Innovation and Learning in Terrorist Organizations: Towards Adaptive Capacity and Resiliency

Nancy K. Hayden
Sandia National Laboratories
nkhayde@sandia.gov
Center for International and Security Studies at Maryland
nhayden@umd.edu

August 16, 2013

We have become more adept at disrupting terrorist networks; nevertheless, our terrorist adversaries continue to learn and adapt, posing an enduring threat to the security of America and its allies and partners.
2010 United States Quadrennial Defense Review

Abstract

The concept of terrorist organizations as complex adaptive systems (CAS) has generated an abundance of models focused on understanding the inherent structural strengths and weaknesses of the organizations with the ultimate goal of disruption and defeat. However, in-depth theoretical analyses combining first-principles of CAS to understanding terrorist organizations as dynamical systems remain few. Specifically, while most experts acknowledge the key role that innovation and learning play in providing terrorist organizations with the capacity to adapt, there is a paucity of systematic treatment of the topic of what influences innovation and learning – and the difference between the two - in these covert organizations. This paper reviews the organizing principles, behavior characteristics, and mechanisms of learning and innovation in complex adaptive systems; discusses how other authors have applied these principles to understanding terrorist organizations; and introduces the constraints imposed by the need for secrecy in these covert organizations. In doing so, I provide a theoretically grounded framework that combines understanding of innovation and learning within covert organizations from a system dynamics perspective with first principles of complex adaptive systems to predict under what conditions innovation is likely to occur within terrorist organizations. Historical evidence of terrorist organizations and their activities over more than thirty years supports the qualitative predictions of the framework.

Introduction

This paper is motivated by the observation that, while the consideration of terrorist organizations as complex adaptive systems (CAS) has become routine within the security community, the evidence suggests that the majority of terrorist organizations and their operations show surprisingly little of the type of innovation that is often characteristic of CAS. Key principles of system dynamics are reviewed in the first section of this paper to generate criteria for applying the paradigm to terrorist organizations. In the second section, a generalized conceptual framework for innovation and learning within CAS are

presented. The third section brings these ideas together in a conceptual systems model for examining learning and innovation within terrorist organizations. The fourth section discusses empirical evidence in support of this model, next steps for further research, and broader implications for other types of covert organizations

1. The Basics

A system is an internally organized whole, where elements are so intimately connected that they operate as one in relation to external conditions and other systems (Meadows & Wright, 2008). A set of objects or a collection of people is not a system unless in regular interactions resulting in system behavior as a whole. An important criterion for applying the CAS paradigm to terrorist organizations, therefore, is that entities within the terrorist organization must be in *regular interactions* that lead to *system behavior* as a whole. While this may seem obvious, many instances of terrorist activities do not meet this fundamental criterion. Some terrorist attacks are actions of "lone wolfs" such as the 2011 car bombing attack of Anders Breivik in Norway. Many others have no known organizational association. According to the Global Terrorism Database at the University of Maryland, approximately 7,600 of 98,000 terrorist events since 1970 are in the latter category(*Global Terrorism Database*, 2012).

Additional criteria for applying the CAS paradigm to terrorist organizations derive from system properties. Systems can be *linear* or *non-linear*, *open* or *closed*, and *simple* or *complex* depending on the nature of the interactions between actors within the organization and between actors external to the organization (Bertalanffy, 1980; Laszlo, 2001; Legasto, Forrester, & Lyneis, 1980). Within terrorist organizations, these properties may change significantly over time, which in turn significantly impacts rates of learning and innovation. Behavioral models of terrorist organizations need to explicitly account for these state properties and how they change in response to the environment.

A linear system is one in which one or more perturbations to parts of the system evoke a response of the system as a whole that is linearly proportional to the stimuli. Cause and effect are easy to observe, as big changes result in big and proportionate responses. In non-linear systems proportionality and summation no longer hold: small changes in initial conditions or interventions can result in massive changes to the system, and vice versa. Nonlinearity makes the relationship between causes and effects difficult to observe, which can be a problem when trying to validate models of innovation in complex adaptive systems, especially those which may be relatively closed, such as some covert terrorist organizations.

A closed system is one that is fully self-contained, and does not interact with its environment. Many systems studied in physics are closed systems. The law of maximum entropy obtained in these systems dictates that they will always be moving in time towards increasing disorder, absent any outside forces. In contrast, open systems support ongoing exchanges of materials and information with the environment. This allows for negative entropy to be maximized; that is, for order to develop without external intervention, as CAS self-organize to find optimal positions in fitness landscapes (Kauffman, 1993) All else being equal then, both open and closed systems can have

mechanisms that act in opposite directions to impact learning and innovation, depending on the structures that develop and whether they impede or amplify the inflow and transmission of information and resources.

Open systems can interact with unorganized elements of the environment or with other systems. When interacting with other systems, one has a system of systems (SoS). Emergent properties will obtain from a SoS different than those of the constituent systems themselves.

Complexity

There are many different reference frames for conceptually differentiating simple systems from complex, drawing on analogies from thermodynamics, information theory, structural mechanics, and graph theory. Crutchfield has demonstrated that deterministic conceptions -- such as temperature, information density, and entropy -- are in reality different measurements of the underlying order, or randomness, in the system(Crutchfield, 2003). This is illustrated graphically in Figure 1.

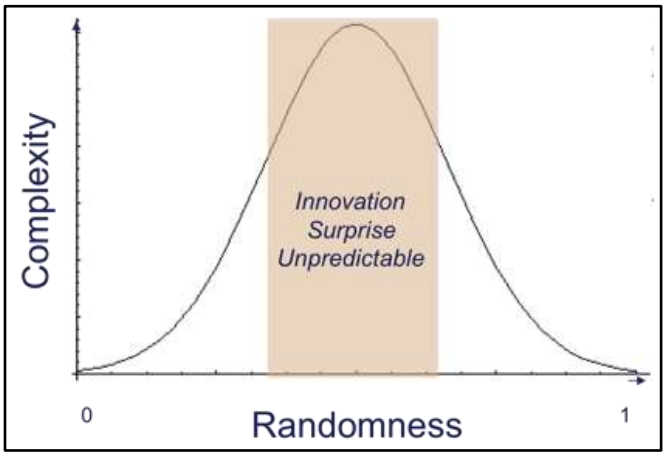

Figure 1 System complexity is a function of both structural organization of interactions between entities in a system and the randomness of the individual entities. The concept of complexity can be likened to the statistical concept of entropy.

At one end of the spectrum in Figure 1, simple periodic processes with high order and low randomness have negative entropy and low structural complexity. At the other end, there is no order to cause and effect and all outcomes are equally likely in the short term. This is the regime of chaos. Complex systems arise between these extremes and are an amalgam of predictable and stochastic mechanisms.

Bar-Yam describes the transition from simple to complex, and from complex to chaotic, with a quadratic equation to describe any system as a collection of interacting agents (Bar-Yam, 1997).

$$f(s) = as\,(1-s), \qquad \text{Eq. 1}$$

where s is an infinite sequence of binary variables, and 0<a<4. In simple systems, 0<a<1 and all agents interact in the same and predictable manner. In complex systems, 1<a< 3, where multiple agents interactions change dynamically in fluctuating and combinatorial ways that follow simple rules (e.g., maximize utility, maintain likeness to neighbors). There is a bifurcation point between 3 and 4 where all order breaks down, however, and a chaotic system ensues. Rogers et al. al argue that the likelihood of innovation increases as one approaches this bifurcation point in a system, but decreases beyond it(Rogers, Medina, Rivera, & Wiley).

Both conceptions of complexity depend on the structure and dynamics of the interactions (information and/or material flow) between the fundamental units, or agents, in the system. Using classical systems theory, one can describe the effects of these interactions on system properties as a series of different equations. Let Q_i (i=1, …,n) be the measure of some property of n elements in a finite system. Then the change in Q_i over time is given by solving the simultaneous set of equations:

$$\frac{dQ_1}{dt} = f_1 (a_{11}Q_1, a_{12}Q_2, a_{13}Q_3, \ldots .a_{1n}Q_n)$$

$$\frac{dQ_2}{dt} = f_2 (a_{21}Q_1, a_{22}Q_2, a_{23}Q_3, \ldots .a_{2n}Q_n) \quad \text{Eq. 2}$$

Eq 2.

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\frac{dQ_n}{dt} = f_n (a_{n1}Q_1, a_{n2}Q_2, a_{n3}Q_3, \ldots .a_{nn}Q_n)$$

System complexity is introduced by allowing self-organizing interaction between the elements. This results in a variety of models of cooperation or competition. In one such model, the predator-prey, the system is capable of reaching a quasi-equilibrium state that is regulated by the interaction between the two elements in mutual dependency. However, in other models of competition no such regulation occurs and the system may become unstable.

Evolution and Adaptation, Innovation and Learning in Complex Systems

Adaptation, evolution, learning and innovation are key features of complex adaptive systems(Bar-Yam, 1997; Bonabeau, Dorigo, & Theraulaz, 1999; Holland, 1995; Jantsch, 1980) that can be conceptualized as the response to feedback from, and interactions with, the environment (Crutchfield, 2003; Sterman, 2000). These behaviors are self-organizing mechanisms by which a system responds to disequilibrium states resulting from initial conditions, from internal drivers (such as competitive goal-seeking) that change resource utilization distributions and impact production/dissolution rates, and from external forces or shocks.

Evolution is the process of natural selection of "accidents", such as mutants, based on their ability to improve the overall fitness of the system relative to its goal (Jantsch, 1980). Evolution occurs over long periods of time through successive generations, as those with the mutation are more successful in surviving and repopulating themselves than those without. Co-evolution may occur, in which the existence of one element (such as a species) is tightly bound up with the existence of another. In the context of Eq 2, evolution is modeled as a gradual change in f_i (i=1,n) over successive generations, due to higher regeneration rates of the mutant Q_i.

Adaptation through learning and innovative occurs on a much different time-scale than evolution. Both involve information exchange with the environment and with elements within the system. Learning is the process of modifying existing knowledge, behaviors, skills, values, or preferences. Learning involves synthesis of different types of information. Imitation occurs by mimicking the activities of others due to observed cause and effects of their actions; whereas repetition generates learning through feedback on one's own actions. Learning can occur at the individual element level or at the system level. In the context of Eq 2, learning by element Q_i results in a change in its *potential* contribution to all other elements of the system and to the system performance as a whole. Whether or not this occurs depends on the interaction functions f_i (i=1…n), and reaction coefficients a_{ij} of element Q_i with the rest of the system. System level learning occurs when a previously unused element Q_i is adopted for use within the system for the same purpose observed in other systems. In the context of Eq 2, this is likened to changing a reaction coefficient a_{ij} from a zero to nonzero value for Q_i, keeping the functional form of the use of Q_i the same as in the observed system.

Bonabeau et al (1999) explain learning as emergent collective intelligence within groups of simple agents among which decision rules based on autonomy and distributed functioning replace control, preprogramming and centralization. Through computational experiments, they showed that such systems perform sub-optimally on regular structures but perform well on complex structures.

Innovation involves the incorporation of a previously unused element into the system, or the recombination of existing elements in new ways (Holland, 1995). Specialized elements are recombined and utilized differently, as reflected in changes to both the functional forms of Eq 2 and the reaction coefficients. As will be discussed in a later section, CAS are postulated to provide optimal conditions for innovation to emerge when channels for information exchange exist with diverse external communities, and the opportunities to exploit new information are not constrained by the internal structure of the system. Even so, the process of emergence of an innovation is not yet well understood.

At a societal level, terrorism may be viewed as emergent phenomena presenting a solution to an otherwise intractable problem to certain subsystems that perceive themselves as disadvantaged and otherwise disempowered within a greater system (Hayden, 2006). As self-organized subsystems, organizations employing terrorist operations seek to create disequilibrium and change the basic functions and distributions of resources within the system to advantage themselves and others. The fact that terrorist organizations have tended to be conservative in their operations, and have not exhibited a propensity to use weapons of mass destruction, in spite of rhetoric threatening to do so, presents a puzzle to the communities of terrorism research scholars and to the national security community alike: when do terrorist organizations use learning and innovation to achieve their goals, and why do we not see more of it? This paper uses system dynamics to explore this question.

Networks, Evolution and Adaptation, Innovation and Learning

A key hypothesis is that network structures that evolve from system dynamics influence and constrain the processes of evolution, adaptation, innovation and learning in terrorist organizations through information exchange mechanisms.

Random networks in which there is equal probability, p, of a connection between any two nodes, result in short average and overall path lengths, providing robust and efficient means of information exchange. However, random graphs evolve slowly, and it is difficult for outliers (where many innovations occur) to have much of an impact on the rest of the network. Even so, there is a critical threshold value of p, related to the number of nodes, n, in the network beyond which a cascade effect will generate a single large, or even "giant" component (Figure 2). In this case, innovations developed by outliers rapidly spread through the network. Research into collaboration networks validates the existence of random networks with giant components among diverse communities of social actors, such as scientists, movie actors, and board directors(Newman, Watts, & Strogatz, 2002). Empirical data suggests the existence of giant components in several "dark" networks, e.g., Islamic jihadists, drug rings, and criminal organizations(Xu & Chen, 2008).

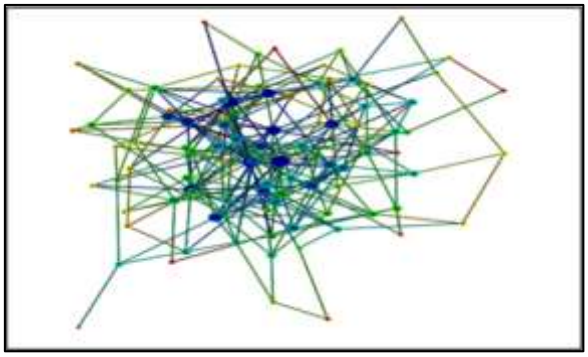

Figure 2 Enros-Renyi Random Network

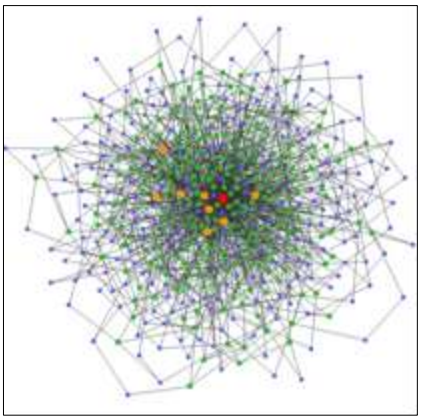

Figure 3 Scale-Free Network

Scale-free networks (Figure 3) are those in which the distribution of connections within the network follows the power law:

$$P(k) = ck^{-\gamma}, \qquad \text{Eq 3.}$$

where P(k) is the fraction of nodes in the network having k connections to other nodes, c is a normalization constant, and γ is a parameter with values typically between 2 and 3. Preferential attachment and evolutionary processes are mechanisms that can generate scale-free networks. Computer simulations have shown that scale-free networks are able to evolve to perform new functions more rapidly than random graphs with equal probability of connections. Scale-free networks are resilient to accidental, random failures. However, they are more vulnerable to directed attacks than random networks. Theoretically, learning and innovation in scale-free networks should exhibit behavior patterns indicative of diffusion and natural evolution mechanisms. While scale-free networks are one of the most ubiquitous in natural, social, and technological systems, they are not prevalent among terrorist organizations.

Small world networks (Figure 4) are characterized by higher clustering coefficients than random graphs while maintaining the same median shortest path length for the overall network.

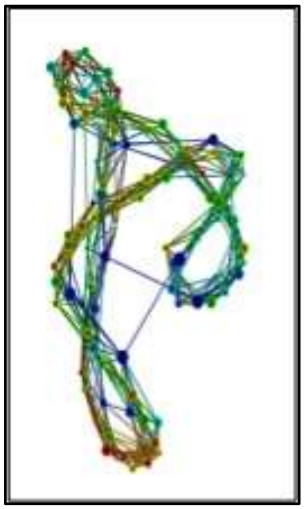

Figure 4 Small World Network

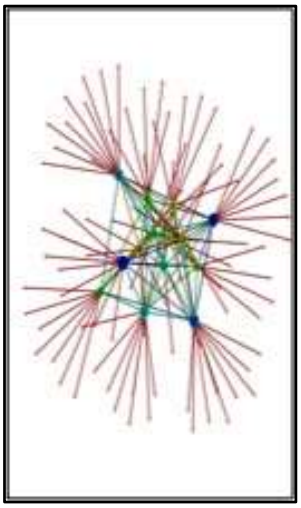

Figure 5 Core Periphery Network

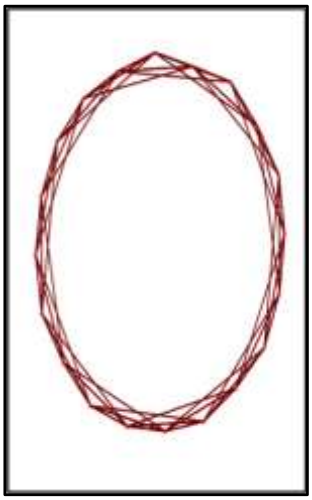

Figure 6 Ring Network

The clustering coefficient measures the degree to which all nodes within a neighborhood are connected to all other nodes in that neighborhood (where a neighborhood of a node j, is comprised of its immediately connected neighbors). The four "weak links" connecting neighborhoods in Figure 4 are critical to maintaining a short average path length. Like scale-free networks, small world networks are ubiquitous in self-organizing natural systems. As one might intuitively expect, learning and innovation in small world occurs in spurts, through a type of punctuated equilibrium process that is highly vulnerable to

the existence of the weak links(Filk & Muller; Gould & Eldrige, 1977). Less obvious is the mechanism for formation and reconstitution of these weak links. Many of the Islamic terrorist organizations today exhibit small-world network properties.

As with scale-free and small-world networks, the core-periphery network exhibits a high degree of clustering. However, as shown in Figure 5, the clustering is confined to a densely connected core surrounded by sparsely connected peripheral nodes. Core-periphery networks evolve as elements on the periphery join the core to exploit economies of scale, or as cores expand into outlying neighborhoods for resource exploitation. Political examples are band wagoning and colonization, respectively. Social examples are found in friendship networks, voting networks, transportation networks(Rombach, Porter, Fowler, & Mucha, 2012). Information diffusion and virus propagation on many on-line networks exhibit core-periphery structures(Gomez-Rodriguez, Leskovec, & Krause, 2010). Terrorist organizations that enjoy state sponsorship, such as Hezbollah, are more likely to evolve into core-periphery networks.

Recent studies on the spread of complex contagions suggest that core-periphery structures can have much higher transmission rates than small worlds. A complex contagion is one requiring multiple exposures for the contagion to spread(Damon & Macy, 2007). High-risk contagions – such as the purchase of an expensive piece of equipment, the participation in a risky political action, or the adoption of an unproven technology – require multiple "social proofs". In small world networks, the linkages between community structures are long (which increases effective transmission rates) but "thin". The thinness of these linkages slows the spread of risky contagion. In contrast, the multiple short paths between nodes in overlapping community structures build many "wide" bridges in the core-periphery network, creating high effective transmission rates(Reid & Hurley, 2011). This has significant implications for state-sponsored terrorist organizations, which enjoy both the resources and the network structure to support innovation against adversaries.

Ring networks (Figure 6) are simple structures in which each node connects to exactly two other nodes, forming a single continuous pathway for transmission events through each node. Obviously, these networks are highly vulnerable to the removal of any one of the links. Typically, this vulnerability is managed through redundancies - by sending simultaneous, duplicative transmissions in opposite directions and by utilizing secondary, overlapping and counter-rotating rings. The idea is that not all transmissions will get through all rings, but that the probability of complete system failure is low, as every node has the information necessary to be transmitted and it does not require a central node to manage the system. For networks of small numbers, ring networks have been shown to provide optimal configuration to protect secrecy while maintaining operational efficiency, if not robustness, but do not facilitate learning and innovation(Lindelauf, Borm, & Hamers, 2009). This finding has implications for small covert terrorist cells, where n may be less than ten, or terrorist organizations in start-up stages, and is consistent with the large numbers of short lived terrorist organizations.

For networks of more moderate size between 20 and 40, the “windmill” and “reinforced wheel” networks shown in Figure 7 have been shown to be most efficient for the achieving the dual objectives of secrecy and efficiency(Lindelauf et al., 2009). The network topologies in Figure 7 are variations on the familiar hub-and-spoke pattern of many distribution systems. These structures were generated in computer experiments to optimize network structures for dual objectives of secrecy and information efficiency in covert networks discussed in the following section. Hub-and-spoke networks evolve naturally to optimize

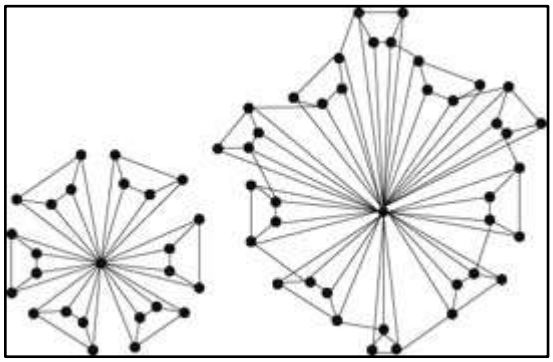

Figure 7 Windmill and Reinforced Wheel Networks

self-organizing distribution systems. Complicated operations that are identically required by every node can be carried out at the hub. Drawbacks include the longer path lengths required for distribution to every node, and the inflexibility of the hub to adapt quickly to changing environmental conditions, constituting a single point of failure for the system. In spite of these drawbacks, the hub-and-spoke paradigm remains ubiquitous in systems that can realize high improvements in efficiencies with centralization of operations.

2. A Framework for Innovation and Learning in Systems

The study of innovation diffusion within CAS is a burgeoning academic field with applications in diverse fields, integrating the pioneering work of Everett Rogers(Rogers et al.) with developing understanding of CAS. While it is beyond the scope of this paper to review this literature, the Cynefin framework proposed by Kurtz and Snowden for innovation management at IBM is particularly relevant (Kurtz & Snowden, 2003). This framework provides an operative context for making sense of a situation and the possibility of innovation based on the system state. Namely, one must first establish whether or not the system is in a state of order, complexity, or disorder before one can study or affect innovation processes within it(Snowden & Boone, 2007). This is relevant to organizations concerned with discovering when, why, and how terrorist organizations learn and innovate.

Each domain in the framework represents a different system state of order, resulting in different behavior patterns and requiring different actions to understand and manage the processes occurring within them. The simple and complicated domains both exhibit order where cause-effect relationships can be known. This ability to perceive cause and effect is an essential feedback mechanism for learning the “right” answers to problems or

discovering optimal solutions through adaptive goal seeking, presuming that those solutions are known to exist. Complex and chaotic domains present no opportunity for such deterministic resolution of cause and effect, and paths forward emerge holistically following innovative leaders.

Systems theory teaches that, all else being equal, closed systems will move towards increasing disorder, absent intervention. In contrast, open systems will move towards increasing order. Thus, one should expect that within a system of systems (SoS) there might be dynamic movement between these subsystem domains, even while maintaining equilibrium at the system level. Indeed, studies of many organizational, social, biological, and physical systems bear this out. The behavior patterns of these movements between domains, in turn, are domain dependent, as postulated by the Cynefin framework.

Kurtz and Snowden postulate that different characteristic network structures will be associated with each of the domains. Simple domain networks provide the most efficient structures for learning, through the process of sensing the environmental state, categorizing the information received according to previous knowledge, and responding accordingly. However, these responses will obviously not be sensitive to changing environmental conditions. In the complicated domain, the network structures are highly connected with a central hub, as in random graphs with giant components. Here, cause and effect is separated in time, and discoverable along some finite possibility paths with some analysis. Hierarchical networks and learning through incremental improvements is characteristic of information transmission between ordered states. The most likely adaptation mechanism in this case should logically be natural evolution or systematic trial-and-error, and innovation is unlikely. This is the path followed by organizations that are low-risk either by structural design or culture, such as the Irish Republican Army (IRA).

In both complex and chaotic domains cause and effect are not knowable a priori and underlying structure constrains the available system response within some bounded set of possible outcomes. It is necessary to probe the system to discover how the structure is likely to respond. In chaotic systems, observed responses can be the result of many different initiators. In this domain, sense-making requires that one takes action, senses the response and adjusts accordingly in a continuous, iterative pattern of actions and reactions.

In contrast, adaptive learning and/or innovation transfer is highly likely to occur within and between systems in the complicated domain and the complex domain. Innovation will most likely emerge within the complex subsystem. The complicated system sense explores the complex domain for new and novel ideas. Since cause and effect can be determined with in the complex domain, these ideas can be analyzed for their potential effect within the complicated domain before adoption. This is the process followed by organizations that provide an internal entrepreneurial unit with self-organizing freedoms (e.g., complexity) to foster discovery. Discoveries in the complex domain are monitored,

and analyzed for potential improvements to overall performance of the complicated domain.

Hub-and-spoke structures can be ideal for SoS that strive to maintain order and reduce exposure to risk while allowing for creativity and discovery. If the complex subsystem fails to perform, the overall system does not suffer, but innovations made within the complex can be quickly distributed to all other spokes if they prove to be advantageous. For terrorist organizations such as Al Qaeda, the existence of safe havens facilitates this kind of innovation and learning.

Using the principles of the previous discussions on network structures and general systems theory, innovations should be most likely to emerge from small world networks characteristic of the complex domain. The individual clusters in a small world network undergo continual learning and increasing specialization. At some point, randomly generated long connections between previously unconnected clusters will lead to discoveries of these differentiated skills and whole clusters can experience a step-change in functionality by whole-sale adoption of the discovery. When enough of these connections happen with complementary discoveries, non-linear, holistic systematic change may occur in "epochal" leaps, yet remain as small worlds. Such organizations are highly conducive to constant innovation, taking advantage of the diversity of the skills and resources of the constitutive clusters. The Liberation Tigers of Tamil Eelam (LTTE), which is exhibit this innovative behavior innovative terrorist

Alternatively, if the structure of the complex system is scale-free, there will be preferential attachments to new ideas generated by particular nodes, resulting in swarming behaviors, with the swarm following new initiatives of a small number of nodes. These initiatives may or may not be the most optimal solutions for the system. Eventually such systems may become increasingly ordered and act more like hierarchical systems. The widespread adoption of tactics first used by Hezbollah is an example of this type of behavior, and indicates the interconnection between terrorist organizations themselves as a SoS.

Chaotic systems are breeding grounds for innovation but require some degree of order to effect optimal benefit within the system. This can be affected by self-organized convergence resulting in a state of complexity, as shown in Figure 11, or through the imposition of order to a state of simplicity. The emergence of improvised explosive devises (IEDs) in Iraq, and subsequent regularization of their production, use, and continual improvements is an example of this type of innovation pattern of convergence from a chaotic to complex to complicated state.

Once an innovation has occurred, the five-step process of diffusion within the system has been well characterized. Each of these steps involves interaction and information exchange with the external environment. First, an agent acquires knowledge of an innovation. This is followed by a period of actively seeking more information. In the subsequent decision stage, an agent accepts or rejects based on the relative advantage, compatibility, ease of use, possibility for experimentation, and visibility of the

innovation. These are all behaviors that are well represented within the framework of self-organizing, goal-seeking CAS.

3. An integrative CAS Framework for Innovation and Learning within Terrorist Organizations

In this section, concepts from general systems theory and purposive CAS are informed by empirical studies of learning and innovation in terrorist organizations to develop an integrated framework for exploring the complex dynamics within different organizations in different contexts. This framework provides insights into who might innovate in the future, under what conditions, and optimal intervention mechanisms.

Previous authors have introduced fundamental principles of CAS – such as emergence, adaptation, and tipping points - as they apply to terrorist organizations (Ahmed, Elgazzar, & Hegazi, 2005; Hayden, 2006; Lichtblau, Haugh, Larsen, & Mayfield, 2006; Marion & Uhl-Bien, 2003; Subrahmanian, Mannes, Sliva, Shakarian, & Dickerson, 2013). Citing (Fonseca, 2002), Marion & Uhl-Biem (2003) point out that complexity theory is primarily about the dynamics of networks and how self-reinforcing, interdependent interaction creates evolution fitness, innovation, and emergent group knowledge. They derive a model of leadership in complex systems whereby leaders are created by the system through a process of aggregation and emergence that fosters interconnectivity and dynamic systems behavior, and argue that this model helps to explain the success of the Al- Qaeda organization.

Starting from the assumption that terrorists are complex adaptive systems, Ahmed et al (2005) apply conceptual learning models from evolutionary game theory and percolation theory in complex adaptive systems to the problem of propagation of terrorist acts among a sympathetic populace to argue that terrorism can at best be contained, but never eradicated. Hayden (2006) conceptually frames terrorism as an emergent phenomenon of a larger system plagued by "wicked" problems in which dynamic responses to interventions create new problems to be addressed, and in which system state, structure, and behavior co-evolve. Lichtblau et al (2006) explore the question of whether organizations or groups that pose asymmetric threats to the US, such as terrorists, are, indeed complex adaptive systems and therefore amenable to analysis for defense purposes through the paradigm of complexity science. They conclude that the analytic paradigm may be useful for strategic purposes to understand the dynamics and underlying law-like rules of systems behaviors governing the threats, but provides little for attaining tactical advantages within constrained timeframes for the operations research community. Subrahmanian et al (2013) use agent-based computational simulations of the Lashkar-e-Taiba group to explore the shifting nature of the group over time from a strict hierarchy controlled by Pakistan to a loosely organized international network, and the effect of those changes on the group's tactics and campaigns over a twenty-year period.

These studies notwithstanding, terrorism experts generally agree that for the most part, terrorist organizations of the past fifty years display surprising lack of creativity, and that most tactical and technological advances are incremental in nature(Clarke, 2004; Dolnik,

2009; *High-Tech Terrorism*, 1988; Horgan & Braddock, 2012; Martin, 2003). Terrorist operations are most often characterized by conservatism, advancing existing technologies to improve the use of conventional methods. Key variables that influence the choice of methods and tactics are ideology and strategy, leadership style, group dynamics (within internal organizational structures and external interactions with other groups), targeting logic, and resources(Rasmussen & Hafez, 2010).

These variables combine and interact in complex ways to shape the behavior patterns that emerge in achieving the group's goals as shown in Figure 8. The key variables interact with each other as shown, and are each at the center of feedback loops that result from those interactions. This model draws on three different "levels" of learning: Level 1 corresponds to natural evolution (e.g., incremental improvements), Level 2 corresponds to adaptation, and Level 3 corresponds to innovation. The likelihood of the learning level can be estimated by considerations of CAS structure and system state.

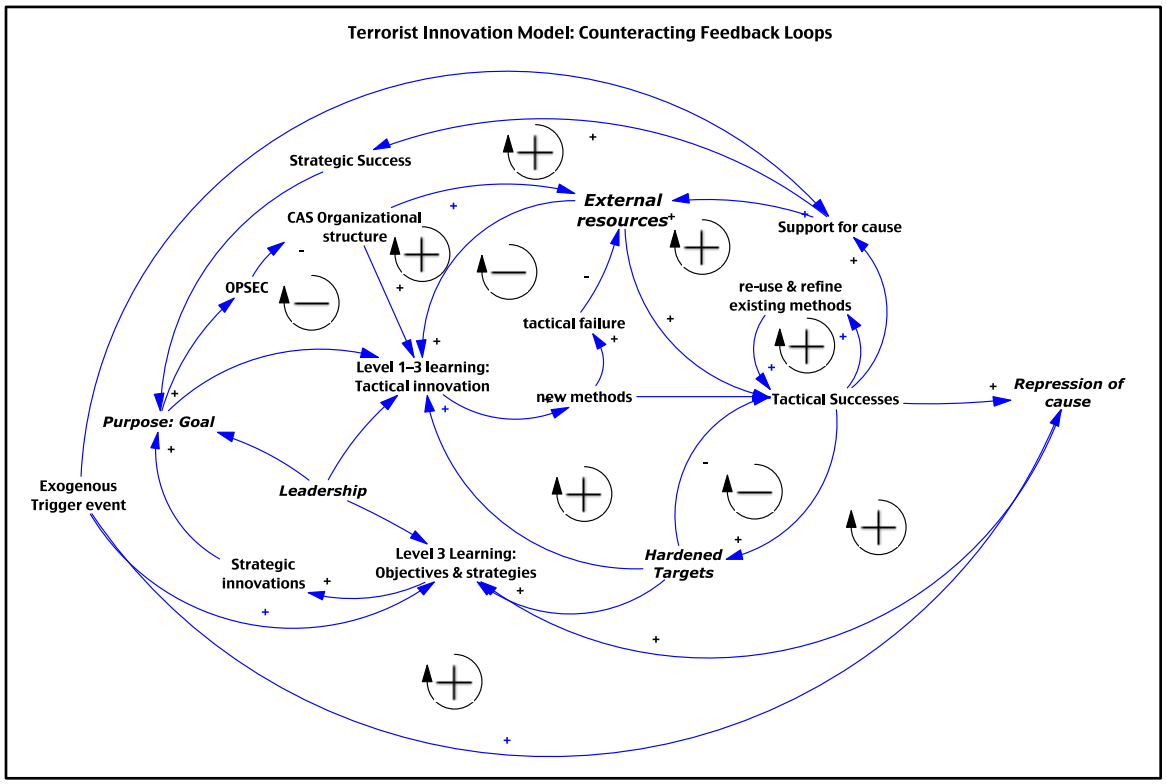

Figure 8 General Innovation and Learning Model within Terrorist Organizations in which successes have both positive and negative reinforcing feedback loops on continued use of existing methods and need for innovation

Strategic Purpose: The strategic purpose (ideology) is in a positive, reinforcing feedback loop with the tactics of the operations by way of the impact of successful operations that foster support for the cause. If these operations fail, support does not increase, but neither does it decrease. Purpose receives initial input from leadership, but may change over time.

Four primary purposes are generally agreed to among terrorist experts. Strategic organizational goals are:

1. Provocation of external actors (especially democratic regimes subject to public opinion) to overreact. Examples are the Al Qaeda bombing of the World Trade Center, the ETA campaigns in Spain, and the National Liberation Front (FLN) in Algeria.
2. Polarization (in divided societies) to entice attacks against "the other", thereby reducing support for moderate policies. Examples are the LTTE attacks that incited Sinhalese in Sri Lanka, the IRA attacks that divided Catholics and Protestants in Northern Ireland, and attacks in Western Europe to divide Muslim and non-Muslim communities.
3. Mobilization and competition to recruit supporters and develop constituencies. Examples are the attacks by Palestinian terrorists on Israeli athletes at the 1972 Munich Olympics; and competition between Hamas, Palestinian Islamic Jihad, and the Al Aqsa Martyrs Brigade.
4. Compellence, whereby a government's commitment to a policy extracts such a high price in the public high that it will be abandoned. Examples are the 1980 bombings in France intended to erode support for the Iran-Iraq war, the Chechens in Russia, and post-2003 insurgent attacks in Iraq.

Leadership: conceives, articulates and transmits the initiating purpose and goals of the organization; leadership nature (e.g., risk averse or risk tolerant; early adapter, etc.) shapes the environment that dictates the Level of learning for tactical innovation, for setting strategic objectives and strategies, and for identifying the need for strategic innovation, which may include reformulation of the purpose and goals. The latter mechanism is driven by a feedback loop with the outcome of operations. If successes lead to extreme repression and/or hardened targets, new strategic objectives and/or tactical innovations may be formulated.

Group Dynamics: are driven by the goal and shaped by the CAS organizational structure. As discussed in the previous sections, this structure will present itself in a network that may be constraining or facilitating to innovation and learning, as discussed in the previous sections. Interactions with outside organizations are represented as linkages to external resources. The purpose of the organization also impacts the structure and provides constraints for secrecy.

Methods: include an integrated choice of weapons, attack types, and targets. Statistical analysis of the Global Terrorism Data Base (discussed in the next section) shows that choices of attacks, and targets over the past 40 years are complex. However, once a choice is made, terrorist groups tend to continue to use them unless some contravening event occurs. Such a contravening effect is provided in the framework by competing feedback loops that result from success. With tactical successes, there is a reinforcing feedback loop to continue to use them, as shown on the right hand side of the figure. Continual learning and refinement occurs, which in turns increase the likelihood of success. At the same time, however, successes generate a response in the form of hardened targets and/or other interventions such as interruptions to supply chains. These

responses form negative feedback loops. The comparative rates of feedback between the negative and positive loops that result from success determine whether more innovation and learning is required at the tactical level to continue to achieve successes.

Resources: are in a positive feedback loop with successes and reinforced learning, and in a negative feedback loop with failures and innovation. They interact with the CAS organizational structure through the mechanisms discussed previously.

The rates of exchanges between the elements in this framework can be estimated and developed into a predictive model using the theoretical construct of general systems theory presented in Section 1 and characteristic parameters of CAS network structures (e.g., clustering, connectivity, path lengths, cycle times, etc.). While there is a large corpus of literature on network structures in general, more research on dark, covert networks would improve such models.

Detailed models of the genesis of innovation in the three levels of learning and innovation, incorporating state-of-the-art understanding of the nonlinear aspects of innovation emergence, are critical to implementation of the framework. Five models are presented in Figures 9-14 for the different system states and network structures considered in this paper. Key concepts include fitness landscapes and punctuated equilibrium previously mentioned. These build from ideas contained in classic system dynamic models of innovation and learning(Sterman, 2000), but account for the different states that terrorist organizations may be in (e.g., closed, open, etc.) depending on other system interactions with their environment.

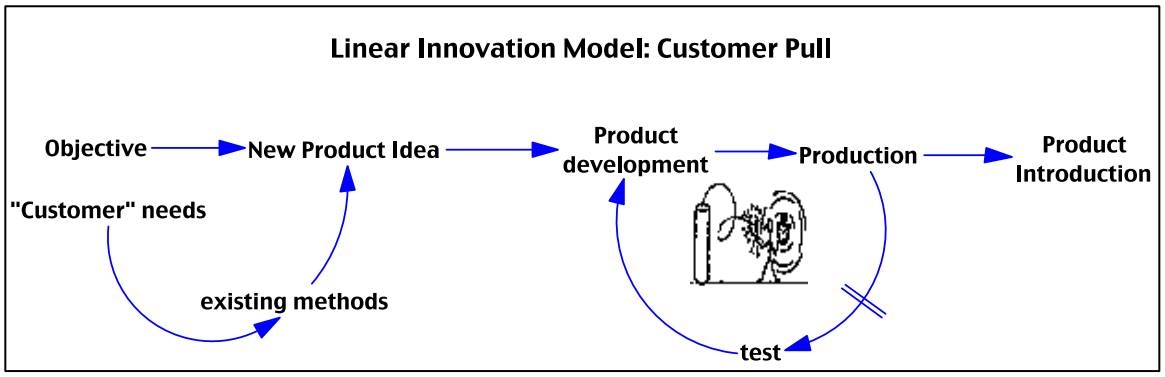

Figure 9 Learning in Simple Systems

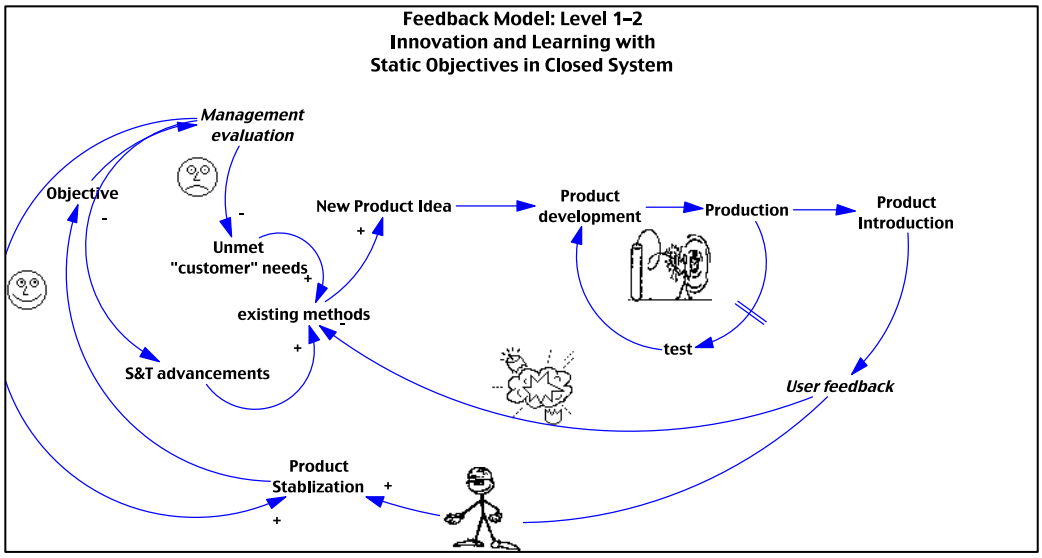

Figure 10 Innovation and Learning in Closed Systems Levels 1-2, with no input of ideas from exogenous sources and no ability to conduct experiments, such as in highly covert organizations

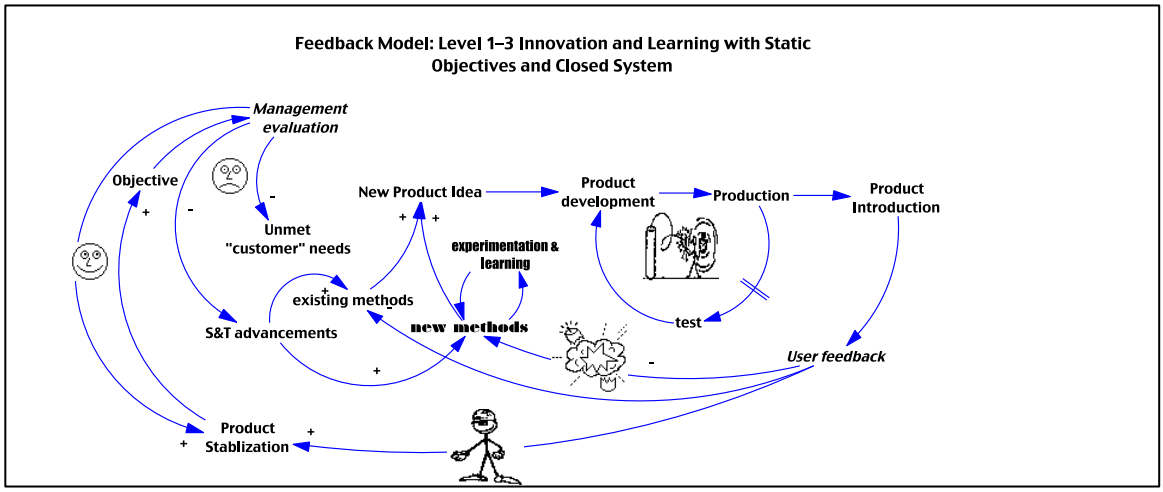

Figure 11 Innovation and Learning in Closed Systems Levels 1-3, Innovation and Learning in Closed Systems Levels 1-2, with no input of ideas from exogenous sources but having the ability to conduct experiments in secret

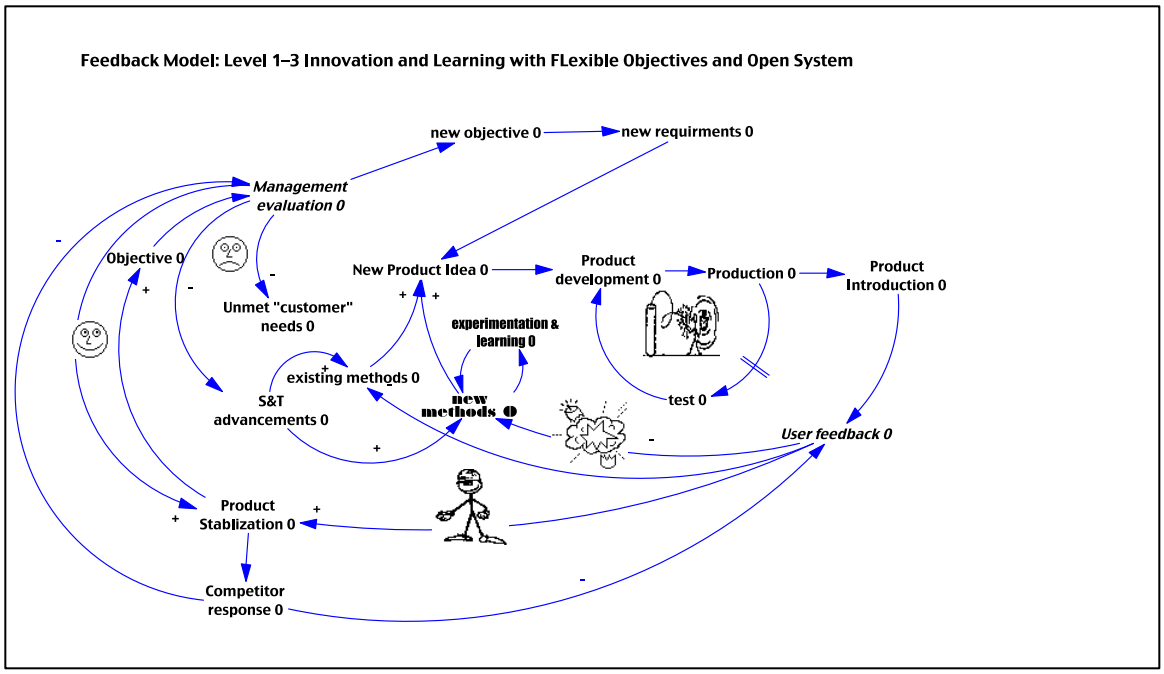

Figure 12 Learning in Open Systems, where ideas for new product development come in to a single organization from outside, and may generate new objectives and requirements

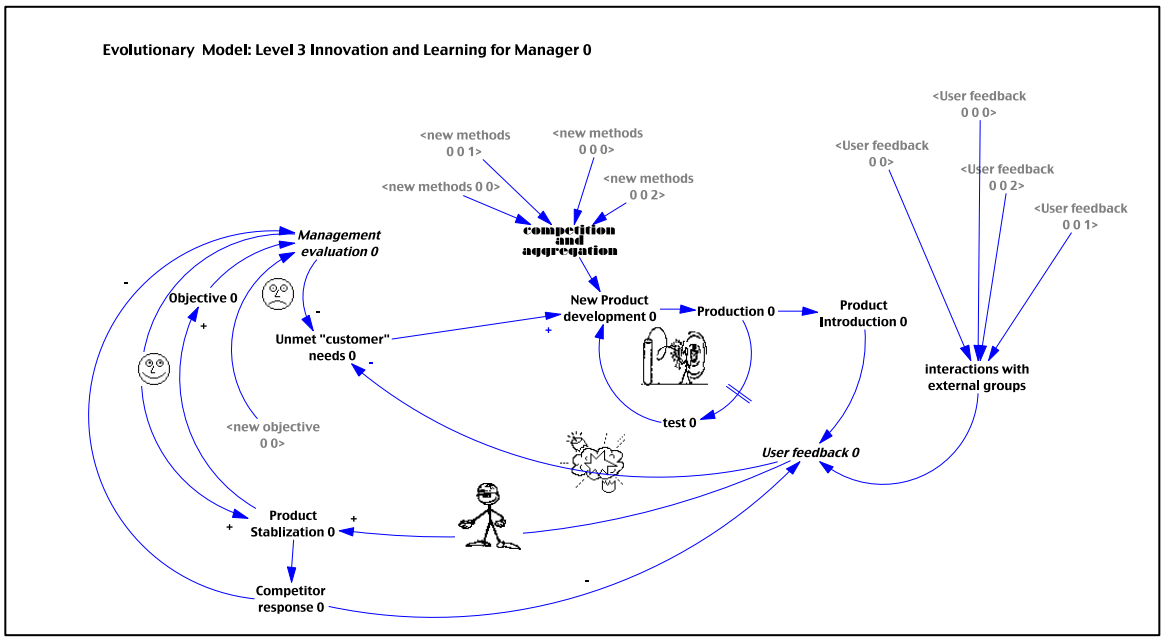

Figure 13 Evolutionary Model of Innovation where learning and innovation is response to interactions with multiple entities outside of the organization, recognizing many different basins of attraction and increasing the likelihood of developing new fitness landscapes by those interactions. This is the most creative but most risky.

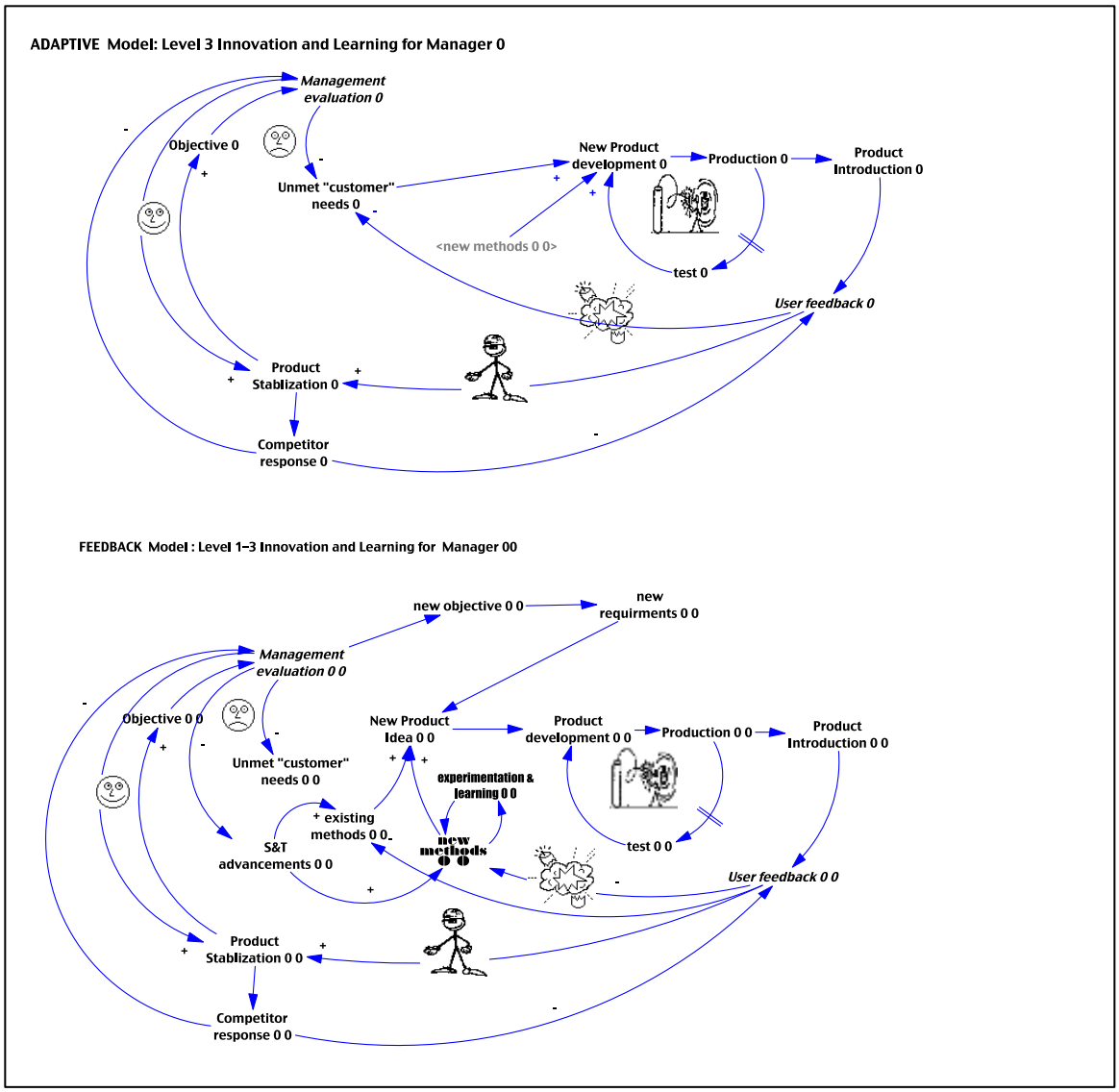

Figure 14 Adaptive Learning Between Organizations with shared goals who co-evolve in the development of new methods, goals, and objectives. For terrorist organizations, this increases risk of exposure and infiltration

5. Corroborating Evidence

Evidence to test the model comes from case studies from the literature, the Global Terrorism Database for terrorist tactics and operations (*Global Terrorism Database*, 2012), and the BAAD database for terrorist organizational structure and history(Asal, 2012). This evidence is summarized in Table 1 and Figures 15-22. While not conclusive, the data corroborates the likelihood of the mechanisms hypothesized in this paper to differentiate innovation propensity between terrorist groups, and provides insight for understanding the puzzle regarding lack of WMD use by terrorists.

Table 1.Terrorist organizations and their structure, age of organization, and level of innovation exhibited

Network Structure	Terrorist Organization	Degree	Est. size	Age	State Sponsor	Innovation	Innovation mode	AOO	Cause
Erdo-Renyi	Entrepreneurial Islamic	1	<100	~5	0	2	all	global	mixed
Windmill	AQ - Two Rivers	9	5000	9	0	2	immitation, evolution	Iraq	regional
Hierarchy	LeT (ISI)	8	300	14	1	2	immitation, evolution	Kashmir	local
Small World	Ansar al-Sunnah	6	700	10	0	3	adaptive	Iraq	regional
Core Periphery	Hizbollah	4	10-100K	32	1	4	adaptive, punctuated equilibrium	Lebanon	regional
Ring	IRA	3	700	95	0	2	learning, evolution	UK	local
Hierarchy	LTTE	0	8000	38	1	1	learning, evolution	Sri Lanka	local
Hierarchy	ELN	8	3000	50	1	1	learning, evolution	Columbia	local

As Table 1 shows, those organizations supported by state sponsors (LeT, LTTE, and ELN) tend to be hierarchical and bureaucratic. While this could provide the resources and support necessary to develop effective WMD use, it also constrains innovation and learning and fosters imitation and evolution. In contrast, organizations such as al Qaeda, Ansar al Sunnah, and Hezbollah, whose structures favor more innovation, do indeed exhibit more propensities for innovation in their choices of targets and tactics.

Figures 15-17 show the shift in target selections by terrorists over the last forty years. The most dramatic shift has been in the rise of attacks on civilian targets relative to attacks on businesses. During that same time period, there have been distinct shifts in the geographic locales of most terrorist incidents, as shown in Figures 18-22. Activities peaked in Central America peaked in 1981 in Guatemala, targeting primarily military, police, businesses, and utilities. Activities in South America started to grow 1982 and peaked in 1984. The last two decades have seen significant decline in activities in Central and South America, significant increase in the Middle East and S. Asia, and a relatively steady level of activity (although changing perpetrators) in Europe.

Summary and Conclusions

At some times, some terrorist organizations exhibit characteristics of complex adaptive systems. This work has shown that as such, the degree to which they can adapt and are likely to exhibit innovative behavior should depend on the structure of the organization, which may change over time in response to system dynamics catalyzed by interactions with their environment. Success by covert organizations stimulates countermeasures. Resiliency requires innovation in the face of countermeasures. Two counteracting feedback loops compete with innovation drivers to strongly influence basins of attraction for terrorist organizations: (1) Need for secrecy and (2) Need for recognized successes (failure intolerant). The more there is a need for secrecy, the less likely innovation will be.

The most likely organizations to exhibit innovation and learning will be those with core periphery structures, where ideas from outliers can be quickly accessed and assimilated and exogenous shocks can be distributed. While statistical data trends affirm the conceptual model for structural influence on innovation mechanisms, detailed process tracing in longitudinal, comparative case studies are necessary for validation. If substantiated, the effective countermeasures that decrease, not increase, network resiliency while suppressing innovation should be pursued.

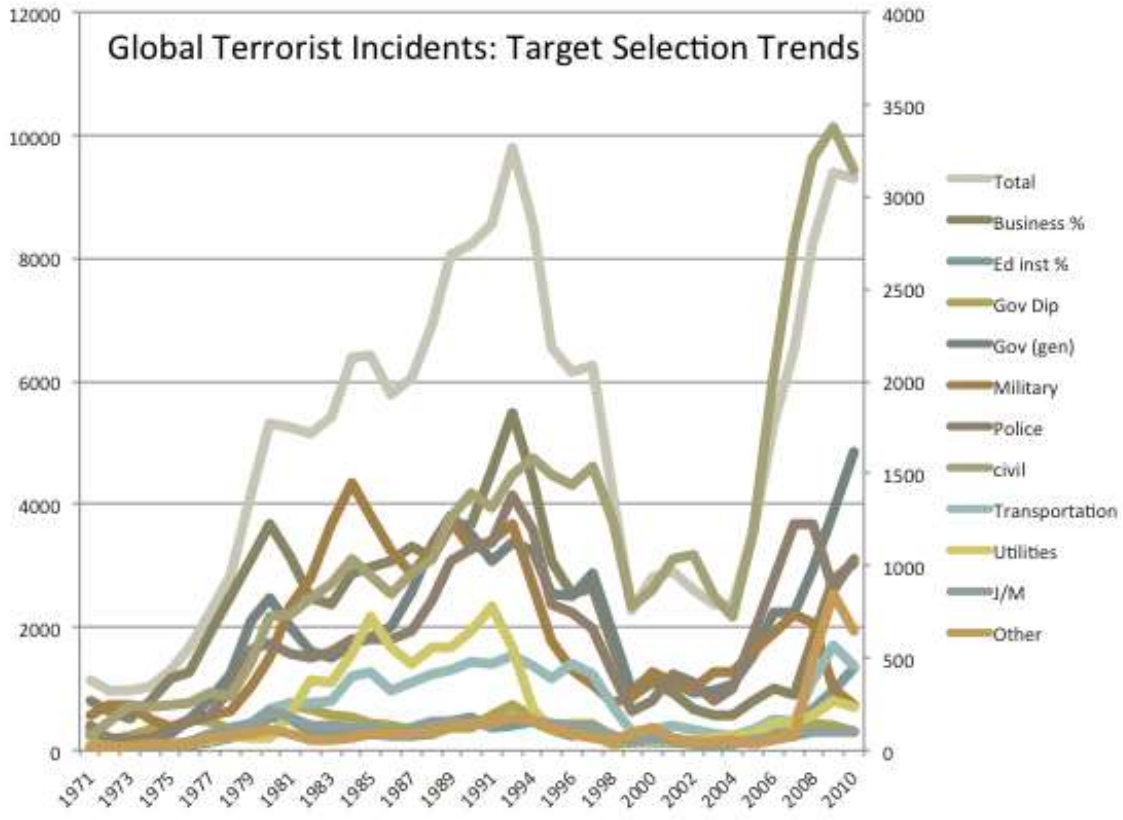

Figure 15 Global Targeting Trends 1970- 2011

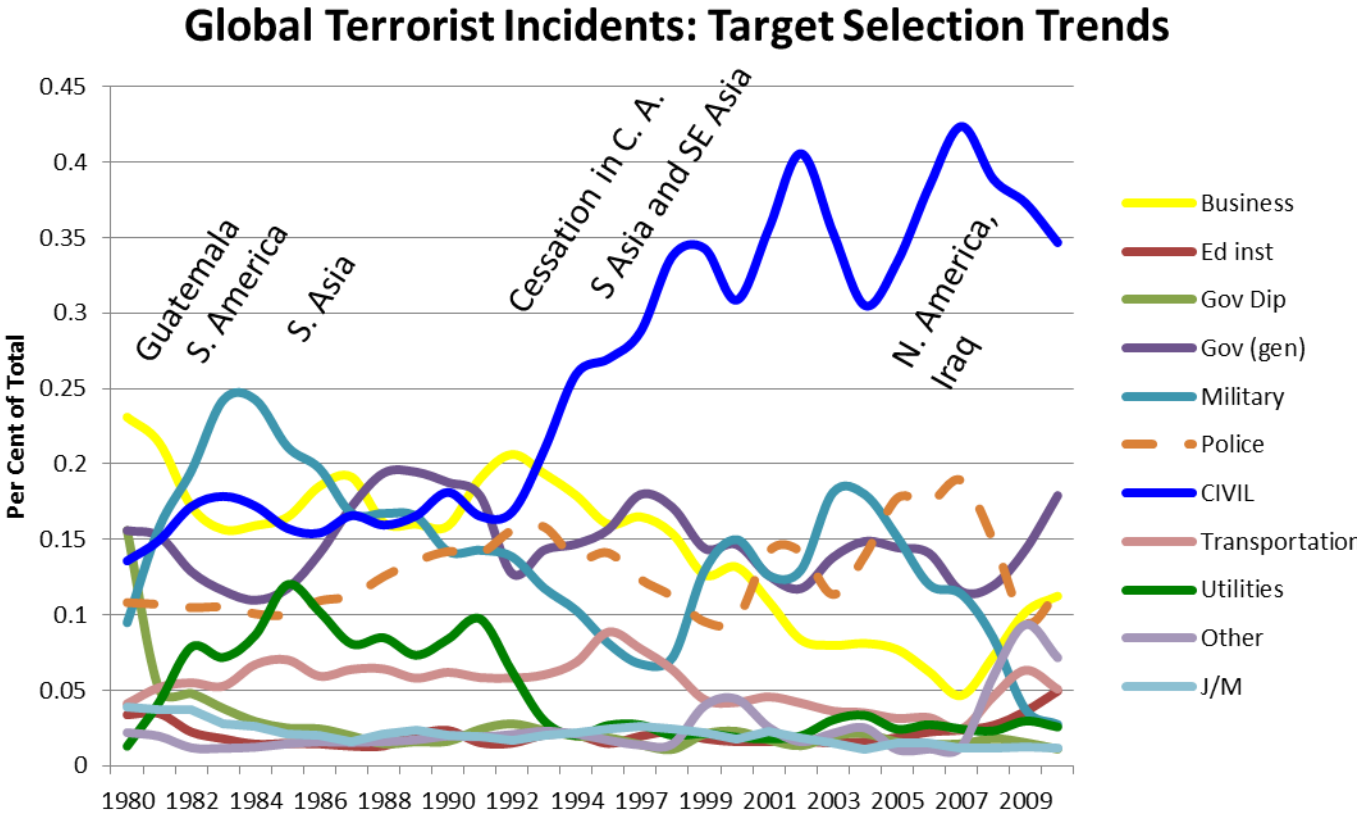

Figure 16 Global targeting trends shift in time and geographic regions

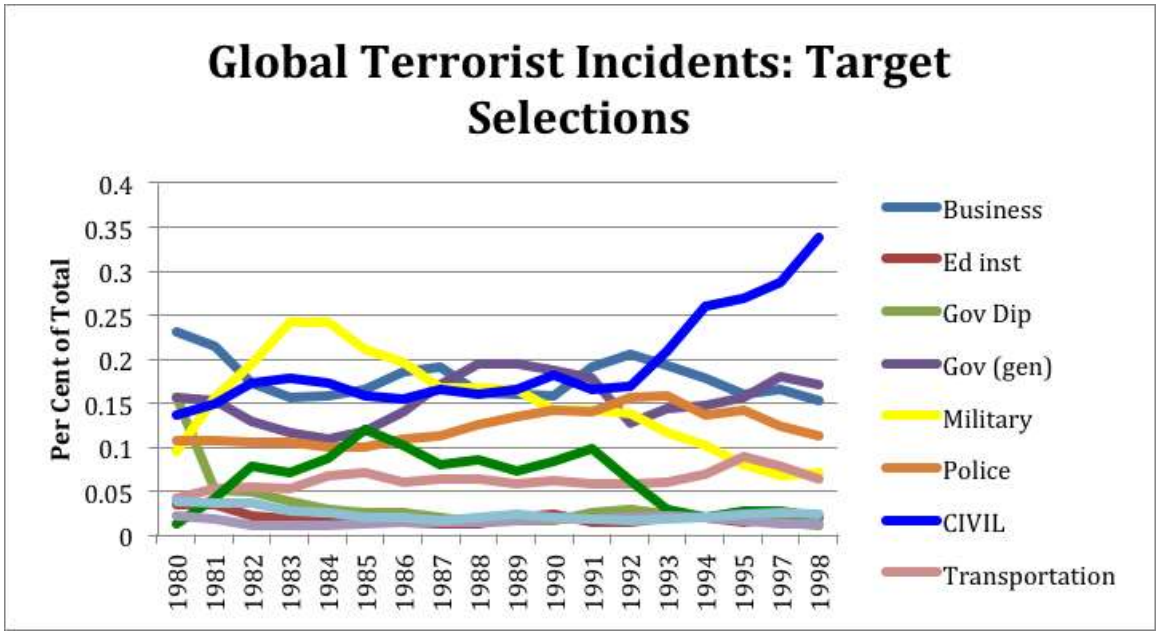

Figure 17Selected targeting Trends 1980 – 2009 illustrate trade-off between military and civilian targets

Figure 18 Global Incidents 1981 – 1983

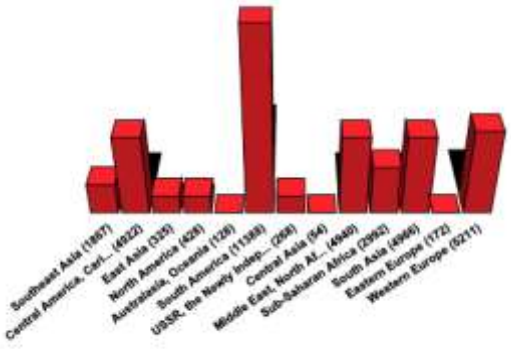

Figure 19 Global Incidents 1984 - 1994

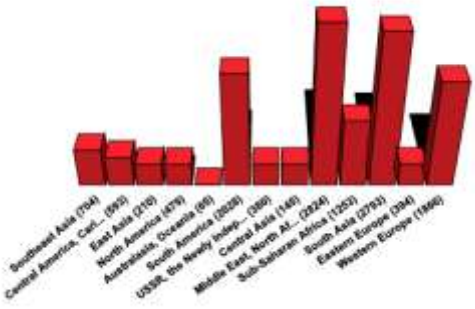

Figure 20 Global Incidents 1994 – 1998

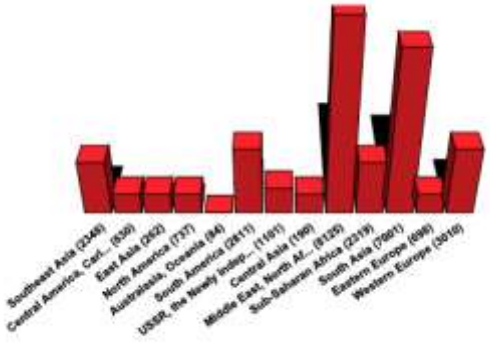

Figure 21 Global Incidents 1998 - 2007

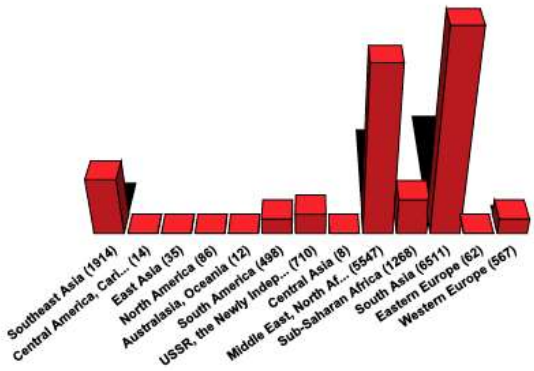

Figure 22 Global Incidents 2007 - 2011

References

Ahmed, E., Elgazzar, A. S., & Hegazi, A. S. (2005). On complex adaptive systems and terrorism. *Physics Letters A, 337*(1/2), 127-129.

Asal, Victor. (2012). *Big Allied and Dangerous (BAAD)*.

Bar-Yam, Yaneer. (1997). *Dynamics of Complex Systems*: Addison-Wesley.

Bertalanffy, Ludwig von. (1980). *General system theory : foundations, development, applications* (Rev. ed.). New York: Braziller.

Bonabeau, Eric, Dorigo, Marco, & Theraulaz, Guy. (1999). *Swarm intelligence : from natural to artificial systems*. New York: Oxford University Press.

Clarke, David (Ed.). (2004). *Technology and Terrorism*. New Brunswick: Transaction Publishers.

Crutchfield, James P. (2003). When Evolution is Revolution - Origins of Innovation. In J. P. Crutchfield & P. Schuster (Eds.), *Evolutionary Dynamics: Exploring the Interplay of Slection, Accident, Neutrality, and Function* (pp. 101-133): Oxford University Press.

Damon, Centola, & Macy, Michael. (2007). Complex Contagions and the Weakness of Long Ties. *American Journal of Sociology, 113*(3), 702-734.

Dolnik, Adam. (2009). *Understanding Terroist Innovation: Technology, Tactics, and Global Trends*: Routledge.

Filk, Thomas, & Muller, Albrecht von. Evolutionary Learning of Small Networks. http://www.igpp.de/english/tda/pdf/filkmueller08.pdf

Fonseca, José. (2002). *Complexity and innovation in organizations*. London ; New York: Routledge.

Global Terrorism Database. (2012). National Consortium for the Study of Terrorism and Responses to Terrorism (START). Retrieved from http://www.start.umd.edu/gtd

Gomez-Rodriguez, Manuel, Leskovec, Jure, & Krause, Andreas. (2010). *Inferring Networks of Diffusion and Influence*. Paper presented at the 16th ACM SIGKDD International COnfernce on Knowledge Discovery and Data Mining. http://las.ethz.ch/files/gomezrodriguez11inferring.pdf

Gould, Stephen Jay, & Eldrige, Niles. (1977). Punctuated Equilibria: The tempo and mode of evolution reconsidered. *Paleobiology, 3*, 115-151.

Hayden, Nancy. (2006). The Complexity of Terrorism: Social and Behavioral Understanding Trends for the Future. In M. Ranstorp (Ed.), *Mapping Terrorism Research: State of the Art, Gaps and Future Direction* (pp. 33-57): Routledge Publishing.

High-Tech Terrorism, United States Senate, Second Session on High-Tech Terrorism Sess. 145 (1988).

Holland, John H. (1995). *Hidden order : how adaptation builds complexity*. Reading, Mass.: Addison-Wesley.

Horgan, John, & Braddock, Kurt. (2012). *Terrorism studies : a reader*. London ; New York: Routledge.

Jantsch, E. (1980). *The Self-Organizing Universe: Scientific and Human Implications of the Emerging Paradigm of Evolution*: Pergamon.

Kauffman, Stuart A. (1993). *The Origins of Order: Self-organization and selection in evolution*. NY: Oxford University Press.
Kurtz, C.F., & Snowden, D.J. (2003). The New Dynamics of Strategy: Sense-making in a complex and complicated world. *IBM Systems Journal, 42*(3).
Laszlo, Ervin. (2001). *The Systems View of the World: A Holistic Vision for Our Time*. Cresskill, NM: Hampton Press, Inc.
Legasto, Augusto, Forrester, Jay Wright, & Lyneis, James M. (1980). *System dynamics*. Amsterdam ; New York New York: North-Holland Pub. Co.
Lichtblau, Dale E., Haugh, Brian, Larsen, Gregory, & Mayfield, Terry. (2006). Analyzing Adversaries as Complex Adaptive Systems. Washington DC: IDA.
Lindelauf, Roy, Borm, Peter, & Hamers, Herbert. (2009). The Influence of Secrecy on the Communciation Structure of Covert Networks. *Social Networks, 31*, 126-137.
Marion, Russ, & Uhl-Bien, Mary. (2003). Complexity Theory and Al Qadea: Examining Complex Leadership: University of Nebraska-Lincoln.
Martin, Gus. (2003). *Understanding Terrorism: Challenges, Perspectives, and Issues*: Sage Publications.
Meadows, Donella H., & Wright, Diana. (2008). *Thinking in systems : a primer*. White River Junction, Vt.: Chelsea Green Pub.
Newman, M. E. J., Watts, D. J., & Strogatz, S. H. (2002). Random Graph Models of Social Networks. Santa Fe, NM: Santa Fe Institute.
Rasmussen, Maria J., & Hafez, Mohammed M. (2010). Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators: Defense Threat Reduction Agency.
Reid, Fergal, & Hurley, Neil. (2011). Diffusion in Networks with Overlapping Community Structure. http://arxiv.org/pdf/1105.5849.pdf
Rogers, Everett M., Medina, Una E., Rivera, Mario A., & Wiley, Cody J. Complex Adaptive Systems And The Diffusion Of Innovations. *The Innovation Journal: The Public Sector Innovation Journal, 10*(3).
Rombach, M. Puck, Porter, Mason A., Fowler, James H., & Mucha, Peter J. (2012). Core-Periphery Structure in Networks. http://arxiv.org/abs/1202.2684v1
Snowden, David J., & Boone, Mary E. (2007). A Leader's Framework for Decision Making. *Harvard Business Review, November*.
Sterman, John. (2000). *Business dynamics : systems thinking and modeling for a complex world*. Boston: Irwin/McGraw-Hill.
Subrahmanian, V.S., Mannes, Aaron, Sliva, Amy, Shakarian, Jana, & Dickerson, John P. (2013). *Computational Analysis of Terrorist Groups: Lashkar-e-Taiba*: Springer.
Xu, Jenifer, & Chen, Hsinchun. (2008). The Topology of Dark Networks. *Communciations of the ACM, 51*(10), 59-65.