

# **Deterrence Discussion Group**

# Deterrence

**Chair: Mr. Pat McKenna – “The Deterrence Analytic Challenge”**

**Co-Chair: Dr. Yuna Wong**

**Dr. Richard Lobban**

**Dr. Loren Cobb**

**Dr. David Siegal**

**Dr. Bill Young**

**Dr. Eunice Santos**

**Dr. Charles Macal**

**Dr. John Sokolowski**

**Mr. Jordan Wilcox (ST)**

**Dr. Katherine Banko**

**Ms. Krista Hendry**

**Dr. Ivy Estabrooke**

**Dr. Myriam Abramson (ST)**

**LT Robin Marling**

**Dr. Peter Tikuisis**

**Mr. James Morris**

**Dr. Jennifer O'Connor**

**Dr. Richard Hayes (ST)\***

**Dr. V.S. Subrahmanian**

**Mr. Skip Cole**

**Mr. Jonathan Jackson**

**Dr. Max Crownover**

(ST) indicates Synthesis Team Member. (ST)\* indicates Synthesis Team Lead

# Approach

- Short summary of deterrence paper
- General discussion for ~1hr
- Broke into groups looking at 5 areas ~2.0hrs
  - ~1hr to discuss
  - ~1hr of outbriefs
- Summary discussion ~0.5hr

# General Discussion

- Phrasing is wrong, it is influence
  - Deterrence is one subset
  - Others
    - Theater security cooperation
    - Dissuasion
    - Containment
    - .....
- Deterrence Operations JOC definition of deterrence assumes rational choice economic models
  - Behavioral aspect needs to be brought in
- Don't necessarily know who attacked us
  - But can target terrorist financiers, logisticians
  - Need to broaden the problem space

# General discussion (cont.)

- Success only measured by lack of behavior?
  - Doesn't make sense: trying to prove a null
  - Indications of “success” exist but can you link a deterrent action to an indication?
  - Can we model deterrence failure instead?
- Decision makers comfortable with partial solutions
  - Small and focused models (not mega models)
  - “Magic” models that incorporate everything may give poor answers
- Needs / approaches discussion
  - Focus groups suggested as an approach to examine deterrence issues
  - Need cognitive models (of who you are trying to deter)
  - Does work in social sciences on deterring criminal activity apply to other actors?
  - Historical case studies (e.g., studies of pre-WWI telegrams)

# Deterrence Levels

<b>X (Actor)</b>	<b>Y (Deterring Entity)</b>	<b>Z (action being deterred)</b>
<b>Individuals (hackers)</b>	U.S. government	Hacking
<b>Small groups (Simbolese Liberation Army)</b>	U.S. government (law enforcement)	Violent acts
Isolated small groups (British med students)		
<b>Organized crime</b> (Colombian drug cartels)	U.S. and Colombian government	Drug trafficking
<b>State (Saudi Arabia)</b>	U.S. government	Building schools that teach extremist ideology
<b>Non-state actors (al Qaeda)</b>	U.S. government	Attacks against U.S. targets (9/11 and now)

# 1. Individual

- Example: hacker
- Motives
  - Build reputation
  - Personal financial gain
  - Direct damage
  - Retaliation
- Issues:
  - Small barrier to entry, one person can cause significant damage
  - Identification of the individual
  - Attribution, location
  - Understanding intent and motivation
  - What they value

# 1. Individual (cont.)

- Carrots:
  - Options for promoting desired behavior?
  - Reward for hacking (challenge – build reputation but in a positive way)
- Sticks:
  - Hack back? But potential escalation
- Tools:
  - Systematically explore motivations for individuals to get to root causes
  - Profile, understand demographics and bound solution space
  - Is it worth it to build expensive tools to deter an individual? Maybe it is, because of the potential damage

## 2. Small Group

- Simbolese Liberation Army
  - Violent actions: kidnapping, bank robbery, agitation, context of 1960s radicalism
  - Motivations: anti-war, anti-authority
- Do we deter?
  - Deter next generation from organizing
- Law enforcement authority
  - How well financed, observed is the authority?
  - How aggressive in operations and in infiltrating?

## 2. Small Group (cont.)

- Issues:
  - Group repurposing – deterrence fails
    - Why do groups repurpose? What are the mechanisms?
  - How to raise flags about isolationist behavior
    - Can we detect it?
    - Can we model it?
  - Surveillance – does it deter? (let's watch UK experience)
- Generalizations:
  - Law enforcement approach generalizes
  - Model functions (e.g, police arrest, surveillance, patrol, etc)

# 3. Organized Crime

- Example:
  - Colombian drug traffickers – loose coalition of opportunistic groups
  - Who is deterring: US and Colombian government
- Who is doing the smuggling?
  - People with long history, experience, education in violence who weren't offered an effective way to repatriate into society
  - How do you send an appetizing message to these types of people?

# 3. Organized Crime (cont.)

- Analytic difficulties:
  - Unintended consequences (rerouting drug flow)
    - Nth order effects
  - Adaptive organizations
  - Governments try only part of the solution set
    - Need to include “host” country elements in tools
  - How to create a niche in a fully formed society for disaffected members
    - Modeling equivalent positions (stature/pay/authority)
- Issues:
  - Groups may be multi-functional?
    - Drug gangs also street gangs who control territory
    - Smuggling drugs may just be providing \$ for other activities
  - Model process from security → criminal organization?
    - Modeling transition of group purpose
  - Corruption
    - Do we apply U.S. view or their view? Is there an “acceptable”/ “expected” level of corruption?
    - Everyone is corrupt except our group – helping own group is not corruption (may even be killed otherwise)
  - Modeling or data collection problem

# 4. Non-state Actor

- Example: US deterring al Qaeda before 9/11 and now
- Issues:
  - Any government will be at a disadvantage when going against a group like al Qaeda b/c it is a set of nodes that do anything they want
  - Network does ideology, financing, but don't have rigid command and punishment structure
  - Any group within the network is agile – can have their own targeting plan, able to adapt to local conditions

# 4. Non-state Actor (cont.)

- Recommendations (cont.)
  - If can't deter, can try to contain (containment is another type of influence)
    - Need model or tools to describe containment strategies and try to see why some work or fail
  - Can try to accelerate demise of al Qaeda by encouraging fractionalization
    - Model of fractionalization in non-state actors
    - What types of exogenous factors increase fractionalization? Also a weakness of decentralized networks
  - Copycat effect
    - How do we model it?
  - Sterilize environment
    - Try to change operational environment to change ability of AQ to spread; and support successful local efforts financially
    - Need tools to model spread
  - Modeling deflection
    - Changing potential terrorist target characteristics to make them less vulnerable (and understand how that causes a shift in likely targets)

# 5. State

- Example: Saudi Arabia
  - Deter Saudi government from building schools with radical ideology
  - Context: Wahabbism, want to maintain relations with the Saudi government
- Analytic issues:
  - Don't want to look like you're against Islam
  - How fragile is the Saudi government?
  - Variables: perceptions of domestic audience
- Generalizeable issues:
  - Overt vs covert deterrence actions
    - Can't look like the US made a government do something
  - Lack of intelligence (lack of data)
  - US biases
  - Nth order implications

# 5. State (cont.)

- Issues cont.
  - Influence, not deterrence
  - Model is of context, not just target, including outside perceptions
  - Small models versus capturing the context (tendency to scale up model to try to capture context)
  - Scale about the seriousness of the threat when deterring states (Saudi textbooks vs. North Korean nuclear weapons, Venezuelan oil output)
    - How should models incorporate implications of deterrence failure? (think allocation of resources to n deterrence challenges – which ones get resources?)
  - Model the entire state
    - Oil: U.S. moving sources to African oil
    - Osama bin Laden is a Wahabbi
    - Saudis also building mosques like crazy – need some kind of antidote to rival or be an alternative (Saudis really opposed to other kinds of groups)
  - Likely need to include more than one state in the tools

# Once around the room discussion

- Whole range of possibilities for influencing makes sense
  - Deflect, deter, influence, attract, etc.
- Unintended consequences
- Building tools – the next workshop?
  - What kinds of tools are being built?
  - Do we know how to build models?

- Backup slides

# Charge to Group

- We are successful if we provide input on:
  - Deterrence definition
  - What is the nature of today's deterrence challenge?
    - Adversary type?, Deter from what?, What are the possible contexts?
    - Priority of types of deterrence challenge
  - What are the tenets of the deterrence analysis?
    - Diversity in ...
    - Three areas: foundational, pre, and post
  - How do theories/methodologies/tools map to the types of deterrence challenges
    - E.g., tools to examine deter nation state from x will likely be different than tools to examine deter terrorist from doing x (Where are macro and micro tools applicable?)
    - Can the same tools be applied across foundational, pre, and post assessment?
    - What are the gaps? What is the priority?

**Context: Inform HSBC modeling initiatives**

# General discussion (cont.)

- Other issues:
  - Including influence gives other metrics
  - Deterrence is just one part of influence
  - Cyber deterrence
  - Challenge of linking US actions to outcomes
- Who is the adversary? (Need to focus problem)
  - To advance the discussion, you have to get concrete: specific examples
  - Decompose goals to create a process, then have something more actionable to watch

# 1. Individual (cont.)

- Other issues:
  - Cyber mechanism – used for trafficking and other destabilizing issues
  - Damage from propaganda
  - Application of contagion framework
  - Cyber bribery?
  - Nigerian fraud rings

# 4. Non-state Actor (cont.)

- Recommendations (cont.)
  - Ideological battle, US should be quiet
  - Raise profile of SMEs and on-the-ground people: improve their access to decision makers (nobody was listening before 9/11 even though bin Laden's activities were clear to Sudanese experts)
- Issues:
  - Deflection: US and Israel deflected embassy attacks (analogy from criminal literature shows that police action deflects criminal activity to other areas)

# Deterrence Central Idea (from DO JOC exec summary)

*The central idea of the DO JOC is to decisively influence the adversary's decision-making calculus in order to prevent hostile actions against US vital interests. This is the "end" or objective of joint operations designed to achieve deterrence.*

*An adversary's deterrence decision calculus focuses on their perception of three primary elements:*

- The benefits of a course of action.*
- The costs of a course of action.*
- The consequences of restraint (i.e., costs and benefits of not taking the course of action we seek to deter).*

*Joint military operations and activities contribute to the "end" of deterrence by affecting the adversary's decision calculus elements in three "ways":*

- Deny Benefits.*
- Impose Costs.*
- Encourage Adversary Restraint.*

*The ways are a framework for implementing effective deterrence operations.*

# Problem Overview

- Deter adversary X from doing Y under Z conditions
- Three broad areas of assessment
  - Foundational elements (or building the baseline understanding of the adversary)
  - Pre-action assessment (or deterrence planning)
  - Post action assessment (or examining the effect of an executed action)
- Complicated by
  - Uncertainty
  - Conflicting theories and approaches
  - Unknown (really not knowable) deterrence threshold
  - Nth order effects
- Applicable methodologies and tool will vary by X, Y, and Z as well as area of analysis

## 2. Small Group (cont.)

- Hypothesis
  - Law enforcement's effective presence must have been factor in decline of these groups in the US
  - Decline of relative gains; prosperity, social cohesiveness, inter-ethnic relations in US
  - Good state suppresses
  - Small group violence has declined with the rise of the state
- Foreign groups
  - Deter, neutralized, kill
  - Classifying: part of larger group? Tools will likely vary depending on answer.

# 4. Non-state Actor (cont.)

- US deterring
  - Too many franchises under the umbrella, extreme decentralization makes them impossible to deter
- Recommendations
  - If can't deter, can try to contain (containment is another type of influence)
    - Need model or tools to describe containment strategies and try to see why some work or fail
  - Best to let regional actors in the Middle East – they have better ways to influence
    - Watch what is working in Saudi Arabia, etc.
    - Means models must be broad (numerous countries)

# 5. State (cont.)

- Generalizeable issues:
  - Can't look like the US made a government do something
    - Attribution of action
  - Lack of intelligence (lack of data)
  - US biases
  - Nth order implications
- Issues:
  - Influence, not deterrence
  - Model is of context, not just target, including outside perceptions

# 3. Organized Crime (cont.)

- Issues cont.
  - Corruption
    - Corruption is an analytic problem for US analysts
      - Do we apply U.S. view or their view? Is there an “acceptable”/ “expected” level of corruption?
    - Everyone is corrupt except our group – helping own group is not corruption (may even be killed otherwise)
  - Modeling or data collection problem
  - What are the situations when arrests don't become convictions?