LOCKHEED MARTIN

Integrated Systems & Solutions

# Emergent Systems

## Applications to Terrorist Networks

Leslie Kain

*Lockheed Martin*
*Information Systems & Global Services (IS&GS)*
*Advanced Technology Office (ATO)*

# *"Man, not space, is the last frontier. We must explore him."*

Ralph Peters (LTC, USA Ret.), "Our New Old Enemies", From *Parameters*, Summer 1999, pp. 22-37

# Fourth-Generation Warfare (4GW) – *Ideologically driven transnational terrorists*

LOCKHEED MARTIN

*Integrated Systems & Solutions*

- Extremist, violent, fringe minority … Claim actions are holy and just
- Distinct from non-violent, conservative Islamist groups
- Loose-knit cells of *self-generating* action groups … ideological convictions
- *Capitalize on weak / failed states' inability to control actions / access*
- Target institutions, infrastructure, civilians … wherever there is vulnerability
- Operate asymmetrically … exploit gaps in capabilities of 3GW armies
- Lever technology … Information Technology (IT) … *media as "terrain"*
- 4GW battlefield … *nonlinear / dispersed … no fronts / boundaries*
- No distinction between war / peace or military / civilian
- 4GW warriors attack all institutions of government / society … *cultural attack*
- Psychological warfare … public opinion, *spread ideology,* obtain recruits

# Counter-Terrorism / Radicalism

- The turn to radicalism in religious, ethnic and cultural beliefs / ideologies is a phenomenon growing / spreading across the globe.
  - This radicalism is changing the nature of national & international conflicts.
  - Radicalism will drive global conflicts for at least the next generation
  - Much like the protracted "Cold War", it will shape our DoD investments and practice.
- Current C4ISR focuses on evidence of behavior, movement, events.
  - The beliefs and other factors driving such activities have already taken hold by the time we observe
- Current C4ISR detects occurrences – the "what". Counter-radicalism must focus on what drives the occurrences – the "**WHY**".
  - What propels the emergence and growth of radical networks?
  - How can we exploit those factors to predict and interdict?
  - How can we locate, identify, understand, and disrupt the spread of radical beliefs that result in irregular warfare, terrorism, genocide, and other threats to global security?

# Man, the Last Frontier

- A key characteristic of social interactions is their *continual change*
- ***Social Networks are a key example of Emergent Behavior***
- Social Networks are not random, but appear to grow based on "who you know" – *preferential attachment*
  - Scale-free; i.e. have the same properties regardless of its number of nodes;
  - Governed by power-law* distribution of degree (number of links per node)
    - Power-law is also key in complex emergent systems algorithms.
    - Hard to predict: the number of interactions between components of a system increases combinatorially with the number of components, thus potentially allowing for many new and subtle types of behaviour to emerge
  - High levels of interconnectedness (a small-world property)

* probability *P(k)* that a node in the network connects with *k* other nodes was roughly proportional to $k^{-\gamma}$

# Shortfall in understanding Networks

2006 Army Science Conference Panel on Network Science found:

- Networks are pervasive in all aspects of life: biological, physical and social. They are indispensable to the workings of the global economy and the defense of the United States.
- Fundamental knowledge needed to predict the properties of large infrastructure networks is primitive, notwithstanding the advanced technological state of global communications and transportation networks.
- There is no science today that offers the fundamental knowledge necessary to design large, complex networks in such a way that their behaviors can be predicted prior to building them.
- Research on networks is fragmented. Current funding policies and practices of federal agencies are focused on specific network applications rather than on accumulating fundamental knowledge about networks.

# *"It takes a Network to defeat a Network"*

Stan Sims, OUSD(I), in "*Joint Intelligence Operations Centers – After Next (JIOC-AN)", February 1, 2007*

# Findings / Recommendations

*Initiate a new field of investigation called Network Science would be appropriate to advance knowledge of complex systems and processes that exhibit network behaviors.*

- *Dynamics, spatial location, and information propagation in networks.* Better understanding of the relationship between the architecture of a network and its function is needed.
- *Modeling and analysis of very large networks.* Tools, abstractions, and approximations are needed that allow reasoning about large-scale networks, as well as techniques for modeling networks characterized by noisy and incomplete data.
- *Increase the level of rigor and mathematical structure.* The current state of the art in network science did not have an appropriately rigorous mathematical basis.
- *Abstract common concepts across fields.* The disparate disciplines need common concepts defined across network science.
- *Better experiments and measurements of network structure.* Current data sets on large-scale networks tend to be sparse, and tools for investigating their structure and function are limited.

# Emergence

*The arising of novel and coherent structures, patterns and properties during the process of self-organization in complex systems.**

*The common characteristics are:*

*(1) radical novelty (features not previously observed in systems);*

*(2) coherence or correlation (integrated wholes that maintain themselves over some period of time);*

*(3) A global or macro "level" (i.e. there is some property of "wholeness");*

*(4) it is the product of a dynamical process (it evolves); and*

*(5) it is "ostensive" - it can be perceived.*

*(6) top-down causation*

* Goldstein, Jeffrey (1999), "Emergence as a Construct: History and Issues", *Emergence: Complexity and Organization* 1: 49-72

# SNA → Social Network Exploitation (SNX)



## *Use Emergent Systems technologies to understand & Exploit Terrorist Networks*

- How do networks evolve? Can we tell something about the stage of a network (forming, mature, decaying) by its structure or behavior?
- What constitutes a healthy and effective network? What constitutes a network likely to fail in its objectives?
- How do we "baseline" a network's behavior? (To track changes, look for anomalies)
- How tied is "good" network structure to the goals of an organization? Can we deduce from the *structure* what the organization is up to?
- Are networks the same across cultures? What are the salient variants?
- How can we more automatically collect data about networks, especially the characteristics (as opposed to mere existence) of the nodes and links?
- How do human and infrastructure networks interact?
- Armed with this kind of information we should be able to more clearly analyze:
  - First, second, and third order effects of positive or negative interventions
  - Leverage points, and ways to use them

# 5GW ??

## Changes in national/global society:

- Globalization - an acceleration of the rate and degree of complexity of all forms of exchange
- Post-Westphalianization - the rise of International, Transnational, Subnational and Non-state Actor challengers to the sovereign primacy of the Nation-State; and finally,
- State-Failure or severe State dysfunction where the ability of a State to constrain and police anarchic, nihilistic and disconnective forces is overwhelmed by post-Westphalian challengers, economic collapse and natural disasters.

## Implications for next-gen warfare:

- Superempowerment: The range of effect for each individual soldier (or terrorist) will be vastly increased even as the economic costs are driven down by market forces and proliferation of dual-use technology to the civilian consumer.
- Fluidity: Globalization makes possible **virtual armies** that are network of networks that are both resilient and adaptable in a Darwinian sense.
- Multidimensional Battlespace: War occurs in the context of everything else - physical space, cyberspace, the logosphere, financial, legal and societal networks - shaping the battlespace itself to the disadvantage of actual and potential opponents will become crucial aspects of strategy and not merely moving more effectively within it.
- Autonomous Surrogates: Active regular military forces are seconded by a variety of substitutes to carry some aspect of the warfighting load - PMC's, NGO's, Paramilitary and Subnational networks, International Peacekeeping missions and increasingly, robotic agents.

# From Simulation to Recognition/Prediction

- ORNL's Xiaohui Cui & Thomas Potok:

  *"Particle Swarm Social Adaptive Model for Insurgency Warfare Simulation"*

- Applied PSO to human social model to *simulate* interaction behavior between insurgent agents, governed by rules:
  - Information Exchange
  - Strategic Searching
  - Dynamical Adaptive
  - Memory Update
- *How can we apply these algorithms to real-world data, to:*
  - Recognize / characterize human behaviors
  - Recognize / identify emergent groups/networks, emergent behavior *patterns / modes*
  - Predict new emerging groups/networks and behaviors
  - Understand influences and "tipping points" enabling/facilitating emergence
  - Determine how best to influence the influencers
  - Build "networks" (human and technological) to exploit/combat terrorist networks