The Challenge of Insurgency

- **Insurgency is one of the oldest forms of warfare - ancient times to today, however …**

- **The culture of most modern Western militaries is still largely focused on preparation for conventional combat operations against the forces of another nation state, for example …**

- **The spending patterns of Western militaries are still overwhelmingly biased toward improving their conventional combat capabilities, however …**

- **There is strong evidence that the in the coming decade or more the armed forces of the Western nations will spend most of their time on "irregular warfare" missions, such as counter insurgency**
  - **Insurgencies last a long time - average is 13 years since 1945; COIN strategies must accommodate that**
  - **23 days of major combat operations in Iraq in 2003**
  - **1,600 (+) days of irregular warfare since then**

RAND

What Has Changed, and What is Still the Same

- **Today, many of the classical principles of COIN are still applicable, for example:**
  - **Insurgents and the government are competing for the loyalty of the people**
  - **Lethal force must be employed with considerable care**
  - **The role of security forces is to create a secure environment so other reforms can take place**
  - **If insurgents have sanctuary in a nearby country(s) the COIN challenge is significantly greater**

- **So, what has changed …**
  - **Information technology has given insurgents new ways to hide, propagandize, recruit, raise money, and coordinate their operations**
  - **The concept of "global insurgency" (i.e. the jihad) is not totally new (early Marxists wanted a global revolution), but today it has ethnic and religious overtones**

RAND

The Evolution of an Insurgency

Strength of the insurgency

Time

Proto-insurgency
Small scale insurgency
Large scale insurgency

Relationship of government security forces

Police intel. in the lead
Police intel. requires some military help
Military in the lead

Proto-Insurgency

- **The insurgency is weak and small**

- **Cadre of "true believers" is seeking to establish itself and bring others into the fold**

- **Possible competition among various radical groups**

- **While the insurgency is little threat to most governments at this stage, the small size of the group makes it hard to detect**

- **Government police and intelligence organizations have the leading role in this stage**

- **Little, if any, role for military forces at this point**

Small Scale Insurgency

- **Insurgents are beginning to make their presence felt**

- **More open propagandizing**

- **Some elements of the population are now on the side of the insurgents**

- **Small scale attacks, kidnappings, assassinations**

- **Possible foreign support**

- **Police and intelligence agencies remain in the lead for the government, but …**

- **The military may have to provide assistance in certain situations**
  - **Protection of key infrastructure**
  - **Supplementing police in high threat situations**

Large Scale Insurgency

- **Insurgents have gained considerable support in the population**

- **They may have seized control of considerable portions of the country**

- **Insurgents are now much more in the open**

- **The rebels now have a good chance of success**

- **The insurgents may have considerable "outside" support**

- **Role reversal between police and military in the government's security forces**
  - **Military now in the lead due to strength of insurgents**
  - **Police and intelligence still have very important roles**

The Dominance of Intelligence

- **In conventional combat, *operations* tends to drive *intelligence***

- **Whereas in a counter-insurgency, *intelligence* tends to drive *operations***

- **Insurgents rarely resemble conventional formations**
  - **They are generally clandestine groups operating in the shadow world**
  - **They commit acts of violence against the established government**
  - **Their operations more closely resemble those of criminal gangs**

- **Counter-insurgency operations therefore resemble law enforcement procedures more than military operations**
  - **In law enforcement, intelligence dominates**

Implications for Analysis

Financing Event: Includes the funding of insurgent attacks. The event can describe either funding-related activities taking place, or that a financier was involved.

Assembly Event: Includes the assembly of makeshift weapons. The event can describe assembly-related activities, a location at which assembly take place, or that a bomb maker was involved.
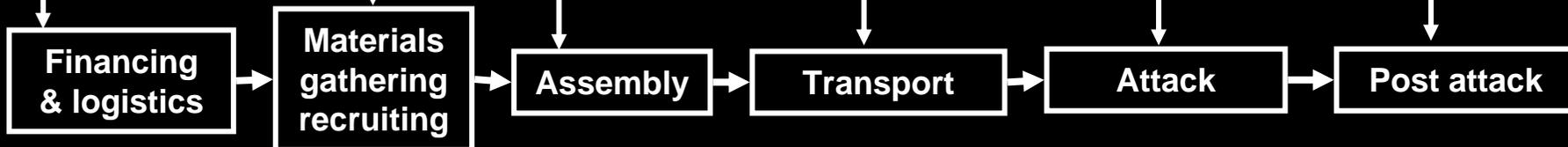
Attack Event: Includes selecting the target and conducting the attack.

Material Event: Includes finding completed weapons, or materiel involved in producing makeshift weapons. Materiel events are subdivided by the type of materiel found: ordnance, electronic components, chemicals, or a combination of the above.

Analysis in support of counter-insurgencies must focus on improving intelligence

Post attack event: Any event that is the result of the attack. I.e., casualties, damage, collateral damage, vehicle damage, etc.

Transport Event: Includes the transportation of weapons.

Financing & logistics → **Materials gathering recruiting** → **Assembly** → **Transport** → **Attack** → **Post attack**

Planning

Planning Event: Includes planning, meeting, command and control, monitoring, surveillance and / or information operations related to carrying out insurgent attacks. The event can describe either planning-related activities taking place, or that a "planner", "leader" or a "high value individual" was involved

Attack event chain

Some First Principles

- **Analysis must be focused on helping the local commander accomplish his mission**
  - **All our conclusions, findings, recommendations must pass the "so what" test**
  - **Academic niceties are an extravagance we cannot afford**

- **Analysts should involve commands in the in the development of new tools and methods**
  - **Local units know the enemy in their area**
  - **Laboratory-development is rarely accepted in the field**
  - **Early engagement facilitates acceptance and use**

- **Whatever we propose must be better than existing "Kentucky windage"**
  - **New methods must be compared to unit-devised techniques**
  - **In many cases, clever soldiers and marines have devised rather effective methods**
  - **Suggestions about how to alter operations are generally not welcome!**

- **Like the insurgency, analysts must realize that analysis is local**

- **Each new method or tool proposed must account for an adapting enemy**

RAND

The Tyranny of Data

- **Data is generally not collected to support analysis**

- **Incident reporting is uneven**

- **The existence of multiple databases is common**

- **There is a lack of a standard lexicon**

- **Friendly data is generally not captured**

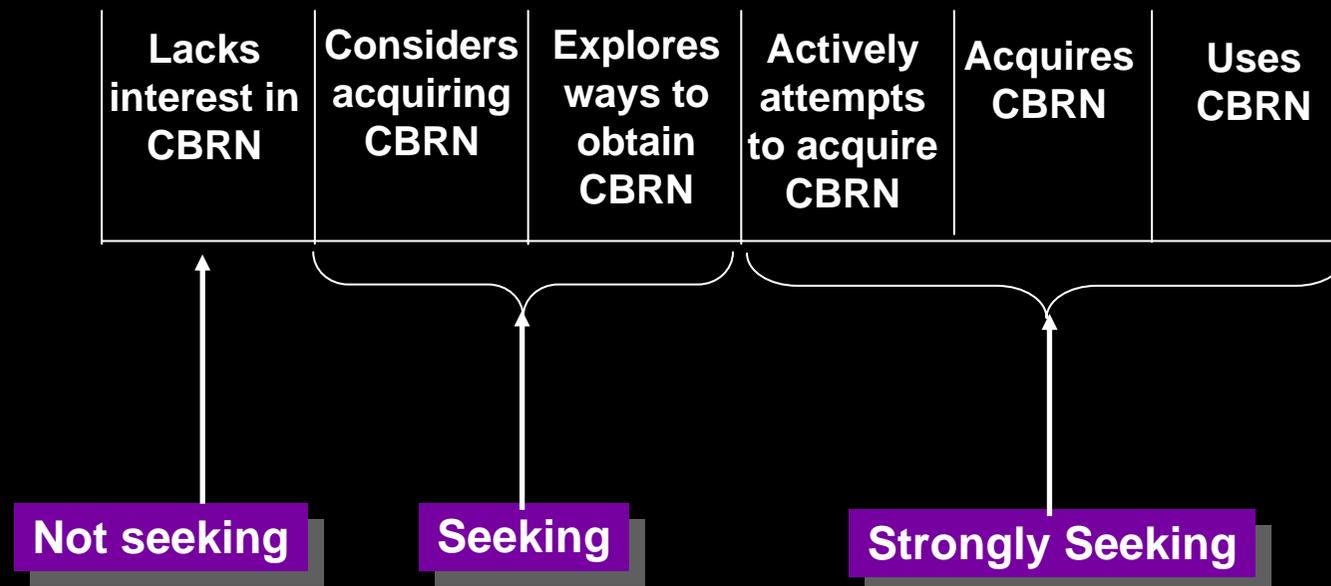- **Sharing intelligence data among U.S. agencies and allies is problematic**

Here are a Few Questions Our Analytic Techniques Might Answer

- **Discerning patterns**
  - **What should commanders look for to detect insurgent activity?**
  - **How do we distill the several factors to a parsimonious set of indicators?**

- **Predictive methods**
  - **Where (and when?) will the next insurgent attack occur?**
  - **How do we ensure that our method facilitate countering the enemy's response?**

- **Social network analysis**
  - **How can we uncover insurgent networks?**

- **Enemy-friendly interaction analyses**
  - **What patterns are friendly forces exhibiting that signal their intentions to the enemy?**
  - **How is the enemy is exploiting those patterns?**
  - **How can the patterns be changed to either preclude enemy detection or to preclude enemy exploitation if preventing detection is not possible?**

An Example: Discerning Patterns
How do we know a terrorist Group is on the Verge of Acquiring CBRN?

Terrorist groups are postulated to be in one of the following mutually exclusive states

Lacks interest in CBRN	Considers acquiring CBRN	Explores ways to obtain CBRN	Actively attempts to acquire CBRN	Acquires CBRN	Uses CBRN

Not seeking

Seeking

Strongly Seeking

An Example: Discerning Patterns

How do we know a terrorist Group is on the Verge of Acquiring CBRN?

- **Examine data to…**
  - **Identify relevant factors – those that best summarize differences in CBRN classes**
  - **Assess the level at which each observation of each group possesses these factors**

- **Develop a classification scheme that**
  - **"Assigns" input observations to CBRN classes**
  - **Minimizes misclassification cost**

- **Develop methodologies to deal with the assessment of new information**
  - **New observations**
  - **Updated data**

Representing Multivariate Data

- **The data set consists of *n observations* of existing terrorist groups**
  - **A single terrorist group may have several observations over time**
  - **A CBRN class is assigned to each observation**

- **An observation, $\mathbf{x}_i$ is a collection of *p factors* so**

$$\mathbf{x}_i = \left[x_{i,1}, x_{i,2}, \cdots, x_{i,p} \right]^T$$

- **The data set therefore is characterized by the matrix:**

$$\mathbf{X} = \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,p-1} & x_{1,p} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,p-1} & x_{2,p} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{n-1,1} & x_{n-1,2} & \cdots & x_{n-1,p-1} & x_{n-1,p} \\ x_{n,1} & x_{n,2} & \cdots & x_{n,p-1} & x_{n,p} \end{bmatrix}$$

Factors Influencing Terrorist Propensity to Acquire and Use CBRN Weapons

Endogenous

Exogenous

The *factors* are the attributes of the observations identified by subject matter experts

We measure the degree to which each group possesses these factors at each observation

- *Capabilities*
  - *Organizational Capacity*
  - *Technical Capacity*
  - *Alternatives*

- *Context*
  - *Opportunity*

- *Motivations*
  - *Leadership Mindset*
  - *Internal Restraint*
  - *Isolation*

- *Vulnerabilities*
  - *External Restraint*
  - *Defensive Aggression*

RAND

Developing the metric

- **Technical Capacity can be further sub-divided**
  - **Access to critical weapons** material
  - **Access to** equipment **for production and fashioning delivery**
  - **Possesses the require** Know-how **for production and delivery**
  - **Possesses the** skill **to act on critical knowledge**

- **The degree to which a group possesses the features at a given observation is determined by conjunctive/disjunctive sets of the sub-features such as Technical Capacity…**

*Is rated…   If the following sub-factors are present…*

High:	**(Skills and Know-how) and [Material or Equipment]**
Medium:	**(Skills and Know-how) or [Skills and (Equipment or Material)] or [Know-how and (Equipment or Material)]**
Low:	**Skills or Know-how or Material**
None:	**otherwise**

Ordinal ranking

Must be mutually exclusive and collectively exhaustive

Classifying the data set

- The existing data set is used to select the best classification algorithm and the optimal weight set, $w = \{w_1, w_2, \ldots, w_p\}$
- For a set of $n = 8$ observations and $p = 2$ features, we can plot the observations as follows:
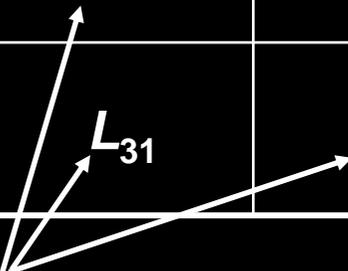
X_1

+

x

$X_j = [x_{j1}, x_{j2}]$

x

+

r

radius

o

o

x

+

X_2
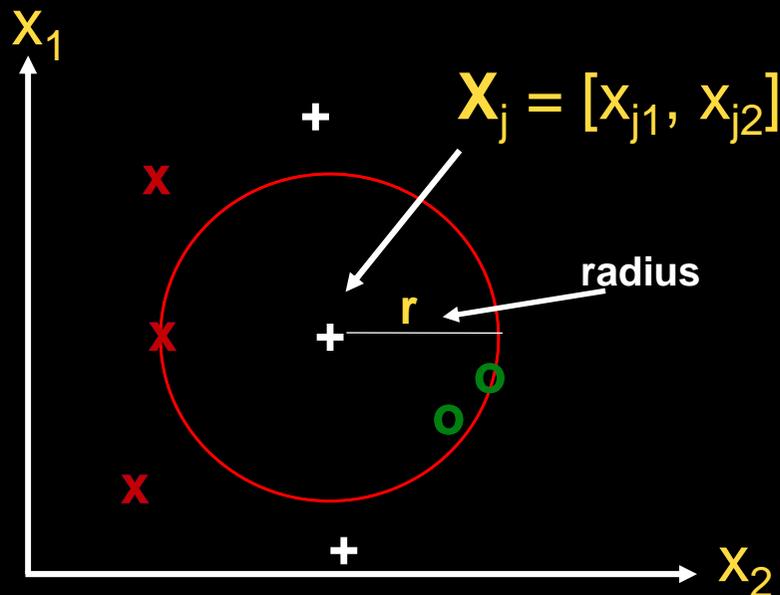
Actual Classes:
o Class A
+ Class B
x Class C

A *kernel* is used to develop a smoothed estimate of the class density at x_i. The bandwidth of the smoothing window is determined by the radius

$$d\left(\mathbf{x}_i, \mathbf{x}_j\right) = d_{i,j} = \left[\sum_{m=1}^{p} w_m \left|x_{i,m} - x_{j,m}\right|^{\gamma}\right]^{1/\gamma} \quad \gamma \geq 1, \quad w_m \geq 0,$$
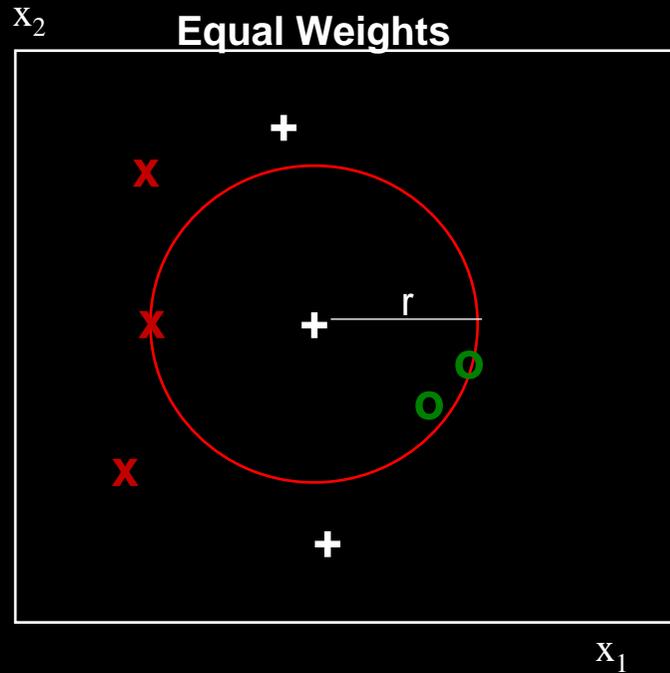
Class Membership and Supervised Classification

		Predicted		
		G_1	G_2	G_3
Actual	G_1	0	L_{12}	L_{13}
	G_2	L_{21}	0	L_{23}
	G_3	L_{31}	L_{32}	0

- **Loss values are inputs to the classifier**

Classification Example:
Demonstrates the Effect of Changing Weights

Equal Weights

x_2

x_1

Shrink x_2 weights

x_2

x_1

Stretch x_1 weights

x_2

x_1

o class A
+ class B
x class C

RAND
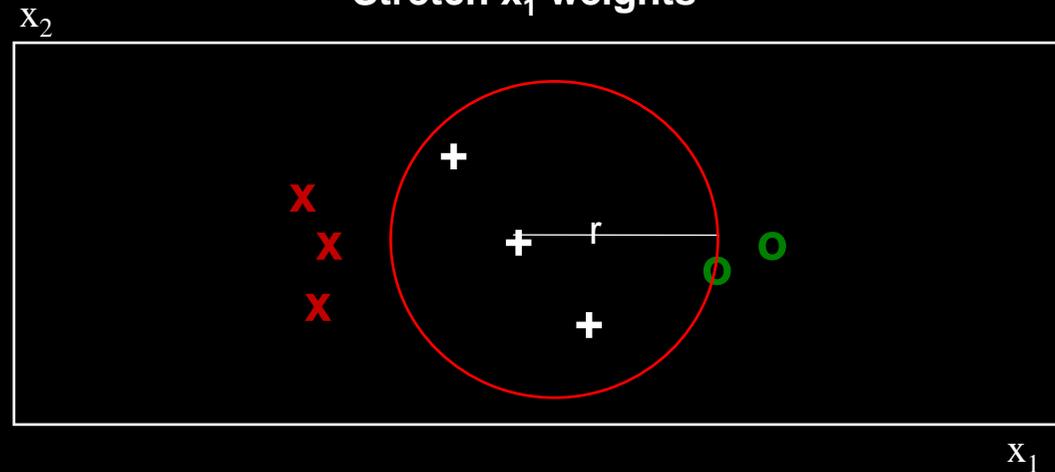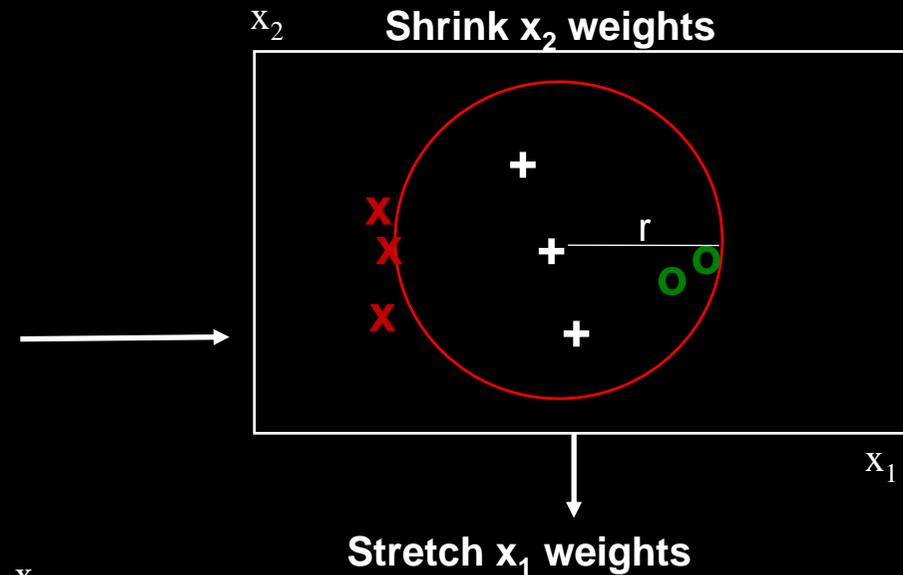
Results

- Number iterations…….. 3,500
- Radius……….………….. 0.2
- Kernel selected………. . $k(d)$ = normal
- Metric……………………… Minkowski ($\gamma = 2$)

Actual	Predicted		
	Not seeking	Seeking	Strongly
Not seeking	0.0	1.0	1.0
Seeking	1.5	0.0	1.0
Strongly	2.0	1.5	0.0

← Loss values

"Optimal" Weights

Technical Capacity …. 0.16

Organizational Capacity …. 0.00

Opportunity …. 0.27

Leadership Mindset …. 0.25

Isolation …. 0.00

Internal Restraint …. 0.00

External Restraint …. 0.21

Defensive Aggression …. 0.11

Available Alternatives …. 0.00

	Not seeking	Seeking	Strongly	Total
Not seeking	22	0	0	22
Seeking	1	7	1	9
Strongly	0	0	6	6
Total	23	7	7	37

The Counter-IED Analysis Team

- **Consists of**
  - **JIEDDO ORSA team**
  - **External partners**
  - **Senior Mentors**
  - **Deployed analysts and data collectors**

- **Members include**
  - **RAND**
  - **IDA**
  - **TRAC**
  - **JFCOM**
  - **CNA**
  - **APL**
  - **AMSAA**
  - **GMU**
  - **Corona**
  - **MITRE**

RAND

RAND Has Tackled Several Issues

- How can we better organize and operate to effectively counter IEDs?

- How do we measure success in the IED fight?

- What role does Information Operations play in counter-IED operations?

- How can the commands sustain intelligence directed action against IED emplacers?

- How do we associate the Iraqis with counter-IED operations?

- How can we assist commanders predict the emplacement location of future IEDs?

- Are the benefits accrued from the missions being conducted worth the IED costs incurred

- How can we learn the organization, and structure of IED cells?

- How can we better employ law enforcement techniques to find capture and detain members of IED networks?

- How can we better advise JIEDDO in selecting effective counter-IED equipment?

- What is the nature of the interaction between coalition force movements and insurgent counters using IEDs?