Foreign Policy Research Institute

E-Notes

A Catalyst for Ideas *Distributed via Fax & Email and Posted at www.fpri.org* **December 2008**

INTELLIGENCE AND RISK MANAGEMENT

by Paul Bracken

Risk management has benefited one field after another. It has improved performance in engineering, environmental protection, finance, space flight, health care, accounting, the control of epidemics--even baseball. There can be little doubt that risk management has enhanced many fields, except one: intelligence has remained largely insulated from it.

Whatever direction the Obama administration's national security strategy takes, it will be far more *risk-centric* than the policies of recent years. Risk assessment and management will be central to any American policy because the costs of "winging it," of "going with your gut," have proven to be very high. This reality--the high price of winging it--is the reason other institutions have embraced risk management to improve their performance.

For intelligence, this leads to a new game. *Risk will take an increasingly central place in national security decision-making*. The intelligence community needs not only to be aware of this, but also to design their work to better assess, clarify, and define the risks that follow from these changes. Intelligence also has to develop a more productive conversation with other operational components of national security, because it is ever more tightly linked to them. Risk management offers a powerful framework to facilitate this conversation.

This paper builds on *Managing Strategic Surprise, Lessons from Risk Management and Risk Assessment* (Cambridge University Press, 2008), which I co-edited with Ian Bremmer and David Gordon. Over two years we worked closely with risk management specialists in finance, health care, engineering, and many other fields. In addition, we worked with intelligence and security experts with great domain knowledge. The project's aim was to see how risk specialists structured their problems and what the implications were for bringing risk management into intelligence and security affairs. This paper summarizes the key insights and conclusions of the project.

RISK MANAGEMENT

The reason risk management hasn't been widely used in the intelligence community is not hard to understand. Few people have given much thought to what it is or how it could be used. The same was once true in other fields. It isn't bureaucratic resistance that's the problem. Rather, the problem is the lack of a clear statement of exactly what risk management is and why it is useful.

It is necessary to dispose of some preconceptions here. One is that risk management consists of using models and mathematical methods--for example, Value at Risk in finance, options theory (also finance), or decision and fault trees in nuclear engineering. There are many modeling techniques, and they may have useful application in intelligence.

But risk management conceived as a collection of methodological tools is much too narrow an approach. Creating a collaborative structure--for example, between intelligence and operations--is more than just disseminating narrowly focused tools. It is about managing the complex interplay that occurs in these disparate networks, of which one of the most important is risk. *The real payoff of risk management lies in its ability to foster a common language for assessing and discussing risk by the different parts of an organization*. It raises the level of conversation about risk in such a way that terms and categories have a consistent meaning.

To see this, we turn to how risk management has transformed other fields. Anesthesiologists in the 1980s paid one of the highest malpractice insurance premiums of any medical specialty. For good reason, they had the highest patient deaths from malpractice of any specialty. But in the 1990s anesthesiology got much safer. Patient deaths declined form about 1 in 5000 to 1 in 250,000 cases. For years anesthesiologists had focused on lobbying for laws protecting them from malpractice. But this approach was changed in favor of a risk-based approach that focused on patient safety. New technology was introduced to prevent common mistakes, risk maps were used to define systematic solutions, and a new organization was stood up that focused on patient safety.

The shift from legal protection to patient protection called for a framework that put patient risk at its center. This is an important point. *The big payoff came from developing a framework that focused on risk, along with distinctions and vocabulary that allowed a productive discussion about it.* This allowed a new procedure or technology to be evaluated in a consistent way. It allowed physicians to take a fresh look at their practice through the lens of managing its risks. Moreover, it allowed them to extend this conversation outside of their network, to hospital administrators, equipment vendors, and insurance companies.

This is very different from a "tools" approach to risk management. To import mathematical models into an organization where most managers don't understand them may produce an improvement here or there, but it won't lead to a productive conversation about risk in the organization as a whole because it won't supply the needed terms, distinctions, and frameworks. Likewise, it won't allow an extended conversation *outside* of the organization, to other institutions, decision makers, and technology suppliers.

RESULTS OF OUR PROJECT

The project on managing strategic surprise came up with a number of important insights.

Surprise Can *Be Managed*

Some people think that managing strategic surprise is an oxymoron. This view, while mistaken, points the way to a powerful insight: dealing with surprise is about a lot more than listing bad things that can happen. Consider what is the most fundamental strategy for risk management in business. The reason for a strong balance sheet is because experienced managers know that surprises will happen. With a strong balance sheet, shocks can be more easily absorbed. Borrowing money, protecting key assets, and renegotiating better terms are all easier for a company with a solid balance sheet.

The insight here is that there are several ways to deal with surprise. This leads to a second conclusion.

Get Away From Prediction

Prediction--that is, warning--is one way of managing surprise. But it is only one way. Assuredly, if the future could be predicted, then optimized resources could be put in place to deal with the surprise.

Academic studies of intelligence often conflate intelligence with warning. Intelligence is defined in narrow terms as the study of the success or failure of warning. Thus the myriad studies of surprise attack over the decades and the many case studies of individual warnings.

The conclusion most of these studies reach is that warning is unlikely to be accurate. Managing surprise through warning is very hard. But this insight is well known. It is difficult to understand why after so many decades of research we still find it advanced as a major insight.

There's another problem with this kind of research. It places failure at the center of analysis. Academic studies of intelligence in this vein have tended to become exercises in sophisticated cynicism. Warning is hard, certainly. But placing failure and cynicism as the center of analysis is highly destructive of energy and morale. It directs attention to only one way of managing surprise, warning, overlooking many others.

Six Ways to Manage Risk

If warning has so many problems, then what else is there? Plenty. Here is where risk management can pull together different organizations for a productive conversation about risk.

A global oil company, for example, doesn't invest all of its capital in a single country based on a prediction of political stability. In the same way, DoD doesn't predict future wars and then optimize its forces around these predictions. Indeed, very few organizations place warning at the center of their risk management.

The key is to see that there are only a small number of ways to deal with uncertainty. There are six, and only six possible ways to manage risk. Risk management amounts to balancing these to fit the problem at hand.[1] Many of these involve organizations outside of one's own. For example, in the intelligence world it may involve DoD operational commands. This is how risk management fosters a cross cutting, productive conversation. It gets people from the disparate organizations to talk to each other using a common set of concepts and distinctions. The six general approaches to risk management are:

1. *Isolating Critical Assets from Uncertainty.* This involves the hardening or protecting of key assets. Roberta Wohlstetter's classic account of Pearl Harbor was not used as a case study of how to get better warning as is commonly believed--quite the opposite. This book was less about Japanese aircraft carriers sneaking cross the Pacific than it was about a Russian surprise attack. Wohlstetter's conclusion was that because warning was unreliable, critical assets like the nuclear deterrent should be built to be survivable without it. This insight had tremendous implications for the United States. The nuclear deterrent was structured to have some major part of it survive without warning. This is one of the reasons so many nuclear missiles were built.

There are many other examples of isolating critical assets. Command-and-control aircraft are often kept back from the battlespace to protect them. Backup intelligence facilities lessen the chance that a single attack can knock out the whole system.

Isolating critical resources from uncertainty is usually quite expensive. For example, hardening of shopping centers against terrorist attack is unlikely to ever make sense, given the costs of protecting what is an open facility. So other risk management approaches are necessary.

***2. Smoothing.* This involves turning a big problem into smaller more manageable chunks. Examples include the Europe-first strategy in World War II and the debates about attacking Afghanistan and Iraq simultaneously or in sequence after 9/11. Smoothing is important because many intelligence sensors and collection systems are limited in their processing capacity. Sizing system capacity is an important investment decision. If crises and events can be smoothed, then it's possible to get away with less processing power. If they cannot, then more processing capacity is required.**

Scaling sensor and collection systems means looking at a range of possible threat scenarios to determine whether or not smoothing is possible. Risk has to be factored into any such assessment.

3. *Warning.* Viewed in terms of risk management, warning is an effort to predict conditions so that tailored responses can be used. When warning is unlikely to be good, marginal investments should be placed in other ways to manage risk.

4. *Agility.* Companies in fields as diverse as consumer products and cement have found that predicting demand (i.e. good warning) is exceedingly difficult. Consequently, they have invested in agile logistic systems rather than new warning systems. Adaptive logistics allows them to quickly switch products to meet uncertain demand.

There are many intelligence and military parallels of this as well. The shift to small satellites and UAVs means that systems can launched much more quickly than giant satellites requiring years of development. The design of modular IT interfaces, while costly, can greatly improve agility. The key point is to recognize agility as an element of risk management. Without it, one may be locked into falling back on less desired approaches, such as warning, or costly hardening of assets.

Looking at agility as one way to manage risks also points to the need to assess enemy risk management strategies. For example, network warfare offers a way to degrade the enemy's agility. The six part framework offered here can be used to map out the enemy's risk management strategy in support of our own operations against them.

5. *Alliances.* Alliances spread risk to several actors, and bring more resources to bear in limiting the consequences of a problem. Outsourcing is an example. Building a strong base of suppliers to the intelligence community lowers the risk that in house approaches might miss an important technological development.

Information-sharing alliances, agreements between component commands and intelligence agencies, and new technologies like cloud computing (which allows rapid expansion of computing architecture) all have

---

[1] My insistence on precisely six ways to handle risk probably sounds pedantic. I would allow that depending on how terms are defined it could be five, or seven, or some other number. But that number is small. The thrust of the argument made here remains the same regardless of this. See Bracken, "How to Build a Warning System," Chapter 2 in *Managing Strategic Surprise*.

important risk management aspects to them.

6. *Environment Shaping.* Managing the environment to make it less dangerous, or less unstable, is the final way to manage risk. Soft power, diplomacy, and all the rest are built on the idea of making the environment less dangerous.

In some instances the goal may be to make the enemy's environment unstable. This will often directly involve intelligence. Cyber attacks and financial warfare are two of many possible examples. The intelligence community, or at least parts of it, have moved from a supporting role to a lead operational one. Risk assessments are especially important here.

This six-part framework for risk management can be used to characterize the overall approach to handling risks by an organization. The six ways can be depicted graphically in diagrams and used as a framework for productive conversations both within and between different organizations.[2]

It also underscores that there are two broad approaches to conceptualizing risk management. One is tactical. It involves things like models and mathematical methods that have a well-grounded academic disciplinary foundation. The other is a strategic management approach. Here, risk management is conceived as developing practical steps intelligence managers can use to transform their organizations to becoming more risk centric. This requires productive conversations about risk both inside the intelligence community, and outside of it. For example, DoD, State, Treasury, DHS, etc., as well as technology suppliers need to be on the same wavelength when it comes to the strategic assessment and management of risk.

It must be admitted that we are in some ways navigating uncharted waters here. Cultural differences, compartmentalization and secrecy, and social factors can be powerful obstacles to holding this conversation across intelligence and security institutions.

But the conversation must be held. Communications, information, and data-mining technologies have raced far beyond the vertical stovepipes of Cold War authority based hierarchies for intelligence and operations. Intelligence has become tightly coupled to operations. It is now embedded in all parts of national security decision making.

The days of Sherman Kent, when the relationship between intelligence and the operational decision maker was one of arms length contact are long gone. The challenge today is to integrate organizational behavior in the face of centrifugal bureaucratic tendencies. Risk management should be one of these integrating frameworks.

You Don't Need Data To Think About Risk

This will sound like heresy to those who conceive of risk management narrowly, as a set of tools and models. But getting better concepts and vocabulary in place has a more important impact. As an example, many of the case studies in our project found that instead of talking about what's *likely* to happen, attention ought to be given to the *variance* of what could happen. The concept of variance is important. Alan Greenspan, who has experience in everything from economic policy to crisis management, makes the point in discussing his use of risk management. He calls for thinking about policy based on a range of possible outcomes--that is, the variance. The distinction between likely outcomes and the variance of outcomes is a perfect example of changing concepts as a way to institute better risk management.

Risk Management Always Goes On

Risk management is always done. It just isn't done in a systematic way.

In a global company, or the intelligence community, there may be tremendous variation in the way risks are monitored, assessed, and managed across different departments. If the work of the organization is loosely coupled, if one part does doesn't affect the other, this may be acceptable.

But the trend in intelligence is for *tighter coupling*. This presents big problems if risk assessment is conducted differently by the relevant divisions.

In our project, Uzi Arad, former Director of Intelligence for the Israeli Mossad, describes his experience in just how enormous the variation can be between military, civilian, and intelligence agencies. Words about risk mean different things to different groups. "Folk wisdom" based on long patterns of established thinking can provide the illusion of risk management.

---

[2] See *Managing Surprise*, pp. 32-38.

There is nothing wrong with having independent views, more so in the intelligence world than most others. However, this may lead to estimates with fundamentally different premises about risk--without anyone's being aware of it.

Folk Wisdom

Some truisms about risk are invoked so frequently that they serve as a signpost that deeper thinking about risk is probably needed. We call this 'folk wisdom.'

A very common response when it comes to risk is the statement that "we took a calculated risk." Whenever this phrase came up in our project we had a prepared question. "Can you show us the calculations, please?" In not one single case did anyone do so. In fact, this question irritated several officials.

Another piece of folk wisdom about risk is that "the greatest risk is in not taking any risks." In a certain sense this is true. But this saying legitimizes virtually any action, which is not very helpful in assessing what its associated risks are.

Folk wisdom about risk should be used in a positive way. It's an indication that deeper deliberation is needed.

Recent Intelligence Reforms Move in the Right Direction

The intelligence community has been restructured in recent years, notably with the creation of the office of the Director of National Intelligence (DNI). There have been many criticisms of this, but our project suggests a different conclusion.

DNI's job is horizontal integration of the intelligence community in the broadest sense. Given the huge variance in the way risk management is done across the hundreds of departments that make up the intelligence community, this is an absolute necessity. Richard Posner and others have argued that DNI only adds another decision-making layer--i.e., that it will gum up an already bureaucratic process.[3] They call for less bureaucracy in intelligence and more streamlining of decisions.

This view shows a lack of understanding of modern organizational behavior. It also overlooks what is happening in global corporations and other large organizations. As globalization, new technology, and new competitors made international business more complex, the response was to develop integration strategies and departments (like DNI). The role of integrating departments was twofold: to make sure subdivisions weren't acting in ways blind to significant risks; and to understand and respond in a coherent way to threats in the outside environment.

Absent an integrated risk management framework, individual departments would head off on their own merry way, with little regard for the enterprise as a whole. If a shock hits, performance is piecemeal. The risk environment is distorted, as bureaucratic politics determines which risks get attention.

Calling DNI another layer of bureaucracy is like saying that insurance giant AIG was right to disband their risk management group that oversaw financial derivatives (which they did) and that this move "streamlined" decision-making. AIG's disbanding of this group led to the destruction of one of the world's most valuable companies.[4] One subdivision went off on it's merry way using internally developed risk models without broader review by senior management. Disbanding the review group did cut down on bureaucracy. It also created conditions where a single subdivision destroyed an entire company, most of which was financially sound.

There is no guarantee, of course, that DNI will effectively integrate the intelligence community. There never are guarantees of this kind. But its establishment sets up the conditions for positive improvement.

Strategic Risk

Putting risk at the center of intelligence can help to clarify *strategic* risk. This is the risk associated with a particular strategy. The intelligence community doesn't formulate strategy, of course. But it does have a responsibility to assess the risks associated with a given strategy.

Strategic risk assessment means going beyond where terrorists will strike next, how many bombs North Korea has, and whether Russia will cooperate with the U.S. It assesses the risk of a strategy--e.g., of preemption, coercion, soft power, or any other strategy. This is a huge gap in U.S. security planning. Strategy tends to be formulated by a team at the top, but they rarely assess its risks.

---

[3] Richard A. Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11* (Roman and Littlefield, 2005).

[4] See the testimony of Maurice (Hank) R. Greenberg before the U.S. House of Representatives, Committee on Oversight and Government Reform, October 7, 2008. Greenberg was the Chairman and CEO of AIG until 2005. His successor's team disbanded the risk review group established by Greenberg.

One lesson of the ongoing credit crisis is that financial institutions didn't adequately assess the risks of their strategy. Their risk management focused on market, credit, and operational (execution) risk. It didn't focus on strategic risk, like borrowing short on global markets and lending long. There are many lessons to be learned from this melt down, and strategic risk is one of them.

It should be emphasized that the failings of risk management by financial institutions in the credit crisis, while real, have not led those institutions to abandon risk management. Not one financial company has done so. There is a thoroughgoing review of risk management practice, as there should be, to come up with improvements.

CONCLUSIONS

Risk management is playing a central role in more and more fields. This alone is good reason to think about it in intelligence. If it advances the state of the art in everything from health care to baseball, in engineering to accounting, it ought to have useful application in intelligence as well. At one time its applicability in every one of these fields was doubted. Yet risk management has had a transformative effect on all of them.

Risk management's most important effect hasn't been to "solve" problems. Rather it has been to reconstitute the basic conversations about them. In our discussions with the experts from the different applications of risk management, nearly all of the leaders emphasized that it was these conversations--the ways problems were discussed and framed--that were more important than the predictions that came out of formal models.

There is a one more point worth emphasizing. This is the need to better understand how risk, and its management, is conceived in other countries and in other societies. In our project we saw this theme in fields as diverse as energy security and the spread of the bomb. A great deal of research shows that risk assessment is hardly an objective science. It is powerfully shaped by cultural, social, and institutional forces. This is an area needing more research attention, because it is often the interaction of national (or group) risk assessments that drives outcomes, rather than one of them alone.

Risk management is a cross-cutting framework that extends beyond the specializations imposed by academia and bureaucracy. This brazen mixing of specialties is one of its most important contributions.

Paul Bracken is Professor of Management and Professor of Political Science at Yale University. He is a leading expert in global competition and the strategic application of technology in business and defense. Bracken's articles for FPRI's* Orbis *include Financial Warfare (Fall 2007), Thinking (Again) About Arms Control (Winter 2004) and The Structure of the Second Nuclear Age (Fall 2003). In 2008, he delivered the Rocco Martino Lecture on Innovation at FPRI; see his Enote "Technological Innovation and National Security." Visit: http://www.fpri.org/enotes/200806.bracken.innovationnationalsecurity.html

This essay is based on Paul Bracken, Ian Bremmer, and David Gordon (eds.),* Managing Strategic Surprise, Lessons from Risk Management and Risk Assessment *(Cambridge University Press, 2008). The author is grateful to Ian Bremmer, President of Eurasia Group, and David Gordon, Director of Policy Plans in the State Department, for their help on the issues in this paper.