DHP P244: TERRORISM & COUNTERTERRORISM

DR. JAMES JF FOREST

Exploiting the Internal Vulnerabilities of Terrorist Networks

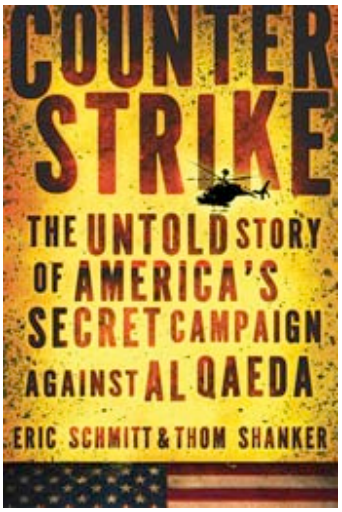
Reading Assignments

- Zakaria
- Hegghammer
- Zirakzadeh
- Abrahms
- Simon & Martini
- Abrahms

Understanding the Enemy

What do terrorists hold dear?

- Operational mobility
- Operational success
- Personal glory
- Reputation and honor
- Dependable supporters
- In-group trust, cohesion
- Family well-being
- Material assets, finances
- Safe havens, weapons
- Strategic success



Vulnerabilities

- Operational secrecy
- Strategic direction and authority
- Morale among members
- Ideological coherence and resonance
- Financial dimensions
- Tactical control

Trust is critical

"To work well, networks require strong shared beliefs, a collective vision, **some original basis for trust**, and excellent communications"

- Brian Jenkins, 2006

In human networks, **trust is established** by various social mechanisms and **shared beliefs**

Anyone can plug into the network if they use the proper protocols (the **"trusted handshake"**), usually enabled by previously established network credentials

Trust is critical

Examples of the "trusted handshake"

- Shared academic/scientific knowledge base
- Mutual friends/acquaintances who vouch for you w/their life
- Family ties, clan, tribe, etc.
- Religion (doctrinal knowledge, credentials, etc.)
- Battlefield veteran status (Afghanistan, Bosnia, Iraq)
- Shared experiences (prison, battlefield, oppression)

Some individuals have a very high level of "betweenness centrality" – these are **critical knowledge brokers** connecting different types of members (e.g., veterans & new recruits; scholars & mujahideen)

Vulnerabilities of Clandestine Networked Organizations

Key vulnerability: OPSEC

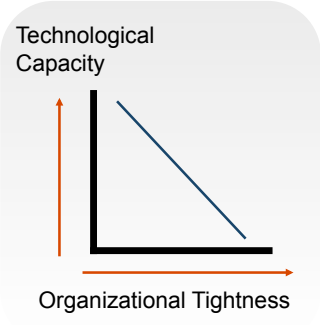
- Any organization involved in clandestine activities faces similar challenges in terms of **operational security**
  - Includes ferreting out spies within the organization
- Must maintain a level of security that facilitates conducting meaningful transactions of information and finance
- Secure long-distance communication can be time consuming and expensive
- Constant fear of (and hiding from) intelligence agencies, law enforcement

Technology and OPSEC

Technology enables organizations to become more "networked"

Constraining their technological capacity (through technology-based intelligence gathering) forces more face-to-face interaction

More frequent face-to-face interaction can increase a clandestine network's vulnerabilities
- technology, eavesdropping
- human intelligence, spies



Idea: Promote the perception that we have the capability to intercept any and all kinds of technology-based communications

Financial Dimensions

Without money, terrorists can do nothing

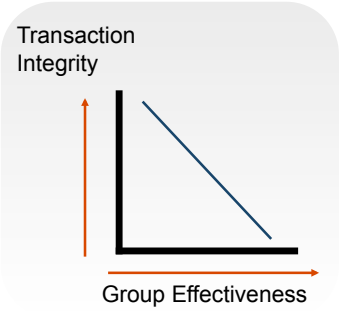
The ways in which terrorists obtain money can also be a vulnerability if deemed repulsive by potential supporters

Problem: **Limited or no accountability** regarding financial transactions, movement of assets, weapons, people

- Because of operational security needs, a clandestine organization cannot offer much transparency regarding its finances
- This allows considerable latitude for **abuse, corruption**

Transaction Integrity

- Strength of any network is based on the level of its integrity for conducting transactions (communication, financial, etc.); **reliability and trust of a network are critical**
- **Expectations** of money to support operations will be made available in a timely fashion
- **Expectations** that individual recipients will do the correct things with those funds



Exacerbating transaction integrity challenges

Slow the transfer of funds, assets from one node to another; cause unexplained transaction delays

Encourage internal looting (or perception of looting)

Get money to disappear with no reason

Have **conspicuous consumption items** (big screen TV) appear in place of the missing money

Encourage acrimonious debates over **preferential treatment**, special benefits given to certain members of the network unfairly

Publicize examples of "**lavish lifestyles of AQ leaders**" focusing on KSM and his playboy antics; al Fadl stealing money in Kenya; the Montreal cell and its money mismanagement, etc. Paint a portrait of these guys as anything but humble, pious, devout Muslims or competent financial decision makers.

Overall objective is making a network's members want to leave, disengage

Exacerbating transaction integrity challenges

Promote suspicion, rumors, mistrust

Publicize accounts of financial mismanagement, **corruption,** misappropriation, fund diversion

Encourage suspicion that donations, funds will not necessarily be used as donor intended (e.g., to pay drug couriers, prostitutes, murderers of schoolchildren, etc.)

Force leaders to consider punitive actions against agents/operatives

Overall goal: degrade the integrity within financial networks; **make asset management more difficult**

Overall objective is making a network's members want to leave, disengage

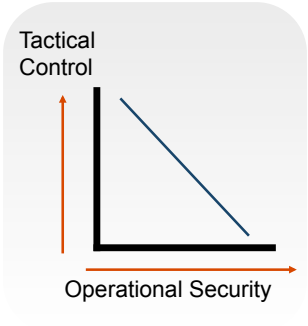
Agency Theory

- A network's members have different preferences, based on personal experiences, perceptions, etc.
- **Preference divergence** impacts the level of trust/ expectations of shared effort toward common goal
- Preference divergence can make it harder for a network's principals to maintain:
  1. Tactical control
  2. Strategic authority

These create vulnerabilities within terrorist networks that can be exploited

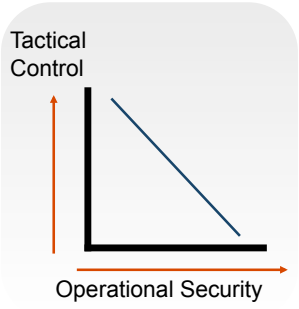
Tactical Control

- Cellular structures complicate C2
- Political and ideological leaders—the principals —must **delegate certain duties** to middlemen or low-level operatives, their agents.
- But because of the need to maintain operational secrecy, terrorist group leaders cannot perfectly monitor what their agents are doing.
- Thus, **preference divergence** creates operational challenges which can be exploited to degrade a terrorist group's capabilities.



Tactical Control

- Preference divergence over **controlled use of violence**
  - Terrorists cannot afford too alienate the center of gravity, or risk losing support
  - Must reign in overzealous members, prevent low-ranking members from initiating their own attacks against strategically high-value targets
  - Difficulties in resolving chains of command
- Preference divergence over who needs what kinds of **situational awareness**
- Preference divergence over what should be done to **maintain security**



*Increased potential for **fratricide ("own goals")***

Exacerbating tactical control challenges

Exacerbate **Tactical Control** challenges - Force leaders to consider punitive actions against agents/operatives

Make information management more difficult; **degrade the C2 network channels** with noise, static

Flood the network nodes with requests for info/requests for clarification of intent, strategy, etc.
Goal: overwhelm the decision-makers from within

Encourage *perceptions* of counterproductive plans or actions among low-level operatives; raise concerns among political ideological leaders about their lack of tactical control

Overall objective is making a network's members want to leave, disengage

Strategic authority

Within all networks, there are forces which influence how the nodes operate. For example:

if Mafia, certain family leaders/patrons . . .
if Jihadis, certain influential scholars . . .

Preference divergence over "**who's in charge**"

Internal dissension within the network's leadership is a challenge

Strategic disagreements within network lead some members to subvert the authority of senior commanders

Principals must combat perceptions of **strategic drift**, **disconnections between rhetoric and actions**

Exacerbating strategic authority challenges

Identify the most influential members within each network; who is trusted most? Whose word carries most weight, and why?

Identify and **exploit rivalries** within each network **and between networks**

- Disagreements already exist in these networks
- How to exacerbate them, make them more acrimonious?
- Encourage debate; force them to defend their ideas

Highlight personal agendas of those who are "in charge"

Influence and promote internal debates about strategic coherence, **leadership competency**, direction

Overall objective is making a network's members want to leave, disengage

Internal Debates

- Discussion forums and social media provide insights about internal debates rooted in religious doctrine and pragmatic necessity

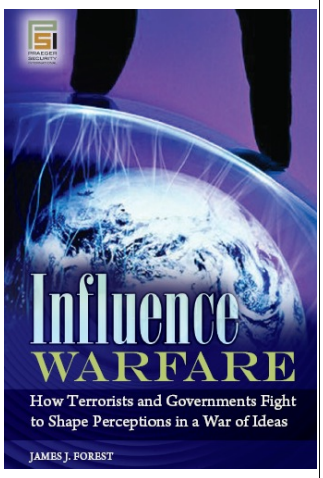
- Questions include:
  - Is it ever appropriate to overthrown an Islamic regime?
  - Is it ever acceptable to kill other Muslims?
  - What should be done about the Shia?
  - Should we focus on "near enemy" or "far enemy"?
  - What credibility does (fill in the blank) have to tell members of this movement what to do?

AQAM "Street Perception"

Influencing "street perception" (*via Info Operations*) of an organization is a powerful component of an overall counterterrorism strategy

AQAM tries to protect its image, to dominate the discourse and shape what people say and think about them

Much of al-Qaida's rhetoric seeks to deflect attention from their own faults, focus the spotlight on others to blame for problems in the Muslim world (*including the problems caused by salafi-jihadists*)



Inconvenient Truths

Perceptions of Importance to Al Qaida?

What kinds of things do al-Qaida's leaders **not** want people – *especially potential supporters* – to hear, think or believe?

If we could read their minds, hear their thoughts, what would we find them worrying about?

Inconvenient Truths

Theme 1: Righteous Confidence

"Our interpretation of Koranic passages used to support our violent ideology **might be wrong"**

"God may not want us to do what we are doing"

"We are afraid; We are less afraid of the Americans and their UAVs than the interrogators in Egypt, Jordan, Syria, Turkey, Israel, Saudi Arabia, etc."

"We are afraid of being honest; we know our faults and ideological contradictions make it harder to attract new recruit or financial support"

"Our "future vision" of an Islamic caliphate is really unlikely to work in the modern age of globalization, economically interdependent nation-states, etc."

Inconvenient Truths

Theme 2: Strategic Competence

"Our strategy of creating local, stable jihadist regimes is doomed. There are no historical examples of a fundamental, salafi-jihadist regime having stability or success."

"We argue among ourselves, often, over issues of strategy, tactics, and especially money"

"We do not understand Americans as much as we sometimes believe we do; perhaps the 9/11 attacks were a big mistake; The West, our enemies, are far more resilient and far less vulnerable than we want to admit"

"The strategy of locally focused terrorism has proved ineffective. Attacks in Muslim countries not only fails to mobilize the masses, it creates substantial coalitions seeking to suppress the jihadists."

Inconvenient Truths

Theme 3: Fighting a Just War, Justly

"We have killed 8 Muslims for every 1 non-Muslim infidel we have killed; **we don't really value Muslim life"**

"We are the only Muslim organization in the world that routinely kills hundreds of innocent children each year"

"We are the only Muslim organization in the world that routinely celebrates when others kill innocent children"

"Through our actions, we have generated and strengthened an anti-jihadist response from Muslim populations worldwide"

"Our enemies aren't really evil; in fact, the U.S. has been, mostly, a force for good in the world"

Inconvenient Truths

Theme 4: Money

"We are desperate for cash because none of us have jobs and bin Laden is broke; *we're not much different from the homeless pan-handlers you see on the streets each day . . ."*

"We need affiliate groups not only to conduct operations on our behalf, but also to send us money"

"A *primary objective* is to acquire money and political power"

"Without adequate long-term support, we will probably atrophy and self-destruct, just like almost all terrorist groups throughout history"

Inconvenient Truths

Theme 5: Integrity

"We don't believe that all Muslims are created equal; some deserve preferential treatment, even within our organization"

"We leaders of al-Qaida don't want or expect our family members to be martyrs"

"We think that many extreme Islamist groups are stupid and ineffectual, including Hamas and the Muslim Brotherhood"

"There is corruption and malfeasance within Al Qaida's rank and file; a lot of money has been stolen; members have engaged in all kinds of criminal activity"

Inconvenient Truths

Theme 6: Operational Capability

"Al Qaida's founders and the Arab mujahideen had very, very little to do with the Soviets leaving Afghanistan in 1989"

"We are armed amateurs – former engineers, doctors, taxi drivers, students – not true, disciplined 'holy warriors'"

"Most new recruits to al Qaida bring nothing of value: no military training, no specialized skills or knowledge, just a desire to do something"

"Gathering useful intelligence on our enemies is much harder than most people think it is, even with the Internet"

Inconvenient Truths

Theme 7: Relevance

"We fear the perceptions of inaction; without actions to back up our words, people will begin to suspect us of being either gutless or incompetent"

"Our biggest fear is being seen as irrelevant"

That's their biggest fear . . . One day Osama bin Laden will issue his 450th proclamation, and no one will really be listening. - - Brian Michael Jenkins [1]

[1] James Kitfield, "How I Learned Not To Fear The Bomb: The Rand Corp.'s Brian Michael Jenkins on facing the threat of nuclear terrorism." *The National Journal* (Saturday, Oct. 18, 2008). http://www.nationaljournal.com/njmagazine/id_20081018_2856.php

Terrorist Network vulnerabilities

Networked organizations have inherent vulnerabilities that can be exploited in order to weaken and destroy them

- Understanding a networked organization's **internal challenges and vulnerabilities** is important for developing effective strategies to combat the threats they pose and to degrade their capability to function
- Networked organizations **require trusted relationships** in order to support information and financial transactions
  - **Distrust** can be much easier to establish than trust
- **Preference divergence** creates challenges for networked organizations that can be exploited
- Increased reliance on technology for financial and information transactions can exacerbate a network's security vulnerabilities

Overall objective is making a network's members want to leave, disengage

Questions?