat." (2014)

Malaysia — PAWS
Panthera, an NGO that is committed to ensuring the survival of tigers and other wild cats, in conjunction with the nonprofit group Rimba, began testing PAWS in forests in northeastern Malaysia, to evaluate its ability to generate effective patrols in the challenging, hilly terrain. (2014)

POSSIBLE FUTURE TEST SITES

Vietnam, Cambodia, Bangladesh, Indonesia — PAWS

FUTURE TEST SITES

Singapore — STREETS
Singaporean traffic authorities could employ STREETS to intelligently randomize police patrols to catch reckless drivers, a big problem in this island nation.

Madagascar — PAWS
Milind Tambe, working with Meredith Gore, an associate professor of conservation social sciences at Michigan State University, and a Malagasy civil society group called Alliance Voahary Gasy (AVG), hopes to eventually employ PAWS in Madagascar to randomize patrol schedules for rangers, police and national park officials to reduce environmental crimes, especially illegal logging.

New applications: cybersecurity, protecting of endangered wildlife and fisheries, protecting forests, audit games, drug design against viruses, traffic enforcement, software code testing, adversarial machine learning

Outline

Public Safety and Security:
Stackelberg Security Games

→ Conservation/Wildlife Protection:
Green Security Games

World Bank Global Tiger Initiative
How I got into AI for Wildlife Conservation

VANISHING ICONS
GLOBAL TIGER INITIATIVE AND BIG CATS INITIATIVE
NATIONAL GEOGRAPHIC
GTI Global Tiger Initiative

INAUGURAL CEREMONY OF THE SECOND GLOBAL TIGER STOCKTAKING CONFERENCE 2014
Chief Guest
SHEIKH HASINA
Honourable Prime Minister
Government of the Peoples Republic of Bangladesh
Bangladesh Forest Department
Ministry of Environment and Forests

SAVE TIGER CONSERVATION LANDSCAPES
SAVE TIGER CONSERVATION LANDSCAPES
WELCOME
The Second Global Tiger Stocktaking Conference 2014
SAVE TIGER FROM THE VERGE OF EXTINCTION

Dhoni and AB speak to you.
Our superstars are roaring for our tigers.
SAVE OUR TIGERS
Join the fight. Every little bit helps.
Join now ▸

Visiting Uganda & Meeting Andy Plumptre

Date: 10/6/2021

Poaching of Wildlife in Uganda
Limited Intervention (Ranger) Resources to Protect Forests

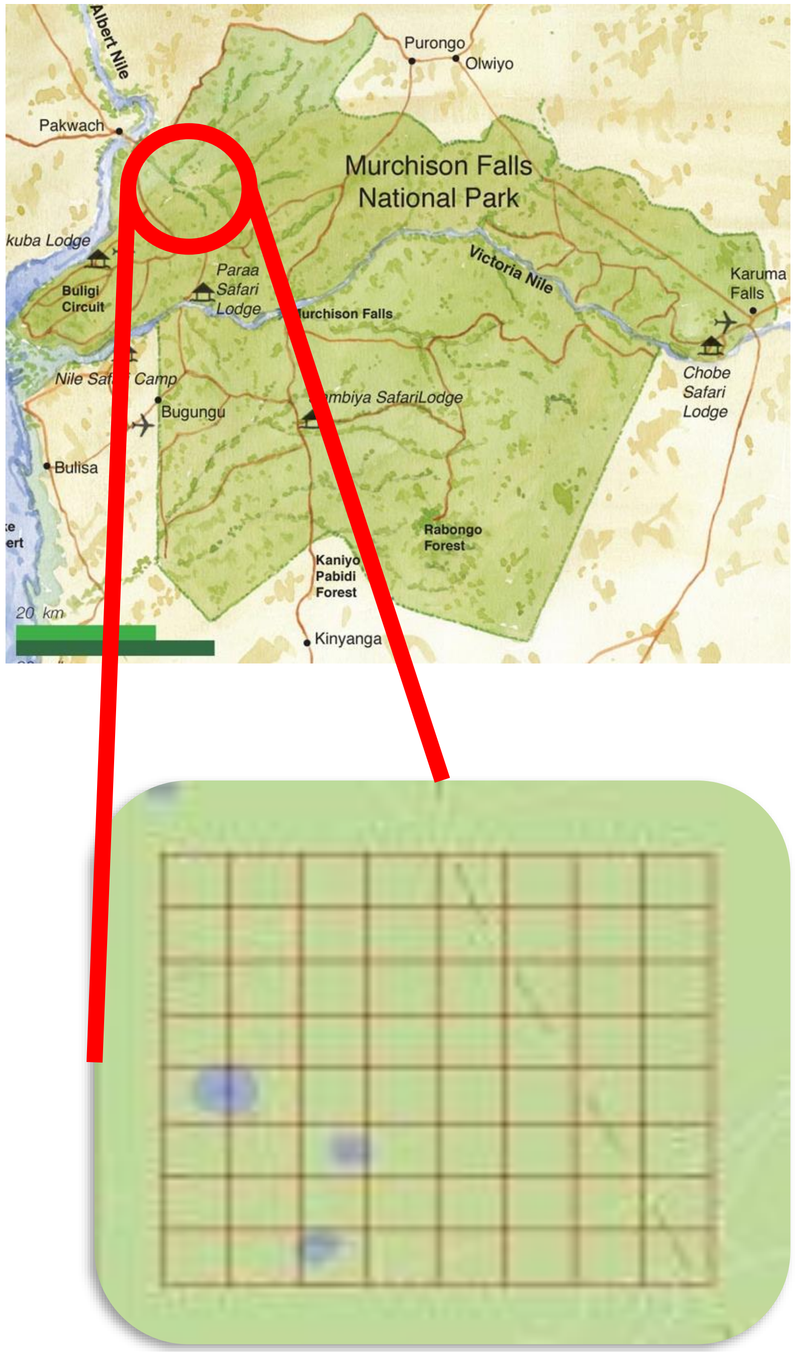
Snare or Trap

Wire snares

Stackelberg Security Games?

Fang

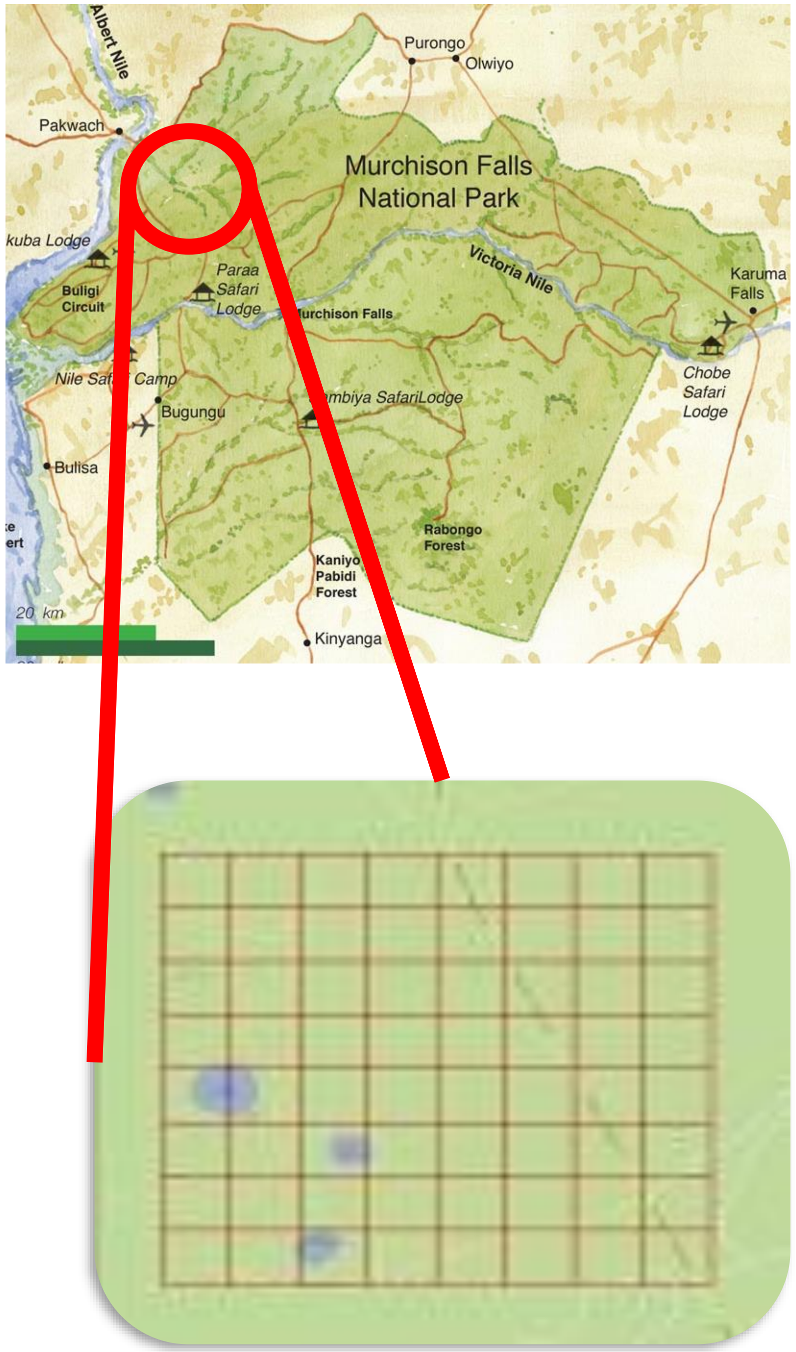
- ➢ ***Stackelberg security games (SSG)***



	Area1	Area2
Area1	4, -3	-1, 1
Area2	-5, 5	2, -1

Green Security Games Combine Stackelberg Security Games and Machine Learning

Fang



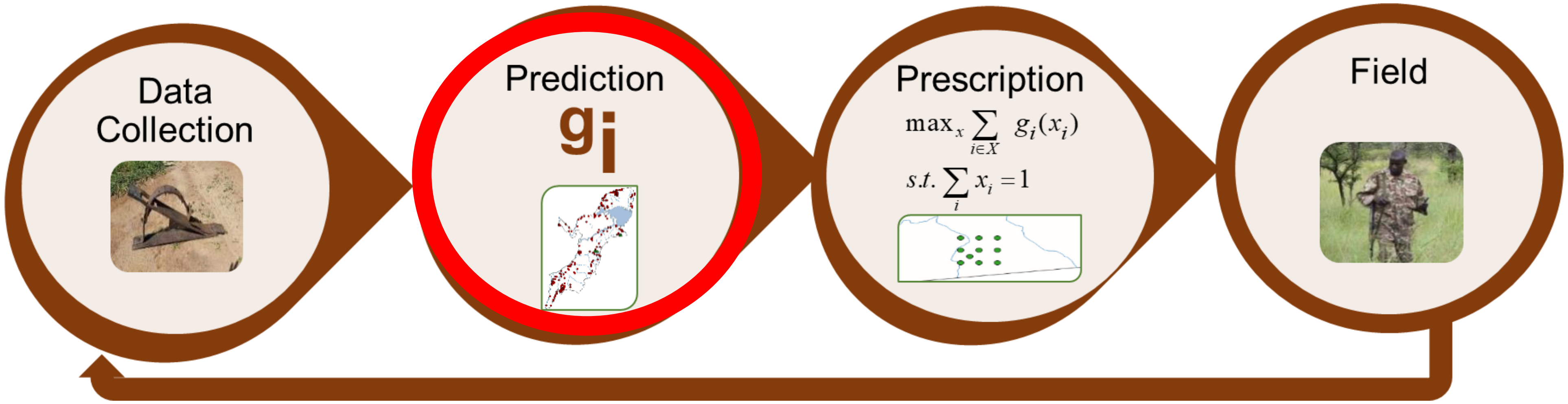
- ***Not fully strategic adversaries***
- ***Boundedly rational poachers, past poaching data***
- ***Learn adversary response model at targets "i"***

	Area1	Area2
Area1	4, -3	-1, 1
Area2	-5, 5	2, -1

Learning Adversary Response Model: Uncertainty in Observations

Nguyen

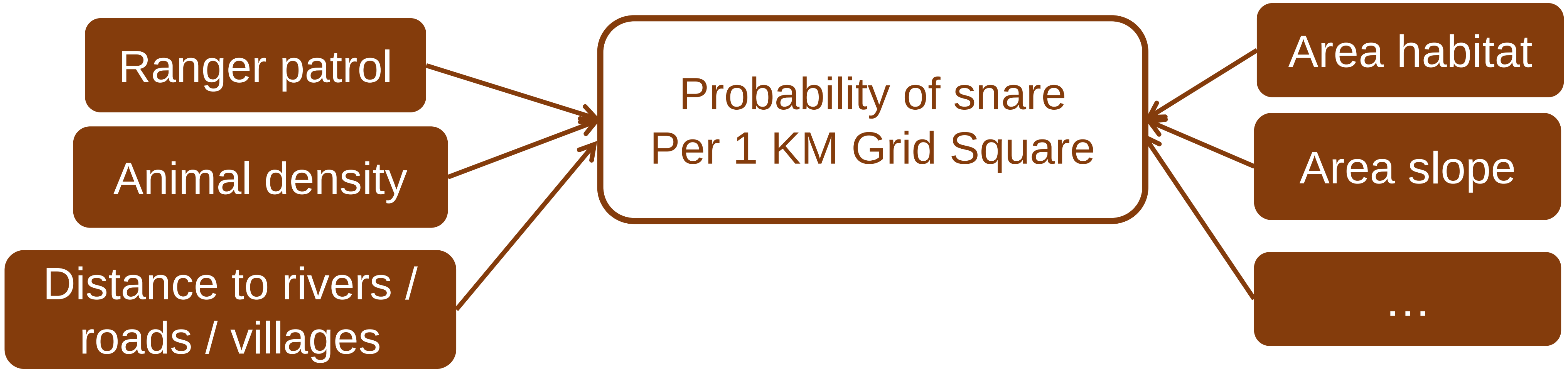
Gholami



Learning Adversary Response Model: Uncertainty in Observations

Nguyen

Gholami



Ranger patrol

Animal density

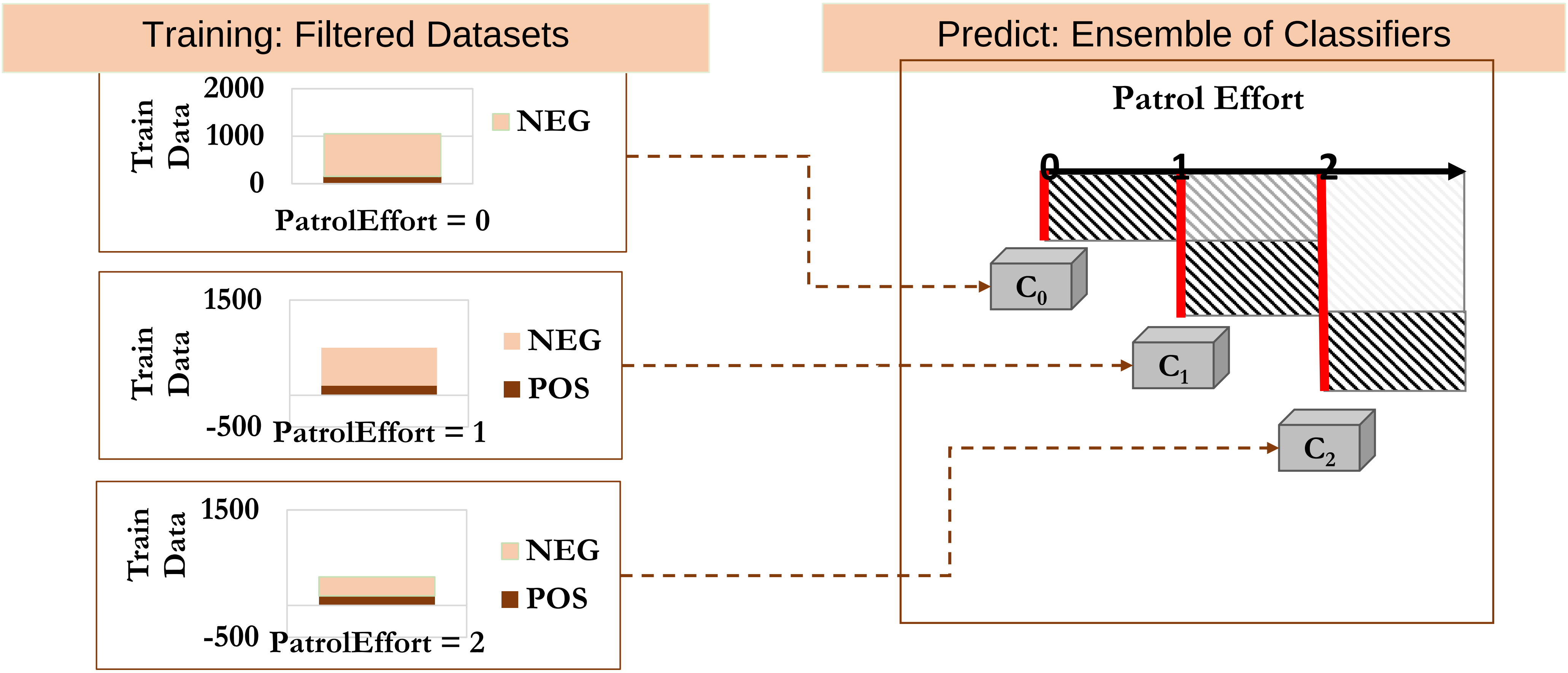
Distance to rivers / roads / villages

Probability of snare Per 1 KM Grid Square

Area habitat

Area slope

…



Training: Filtered Datasets

Predict: Ensemble of Classifiers

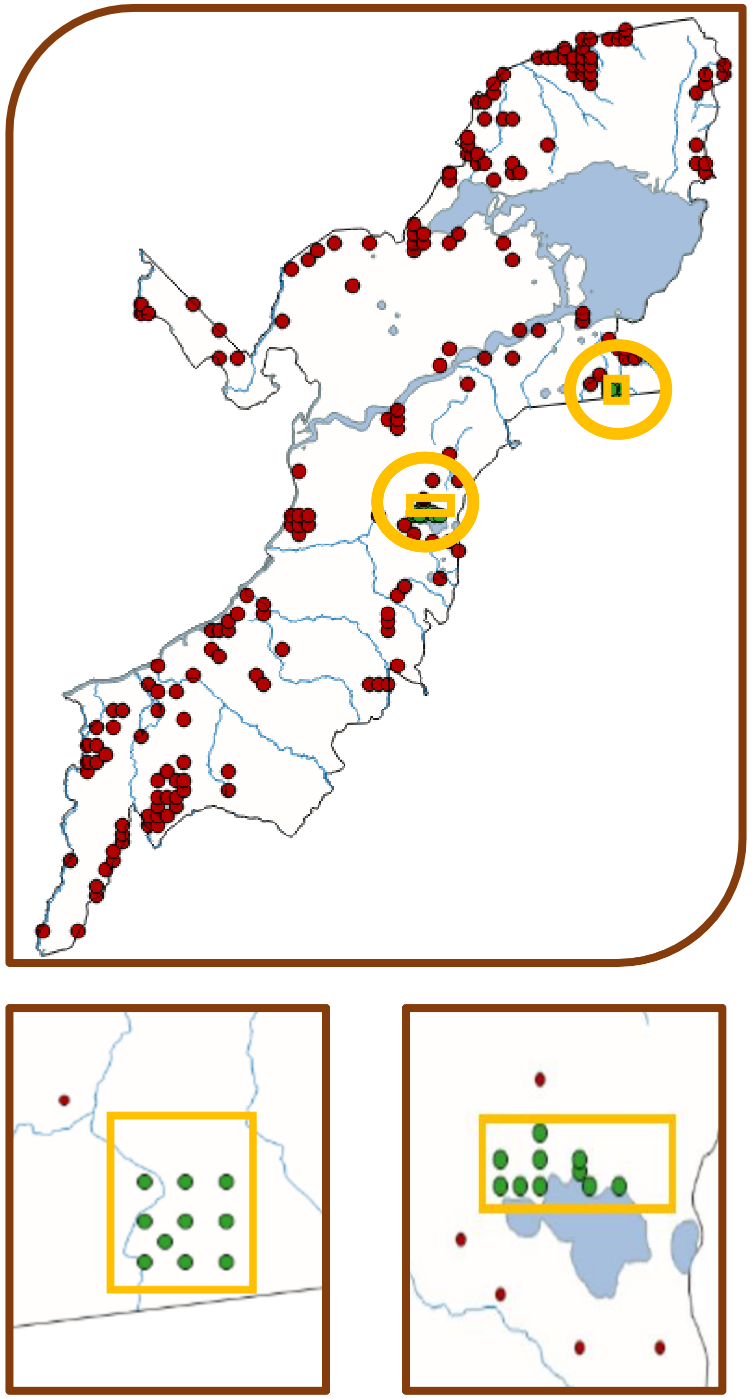
PAWS: First Pilot in the Field

(AAMAS 2017)

Ford

Gholami

- Two 9-sq.km areas, infrequent patrols



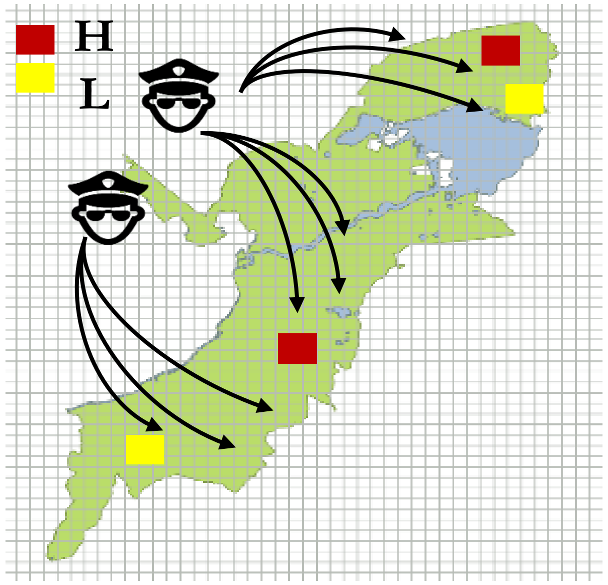
- Poached elephant
- 1 elephant snare roll
- 10 Antelope snares

PAWS Predicted High vs Low Risk Areas: 3 National Parks, 24 areas each, 6 months

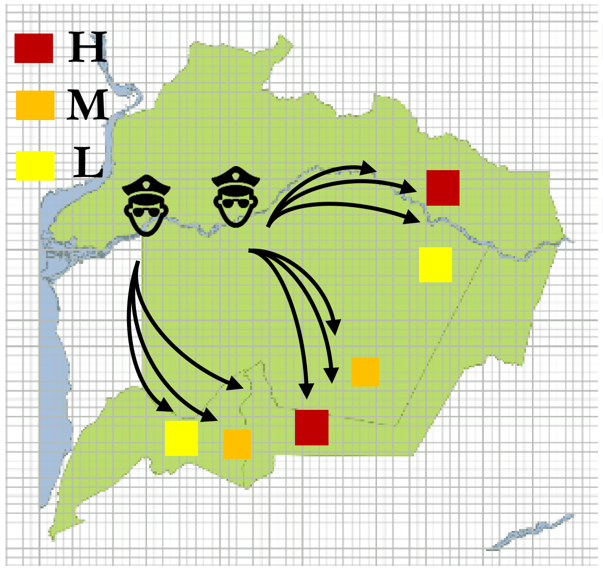
(ECML PKDD 2017, ICDE 2020)

Xu

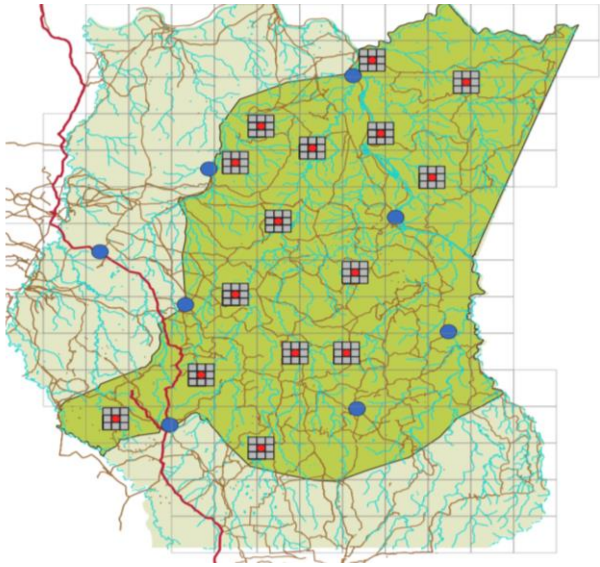
Gholami



Queen Elizabeth National Park

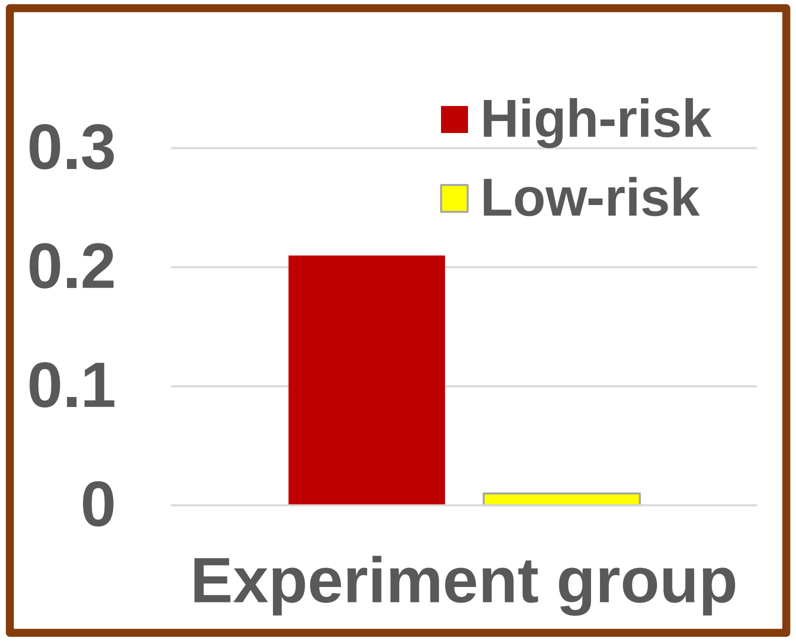


Murchison Falls National Park

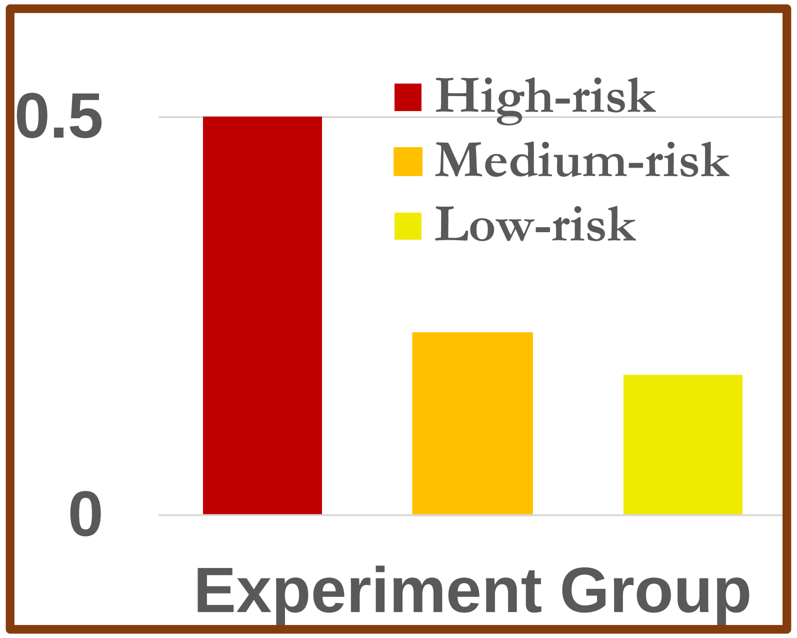


Srepok Wildlife Sanctuary

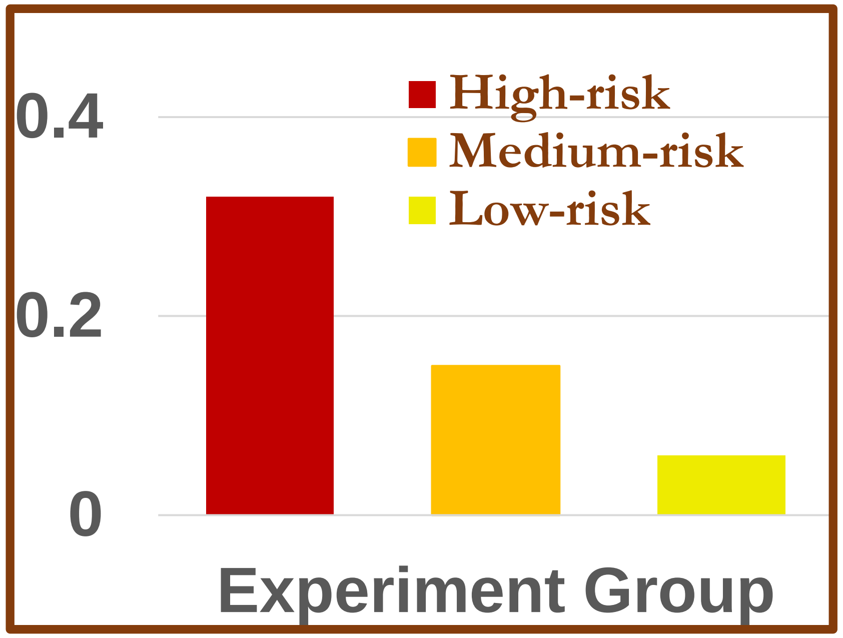
Snares per patrolled sq. KM



Snares per patrolled sq. KM



Snares per patrolled sq. KM



PAWS Real-world Deployment Cambodia: Srepok Wildlife Sanctuary

(ICDE 2020)

Xu

2019 PAWS: *521 snares/month*

vs

2018: *101 snares/month*

2021 PAWS

1,000 snares found in March

PAWS GOES GLOBAL with SMART platform!!

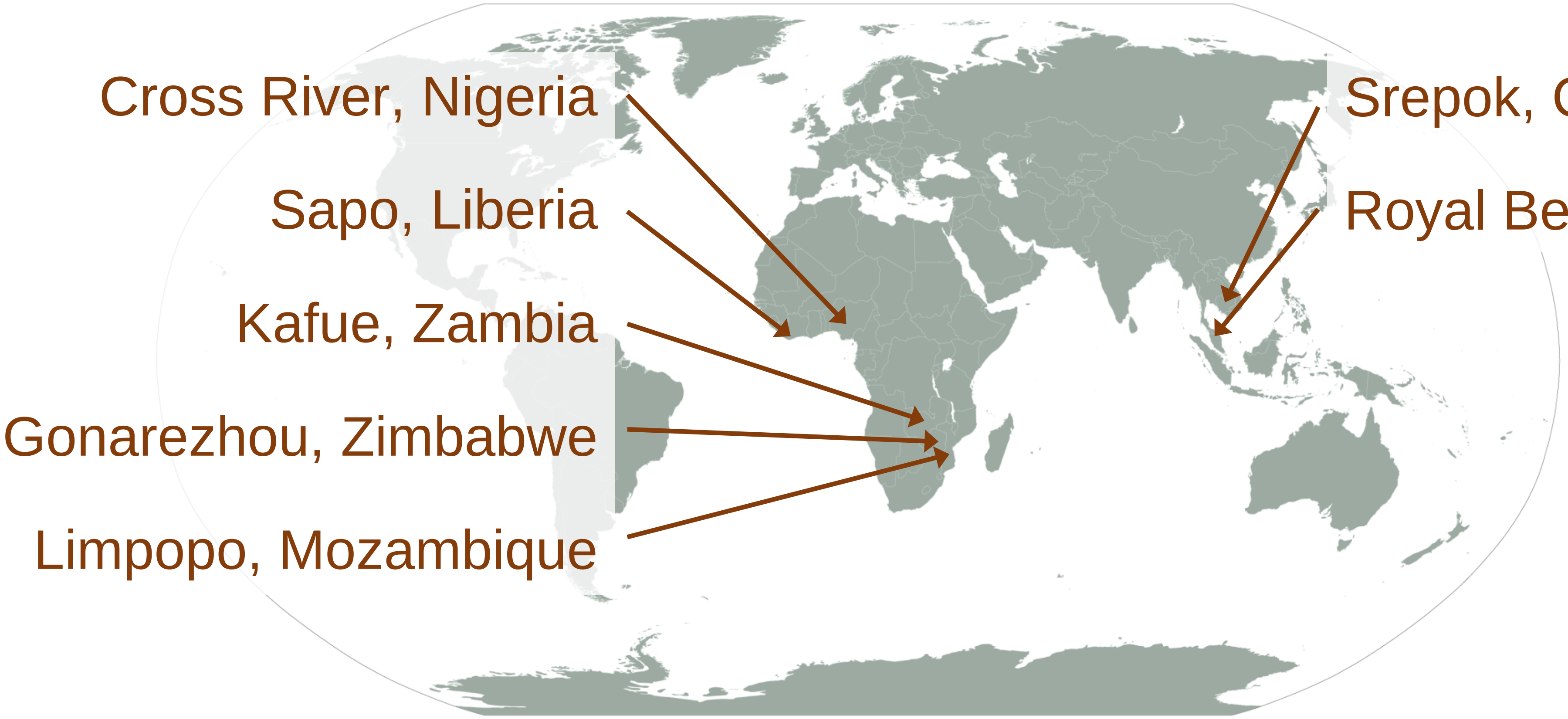
SMART

WWF

PEACE PARKS FOUNDATION · THE GLOBAL SOLUTION

WCS

Protect Wildlife
800 National Parks
Around the Globe



Cross River, Nigeria

Sapo, Liberia

Kafue, Zambia

Gonarezhou, Zimbabwe

Limpopo, Mozambique

Srepok, Cambodia

Royal Belum, Malaysia