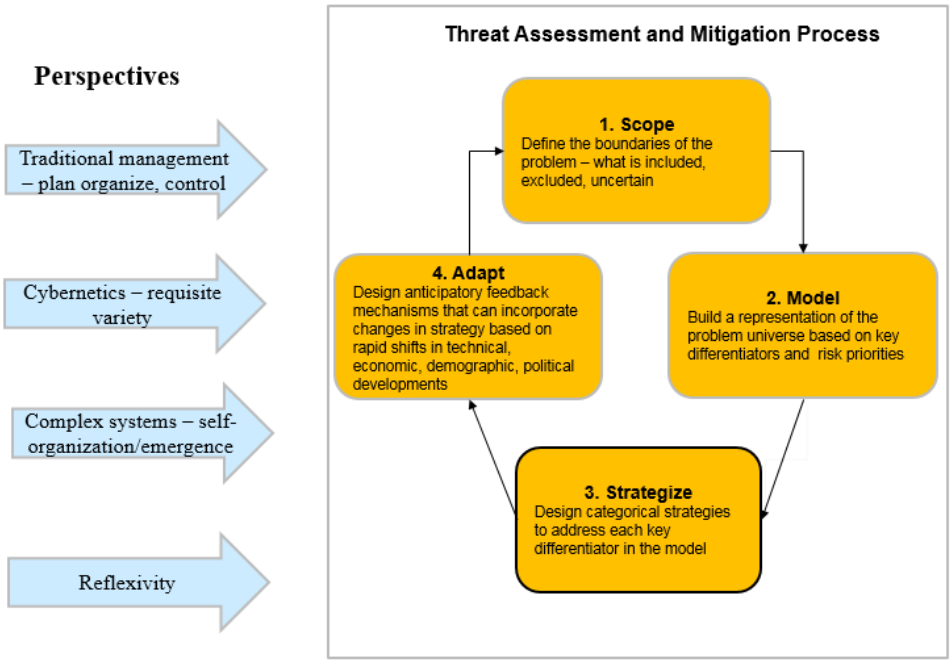
A Proposed Framework for Threat Assessment and Mitigation



Introduction

The current and evolving body of work in the social and behavioral sciences offers tremendous potential for gaining an in-depth understanding of global adversaries and allies; and their future intentions that may impact U.S. interests. In this paper I propose a conceptual model that draws on several perspectives from a variety of social and behavioral science arenas; and integrates them into a synoptic approach for identifying, assessing and acting upon threats to U.S. interests; and capitalizing on opportunities. The essential constructs of the model can be divided into two categories:

1. The basic steps involved in threat assessment and resolution; and
2. The lenses, or perspectives through which these steps can and should be viewed.

The basic steps involve: **a) Scoping** - defining the boundaries of the problem; **b) Modeling** - building a representation of the problem from the perspective of the problem solver (s); **c) Strategizing** - designing approaches that address the most important aspects of the problem; and tailoring the strategies to match the particular economic, technological, political, and cultural environment being addressed; and **e) Adapting** – Building feedback mechanisms that allow strategies to be modified in the light of changing conditions.

The lenses through which threat assessment and resolution must be viewed are a critical component – and perhaps the most fundamental aspect of the framework. These lenses allow the deepest understanding of the framework because they are embedded into the ontology and epistemology of the actors involved in the assessment and resolution process.

Gibson Burrell and Gareth Morgan provided a fundamental taxonomy for classifying the way social science problems are viewed and understood. (Sociological Paradigms and Organizational Analysis 1979). They arranged a two-by-two matrix into four quadrants that were based on two kinds of assumptions about how the social world is understood: 1) the objective vs. subjective nature of reality; and 2) a view of the social world where the default position is stability vs. conflict. From these two assumptions, four epistemological models are developed:

- Functional – assumes the world is objectively real and sufficiently stable to allow prediction
- Interpretive – assumes the world is subjectively constructed and can remain stable through agreed upon constructions
- Radical structuralism – which is essentially Marxism, and is based on the objective reality associated with dialectical materialism; there will always be an antithesis to a thesis and a resulting synthesis. The world, thus, is in perpetual conflict
- Radical humanism – assumes the world is socially constructed, but competing views of reality will continuously attempt to supplant the dominant views

Based on these fundamental epistemological positions, I have built different lenses into the threat assessment process. Although not exactly mirroring Burrell and Morgan's taxonomy, they are based on the same idea that these assessments are viewed through different lenses, which must be considered in a comprehensive solution to threat or opportunity assessment.

The lenses I incorporate into the framework include:

- Traditional management approaches which involve planning, management and control tasks. Most of these approaches can be associated with the 'functionalist' perspective in which the world is sufficiently stable and thus subject to predictive analytics.
- Cybernetics-based approaches – In this case the Law of Requisite Variety, championed by Ross Ashby (Design for A Brain 1958-), is based on the concept that an efficient regulatory or management mechanism is one that incorporates sufficient variety or complexity in its management mechanism to match the variety or complexity in the problem being managed. Traditional, or first order cybernetics is usually associated with the functional perspesctive.
- Self organization – This perspective has its roots in complex systems theory, which is based on the idea that the most effective holistic solutions to problems naturally emerge from the interaction among independent actors, rather than from a central regulator. Self organizing systems may be viewed from both functional and interpretive perspectives. The emergent, albeit unpredictable solutions to complex

problems can be considered as an objective reality. To wit, an effective screening mechanism for terrorist threats at airports may be the result of creative thinking that simultaneously occurred in many parts of the global security network; and gained momentum through successive positive feedback loops. The fact that the screening system works is an objective reality, and thus is associated with a functionalist perspective. On the other hand, the growing acceptance of profiling as a technique for detecting the most serious security threats, may be the result of a dynamic social influence process. In this process ideas gain momentum as broader agreement is reached, and resources soon follow which enable implementation of the ideas. This eventually results in the social construction of a reality. As such, this kind of self organization falls squarely in the interpretive realm.

- Reflexivity – Closely associated with second order cybernetics, Chris Argyris' idea of double loop learning, and the phenomenological reduction process (Edmond Husserl), which has its roots embedded deep within the interpretive epistemology. The essence of this approach is intense self-awareness of the lens with which one views the problem. Before we can examine the problem we must examine our own world view. This enables us the freedom to escape from pre-conceived world views and see other possible ways of understanding the world around us.

Below I provide examples of how the various lenses of traditional management thinking, cybernetics, self organization. and reflexivity can be applied in each step of the threat assessment and mitigation process.

Scoping - The first step in this process, scoping, is a mix of functionalist and interpretive thinking. Defining the boundaries of the problem to be addressed should be both an objective and subjective exercise. To illustrate, how should one define the scope, or boundaries, of the problem associated with threats to this country posed by insufficient vetting of immigrants? From a traditional management and cybernetics perspective, the boundaries of the problem may be stipulated by provisions in the U.S. Constitution and/or in statute. Such provisions suggest processes that may and may not be used in defining threats. For example, the establishment clause in the U.S. constitution prohibits Congress from preferring or elevating one religion over another. This would appear to limit Congress or the Administration from using religion as a basis for differentiating threat levels. From a self-organizing perspective, the extensive exchange of opinions among large networks of stakeholders via social media produces an emergent definition of the boundaries of the threat posed by immigration. The emergent shape and characteristics of the threat cannot be accurately predicted; rather, the parameters of the threat gain strength and support through positive feedback loops and mutual reinforcement. Thus, there is a potential conflict between two characterizations of the threat that must be resolved. Responsibility for problem definition ultimately rests with policy decision makers. But these decision makers must adopt resolution mechanisms to adjudicate between the different versions arising from managerially defined vs. emergent dynamics. Finally, a reflexive perspective should add a leavening aspect to the problem definition process. Elevated self-awareness regarding preconceived world views can uncover inherent

biases that frame how decision makers view the problem; and facilitate new ways of viewing problems and solutions. Processes such as values clarification, and phenomenological reductions are examples of how pre-conceived world views can be made more transparent; and can lead to new and valuable ways of conceiving the problem

Modeling – Once problem parameters are defined, the modeling step entails building a representation of the problem that highlights the most critical aspects of the problem that must be attended to; and which are used as guide posts to direct resources and strategies. I will again refer to the threat arising from increased immigration to illustrate how different lenses can be used to construct a robust model. Traditional management and cybernetics approaches will tend to rely on data-driven models that can be used to prioritize those aspects of the problem that need more immediate attention. An example of this empirical approach would be to build a model of the problem based on those areas of the world that represent the most frequent cases of terrorist attacks on our country; and the validity of this model would be supported by data showing frequency of attacks by area. From a self-organizing perspective, the operational model of the problem would be built on emergent views facilitated by the large volume of information and opinions exchanged through social networking. Those key aspects of the problem that gain the most 'hits' are the most likely to stay foremost in the public consciousness. Thus, a model of the immigration threat problem is built on the principles of frequency, repetition and inflationary reinforcement; and may bear little resemblance to the model that is constructed based on empirical evidence. Berger and Luckman's tome on "The Social Construction of Reality" pre-dates the social networking era by at least forty years; but the basic dynamic underlying the process of social construction holds true, whether we are referring to the evolution of scientific paradigms, or the emergence of perceived threats from immigration fueled by social networking. Once again, the ultimate decisions about which model is most relevant rests with policy decision makers. But they would be wise to establish processes that can mediate between managerially determined models based on empirical evidence; and the emergent models that provide the light and heat generated by the social media; and which are most probably foremost in the mind of the citizenry. The reflexive perspective should also enter into the process of problem modeling. As was the case in defining problem boundaries, a self-reflecting process should be involved in clarifying the biases of decision makers that are responsible for generating relevant representations of the threat from immigration.

Strategizing– This third element of threat assessment involve: 1) formulating strategies and allocating appropriate resources to address the most critical aspects of the problem that are designed into the model, or problem representation identified in Step Two; and 2) tailoring the strategies to match the particular economic, technological, political, and cultural environment being addressed. The crux of this challenge is to design a threat mitigation initiative with a sufficient variety of strategies to match the complexity inherent in the threats posed by immigration across our borders. Insufficient variety does not effectively address the range of possible threats. An illustration of insufficient variety in strategy formulation is to provide a

single vetting protocol for all immigrants entering our country. Too much variety poses fundamental challenges in managing the threat mitigation effort. An example of over-complicating threat mitigation strategies would be to establish an inordinate number of vetting protocols to match the many individual circumstances that characterize immigrants. If Homeland Security attempted to establish different vetting strategies for each combination of country, ethnic origin, gender, age, etc., the vetting process would collapse of its own weight. Ross Ashby, a pioneer in the field of cybernetics, captured the Federal administrator's dilemma, in his 'Law of Requisite Variety' (LRV), introduced in the 1950s (Ashby, W.R. 1958, Requisite Variety and its implications for the control of complex systems, Cybernetica (Namur) Vo1 1, No 2, 1958). While effective problem definition and modeling should be based on the combined perspective of traditional management, cybernetics, self-organizing/emergence and reflexivity, strategy formulation should be the province of traditional management approaches coupled with a reflexive process that allows strategy formulators to become self-aware of the lenses through which they view the problem and its potential solutions.

During the strategy formulation and tailoring process, the law of requisite variety is applied in order to generate a reasonably manageable set of strategies to address the problem as modeled. In the application of this law, two plausible scenarios emerge: 1) A central, or dominant regulator makes final decisions on strategies, and local adjustments based on the consultation and advice of subject matter experts and other stakeholders. 2) A network of stakeholders with comparable authority and influence. In this scenario threat mitigation strategies are negotiated among stakeholders. It is critical in this scenario to design processes that facilitate reaching consensus decisions. Two types of errors can occur during the strategy formulation process, both of which are based on a miscalculation concerning the distribution of power and influence. First, a dominant regulator approach may be attempted in an environment characterized by wide distribution of power and influence among stakeholders. Second, a distributed regulator approach may be attempted in an environment that requires a dominant regulator to take charge.

Adaptation - This final stage of the threat assessment and mitigation process is characterized by constructing feedback loops that allow management to absorb new information about the nature of the problem and how well problem solutions are working. If the current approach to threat assessment and mitigation is working effectively the feedback received should require few resources to maintain the stability of the current approach. If the current approach is not working feedback loops should provide information that signals a need to change the current approach; and which may require significant investment in resources to implement the change. These investments are not confined to monetary resources. The change may also require a significant investment to change psychological, managerial and cultural mind sets. In general, feedback loops are effective mechanisms in an open systems environment. Feedback loops can also be relatively closed. To the extent that management (however it is construed) has a vested interest in accepting only information that supports continuation of current strategies, the management regime can be characterized as a relatively closed system – closed that is, to

new information that may require a change in direction. Vested interests are inclined to interpret feedback in a way that may require significant resources to maintain the stability of the current approach. This is essentially pouring good money after bad. I suggest in this paper that viewing the nature of feedback loops through traditional management, self-organizing and reflexive lenses will result in a more robust adaptation phase in the threat assessment and mitigation process.

From the traditional managerial and cybernetics perspectives, the feedback loop should be designed to differentiate between negative and positive feedback. Negative feedback is an indication of a stable strategy that requires only minimum adjustments to current strategies. As an example, information on the political leanings of a new regime in a country of interest may require only minor adjustments in threat mitigation strategies directed toward that country, if the new regime is replacing a regime within the same political party. Positive feedback is an indication of a needed change in strategies. If the new regime in that country represents a significant departure from the prior regime in policy positions, and the new postures represent a potential threat to this countries interests, this represents positive feedback; and it indicates a need to rethink this countries risk mitigation strategies.

From the self-organizing perspective, adaptation is an ongoing characteristic of emergent thinking. Feedback loops, in fact, are the core idea of the self-organizing system; and represent the 'engine' that drives new ideas into existence. Since the nature of emergent strategies are fueled by inflationary, or positive, feedback loops this can be a favorable or unfavorable dynamic. It is a favorable dynamic if one agrees with the emergent concept; and unfavorable if one disagrees. In emergent systems, negative, or stabilizing feedback loops are the mechanisms that 'deflate' new strategies. In essence, negative feedback loops result in 'dead ends' for new potential strategies that never come to fruition. To prevent a strategy from achieving 'emergent status' in a self-organizing system, opponents of the strategy must be able to design negative (deflationary) feedback loops and inject them into the self-organizing dynamic. This is illustrated by the emergent, self-organizing dynamic of social networking as fuel for energizing home-grown terrorists. To reverse this dynamic, counter information must be strategically placed into the social networking environment that short-circuits the inflationary nature of terrorist thinking.

The reflexive perspective can help to increase the self-awareness of those who manage the adaptation phase and the feedback loops that accompany the adaptation process. The establishment of reflexive processes enable managers to more clearly see when they are interpreting feedback in a way that supports continuation of their current strategic approaches – even in light of contradictory information. The ability to distinguish between negative (stabilizing) and positive (inflationary) feedback is often a matter of becoming aware of the lenses through which you are viewing the situation. Increasing self-awareness of how one is interpreting feedback can also result in significant resource savings – particularly when large investments in maintaining an obsolete status quo can be redirected toward the implementation of more relevant strategies. The table below summarizes how the different

perspectives discussed in this paper influence the four phases of threat assessment and mitigation.

Threat Assessment and Mitigation Process

Perspectives	**Assumptions**	Scope	Model	Strategize	Adapt
LRV – Dominant regulator	Central regulator makes final decisions on problem scope, key parameters, regulatory strategies, local adjustments and the nature of feedback loops	Centrally determined	Model complexity limited by what can be centrally managed	Strategy complexity limited by what can be centrally managed	Effective use of negative and positive feedback loops
LRV – multiple regulators	Threat assessment and mitigation roles are divided among stakeholders; mechanisms must be established to achieve consensus	Negotiated among stakeholders	May be more elaborate based on distributed capacity to manage	Strategies may be more elaborate, but also in conflict	Multiple stakeholders increase feedback volume, but quality may suffer
Self-organization	Local interaction among agents generate patterns of problem definition and solution through inflationary feedback loops; emergent solutions are difficult to predict; could be lots of false starts	Emergent definition	Unpredictable; but emergent model may compete with policy makers' models	Emergent strategies are the result of growing network consensus	Positive feedback loops are the engine that drives emergent strategies
Reflexivity	Elevated self awareness regarding preconceived world views; enables new ways of viewing problems and solutions	Unfreezes traditional definitions of problem boundaries	Increases self-awareness of biases in building representations	Opportunity to reflect on how biases shape strategic thinking	Recognition of biases in interpreting feedback

References

Ross Ashby, Design for a Brain, 1958

W. Ross Ashby, "Requisite Variety and its implications for the control of complex systems," Cybernetica (Namur) Vo1 1, No 2, 1958).

W.R. Ashby, MD, Principles of the Self-Organizing Dynamic System, The Journal of General Psychology, July 6, 2010

Chris Argyris, "Single Loop and Double Loop Models in Research on Decision Making" Administrative Sciences Quarterly, 1976

Gibson Burrell and Gareth Morgan, Sociological Paradigms and Organizational Analysis 1979

P. Cilliers and David Spurrett, "Complexity and Post-Modernism: Understanding Complex Systems" published online September 16, 2014

Barney Glaser and Anselm Strauss, The Social Construction of Reality, 1967

Maurice Perleau-Ponty, Husserl at the Limits of Phenomenology, Northwestern University Press, 2002