Yale SCHOOL *of* MANAGEMENT

YALE UNIVERSITY
School of Public Health

YALE UNIVERSITY
School of Engineering and
Applied Science

Terror Queues: Detection and Staffing

Edward H. Kaplan

William N and Marie A Beach Professor of Operations Research
Yale School of Management

Professor of Public Health
Yale School of Public Health

Professor of Engineering
Yale School of Engineering and Applied Science
New Haven, Connecticut

2017 LNMB Lunteren Conference, Lunteren, The Netherlands

What's New with the Terror Queue?

- Terror Queues *Operations Research* 58:773-784, 2010
- Intel Queues with Jonathan Feinstein *Military Operations Research* 17:17-30, 2012
- Estimating the Duration of *Jihadi* Terror Plots in the United States *Studies in Conflict & Terrorism*, 35:880-894, 2012
- Staffing Models for Covert Counterterrorism Agencies *Socio-Economic Planning Sciences*, 47:2-8, 2013
- Socially Efficient Detection of Terror Plots *Oxford Economic Papers*, 67:104-115, 2015.
- Optimal Control of a Terror Queue with Andrea Seidl, Jonathan P. Caulkins, Stefan Wrzaczek and Gustav Feichtinger *European Journal of Operational Research*, 248:246-256, 2016.
- Differential Terror Queue Games with Stefan Wrzaczek, Andrea Seidl, Jonathan P. Caulkins, and Gustav Feichtinger *Dynamic Games and Applications* (in press, 2016)

Motivation

- “Intelligence is the heart and soul of operational counterterrorism” (Amos Guiora (2008), *Fundamentals of Counterterrorism*)
- Terror queues simultaneously model stocks of undetected and detected terror plots along with the status of covert counterterrorism agents
- Today’s focus is on the use of undercover agents and/or informants to reduce the rate of successful terror attacks

Mosab Hassan Yousef. (Yossi Sasson)

Last update - 14:32 24/02/2010

Haaretz exclusive: Hamas founder's son worked for Shin Bet for years

By Avi Issacharoff

Tags: Israel News, Shin Bet, Hamas

The son of a leading Hamas figure, who famously converted to Christianity, served for over a decade as the Shin Bet security service's most valuable source in the militant organization's leadership, Haaretz has learned.

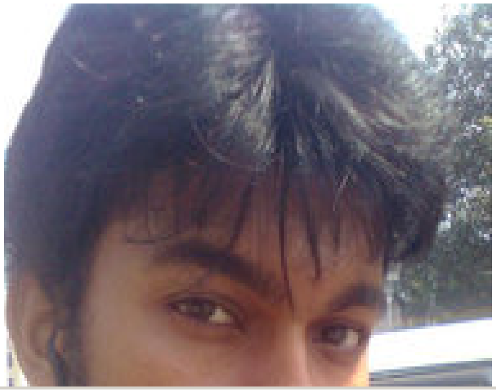
Mosab Hassan Yousef is the son of Sheikh Hassan Yousef, a Hamas founder and one of its leaders in the West Bank. The intelligence he supplied Israel led to the exposure of a number of terrorist cells, and to the prevention of dozens of suicide bombings and assassination attempts on Israeli figures.

N.Y. / Region

Man Is Charged With Plotting to Bomb Federal Reserve Bank in Manhattan

By MOSI SECRET and WILLIAM K. RASHBAUM
Published: October 17, 2012

Federal prosecutors in Brooklyn charged a 21-year-old Bangladeshi man with conspiring to blow up the Federal Reserve Bank of New York, saying he tried to remotely detonate what he believed was a 1,000-pound bomb in a van he parked outside the building in Lower Manhattan on Wednesday.



But the entire plot played out under the surveillance of the Federal Bureau of Investigation and the New York Police Department as part of an elaborate sting operation, according to court papers.

Today's Question

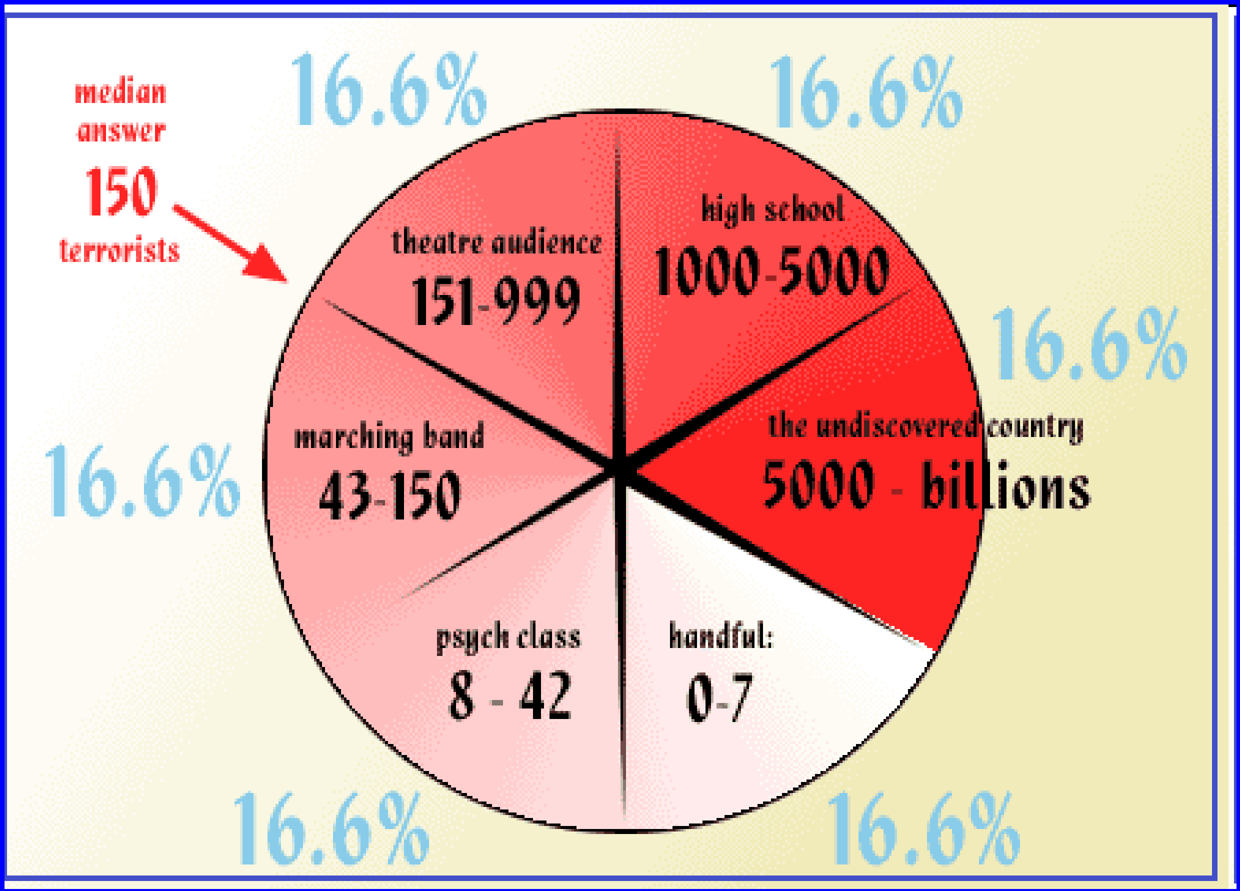
- How many good guys are needed to catch the bad guys?
- This is a *staffing problem*: how many servers are needed to staff a queueing system to satisfy a stated objective?

To Answer Our Question We…

- Introduce Markov terror queue model
- Apply Markov model to staffing problems
  - presumes terror plot durations exponentially distributed
- Estimate duration of *Jihadi* plots in the US
  - estimated plot duration distribution *not* exponential
- Model terror queues with proportional hazards
- Present staffing models with proportional hazards

How Many Terror Plots Are There?

- Three. And two of them are ex-girlfriends.

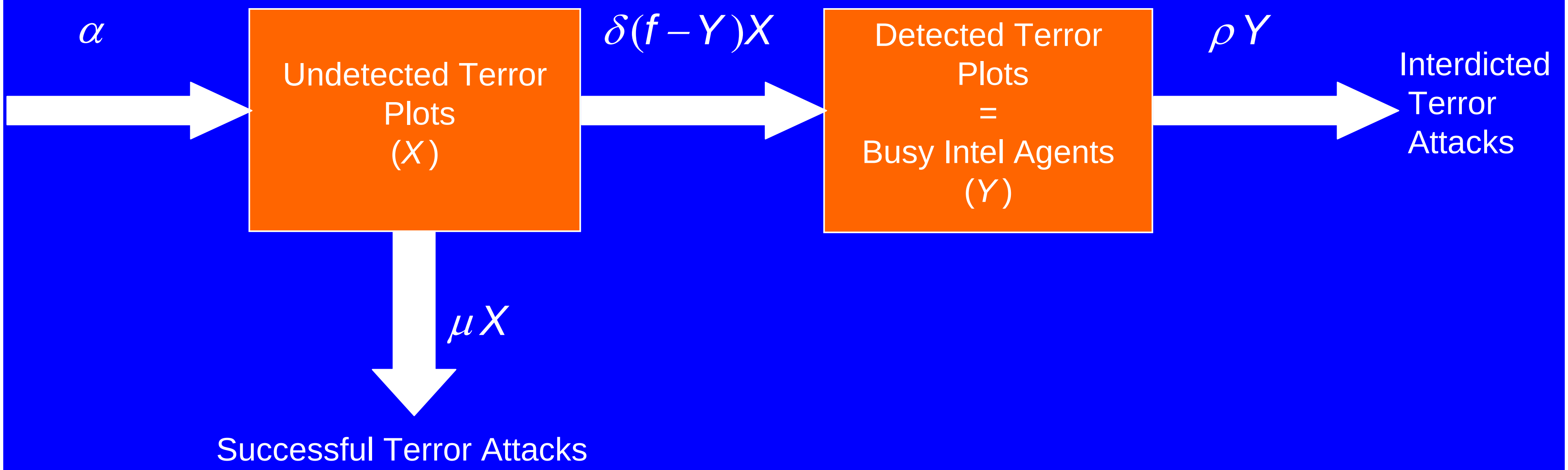


http://www.cockeyed.com/citizen/terror/terror_results.html

Terror Queues

- Consider terror plots as "customers"
- Customers arrive (new plots are hatched) in accord with Poisson process
- "Servers" are undercover agents or informants
- "Service" commences when a plot is detected by an "available" agent (servers have to find customers), and concludes when the plot is interdicted (agents occupied with specific plots are "busy")
- Successful terror plots are equivalent to customers who abandon the queue (drop out) before receiving service
- *Idle servers and waiting customers co-exist!*
- *Servers want to provide good service, but customers don't want to be served!*

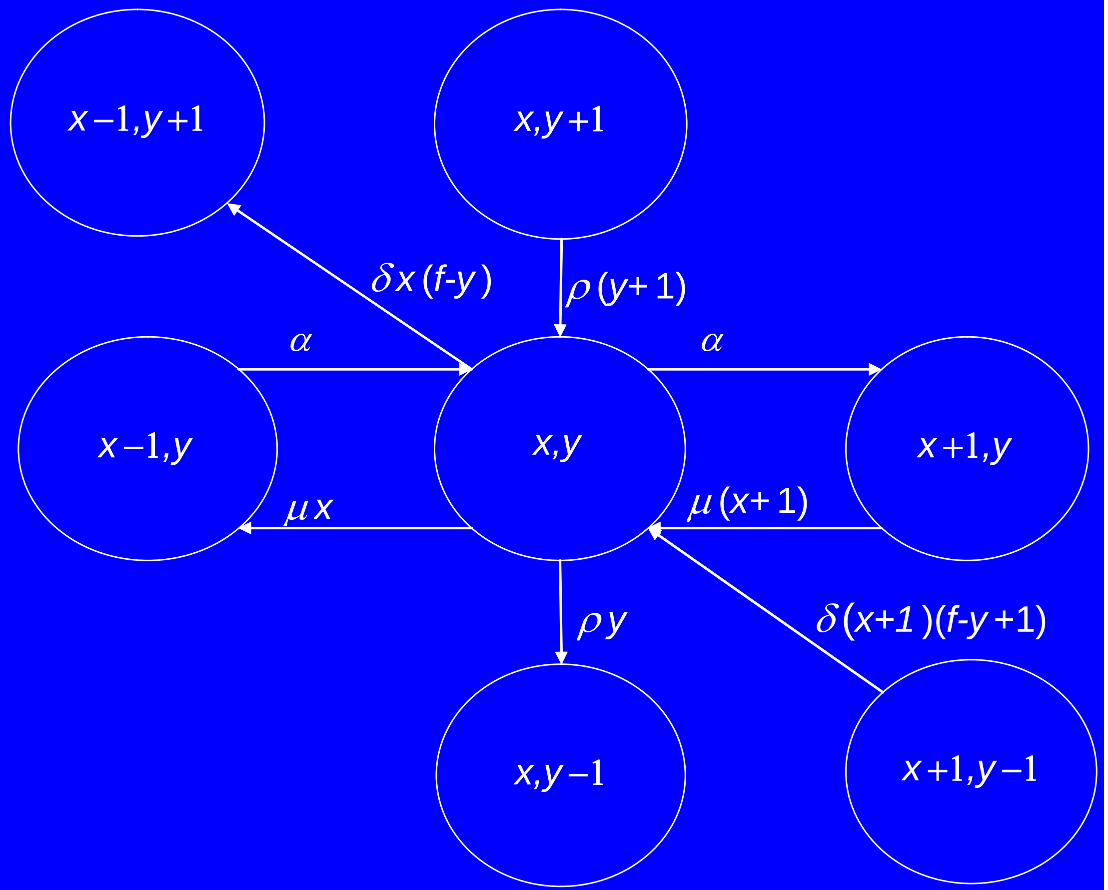
Terror Queue Model



Parameters	State Variables
$\alpha =$ terror plot arrival rate	
$\mu =$ unobstructed terror plot completion rate	$X =$ number of undetected terror plots
$\delta =$ terror plot detection rate	
$\rho =$ detected terror plot interdiction rate	$Y =$ number of detected terror plots/busy intel agents
$f =$ total number of intel agents	

Goal: determine the joint probability distribution of undetected (X) and detected (Y) terror threats:

$p_{xy} = \Pr\{X = x, Y = y\}$



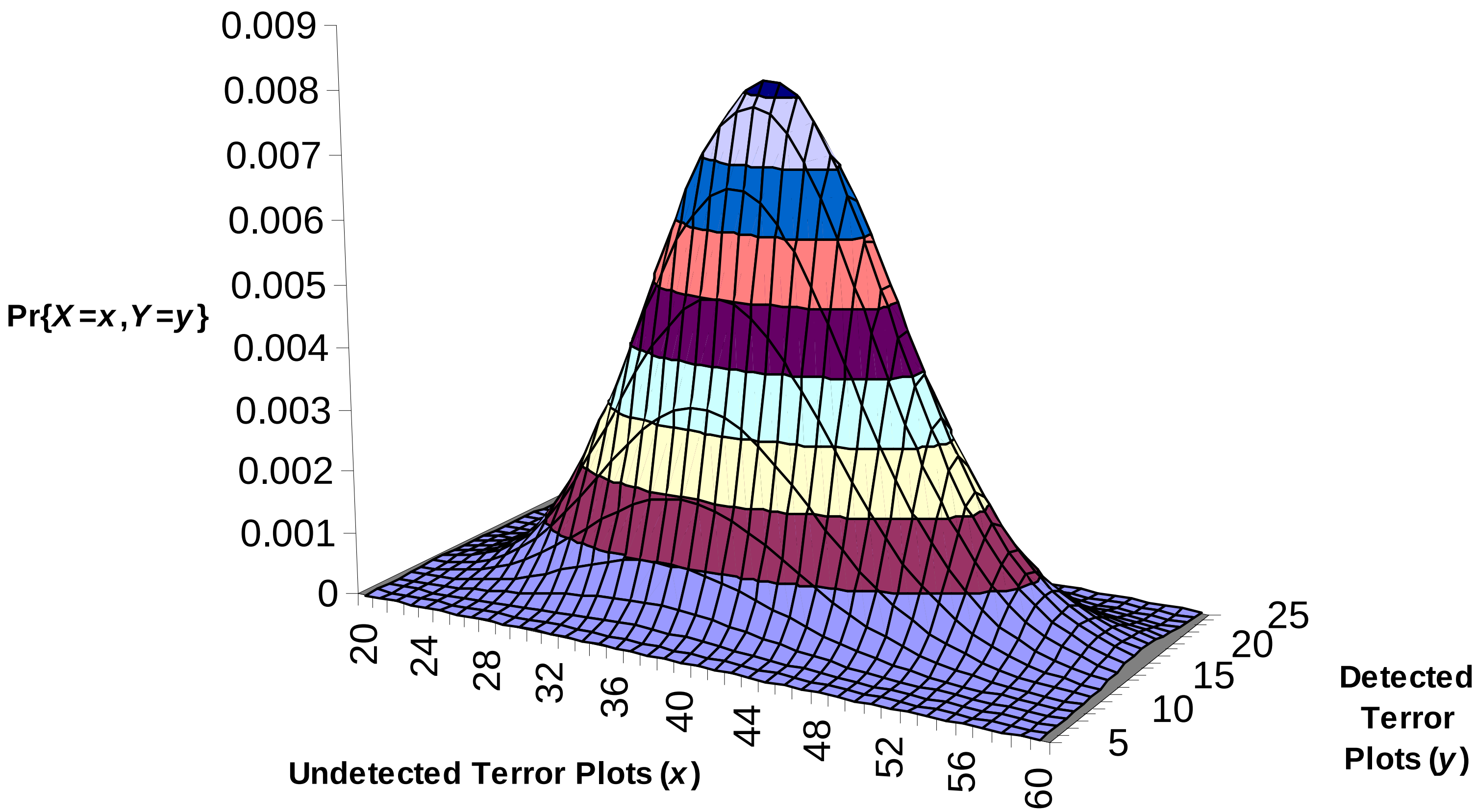
Generic balance equation:

$$(\alpha + \mu x + \rho y + \delta x(f - y))p_{xy}$$

$$= \alpha p_{x-1,y} + \mu(x+1)p_{x+1,y} + \rho(y+1)p_{x,y+1} + \delta(x+1)(f - y + 1)p_{x+1,y-1}$$

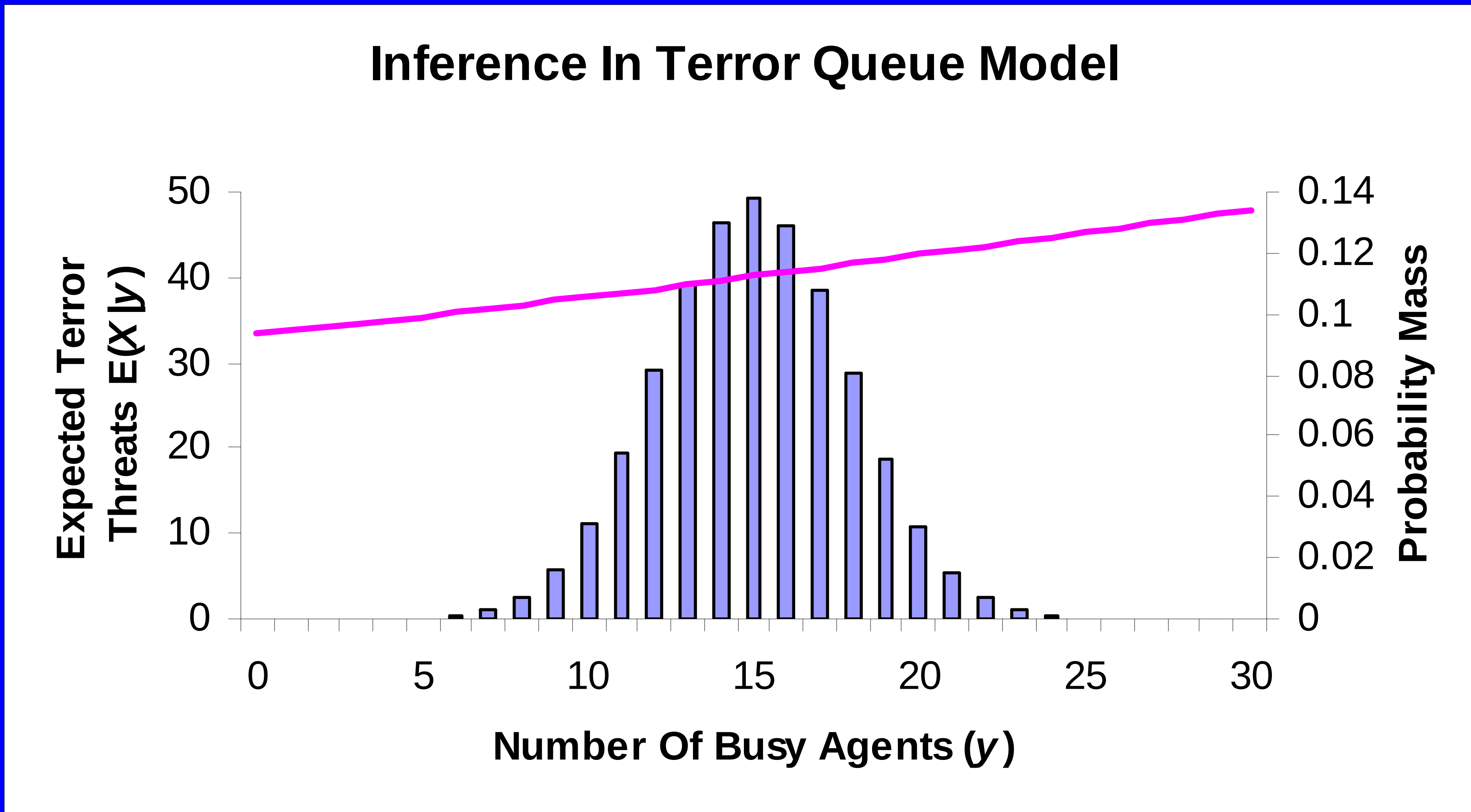
Also boundary equations for x=0 and y=0, f plus probability conservation

Joint Distribution of Undetected (X) and Detected (Y) Terror Plots



Looks like bivariate normal distribution…

Inference in Terror Queue Model

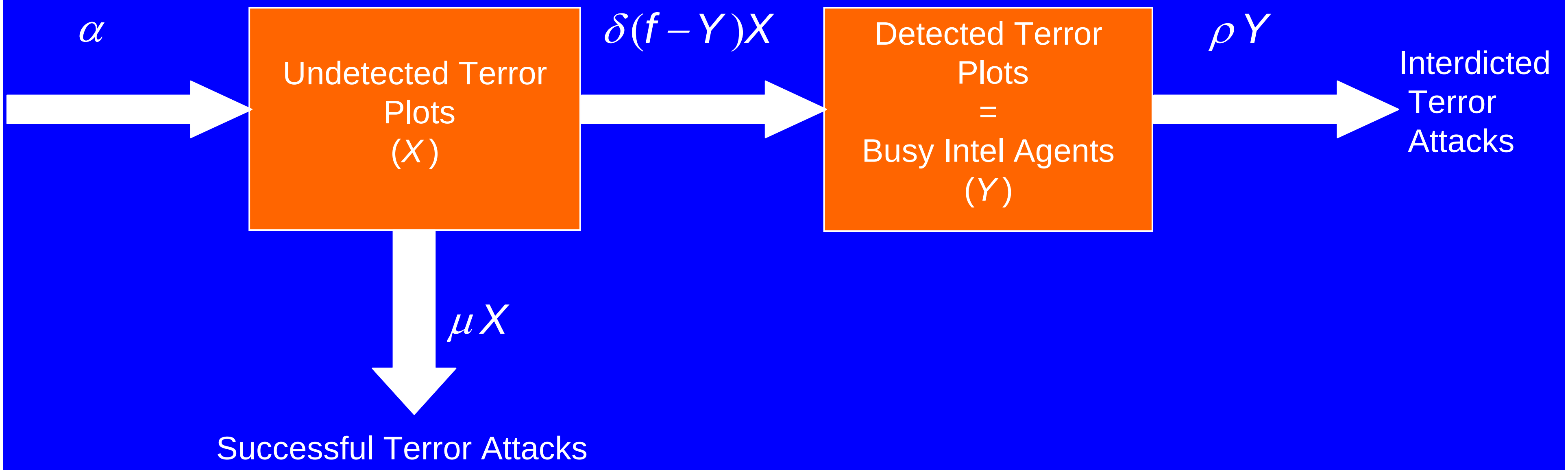


Note that $E(X|Y=y)$ is linear in y

Ornstein-Uhlenbeck Terror Queue

- Motivated by approximate joint normality, formulate diffusion approximation (Barbour, *Adv Appl Prob* **8**:296-314, 1976 among others)
- First formulate fluid model for expected number of undetected and detected terror threats
- Then construct diffusion approximation for joint stochastic fluctuations around expected values
- Instead of having to solve infinite system of linear equations as in Markov model, now only need to solve 2 nonlinear and 3 linear equations

Deterministic Flows



- Solve: $$\alpha = \mu x^* + \delta x^*(f - y^*)$$ $$\delta x^*(f - y^*) = \rho y^*$$

for $x^* \approx E(X)$ and $y^* \approx E(Y)$

Diffusion Model

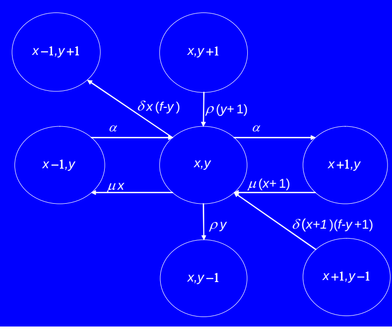
- Let $X(t)$, $Y(t)$ denote the (random) number of undetected and detected terror plots

- Define $\Delta X(t)$ ($\Delta Y(t)$) as $X(t + \Delta t) - X(t)$ ($Y(t + \Delta t) - Y(t)$)

Diffusion Model

- Conditional joint probability distribution of $\Delta X(t)$ and $\Delta Y(t)$ given that $X(t) = x$ and $Y(t) = y$ shown below:

	$\Delta Y(t) = -1$	$\Delta Y(t) = 0$	$\Delta Y(t) = +1$
$\Delta X(t) = -1$	0	$\mu x \Delta t$	$\delta x(f-y)\Delta t$
$\Delta X(t) = 0$	$\rho y \Delta t$	$1-(\alpha+\mu x+\rho y+\delta x(f-y))\Delta t$	0
$\Delta X(t) = +1$	0	$\alpha \Delta t$	0



Local Drift

- From the joint distribution of $\Delta X(t)$ and $\Delta Y(t)$, the local drift is given by

$$E(\Delta X(t)) \;=\; (\alpha - \mu x - \delta x(f - y))\Delta t$$

$$E(\Delta Y(t)) \;=\; (\delta x(f - y) - \rho y)\Delta t.$$

Local Drift Approximation

- Rather than working with the exact nonlinear drift equations, we linearize as

$$\begin{pmatrix} E(\Delta X(t)) \\ E(\Delta Y(t)) \end{pmatrix} \approx A \begin{pmatrix} x - x^* \\ y - y^* \end{pmatrix} \Delta t$$

where $$A = \frac{1}{\Delta t} \begin{pmatrix} \frac{\partial E(\Delta X | x,y)}{\partial x} & \frac{\partial E(\Delta X | x,y)}{\partial y} \\ \frac{\partial E(\Delta Y | x,y)}{\partial x} & \frac{\partial E(\Delta Y | x,y)}{\partial y} \end{pmatrix}_{x=x^*, y=y^*}$$

Local Covariance Matrix

- We again use the joint distribution to compute the local covariance matrix of $\Delta X(t)$ and $\Delta Y(t)$, and evaluate at x^* and y^*

$$S^* = \frac{1}{\Delta t} \begin{pmatrix} Var(\Delta X(t)) & Cov(\Delta X(t), \Delta Y(t)) \\ Cov(\Delta X(t), \Delta Y(t)) & Var(\Delta Y(t)) \end{pmatrix}_{x=x^*, y=y^*}$$

Steady State Diffusion Model

- In steady state, $X(t) \rightarrow X$, $Y(t) \rightarrow Y$, and X, Y are distributed *bivariate normal* with means $E(X) = x^*$, $E(Y) = y^*$, and covariance matrix Σ given by solution to

$$A\Sigma + \Sigma A^T = -S^*$$

- This reduces to three linear equations in the three unknowns $Var(X)$, $Var(Y)$, and $Cov(X,Y)$

Conditional Distribution of Undetected Terror Plots

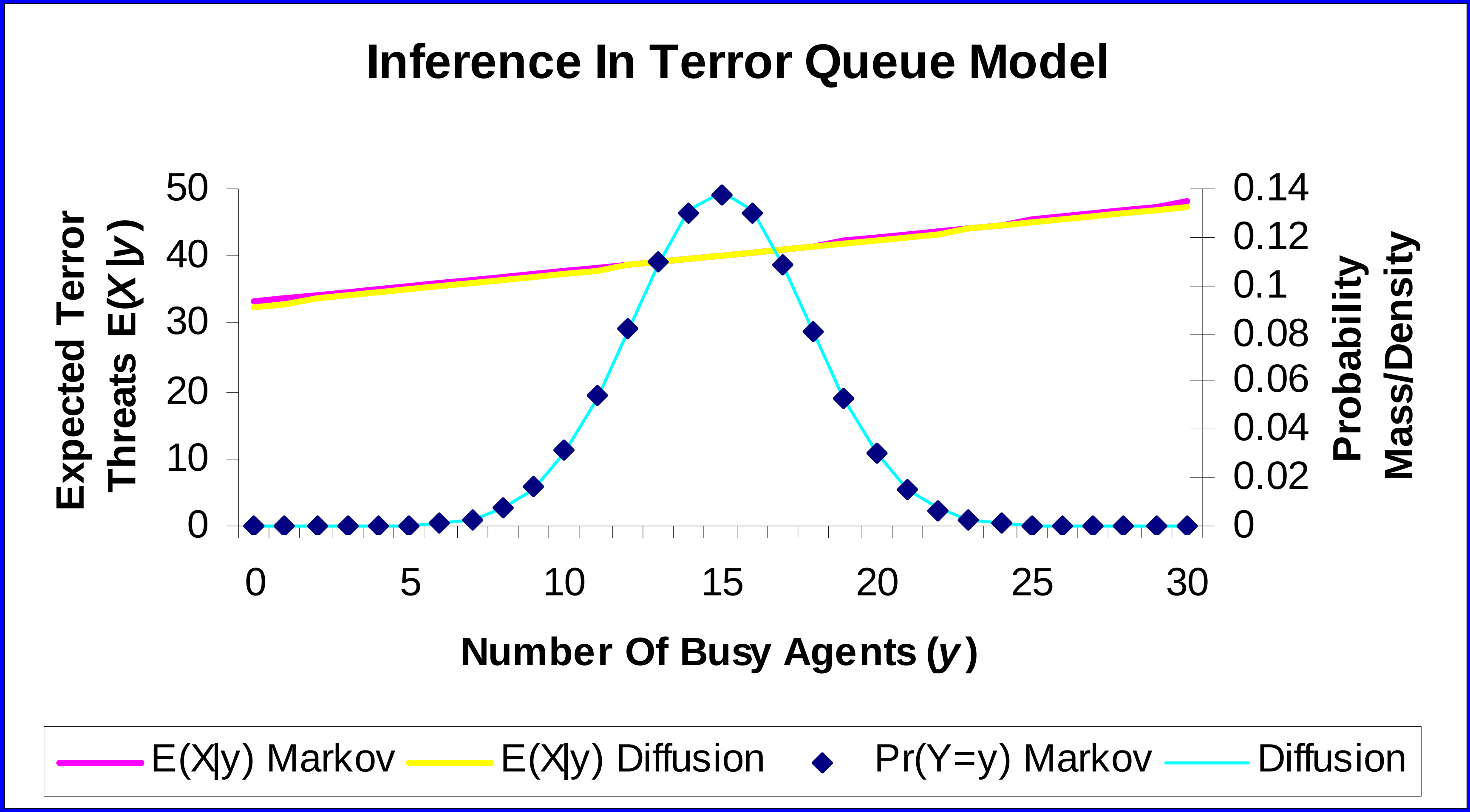
- Due to the bivariate normality, given the observed number of busy intelligence agents *y*, the number of undetected terror plots is normally distributed with mean

$$E(X|Y=y) = E(X) + \frac{Cov(X,Y)}{Var(Y)}(y - E(Y))$$

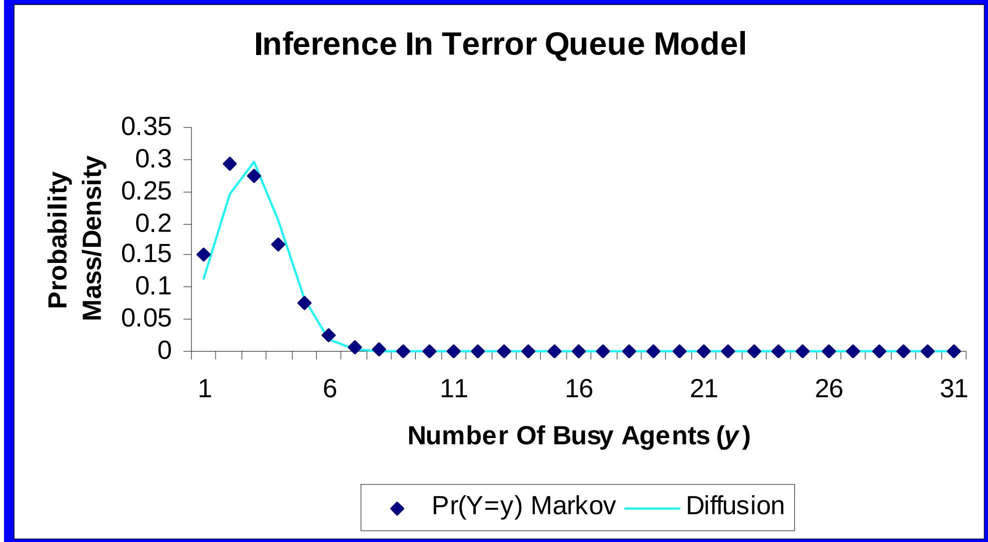
and variance

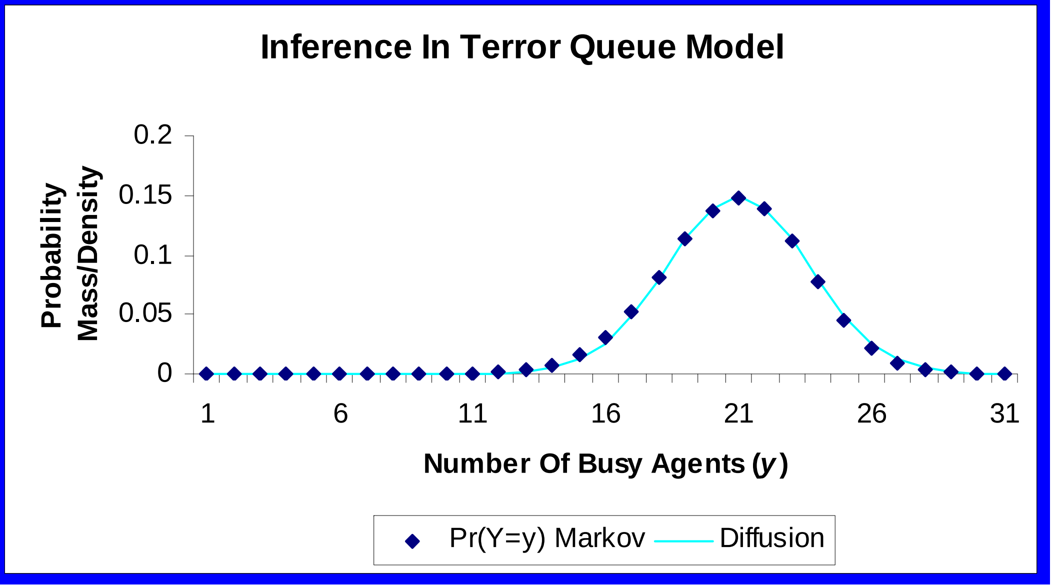
$$Var(X|Y=y) = Var(X)(1 - Corr^2(X,Y))$$

Comparing Markov and Diffusion Models for Hypothetical Example



Diffusion Works Well Providing *Y* Far Enough from Boundaries at 0 or *f*





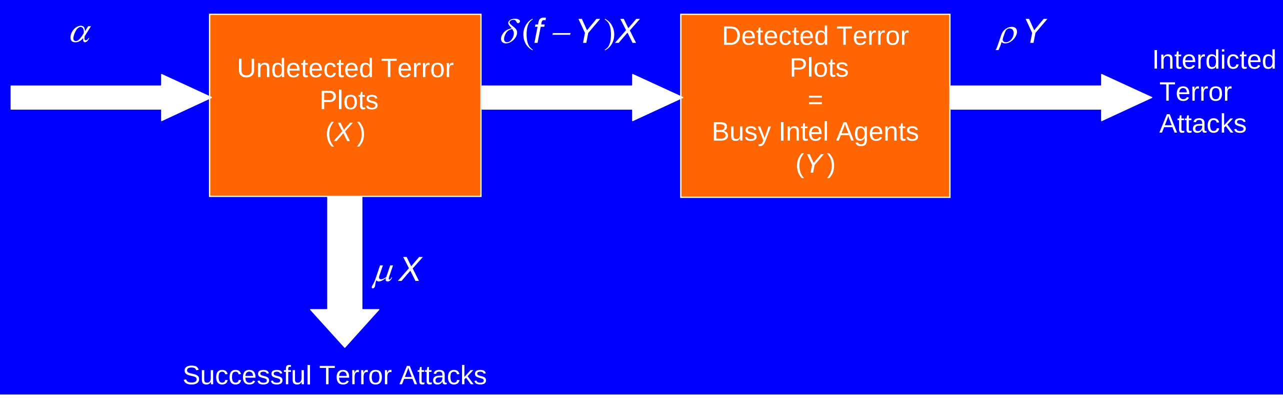
Simple Boundary Approximations Based on Flow Diagram

- $Y \approx 0$, then X is like the number of customers in infinite server queue

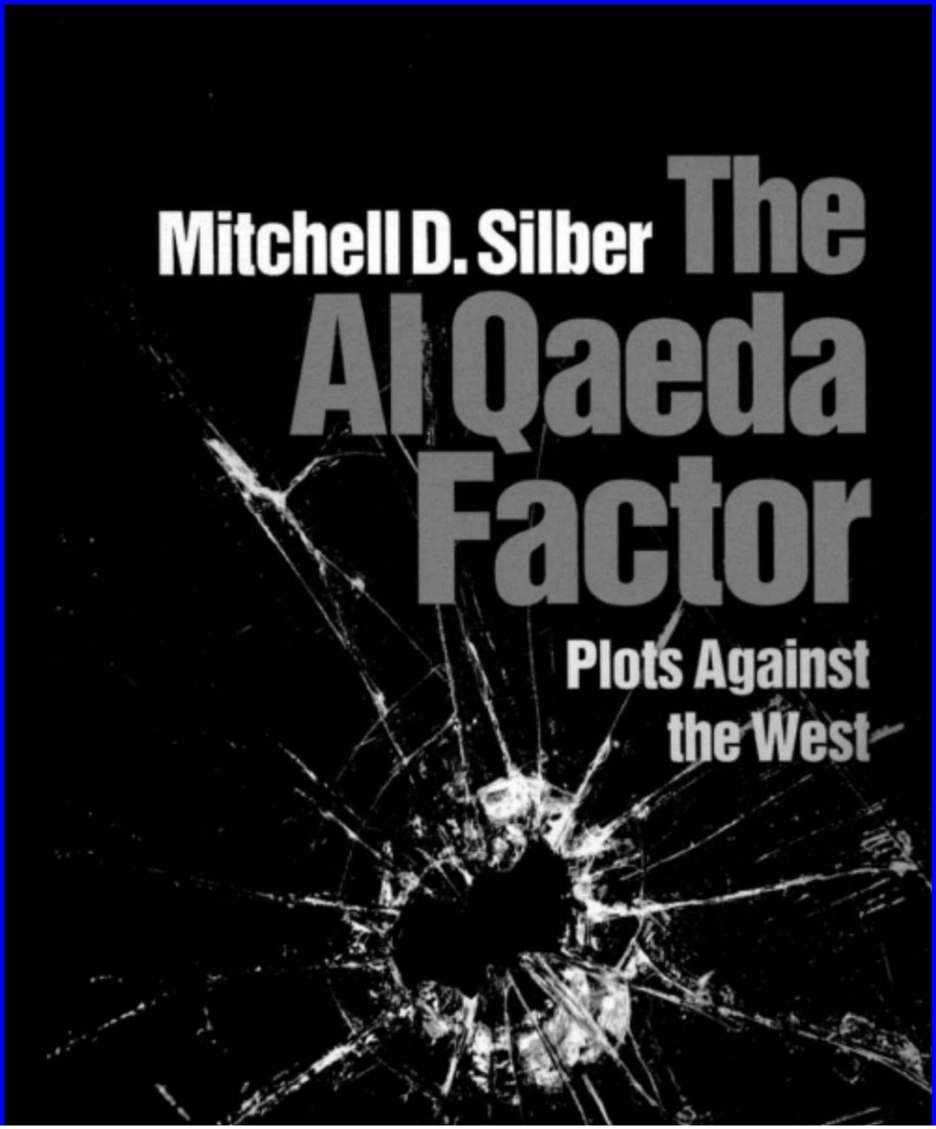
$$E(X) = Var(X) = \frac{\alpha}{\mu+\delta f}$$

- $Y \approx f$, then X is like customers in $M/M/1$ queue with reneging

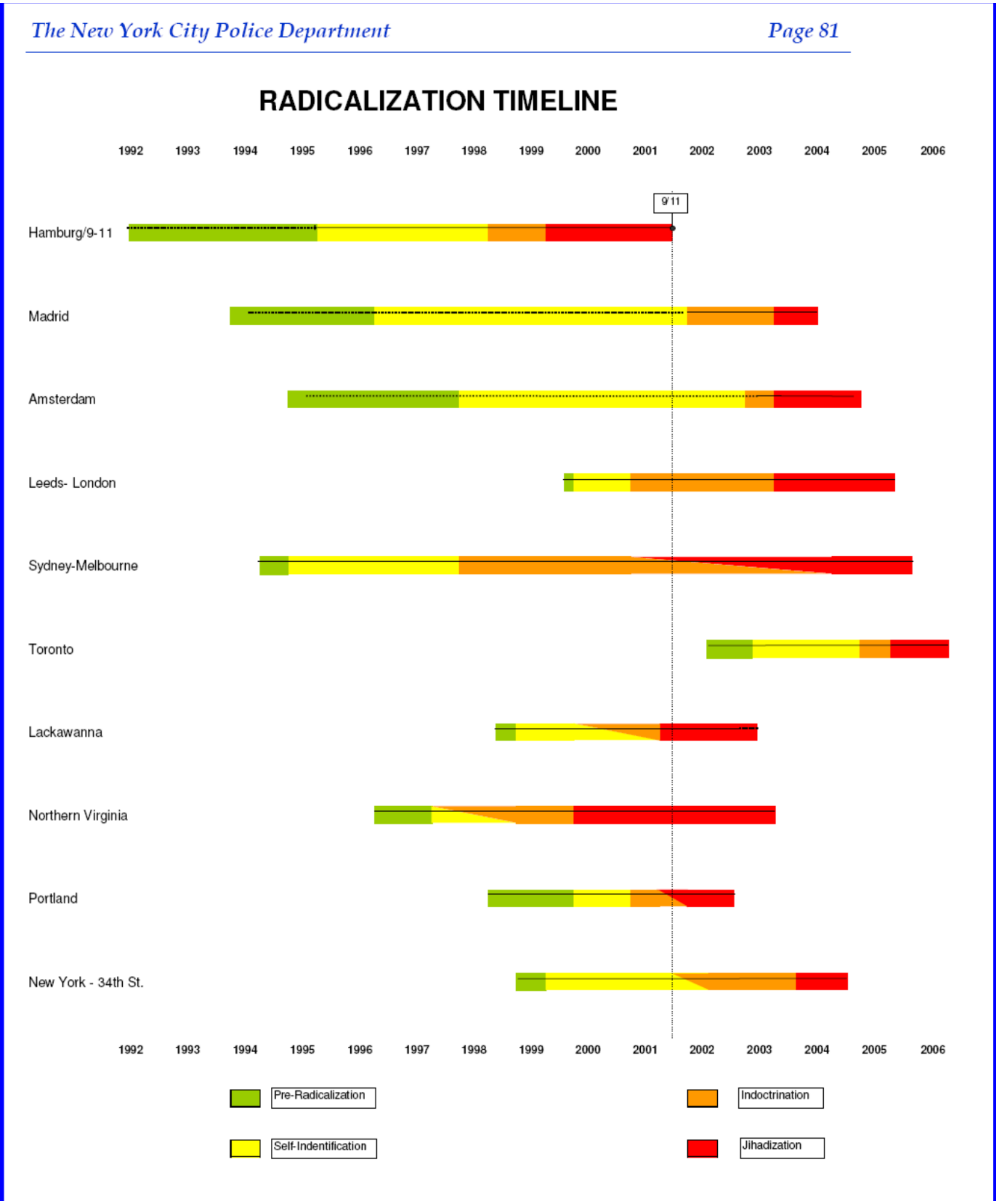
$$E(X) \approx \frac{\alpha-\rho f}{\mu} \qquad Var(X) \approx \frac{\alpha}{\mu}$$



Jihadi Terror Plots in the United States

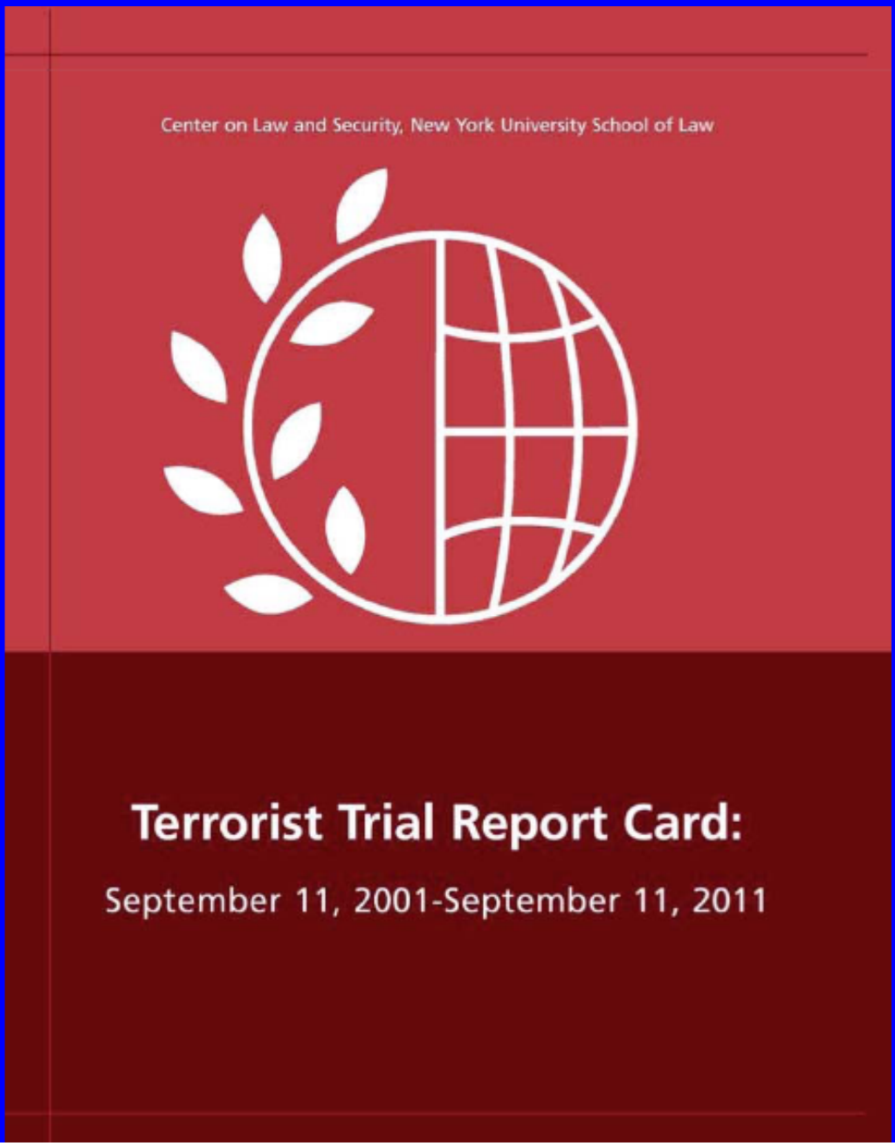


- "…most of the operations against the West have been manned by inspired volunteers who join it from the 'bottom up'…"
- "…that al Qaeda Core's role in plots is in general decline is a critical finding…"



Silber, MD and Bhatt, A (2007) *Radicalization in the West* (NYPD)

Terror Plots in the United States



- The *Terrorist Trial Report Card* (TTRC) tracks and analyzes all federal criminal prosecutions since September 11, 2001 that the Justice Department claims are terror-related
- 55% of TTRC cases are *Jihadi*
- Overwhelming majority of those prosecuted did not link to specific terror plots targeting the United States

Jihadi Terror Plots in the United States

- TTRC's definition of *Jihadi* cases "...includes defendants who were formally or informally associated with an Islamist terror group -- whether one with a global jihadist ideology (i.e. Al Qaeda) or a local Islamist movement (i.e. Hamas). It also includes defendants unaffiliated with a terror group who aspired to such affiliation or who subscribed to a global jihadist ideology."

Jihadi Terror Plots in the United States

- Review of *Jihadi* cases identified 26 cases linked to plans to attack Americans in US
  - thanks to NYPD's Mitch Silber for help eliminating non-plots, campfire plots, "let's play *Jihadi*" plots, etc.
- Cross check with Strom *et al* (2010) identified additional nine plots; 35 total
  - Sample includes: shoe bomber, captain underpants, Herald Square subway bomb, JFK fuel tanks, Time Square bomb, LAX shootings, etc.
  - Sample *excludes* Lackawanna 7, Bly Oregon camp, Northern Virginia Paintball, Atlanta casing plot, etc.

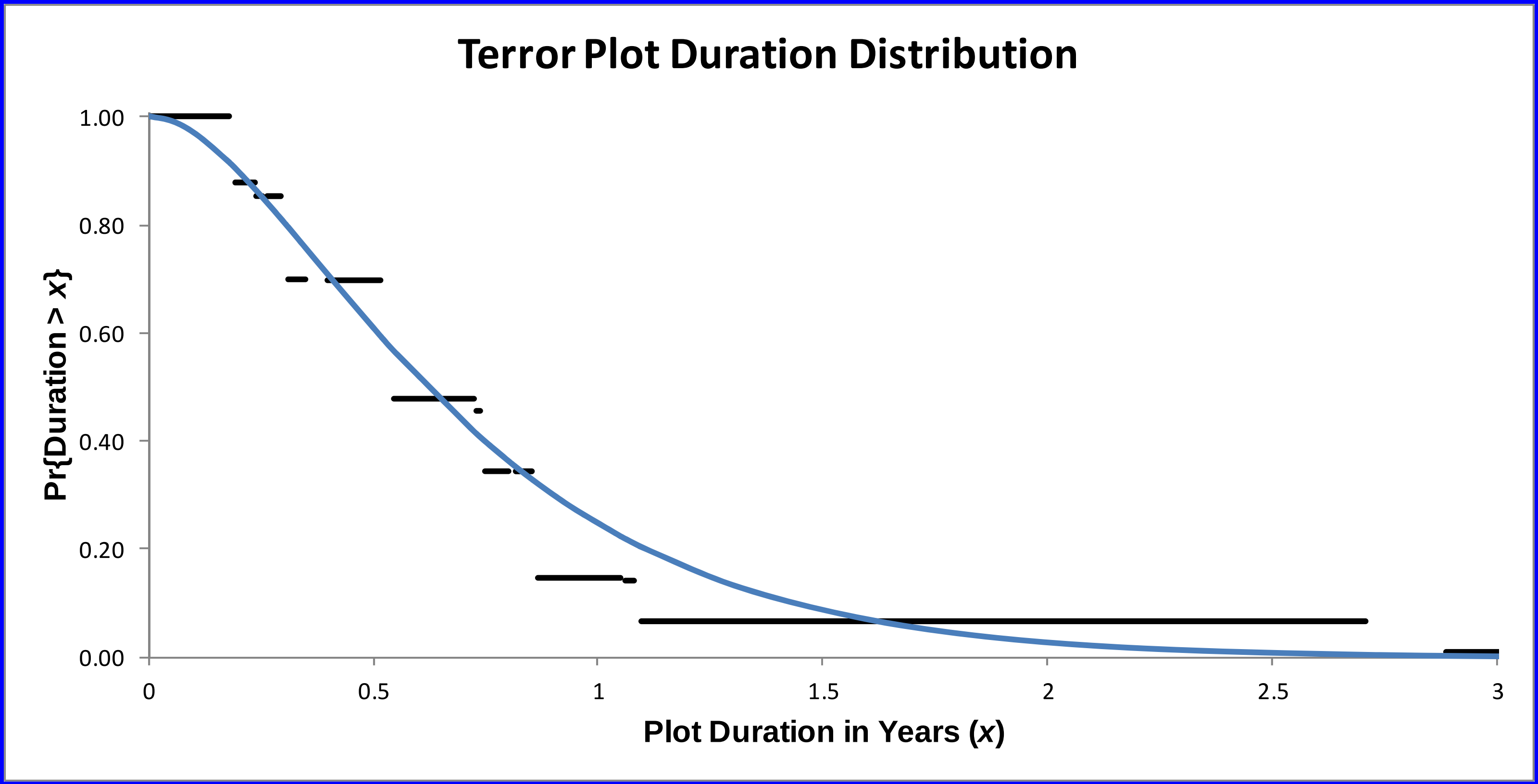
Estimating the Duration of *Jihadi* Terror Plots in the United States

- When does a terror plot begin?
- Hard to know; indeed terrorists probably don't know exact date either
- Futile to attempt pinpointing *the* start date
- Not futile to determine upper and lower bounds
  - "Early start" – plot had not begun before this date
  - "Late start" – plot had certainly begun as of this date
- Estimated early and late start dates from relevant court records such as indictments, criminal complaints, and other supporting legal documents in addition to media reports and other public sources

E.g. Fort Dix Plot

- From criminal complaint, “On or about January 3, 2006, MOHAMAD SHNEWER, DRITAN DUKA, ELTVIR DUKA, SHAIN DUKA, and SERDAR TATAR conducted firearms training in Gouldsboro, Pennsylvania,”
- “On or about August 11, 2006, CW-l (note: CW = cooperating witness) and MOHAMAD SHNEWER traveled to the Fort Dix military base to conduct surveillance...When CW-1 asked what made SHNEWER think of Fort Dix as a target, SHNEWER replied, ‘My intent is to hit a heavy concentration of soldiers...’ As SHNEWER and CW-l drove into a specific area at Fort Dix, SHNEWER said, ‘...this is exactly what we are looking for. You hit 4, 5, or 6 humvees and light the whole place [up] and retreat completely without any losses.’ ”
- On this basis, early and late start dates were assigned to January 3 and August 11 respectively

Empirical US Jihadi Terror Plot Duration Distribution



- Mean=270 days (SE 43)
- 95% probability interval 1 – 25 months

How Many Terror Plots?

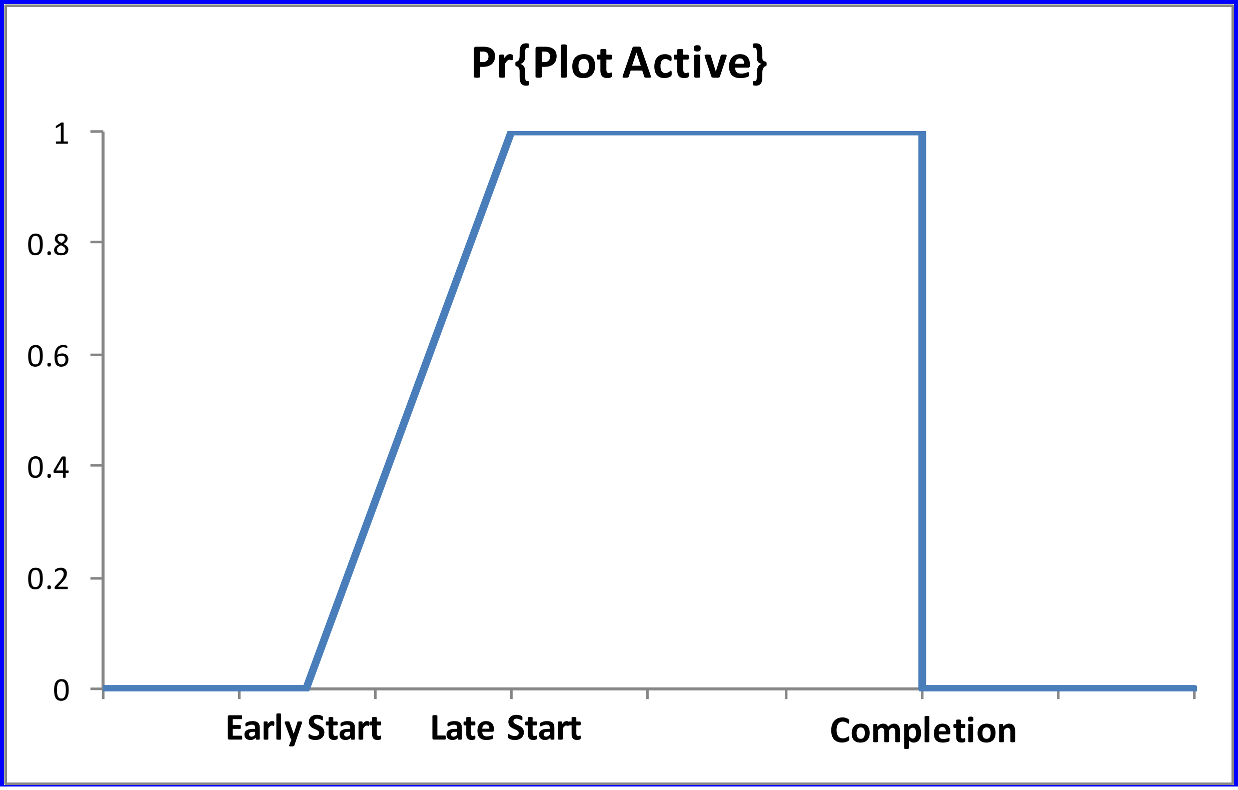
- Again, if N is number of terror plots in progress, and α is the plot initiation rate, then

$$E(N) = \alpha E(D)$$

- Plugging in estimates for mean duration (270 days) and arrival rate (35 plots/9.8 years) yields $E(N) = 2.64$ – not a large number!

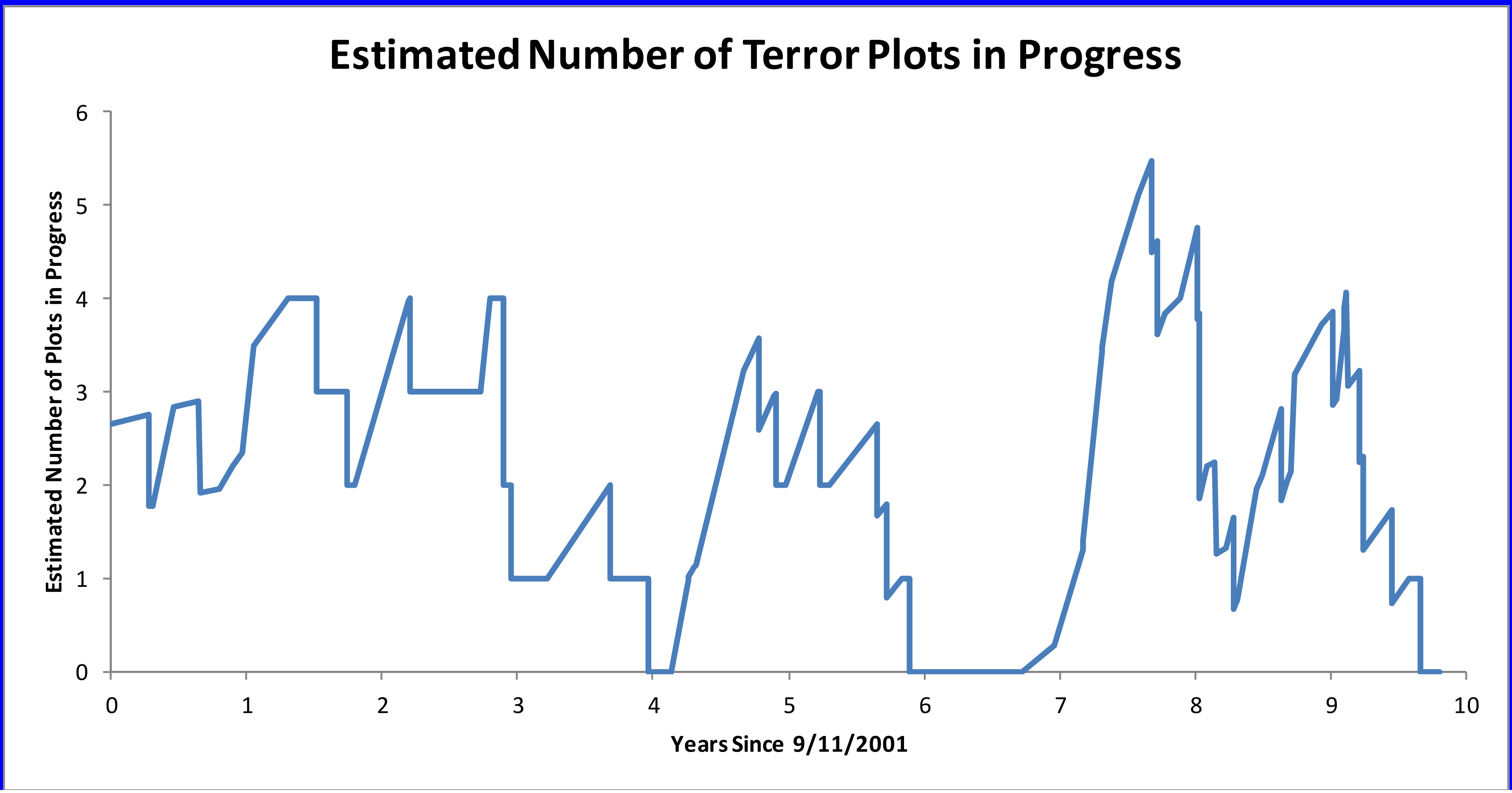
Plots Over Time

- Let $p(t)$ denote the probability that a particular plot is in progress at time t
- $p(t)$ looks like…



Plots Over Time

- Summing $p(t)$ over all plots gives expected number of "observable" active plots in data over time



Modeling Expected Observable Plots

- For first several years, expect to see $\alpha E(D)$ observable plots
- But as approach end of study period, number must decline due to end-of-study truncation (all plots end by τ_f)

$$E[N(t)] = \int_{-\infty}^{t} \alpha \Pr\{t - s < D \leq \tau_f - s\} ds$$

Modeling Expected Observable Plots

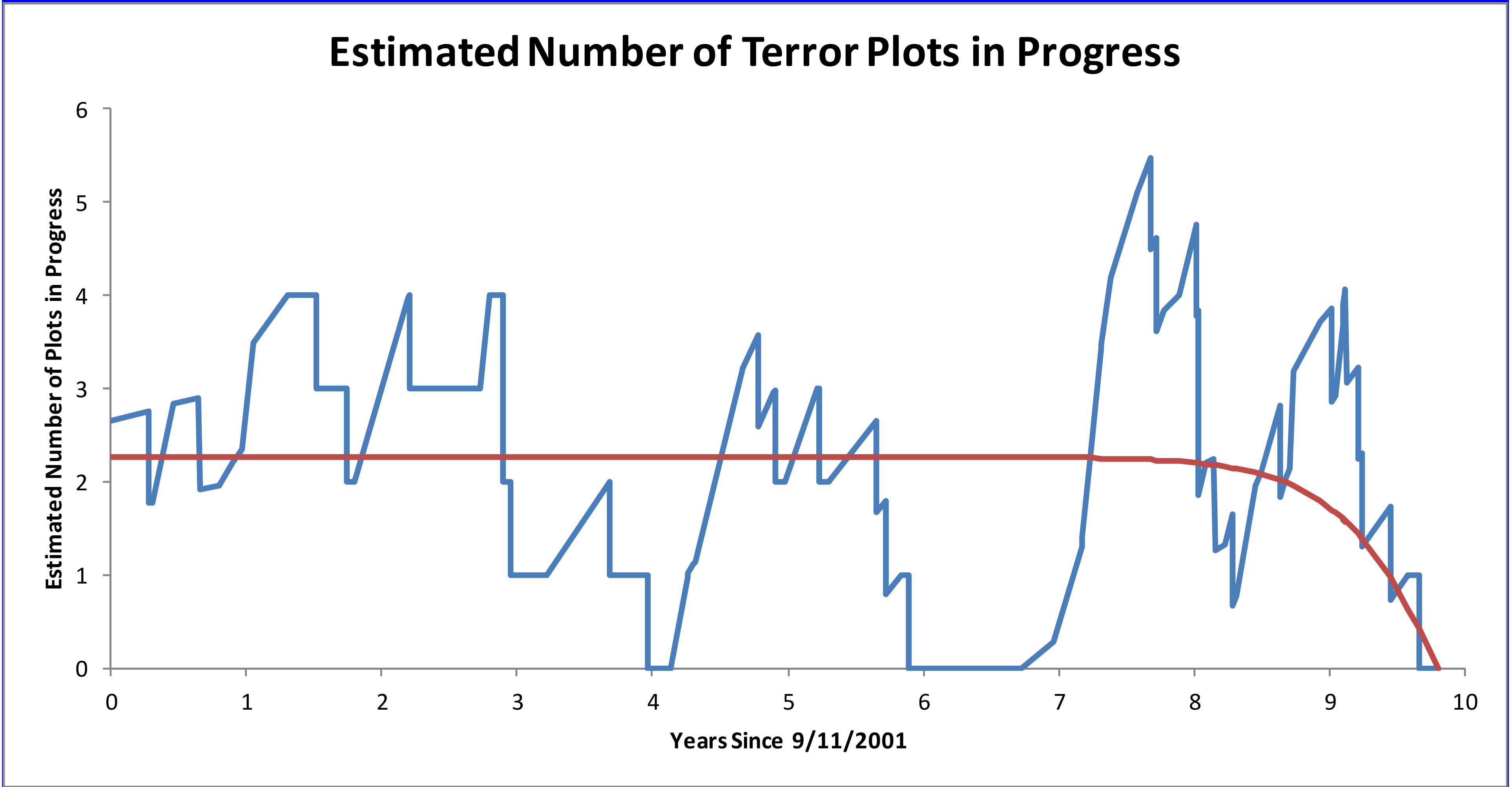
- For first several years, expect to see $\alpha E(D)$ observable plots
- But as approach end of study period, number must decline due to end-of-study truncation (all plots end by τ_f)

$$E[N(t)] = \int_{-\infty}^{t} \alpha \Pr\{t - s < D \leq \tau_f - s\} ds$$

$$= \alpha E(D) \Pr\{D^* \leq \tau_f - t\}$$

where D^* is the residual plot duration given random incidence, that is, how much longer a plot that is currently active will remain so until execution or interdiction

Compare to Model



How Many Good Guys Do You Need To Catch The Bad Guys?

- In the US, since 9/11 the FBI "...increased the number of Special Agents working terrorism matters from 1,351 to 2,398."

http://www.fbi.gov/stats-services/publications/fbi_ct_911com_0404.pdf

- Not all FBI Special Agents operate covertly, but other law enforcement agencies such as the New York Police Department also deploy undercover officers to disrupt terror plots
- Agents are "tip of the spear"

Attack Level Staffing

- How many agents f are needed to detect and interdict a given fraction θ of attacks?
- For Markov terror queue, solution given by

$$f = \frac{\alpha}{\rho}\theta + \frac{\mu}{\delta}\frac{\theta}{1-\theta}$$

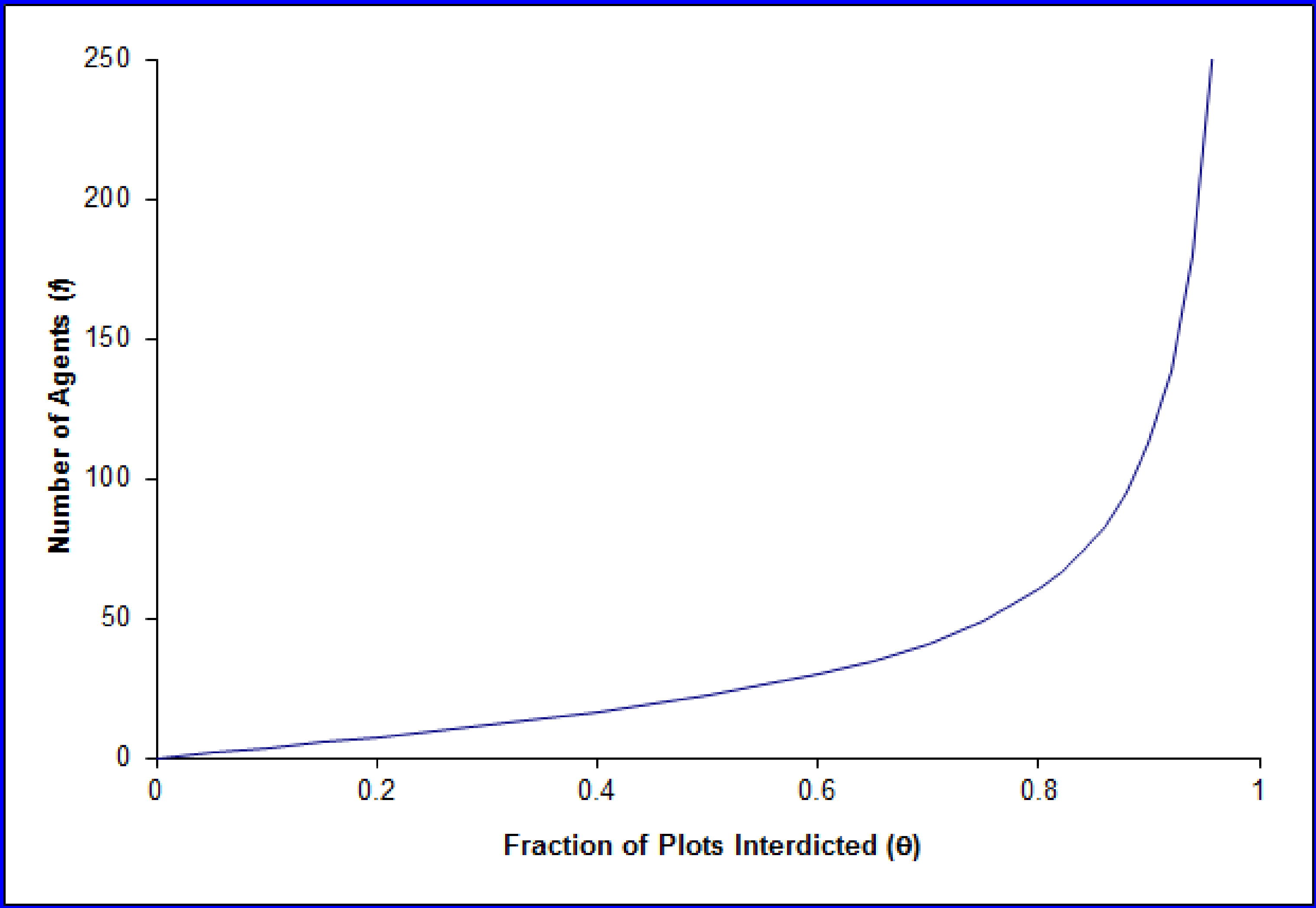
Attack Level Staffing

$$f = \frac{\alpha}{\rho}\theta + \frac{\mu}{\delta}\frac{\theta}{1-\theta}$$

- Can think of this as $f = f_b + f_a$ where
  - $f_b = \alpha\theta/\rho$ is the number of busy agents and
  - $f_a = \mu\theta / (\delta(1-\theta))$ is the number of agents available for detection, and solves

    $f_a\delta / (f_a\delta + \mu) = \theta$ (i.e. Pr{Detect} = θ)
- For large θ, $f_a >> f_b$

Attack Level Staffing



Attack Level Staffing

- In model, all terror plots either result in attacks, or are detected and interdicted
- *Understates* true prevention, in that fraction detected ≤ fraction detected or deterred:

$$\frac{\text{Detected}}{\text{Detected + Attacks}} \leq \frac{\text{Detected + Deterred}}{\text{Detected + Deterred + Attacks}}$$

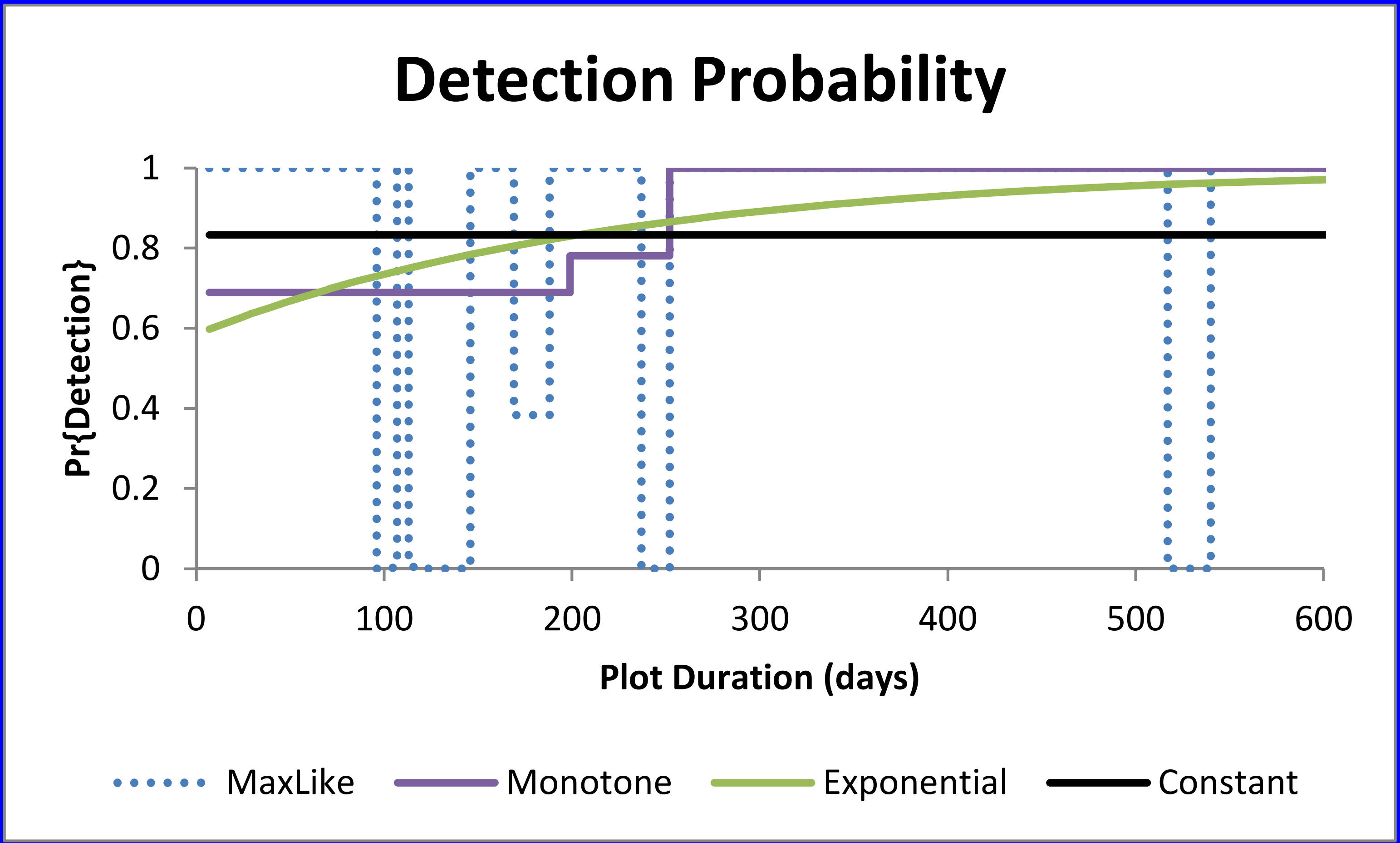
Other Staffing Objectives

- Maximize the net benefits of preventing attacks, accounting for the cost of agents
- Allocate a fixed number of agents across different regions (or focusing on different terrorist groups) to prevent as many attacks as possible (or prevent as many attack casualties as possible)
- Game theory version – terrorists select attack rate to achieve objectives, recognizing optimal terror queue staffing

Plot Durations With Proportional Hazards

- When is a plot more likely to be detected?
- When there is more plot activity
- A good measure of plot activity is attack hazard!
- So, take the attack hazard as “baseline,” and take detection hazard as proportional to baseline
- That is, assume $\delta(u)$ is proportional to $\mu(u)$
- This yields constant detection probability with age of plot, and hence constant detection probability overall

For *Jihadi* Plots In US Data



- Likelihood ratio tests: cannot reject hypothesis of constant detection probability with age of plot

Staffing With Proportional Hazards

- The proportional hazards assumption is

$$\delta(u) = k\,\mu(u)$$

- Thus the detection probability equals

$$\begin{aligned} p &= \frac{f_a k \mu(u)}{f_a k \mu(u) + \mu(u)} \\ &= \frac{f_a k}{f_a k + 1} \end{aligned}$$

What About Busy Agents?

- Recall that f_b is the expected number of busy agents
- If on average it takes $1/\rho$ time units to interdict detected plots, a fraction p are detected, and the attack rate equals α, then as before we have

$$f_b = \alpha p / \rho$$

Attack Level Staffing Formula

- Recall the decompostion $f = f_b + f_a$
- For attack level staffing, set

$$f_b = \alpha\theta/\rho$$

- f_a solves $k\,f_a\,/\,(k\,f_a + 1) = \theta$, that is

$$f_a = \frac{1}{k}\,\frac{\theta}{1-\theta}$$

- Overall attack level staffing then equals

$$f(\theta) = \frac{\alpha\theta}{\rho} + \frac{1}{k}\,\frac{\theta}{1-\theta}$$

Special k?

- If you know fraction of plots detected for *some* staffing level f^*, $p(f^*)$, can set

$$f_a^* = f^* - \alpha p(f^*)/\rho$$

and set k equal to

$$k = \frac{1}{f_a^*}\frac{p(f^*)}{1-p(f^*)}$$

- Expect $\alpha p(f^*)/\rho$ to be small; can often ignore

Example

- Recall that in US have detected 80% of Jihadi terror plots
- FBI reported have assigned ≈ 2400 special agents to terrorism
- Take $f_a^* = 1{,}600$ for this example
- Special k given by (1/1600) * .8 / .2 = 1/400
- If doubled available agents to 3,200 would prevent (3200/400) / (3200/400 + 1) = 8/9 ≈ 89%

Example

- Want to prevent 95% of Jihadi plots
- Using staffing formula given prevent 80% with f^*=1,600, would need

$$f_a = \frac{1}{1/400} \times \frac{.95}{1-.95} = 7,600$$

- Is it worth it?

$$\max_{0 \leq \theta < 1} b\alpha\theta - cf(\theta)$$

What If Don't Know f^*?

- Suppose all you know is current probability of detection p
- Want to increase this by $100\varepsilon\%$
- Using staffing formula, easy to show that need to increase number of agents by

$$100\frac{\varepsilon}{1-(1+\varepsilon)p}\%$$

Example

- Don't really know how many agents there are, but know now catching 80% of plots
- Suppose want to catch 95%, an increase of 18.75% in the detection probability
- Need to increase existing covert force by

$$100 \times \frac{0.1875}{1-(1+0.1875)\times 0.8} = 375\%$$

(that is, a factor of 4.75)

Example: Allocate Agents Across Groups

- Suppose have *n* different geographic regions/groups
- Constrained to *f* agents in total
- How to allocate agents across groups?

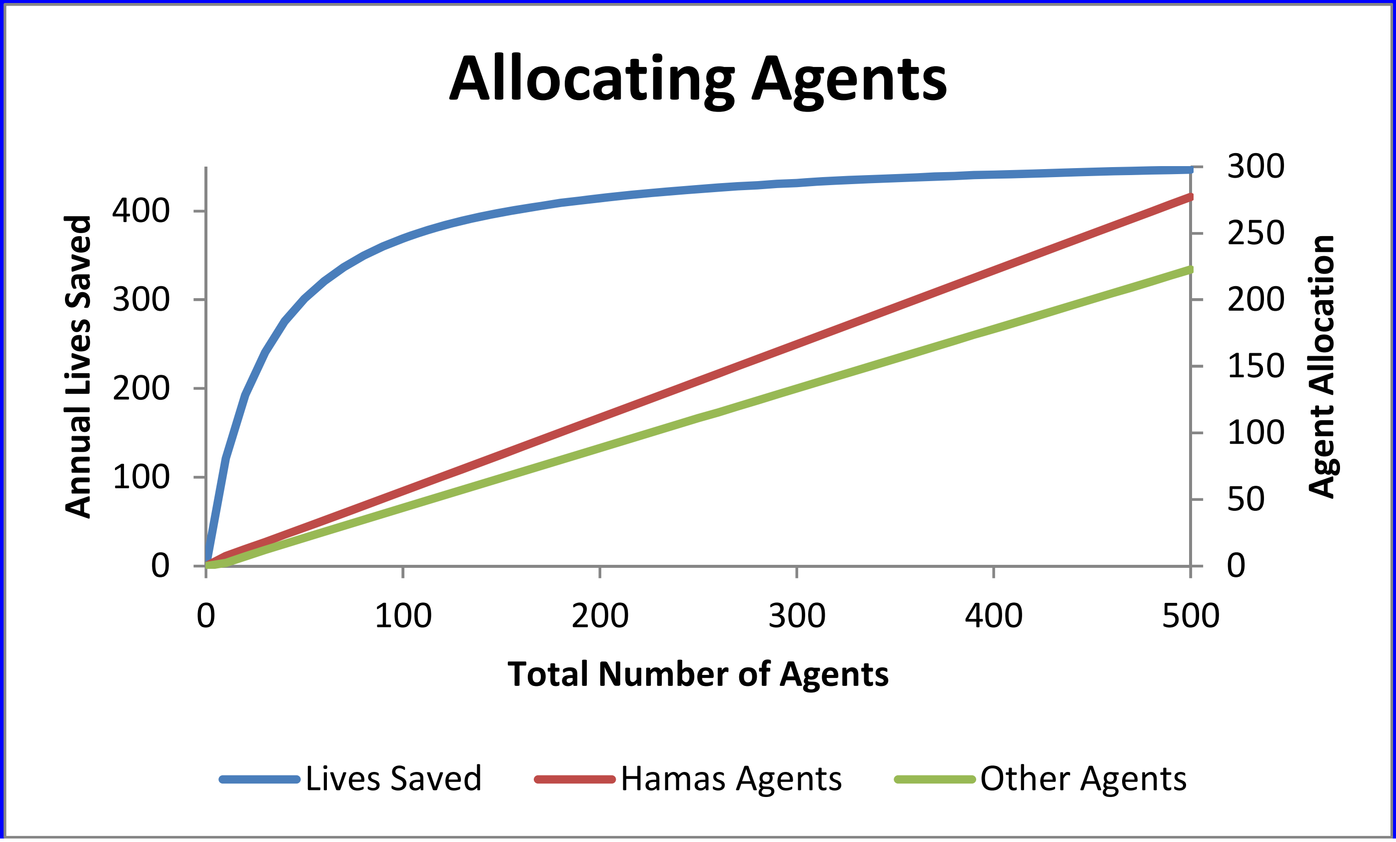
$$\max \quad \sum_{i=1}^{n} b_i \alpha_i \theta_i$$

$$\text{st} \quad \sum_{i=1}^{n} f_i(\theta_i) \le f$$

$$0 \le \theta_i < 1 \text{ for } i = 1, 2, \ldots, n.$$

Intifada Example

- Hamas suicide bombers killed 8.9 civilians/attack (other groups 3.5)
- Allocate agents to maximize lives saved



Summary

- Terror queue framework connects attempted attacks to outcomes via detection/interdiction by undercover agents
- Available data suggests a duration distribution for *Jihadi* plots in the US
- Same data suggest that hazard functions for time to detection/attack are proportional
- Sensible if detection more likely when terrorists more active, and attack hazard marks terrorist activity

Summary

- Proportional hazards assumption enables simple staffing models that do not otherwise depend on the specific probability distributions of times to detection or attack!
  - Attack level staffing; force allocation; even game theoretic version where terrorists strategically select attack rates
- Models do assume agent times to detection are mutually independent
  - Correlation across times to detection equivalent to reducing number of independent agents
- Models exhibit strong diminishing returns in attack detection as # agents increases