2006-07-01

Intelligence and Nuclear Proliferation: Understanding and Probing Complexity; Strategic Insights, v. 5, issue 6 July 2006

Williams, Phil

Monterey, California. Naval Postgraduate School

Strategic Insights, v.5, issue 6 (July 2006)
http://hdl.handle.net/10945/11460

Intelligence and Nuclear Proliferation: Understanding and Probing Complexity

Strategic Insights, Volume V, Issue 6 (July 2006)

by Phil Williams

Strategic Insights is a bi-monthly electronic journal produced by the Center for Contemporary Conflict at the Naval Postgraduate School in Monterey, California. The views expressed here are those of the author(s) and do not necessarily represent the views of NPS, the Department of Defense, or the U.S. Government.

For a PDF version of this article, click here.

Introduction

Nuclear proliferation is not what it used to be. In the 1960s proliferation issues were integrally related to alliance management, causing divisions in NATO that were perhaps most obvious when Secretary of Defense Robert McNamara, in a famous speech at Ann Arbor, Michigan characterized independent nuclear deterrent forces as “dangerous, expensive, prone to obsolescence and lacking in credibility.” Directed primarily at France but also at Britain, this speech—and the sentiment it embodied—created tensions in Atlantic relations that were not fully resolved until the end of the Cold War.

During the mid-1970s, intra-alliance tensions took on a different form as the United States condemned West Germany’s deal to supply a nuclear reactor to Brazil.

In 1981, concerns over Iraq’s nuclear program led to Israel’s pre-emptive strike against the Iraqi nuclear reactor at Osirak. Although this was a major setback to Iraq’s nuclear ambitions, the impact was not as salutary as the proponents of nonproliferation had hoped. The gap between aspirations and the capacity to achieve them continued to diminish during the remainder of the decade.

During the 1990s concerns about nuclear proliferation focused on regional competition between India and Pakistan, the nuclear ambitions of rogue states such as North Korea, and the problem of “loose nukes” in the former Soviet Union. Today, in what might be described as the latest iteration of the proliferation problem, the three components of the 1990s have merged in a way that poses unprecedented challenges—both for the nonproliferation regime and, more specifically, for the United States intelligence community. The focus is now in large part on proliferation networks. These networks range from criminals trafficking nuclear materials from the former Soviet Union through the Caucasus, Balkans, and Central Asia, to the A.Q. Khan network which was, in effect, a privatized nuclear diffusion network.

Nuclear Smuggling

The seriousness of the nuclear materials trafficking problem first became evident in disclosures about the theft of 1.5 kilograms of highly enriched uranium (HEU) from a nuclear facility in Podolsk, Russia, in 1992. Two separate incidents in Germany in 1994 magnified the visibility of the issue. The first was the fortuitous discovery, in May 1994, of more than six grams of weapons grade plutonium, made by police searching the premises of a known counterfeiter, Adolph Jaekle. The second was a controversial German sting operation which resulted in the seizure of 363.4 grams of weapons grade plutonium-239, enriched to a level of 87 per cent, and 201 grams of lithium 6, which had been brought from Moscow to Munich on a Lufthansa flight. Two Spaniards and a Colombian were arrested. Although this incident led to speculation about links to terrorists, it turned out that the men were simply amateurs trying to make money. Even so, they were able to acquire weapons grade materials.

Nevertheless, the arrests appear to have had something of a deterrent effect and during the second half of the 1990s, there was a major decline in the number of incidents of nuclear material trafficking in Western Europe. No significant seizures occurred in Germany during the second half of the 1990s and there were very few in the rest of Western Europe. Yet if traffickers were less inclined than they had been in the first half of the 1990s to seek buyers in Western Europe, their inhibitions did not result in a prohibition. In July 2001, three men were arrested in Paris, and authorities seized five grams of highly enriched uranium.[1]

Although the Paris incident underlines the need for continued vigilance in Europe, it was something of an anomaly. By 1997, the main axis of nuclear material trafficking had shifted to the southern routes—through the Caucasus, Central Asia, Turkey, and the Balkans. This shift has been solidified by trends and events over the last nine years. Three seizures of enriched uranium occurred in Batumi, a Georgian Black Sea port, between 1999 and 2001. A number of arrests and seizures have also taken place in Turkey.[2] This shift to the southern routes implies both learning and adaptation by traffickers. They are looking for end users in the Middle East and Southwest Asia and are attracted by the easier transshipment opportunities of the southern routes.

As for the traffickers themselves, it is possible to identify several kinds of participants in the nuclear and radioactive materials trafficking business:

- *Opportunistic individuals and small groups*. These traffickers are galvanized by economic crisis. They exploit friendships or family affiliations with workers in nuclear installations who have access to the materials. These small groups lack sophistication and their efforts are usually detected fairly easily.
- *Ethnically based smuggling organizations.* Prominent among this group are Turkish and Chechen networks which simply move from one product line to another depending on either availability or demand. In some cases, Turkish antiquities smugglers have changed their product line to nuclear and radioactive materials.
- *Russian organized crime.* Although the number of nuclear trafficking cases involving organized crime is not large, it is significant enough to challenge arguments that organized crime is unwilling to accept the risks involved in this illicit business. There has long been speculation, for example, that in 1994 members of one of Moscow's major criminal organizations, the Solntsevo group, were involved in efforts to sell 27 kilograms of uranium-238 for $1.5 million. A more recent case involving Russian organized crime occurred in March 2001, when members of the Balashikha criminal organization in the Moscow region were arrested while trying to buy cesium. Authorities also seized $250,000 in cash, which was thought to have been an advance payment in a deal that could have been worth as much as $1.5 million. Reportedly, the gang members were acting as intermediaries and already had buyers from the Middle East lined up.[3] Six members of the same group were arrested in December 2001, while trying to sell 1.068 kilograms of uranium for $30,000.[4] In yet another case in September 2002, six members of an organized crime group were arrested in Krasnodar Kray while trying to sell 40 kilograms of mercury and radioactive materials.[5] Cases of organized crime

involvement in nuclear material trafficking have also occurred in various parts of Ukraine, including Odessa and Dnipropetrovsk.

- *"Comrade criminals."*[6] Some officials in nuclear cities, nuclear installations, nuclear storage sites, and nuclear laboratories almost certainly have links with organized crime. Others, however, seek to go into business for themselves. One such case occurred in August 2003 when Alexander Tiulyakov, deputy director of Atomflot, was arrested in Murmansk by undercover agents as he tried to sell 1.1 kilograms of radioactive material (which was probably spent fuel) for $55,000.[7]
- *Hybrid trafficking networks.* These consist of various kinds of groups and individuals operating in alliances of convenience. They are particularly difficult to track because of their ubiquity and their ability to emerge suddenly and with little warning.

Although all these particular types of players in the market (and there could be others) and their geographical routes are well-known, the dynamics of the market, the scale and frequency of transactions, the cost structure for different materials, and, most importantly, the number and type of buyers remain elusive. This is particularly disconcerting in an era when nuclear proliferation and terrorism are the two most pressing issues on the global security agenda.

Yet these known criminal networks pale in significance when compared with the network created by Pakistani scientist A.Q. Khan. Indeed, in a remarkable and unforeseen reversal of function, the A.Q. Khan network, which had initially been created to assist in the development of nuclear weapons by Pakistan, became instead a supply network providing assistance to North Korea, Iran, and Libya. Although the core of the network was provided by Khan and B.S.A. Tahir, a Sri Lankan businessman based in Dubai, the network was extensively transnational in scope.

Transactions of one kind or another took place in Switzerland, the United Kingdom, the United Arab Emirates (UAE), Turkey, South Africa, Malaysia and several other countries. For over a decade, the network—and this is similar to other "sovereignty-free" organizations—was able to "obfuscate, even elude, the jurisdiction"[8] of the Pakistan government, the United States government, and the international nonproliferation community.

Many questions remain, of course, about the complicity of military and government authorities in Pakistan. The only real issue is whether the authorities tacitly acquiesced or actively connived with the network and its illicit commercial activities. Whatever the case, the network succeeded in identifying a space in which it was able to operate for a decade or so with little interference.

The network also exploited the facilitators of global trade, including free trade zones and the global financial system. The system's capacity to move money rapidly and anonymously, and the massive growth in global trade, makes it much easier to embed illicit trade within legitimate trade. Indeed, in some respects global trade has become more opaque rather than more transparent partly because of its volume, the number of import-export companies, the diversity of freight-forwarders, and the existence of flags of convenience which make the maritime industry itself non-transparent. Moreover, traffickers took care to avoid jurisdictions where inspection was more stringent and surveillance more intrusive in favor of more permissive countries. This is a form of jurisdictional arbitrage that is very familiar to those who study organized crime. In this connection, "the international free zone in Dubai, through which shipments are still subject to few meaningful controls, was particularly critical to the network. Indeed, most items found in Libya were transported through Dubai, in some cases more than once."[9]

In effect, nonproliferation was trumped by globalization. Production capabilities for nuclear weapons development became merely another set of commodities to be moved and sold like any other. Although the scope of Khan's operations was revealed in a series of investigations following the interdiction of the ship *BBC China*, the Libyan decision to abandon its nuclear program and open its facilities to inspection further demonstrated the extent of the Khan network.

It is not surprising, therefore, that many observers remain concerned that the A. Q. Khan network has not been fully dismantled; it is also possible that the network is simply one of several that existed and the others continue to operate below the radar. Even if this is not the case, observation of other criminal and black market networks suggests that even when a network is very seriously degraded it can still regenerate itself. This capacity is often accompanied by an ability 1) to adapt in ways that overcome or circumvent constraints, 2) to morph into new forms that are difficult to detect, and 3) to learn from mistakes. Consequently, the privatization of nuclear supply networks is likely to continue to pose a major challenge to efforts to maintain the nonproliferation regime.

This brief and inevitably superficial survey of the evolution of nuclear proliferation reveals several distinct trends:

- the inability of the United States and the international community to maintain an effective nonproliferation regime;
- the growing difficulty of controlling technology diffusion in an era of globalization and dual-use technologies;
- the increased role of non-state actors, be they a) networks of scientists driven by desires for personal enrichment, senses of obligation to support Islamic nations seeking to augment their military power, or resentment toward U.S. efforts to control the spread of nuclear weapons, or b) criminal networks concerned only with profit.

Against this background, it is necessary to examine the role of the United States intelligence community in responding to the new challenges of what might be termed complex nuclear proliferation.

Nuclear Proliferation as a Complexity Problem for Intelligence

As nuclear proliferation has become a more serious and urgent problem—both in terms of actual and would-be proliferators and the increased diversity of proliferation channels and methods—the performance of U. S. intelligence in meeting the challenge has appeared to be increasingly inadequate. The failure to foresee the Indian nuclear test, the underestimation of the Iraqi nuclear program prior to the Gulf War of 1991, the over-estimation of Iraq's program prior to the U.S.–led invasion of 2003, and the failure to detect many of the activities of the A.Q. Khan network throughout the 1990s all suggest that major efforts need to be made to reform the intelligence community in general and its handling of the problems of nuclear proliferation (and terrorism) in particular.

The focus of public attention has largely been on the false positives that appeared to justify the invasion of Iraq. Yet, it is arguable that the failure to provide early detection of the operations of the A.Q. Khan network was an equally important intelligence failure—and one where the constraints on intelligence collection and analysis were not as formidable as in Iraq. At the same time, the failure to detect the activities of the Khan network is understandable. The proliferation environment has changed significantly, becoming much more complex and posing more difficult challenges than in the past.

Unfortunately, assumptions, ways of thinking about challenges and threats, and methods of analysis are not that different from those that dominated earlier phases of proliferation. As one judicious study pointed out,

Although U.S. intelligence agencies have made some progress in tracking the proliferation problem, efforts in this area remain a challenge, and the risk of a substantial surprise continues to grow. As weapons-related technologies spread and information flows over time, proliferators have become more adept at concealing their activities. Reducing the risks and consequences of

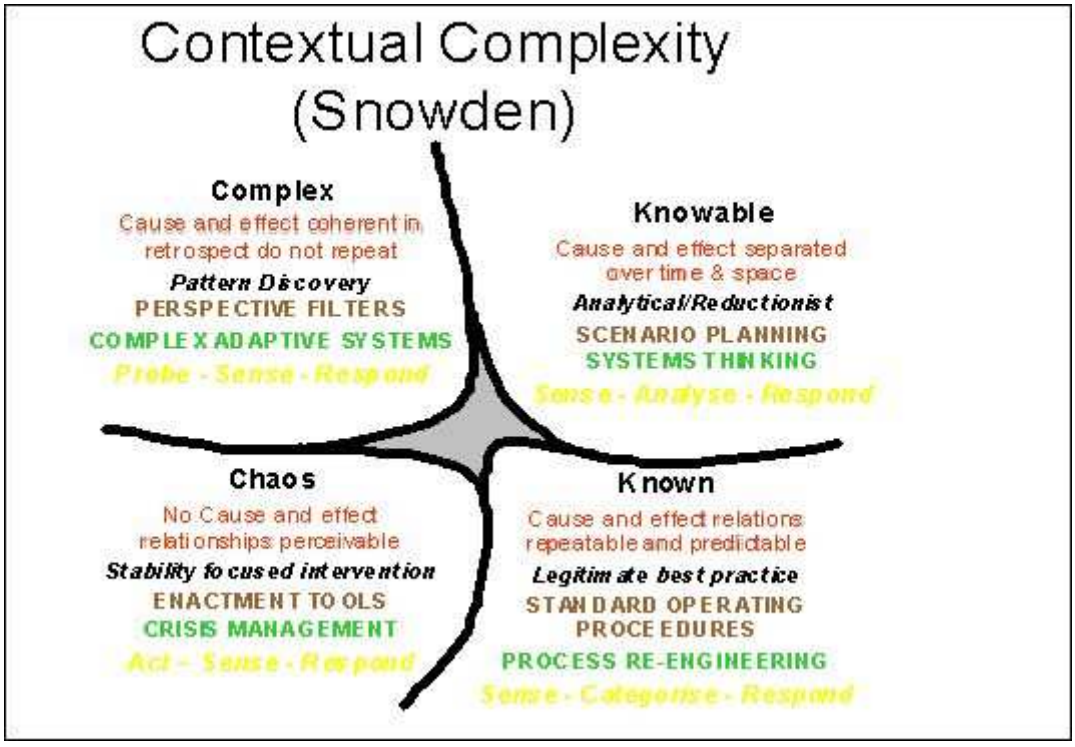
surprise requires intelligence agencies to adapt to this rapidly changing environment, retooling collection capabilities and analytic processes.[10]

Some of the ways in which this might be done have been captured in an analysis by David Snowden. Although Snowden's focus is primarily on management and information science, his insights about the acquisition and management of knowledge are enormously relevant to the world of intelligence analysis.[11] So too is his argument that

the conceptual changes required for both academics and management are substantial, effectively bounding or restricting over a hundred years of management science in a similar way to the bounding of Newtonian science by the discoveries and conceptual insights of quantum mechanics et al in the middle of the last century. These changes are not incremental, but require a phase shift in thinking that appears problematic, but once made reveals a new simplicity without the simplistic and formulaic solutions of too much practice in this domain.[12]

According to Snowden, this paradigm change or conceptual shift is essential because of the shift from known and knowable environments where there is order to environments in which there is "un-order" characterized by complexity or by chaos. These four domains—along with the approaches required to respond to or cope with each one of them—are explored and elucidated by Snowden in the following figure [Figure 1].

Figure 1: Contextual Complexity[13]



In Snowden's judgment, both the known and knowable domains are analytically tractable. Surprise can certainly occur, especially in the knowable domain where many things are still undiscovered and there is a natural tendency to assume that existing, well-understood, and precisely delineated patterns of behavior will continue into the future—without sufficient consideration of change or novelty within the domain itself. With caution and care, however, the potential for surprise can be minimized. Intelligence analysts can be expected to get their forecasts right most of the time. When the domains shift to complex and chaotic, however, the

difficulties of forecasting or anticipating become immensely more difficult. It is the difference between predicting Soviet strategic behavior during the Cold War—which was known and knowable—and predicting the collapse of the Soviet Union at the end of the Cold War. The dynamics of political and economic collapse were not well understood, and with the focus on the monolith itself, the cracks in the foundation were given little attention. Yet, the enormity of this task should not really be surprising. State or system collapse is a highly complex phenomenon and complexity can be difficult to comprehend and navigate, let alone to predict or anticipate. In effect, a world of complexity is full of surprises.

Complexity theory or complexity science, as it is sometimes known, is most commonly associated with work done at the Santa Fe Institute. It is a radical departure from the traditional reductionist approach to science that involves breaking things down into their constituent parts. Instead of constantly disaggregating, complexity theory adopts a systems-level approach that focuses on the interactions of parts. In effect, it offers an alternative to Newtonian science and its laws that explain readily predictable behavior. Complexity theory, in contrast, deals with unpredictable or non-linear behavior and outcomes. As such, complexity theory has significant implications both for thinking about and analyzing nuclear proliferation.

Ideas that come from complexity theory include, but are certainly not confined to: the notion of holistic analysis, which requires understanding that a system, whether an ecosystem or a threat system, is much more than the sum of its parts; the centrality of networks, connections and interactions; and the idea of emergent behavior, which suggests that emergent threats are particularly elusive and intractable. Complexity itself is best understood as the space or domain between chaos and order. It can move in either direction, often as a result of small changes. This is why complexity is sometimes described as being located at the “edge of chaos” or as the zone between chaos and order.[14]

A key theme in complexity theory is that the system as a whole has to be the focus of considerable attention. As Baruch Blumberg noted, “for nonlinear systems the whole is greater than the sum of the parts, and they can only be understood by examining ‘global’ behaviors in addition to the individual agents of which they are comprised.”[15]

A complex system is also a non-linear system in which “small inputs can lead to dramatically large consequences,” something that is often summarized as the butterfly effect.[16] Moreover, these effects can differ dramatically since “very slight differences in initial conditions produce very different outcomes. That’s the basis of their unpredictability.”[17] Outcomes depend critically on the context or the initial conditions surrounding the starting point.

Transitions are an important part of complexity theory and can be understood as what are sometimes termed “phase changes” or “tipping points.”[18] This is a notion popularized by Malcolm Gladwell in a study that seeks to explain a variety of phenomena ranging from epidemics to fashion trends, a form of social contagion involving imitative behavior.[19] Gladwell emphasizes that little changes can have big effects and can tip the system from one condition to another.

Complex systems are characterized by self-organization and emergent behavior. Self-organization involves tacit rather than explicit coordination and does not require leadership or top-down hierarchical structures. The notion of emergent behavior also contains the idea of learning and, by implication, the learning organization. Emergent systems create a complex global order out of very simple decision rules. But as order evolves, the decision rules can become more sophisticated. The idea of adaptability and, in the context of organizations, the notion of organizational learning, is critical—and highly relevant to the understanding of transnational threats.

A corollary of adaptation is co-evolution, a phenomenon that is ubiquitous in nature. As Mark C. Taylor has written, “Since complex systems are adaptive, their evolution tends to be co-evolution. When systems as well as networks adapt to systems and networks that are adapting to them, change is necessarily correlative.”[20] Examples of this are “parasites, symbionts and tightly coupled dances” such as that between the parasite and the milkweed.[21]

A closely related feature of complexity is the notion of inter-connectedness. This manifests itself largely through networks, which can be understood as one form of emergent system. Indeed, the notion that networks are a sub-component of complexity theory has been most fully articulated by Barabasi, who in the last few years has provided some very illuminating analyses of the topologies of networks and how some are more resilient than others in the face of external attacks on the network.[22]

Another concept in complexity theory relevant to the tasks of intelligence is the notion of a fitness landscape and fitness peaks. “A fitness landscape is a mountainous terrain showing transition locations of the global maximum (highest peak of fitness) and global minimum (lowest valley). Fitness is a biological concept which describes the relative ‘success’ of a species in relation to others in its environment.”[23] The height of a feature becomes a measure of its fitness.

Because complexity theory deals with unpredictable, non-linear behavior and outcomes it has appropriately been described by John L. Casti as “the science of surprise.”[24] Casti’s analysis is a useful complement to that of Snowden in that it explicitly differentiates between simplicity (known and knowable in Snowden’s terms) and complexity. According to Casti, simple systems are those in which behavior is predictable and there are no surprises. “Complex processes, on the other hand, generate counterintuitive seemingly a-causal behavior that’s full of surprises.”[25] Part of the reason is that simple systems generally involve a small number of components with few interactions among them. There are few feedback loops that accentuate stress, change, or instability and thereby generate a wider range of behavior and outcomes. Complex systems, in contrast, exhibit significant feedback loops, as well as random interactions among components. The result is unexpected, but far-reaching, consequences and unanticipated, but serious, problems.[26] Another difference is that simple systems generally involve centralized decision making, whereas complex systems are usually characterized by a diffusion of authority and power.[27] Moreover, in a complex system, outcomes from the interactions of parts are very sensitive to changes in the initial conditions or context—which is one reason why pattern detection is so difficult and why efforts to discover new patterns are essential. Yet another source of surprise is emergent behavior that in scope and direction differs from anything that has preceded it.

Indeed, from the general discussion of complexity offered above and the analysis provided by Casti, it is possible to identify four major sources of surprise—each of which is highly relevant to nuclear proliferation.

Paradoxical Outcomes

The first source of surprise has been described by Casti as logical tangles leading to paradoxical conclusions, exacerbated by complex interdependencies. In effect, this translates into the counter-intuitive proposition that positive governance mechanisms have negative consequences that sometimes outweigh any benefits. The implication is that the nonproliferation regime might encourage, rather than discourage, nuclear proliferation. Indeed, for any state with serious anti-hegemonic pretensions, challenging the nuclear nonproliferation regime is essential. From this perspective, nonproliferation regimes and restrictive policies might actually create demand.

Moreover, the tendency to think in terms of regimes—critical to United States policy—can itself create blinders. A regime imposes constraints that, from a complexity perspective, are self-

defeating. Rather than being understood as a set of norms and rules that all parties can be expected to observe, the nonproliferation regime is better understood as a set of restrictions that generate market mechanisms, processes, and incentives. Over time, these mechanisms, processes and incentives will lead to behavior that invariably circumvents or erodes the regime. In a sense, the nonproliferation regime is similar to sanctions or embargoes imposed on conflict situations. The very act of restricting things that are in demand—in this case nuclear weapons, strategic materials, or nuclear production capabilities—increases their value and encourages new suppliers to enter the market. From both market and complexity perspectives, therefore, the nuclear nonproliferation regime contains the seeds of its own destruction. Moreover, an enhanced nonproliferation regime that really imposes effective constraints on indigenous production of nuclear weapons could result in the theft or purchase of a nuclear weapon by a proliferating state or terrorist organization as the only alternative available.

Discontinuity and Tipping Points

Casti's second mechanism is discontinuity from smoothness. He describes this mechanism as catastrophes, but it can be more broadly reformulated in terms of the "tipping point" analysis enunciated most effectively by Malcolm Gladwell. Indeed, Gladwell's analysis shows how small changes can have big effects and create a transition from stable disease patterns to epidemics. The analogy can be applied to proliferation. While critics might dismiss notions of a proliferation epidemic as hyperbole, the 1990s clearly saw a marked change in proliferation dynamics. Back to Gladwell's analysis, key figures with special qualities can have a major impact in creating a tipping point. In the case of HIV/AIDS, for example, a highly promiscuous Canadian flight attendant acted as a "super-spreader." A.Q. Khan played a very similar role as "super-spreader" of nuclear weapons production capabilities and know-how during the 1990s, the full impact of which is still being assessed. Khan introduced a major new dynamic into the proliferation environment—and it would not be surprising if others tried to imitate and emulate his activities.

Irreducibility of Systems

A third source of surprise stems, in Casti's terms, from the irreducibility of systems. Since any system is more than the sum of its parts, it creates outputs and outcomes that are not obvious from a perspective that focuses at a sub-system level. The implication is that proliferation can be understood as a system. Its constituent parts include a wide array of suppliers, many of whom are sub-contractors; technologies, tools and materials that are essential to the process of nuclear weapons development; those states and sovereignty free actors who want to acquire nuclear weapons; and a series of middle-men whose role is to link demand and supply.

Moreover, if we accept the idea of co-evolution between proliferation dynamics and processes on the one side, and the nonproliferation regime or system on the other, then the two systems can be understood as being in competition in the fitness landscape. The problem is that the proliferation system—which consists of a complex mix of players operating according to market dynamics and through network forms of organization—is doing better in terms of its evolution in the fitness landscape than is the nonproliferation system, even taking into account efforts such as the Proliferation Security Initiative designed to strengthen and enforce restrictions. Put more simply, governments, international norms, and regimes are always trying to catch up with a rapidly changing reality. The capacity of the proliferation system to morph in ways that are unexpected will continue to be a source of surprise.

Emergent Behavior and Morphing Networks

A fourth and closely related source of surprise stems from emergent behavior and emergent networks. Once again, the Khan network is a case in point. The network morphed from an acquisition and procurement network into a supplier network that was able to operate largely

under the radar before coming to the attention of British and United States intelligence agencies. Khan and several close associates acted as the critical nodes in a network that evolved to meet market demand and that facilitated a series of commercial transactions that circumvented the nonproliferation system. Although concerns about rogue scientists had been evident ever since the collapse of the Soviet Union, the focus was on their scientific expertise on behalf of states intent on acquiring nuclear weapons, rather than their business sense and commercial acumen in acting as suppliers of production equipment and knowledge.

Intelligence Responses to Complex Proliferation

The preceding analysis not only accentuates the distinctions made by Snowden, but also clarifies the differences between the proliferation environment of the 1960s and 1970s—which was largely about alliance management—and the proliferation environment of the 1990s and the present. Today, the proliferation problem is more diffuse and less tangible, and those involved are an increasingly diverse set of actors, many of whom are highly adaptable and adept at denial and deception. In this environment, the challenges confronting the intelligence community are more formidable than ever. One of the first steps in responding to these challenges is to extend the old Sun Tzu adage about knowing the enemy to understanding the environment. To achieve this, it is essential to think in terms of complexity.

The ideas in complexity theory provided above could assist us in the way we think about and analyze nuclear proliferation.[28] Complexity theory can be helpful both as a heuristic device and as a more direct way of understanding the current phase of nuclear proliferation. This is not to claim that it is any kind of silver bullet. Indeed, the nature of the theory itself makes clear precisely why there is no silver bullet. Nevertheless, it is possible to obtain a better understanding of an environment characterized by complexity. In effect, moving from Casti's simple systems to complex systems—or from the known and knowable domains of Snowden's scheme to the complex (and potentially the chaotic) domain—requires changes both in thinking and in methods of analysis, as well as the adoption of a probing methodology that helps in making sense of the environment.

Ways of Thinking

One key way of thinking is to create both individual attitudes and organizational cultures which emphasize what Weick and Sutcliffe, in *Managing the Unexpected*, termed mindfulness. As they note, "People who persistently rework their categories and refine them, differentiate them, update them and replace them notice more and catch unexpected events earlier in their development. That is the essence of mindfulness."[29] Intelligence analysts constantly need to re-examine and refine, or reject, the concepts, categorizations, and implicit models they use to understand the world.[30] This is highly pertinent to some of the surprises discussed above. The morphing of the Khan network from an acquisition network to a supplier network, for example, might have been picked up sooner if analysts were challenging and refining their own assumptions and concepts. In terms of thinking about the future evolution of proliferation, there are several ways in which explicitly challenging assumptions could generate important insights that make surprise less likely. Although it is impossible here to provide an exhaustive list, several pertinent examples might be useful in challenging some of the orthodoxies and thinking more creatively about nuclear proliferation.

Is the distinction between legitimate and illicit transactions of much value in a world where the product is less important than the recipient? In the cases of many dual-use technologies, it is only the diversion to a particular end user that is problematic. How can this best be captured and accounted for in monitoring commodity and equipment flows pertinent to nuclear proliferation?

In terms of end users, is it really beyond the capacity of a terrorist network to develop and deploy a nuclear weapon? Most analyses seem to assume that only a government has the capacity to develop nuclear weapons. Indeed, after September 11th, some observers doubted that a network was capable of planning and implementing such an attack and that a state had to be responsible. Yet, networks are not only highly adaptable, but also have an ability to concentrate resources when necessary. Consequently, it would be a major mistake to continue to underestimate networked adversaries. Moreover, it would be dangerous to assume that such networks are not linked in some way to sympathetic, though not necessarily sponsor, states. Saudi financing, for example, played a major, though still not fully acknowledged, part in financing al Qaeda prior to September 11th. Is it inconceivable that a similar network could not emerge to assist a terrorist network in going nuclear?

In a world of complex proliferation, what kinds of cascading effects might be expected in the future, and to what extent might these differ from those of the past? Cascading effects in the nuclear proliferation world have been evident, albeit with long lead times, in the Chinese, Indian, and Pakistani nuclear weapons developments. What kind of shorter, more intense proliferation cascades might emerge in the future? How can these be prevented or managed to maintain a semblance of stability?

Following the earlier discussion of surprise, it is necessary to think much more explicitly about both buyers and suppliers in a nuclear proliferation system. Specifically, consideration needs to be given to those entities, both state and non-state, seeking to acquire nuclear weapons, as well as those entities—states, firms, individuals, and criminal organizations—that wittingly or unwittingly, become involved in the supply of knowledge, materials, or production equipment that facilitate the acquisition of nuclear weapons. Moreover, the nuclear proliferation system is co-evolving in a fitness landscape with nonproliferation policies, strategies, norms, and institutions. Consequently, it is adapting in ways that circumvent the constraints and restrictions imposed by nonproliferation efforts. Its continued ability to do this depends on the relative capacity of each side for learning.

How might proliferation networks morph in the future? It is clear that proliferation networks and their relationships, commodity flows, and financial flows constantly morph in response to pressures and opportunities. One possibility, therefore, is to think in terms of multiple networks—each with its own distinct characteristics and approach (within technological constraints) to facilitating nuclear weapons development. In a world of inter-connectedness, it is also necessary to consider the possibility of some kind of association or linkage between criminal networks which have obtained access to fissionable material and a network akin to that of A.Q. Khan.

How feasible is a “tipping point” or phase transition in the nonproliferation system, one that could, under some circumstances, be one of collapse (a phase-change) into chaos and unrestricted nuclear proliferation? Alternatively, an awareness of how dangerous the system is becoming could lead to the imposition of a new order that successfully re-imposes meaningful constraints and restraints on potential proliferators. What are the positive consequences of a bad outcome for nonproliferation? Conversely, what are the negative consequences of a stronger, more inclusive regime?

These issues and questions are far from exhaustive. In most cases, they need to be refined by those with far more detailed knowledge and expertise about nuclear proliferation. The crucial point, however, is that thinking in complexity terms requires constant questioning—not only about the environment, but also about the assumptions underlying analyses of the environment. Complex proliferation also requires analytic approaches that challenge existing assumptions and consider a wide variety of possible developments and outcomes.

Methods of Analysis

Three methods of analysis stand out as relevant to analysis of nuclear proliferation. These may be termed zero-based analysis, multiple alternative competing hypotheses, and strategic network analysis.

Zero-Based Analysis. Zero-based analysis is a technique that could help prevent previous analytic inertia (and especially previous assessments) from dominating the intelligence process.[31] It is an approach to analysis that takes nothing for granted, does not assume that the future will necessarily be like the past, and starts from a fresh set of assumptions. At the same time, it does not try to avoid the mistakes or shortcomings of previous analysis and assessments. Over-reacting to the previous "failure" is as rooted in the past as continuity of assumption and assessment.

It is also an approach that runs directly counter to the prevailing methodology in much of the intelligence community. As Dennis Gormley has noted,

The most conspicuous features of this methodology are the historical, social and organizational influences that shape the outcome. Looking to what has been written before (quite often products authored by an intermediate supervisor), instead of first collecting data and formulating multiple hypotheses, biases the analyst toward an accepted organizational response. Social pressure is also likely to play into any analytic process that relies heavily on group brainstorming to verify a particular analytic line of reasoning.[32]

Rob Johnston makes a similar point in his work on analytic culture in the U.S. intelligence community. In Johnson's view, one of the major problems of intelligence analysis is "confirmation bias" in which analysts tend to develop "a mental model based on previous corporate products" and then try to "augment that model with current data in order to support the existing hypotheses."[33] Zero-based analysis provides an important and legitimate counter-weight to both overt pressures to conform and more subtle incentives "to maintain a corporate judgment."[34] It also avoids a form of intellectual blindness resulting from continuity and incrementalism rather than discontinuity and paradigm shifts. Although it has costs both in the expenditure of intellectual energy (which in some cases would be devoted to re-inventing the wheel) and in taking analysts out of their comfort zone, these are costs worth incurring. What might initially appear to be re-inventing the wheel would more often than not be an intellectual validation of the wheel's utility and appropriateness rather than a simple reaffirmation of faith.

Zero-based analysis is the antithesis of faith-based analysis, the conventional wisdom, and the corporate judgment. It also makes it easier to recognize non-linear developments, and better enables analysts to make accurate judgments and forecasts. In effect, it is an analytical technique that seeks to operationalize the concept of mindfulness and to ensure that the constant challenging of assumptions is invariably a key part of analysis.

A zero-based analysis of proliferation networks, for example, would ask the following questions related to the A.Q. Khan network:

- Is it clear that the A. Q. Khan network has been completely destroyed, or is there a likelihood that important remnants continue to operate and that the network can regenerate itself?
- Are there A.Q. Khan clones, A.Q. Khan "wannabes" and A.Q. Khan network variants or successors out there? If so, who are the members and where and how are they operating?
- Is it possible that a major organized crime network will become heavily involved in nuclear material trafficking? Could it obtain both the expertise to identify and obtain access to weapons-grade material and the contacts to find ready customers either among states and their intelligence agencies or among terrorist organizations?

- What are the possibilities of an alliance of convenience among rogue scientists and members of organized crime?

Such questions are not meant to be exhaustive, but simply to illustrate the kinds of questions that need to be asked as part of zero-based analysis.

Multiple Alternative Competing Hypotheses. A second approach to the incorporation of complexity into analysis involves the development of multiple, alternative competing hypotheses. This notion is merely an extension of Richards Heuer's emphasis on the need for alternative competing hypotheses. It combines Heuer's methodology, however, with an appreciation that change can be gradual and incremental or revolutionary, non-linear, and discontinuous—and that it can either alleviate or exacerbate security threats.

When added to the prospect of things continuing more or less as they are, it requires the analyst to develop at least five scenarios for any future problem. The addition of at least one wild-card scenario that involves some kind of complex interdependency, different from the positive and negative non-linear change scenarios, brings it to six scenarios. With added consideration given to negative consequences of positive scenarios and positive consequences of negative scenarios, the approach requires development of at least eight different possible outcomes. The objection to this approach, of course, is that the drains on the analyst's time and energy are likely to be prohibitive. Yet this should not be a deterrent to the analyst. The purpose of the multiple scenario approach is not to provide an exhaustive account of each scenario. Rather, it is to sensitize analysts to the likelihood of non-linear change and some of the forms this might take. In terms of proliferation, particular consideration needs to be given both to negative revolutionary changes—such as the collapse of the nonproliferation regime or the terrorist acquisition of nuclear weapons—as well as positive revolutionary changes such as the development of technologies which greatly enhance the capacity for tracking the operation of the nuclear market-place.

The problem is that this approach requires the expert to put his expertise aside, an enormously difficult task given the massive investment they have made in developing that expertise. He needs to step out of his comfort zone and adopt a systematic methodology designed to elicit pattern discovery rather than relying on the intuitive pattern recognition that is a key component of expertise. Nevertheless, in a complex world characterized by non-linear change, multiple alternative competing hypotheses, or multiple scenarios, approach is an essential method in complexity analysis.

Strategic Network Analysis. The third approach to the analysis of complex proliferation is to engage in strategic network analysis, focusing on the networks through which strategic materials, production capabilities, and expertise flow to the end users. As suggested above, networks are a key component of complexity and provide the infrastructure for the flows of commodities, expertise, and money that are integral to the proliferation process. The networks can be criminal networks such as those described in the introduction to this article, or illicit networks based largely on commercial considerations and organized around a relatively small number of critical nodes or super-hubs like the A.Q. Khan network. A 1994 article co-authored by Phil Williams and Stephen Black compared drug trafficking and weapons proliferation. It emphasized the extent to which the nonproliferation regime had already been undermined "by the operation of a market involving both licit and illicit businesses."[35] It also noted that "the participants in the WMD market form supply networks that are able to circumvent complex, multi-layered export control regimes and move the most advanced technology to the consumer state with near impunity. And, when an individual supply or front organization link is closed down by export enforcement agents, another is ready and willing to replace it."[36] Although when they wrote this the authors had no knowledge of the Khan network, revelations of the last few years have only underscored the accuracy of this description.

Against this background, one of the key tasks for analysts of proliferation is to map the proliferation supply network of A.Q. Khan, to consider the redundancy in the network, and to see to what extent the network might provide a prototype for and harbinger of future proliferation networks. All this could be considered as little more than the application of traditional social network analysis to proliferation. Where strategic network analysis differs, however, is its close and explicit relationship with efforts to degrade the network. In the case of Khan's network, the degradation seems to have been belated but effective. In future cases, however, efforts to analyze and attack proliferation supply networks not only have to occur earlier in the life of the networks but also be part of a holistic process involving iterative efforts at degradation. This can be achieved through the exploitation (e.g., for monitoring communications) or the removal of critical nodes, network damage assessments to guide follow-on attacks, and efforts to minimize the prospects for network recovery and regeneration. The interdependence of mapping and the attacks is central. More accurate network mapping will be achieved through a mixture of targeted node removal and analysis of the network response. Such an approach can be understood as probing the network, and it is to Snowden's concept of probing that attention must now be given.

Probing Complexity

As Snowden has pointed out, in a complex system or complex environment, cause and effect are not readily distinguished, independent and dependent variables merge into interdependent variables, and it is only in retrospect that a coherent picture can be determined—a phenomenon that he terms "retrospective coherence."[37] At the same time, it is possible to identify and even influence interactions—partly through probing behavior—and discern emergent patterns. "In a complex space we cannot sense and respond, but must first probe the space to stimulate pattern understanding or formation, then sense the patterns and respond accordingly."[38]

Taking this injunction and applying it to complex proliferation, it is possible to identify at least three kinds of probing strategies and targets: 1) probing the market in ways that help determine the dynamics of both supply and demand and elicit knowledge about the operation of supplier networks.2) creating market perturbations that lead to adaptive responses, the patterns of which can be delineated and assessed; and 3) probing the supply networks to identify critical nodes and connections, determine degrees of redundancy and resilience, and identify ways in which the networks morph when under pressure.

Perhaps the most effective way of probing the illicit nuclear proliferation market is to engage in undercover operations. Such operations can prove critical in obtaining information and developing knowledge about the market, the key players, key financial transactions, and transportation routes and methods. Undercover operations could help clarify: the nature and extent of networks of traffickers and legal companies which provide machine tools and other goods necessary for nuclear weapons development; the modes of transportation and the methods of concealment or diversion; the ways in which traffickers and commercial firms link up with buyers; and the kinds of prices that prevail for certain kinds of materials and equipment. Such operations can utilize informants, controlled deliveries, front companies, ostensible financial institutions to provide services to the proliferation networks, and infiltration of the scientific and business communities. Although all these approaches can be helpful in knowledge acquisition, probably the most far-reaching undercover operation the controlled delivery. This technique allows the process to be traced from initial supply to final customer and, if done well, can provide enormous insight.

A second approach is to create perturbations. This can be achieved through seizures and interdiction that are carried out not for their denial effects, but for the adaptive responses they generate in those involved in nuclear proliferation. With care and effort, it might be possible to discover the patterns inherent in such responses and, from there, discern broader patterns of behavior. Creating perturbation, of course, requires a certain knowledge base in order to be effective and, therefore, is likely to follow, rather than precede, probing designed for knowledge elicitation.

A third approach is to probe the supply networks, identifying and removing critical nodes, and observe how the network reacts to the attack. For example, the removal of a supplier of key parts will provoke a search for substitute suppliers, substitute parts, or alternative production methods. It is important to emphasize that probing the network in this way is not synonymous with degrading the network. Rather, is it an attempt to provoke the network into actions that inadvertently reveal key aspects of its topology, functional and role specialization, degree of clustering, capacity for adaptation, and the like. In this sense, as suggested in the discussion of strategic network analysis, probing will often be a precursor to more effective degradation strategies based on greater knowledge and understanding.

Although these probing approaches might appear to be little more than the adoption of law enforcement strategies and tactics, they reflect two realities: the success of law enforcement in developing very effective methods of probing the criminal environment and the need to treat the problem of nuclear proliferation as a complex criminal market rather than simply as a technological, strategic, or diplomatic issue.

Conclusion

The 9/11 Commission concluded that one of the great problems with the United States intelligence community was a lack of imagination. Applying complexity theory in relation to transnational threats in general, and nuclear proliferation in particular, is useful for several reasons, not the least of which is that it encourages a more imaginative approach to intelligence. It also generates greater insight and understanding of the current proliferation challenge and recognition that both criminal trafficking networks and the Khan network are manifestations of a new reality in a novel and more intractable environment. At the same time, complexity theory cautions that however good the analysis and however effective the probing mechanism, in a world of complexity, surprise is both endemic and inevitable. Perhaps the most that can be done, therefore, is to reduce the frequency of surprise and its strategic significance. To succeed in doing this in the realm of nuclear proliferation would at least be an improvement on the recent record of the intelligence community.

About the Author

Dr. Phil Williams is Professor of International Security in the Graduate School of Public and International Affairs at the University of Pittsburgh. From 1992 until April 2001, Dr. Williams was the Director of the University's Matthew B. Ridgway Center for International Security Studies and he is currently the Director of the Ridgway Center's Program on Terrorism and Transnational Crime. Professor Williams has published extensively in the field of international security including *Crisis Management*, (1976) *The Senate and US Troops in Europe*, (1986) and (with Mike Bowker) *Superpower Detente: A Reappraisal* (1987). He has edited or co-edited books on the Carter, Reagan, and Bush Presidencies, as well as on Classic Readings in International Relations. During the last ten years his research has focused primarily on transnational organized crime and he has written articles on various aspects of this subject in *Survival, Washington Quarterly, The Bulletin on Narcotics, Temps Strategique, Scientific American, Criminal Organizations*, and *Cross Border Control* . In addition, Dr. Williams is editor of a journal titled *Transnational Organized Crime.*

He is a consultant to both the United Nations and United States government agencies on organized crime and transnational threats and has also given congressional testimony on the subject. Most recently he has focused on alliances among criminal organization, global and national efforts to combat money laundering, and trends and developments in cyber-crime. Dr. Williams has edited a volume on *Russian Organized Crime* and a book on *Illegal Immigration and Commercial Sex: The New Slave Trade*. He is also co-editor of a recent volume on *Combating Transnational Crime*. He is currently completing a book for Polity Press on *Transnational*

Organized Crime. In 2001-2002 he was on Sabbatical from the University of Pittsburgh and was a Visiting Scientist at CERT/CC Carnegie Mellon University, where he worked on computer crime and organized crime. Dr. Williams is currently directing a project for the Defense Intelligence Agency on the Financing of Terrorism. He is also focusing on methods of degrading criminal and terrorist networks.

References

1. "Portuguese Police Detain Suspected Uranium Smuggler," *Agence France Presse*, July 11, 2002; see also "Portuguese 'Dirty Bomb' Pastor to Stay Behind Bars," *Agence France Presse*, July 12, 2002.

2. L. Zaitseva, "Illicit Trafficking in the Southern Tier and Turkey Since 1999: A Shift from Europe?" *The Nonproliferation Review*, Fall/Winter 2002, 168-182.

3. "Russian Police Apprehend Illegal Cesium Deal," *BBC Worldwide Monitoring*, March 10, 2001; see also "Russian Police Arrest Cesium-137 Smugglers," *BBC Worldwide Monitoring*, March 31, 2001.

4. "Police Investigate Source of Enriched Uranium Seized from Criminal Gang," *Daily Report: Central Eurasia*, CEP20011206000300, December 6, 2001.

5. "Russian Crime and Corruption," *Daily Report: Central Eurasia*, CEP20020920000423, September 20, 1002.

6. See Stephen Handelman, *Comrade Criminals* (New Haven: Yale University Press, 1995).

7. V. Gudkov, "Atomflot Deputy Director Sold an Atom Bomb," *Current Digest* 55 (October 29, 2003) 7.

8. The analysis here uses James Rosenau's words, even though he was not referring to the Khan network but making a generic observation about sovereignty-free actors. See James N. Rosenau, *Turbulence in World Politics* (Princeton, N.J.: Princeton University Press, 1989).

9. David Albright and Corey Hinderstein, "Unraveling the A.Q. Khan and Future Proliferation Networks," *Washington Quarterly* 28, no.2 (Spring 2005) 120.

10. Center for Counterproliferation Research, National Defense University, "*At the Crossroads: Counterproliferation and National Security Strategy*," (April 2004) 13.

11. David Snowden, "Complex Acts of Knowing: Paradox and Descriptive Self-Awareness," *Journal of Knowledge Management* 6, no. 2 (May 2002).

12. *Ibid.*, 2.

13. *Ibid.*, 5.

14. See Roger Lewin, *Complexity: Life at the Edge of Chaos* (Chicago: Chicago University Press, 1999).

15. Quoted in Peter Coveney and Roger Highfield, *Frontiers of Complexity* (New York: Fawcett Columbine, 1995), xi.

16. Lewin, *Op. Cit.,* 11.

17. *Ibid.*

18. Chris Langton, quoted in Lewin, *Ibid.,* 17.

19. Malcolm Gladwell, *The Tipping Point* (Boston: Little, Brown, 2000).

20. Taylor, 188-9.

21. Kevin Kelly, *Out of Control: The New Biology of Machines, Social Systems, and the Economic World* (Cambridge, MA: Perseus, 1994), 75-6.

22. A.L. Barabasi, *Linked: The New Science of Networks* (Cambridge, MA.: Perseus, 2002).

23. Arthur Battram, *Navigating Complexity* (London: The Industrial Society, 1999), 210.

24. John L. Casti, *Complexification: Explaining a Paradoxical World through the Science of Surprise* (New York: Harper Collins, 1994).

25. *Ibid.*, 271.

26. *Ibid.*

27. *Ibid.*

28. For a more complete discussion of some of these concepts, see T. Irene Sanders, *Strategic Thinking and the New Science* (New York: Free Press, 1998).

29. Karl Weick and Kathleen Sutcliffe, *Managing the Unexpected: Assuring High Performance in and Age of Uncertainty* (San Francisco: Jossey-Bass, 2001).

30. For both this observation and the relevance of Weick's analysis, I am grateful to Warren Fishbein.

31. The author would like to express his appreciation to Davis Bobrow for suggesting this line of argument.

32. Dennis M. Gormley, "The Limits of Intelligence: Iraq's Lessons," *Survival* 46, no.3 (Fall 2004).

33. Rob Johnston, *Analytic Culture in the U. S. Intelligence Community* (Washington, D.C.: Center for the Study of Intelligence, 2005), 23.

34. *Ibid.*

35. Phil Williams and Steve Black, “Transnational Threats: Drug Trafficking and Weapons Proliferation,” *Contemporary Security Policy* 15, no.1 (April 1994) 127-151.

36. *Ibid.*

37. Snowden, *Op. Cit.*, 7.

38. *Ibid.*, 8.