Managing the "Reliability Cycle": An Alternative Approach to Thinking About Intelligence Failure

Scott J. Hatch

Soon after becoming the director of the Intelligence Success and Failure Course of CIA University's Kent School for Intelligence Analysis, I realized that much of the literature on intelligence success and failure made no mention of insights from professions outside of our intelligence domain. Many of these professions also face severe consequences for failure. Increasingly, as I taught the class, I came to draw from business and organizational literature on so-called high reliability organizations (HRO) and normal accident theory. In this article I have adapted the material contained in the literature to the domain of intelligence analysis. I believe a shift in our thinking about this subject would allow the Intelligence Community to think more proactively and holistically about the ways to increase the reliability of our intelligence analysis.

v v v

> ***"The IC should consider applying the lessons High Reliability Organizations have learned in thinking about failures of intelligence analysis."***

During the past few decades, business researchers have produced a substantial body of literature on organizations that achieve high reliability under conditions of dynamic uncertainty, inherent complexity, high risk, and potentially catastrophic costs should they fail. The researchers have focused on are in fields like aviation safety, nuclear power plant operations, chemical or oil processing, medicine, and wildfire control.

Given that Intelligence Community (IC) organizations face challenges of ensuring reliability under conditions in some ways similar to those faced by HROs, I believe the IC should apply the lessons HROs have learned in thinking about failures of intelligence analysis. Doing so may yield not only additional lessons for the community but could help managers of intelligence analysis think more effectively about their own environments in order to avert or mitigate risk of failure and improve prospects for success.

In this essay, I will translate HRO and accident-management insights to the domain of intelligence analysis and sketch out an HRO framework for intelligence analysis.[1] More work, of course, would need

[1] Among the leading researchers in studying HROs are Karl E. Weick, Kathleen M. Sutcliffe, Karlene Roberts and David van Stralen. Weick and Sutcliffe together authored, *Managing the Unexpected: Resilient Performance in an Age of Uncertainty* (Jossey-Bass, 2007), probably the most frequently referenced book in the field.

Impact, informing decisionmaking, is what we aim for as intelligence analysts.

to be done to apply this framework to daily work practices in the IC's analytic components.

What We Are Aiming For

Any effort to improve organizational performance must begin with a clear sense of aims so that benchmarks can be set up to gauge progress.

In my experience, analysts in CIA's intelligence successes and failures program have found it challenging to define failure. Much of the literature on intelligence failure has focused on "making the right call" and identifying the cognitive elements that might have gone into "failed" analysis.

But intelligence analysts know they must aim for more than just the "right call." They rightly observe that factors having to do with organizational and policy environments are always involved as well. Moreover, because most studies of intelligence success and failure tend to be case-specific, it is natural to fixate on specific events, rather than on success and failure as part of a process that transcends particular moments or events.

In reality, I believe we should not be interested in a "win-loss" balance sheet but in how our successes and failures factor into our ongoing efforts to be *consistently* reliable in *supporting* our consumers in the many ways they demand of us. With this in mind, I believe we should think of our analytical mission—and hence the ways in which we measure success and failure—in the following way. Our goal in analysis should be to

- have a *positive impact* in informing our consumer's decisionmaking…
- by delivering to the consumer the *right insights* …
- in a *timely and useful manner*…
- *consistently* over time.

Impact—informing decisionmaking—is what we aim for as intelligence analysts. Even granting that impact may be difficult to measure, considering impact forces us to look at real measures of effectiveness rather than just at the numbers of products produced, briefings delivered, and other similar quantitative measures (number of graphics, for example). These latter attributes only have indirect effects on impact. Our goal as analysts is not to simply write papers, throw them over some official's transom, and hope they get read. Stressing impact enables us to start thinking about how to measure effectiveness, not just performance.

Second, the "right insights" can be defined as those insights that *accurately* describe a situation, *add value* for a consumer, are *rigorously arrived at,* and *are soundly reasoned*. Accuracy and value-added are essential to having the right insights, and without them one is left with either something that is wrong or merely obvious. Failure would come from the absence of the right insights or the delivery of insights (even if the right ones) in ways that were neither timely nor useful to policymakers. This is clear-cut: if we do not do these things, then we have failed. At the same time, meeting these two conditions is necessary—but not sufficient—for success. Success goes beyond "getting it right": It concerns impact and achieving consistency over time.

The goal of analysts and managers is to have policymakers and policy implementers keep coming back to analysts over time. While luck may be—and often is—a component of any given success or failure, we cannot rely on it. Thus, by always being rigorous in tradecraft, persuasively presenting assessments, and managing relations with our consumers, we demonstrate the marks of reliability. To use a manufacturing analogy, it is not enough to minimize production-line defects. To achieve success we must actively manage our corporate brand, and that means striving for reliability.

Lastly with the above four-part definition of our mission we have a way to identify partial success or partial failure so that we can think about how to do things better and avoid the overgeneralization inherent in today's use of the terms "success" and "failure." Moreover, it provides more clarity for accurate benchmarking.

Developing Attitudes to Facilitate Reliability

Having a sharp definition of goals is only a first step toward greater reliability. A second is adoption of the appropriate attitude toward failure. Organizations typically either acknowledge failure or they deny it. A denial mentality is often characterized by the phrase (attributed to Gene Kranz, the NASA flight director dur-

ing the Apollo 13 mission), "Failure is not an option." In contrast, an "acknowledgement mentality" is captured in the sentence, "We are always one step away from failure." Both attitudes set up formal and informal incentives throughout an organization. The latter attitude facilitates learning; the former does not.

The saying "failure is not an option" may be well intended. At the same time, however, some managers and employees may draw from the expression the sense that failure should not even be considered. When failure does occur, such attitudes could create incentives for individuals to look for ways of denying it has occurred or to try to deflect responsibility. Such behavior is unproductive and costs organizations energy, time, and focus that could be better spent recovering from failure.

The opposite mentality, the one that adopts the attitude of "we are always one step away from failure" is the mark of the high reliability organization. It is an attitude that, proponents of the HRO concept argue, produces different organizational incentives.

HROs and the Reliability Cycle

According to Weick and Sutcliffe, HROs constantly try to anticipate failure, and they recover quickly and effectively when failures occur. In the field of intelligence analysis, I suggest these qualities can be further refined into the five elements shown in the graphic below. I believe management of this cycle holds the key to increasing our analytic reliability. Its application would move us from dealing purely *retrospectively* with failure to a continuous and *forward-looking* process for dealing with the *possibility* of failure. The former looks for lessons after a failure. The latter identifies the risks and potential causes of failure and works to avoid them.

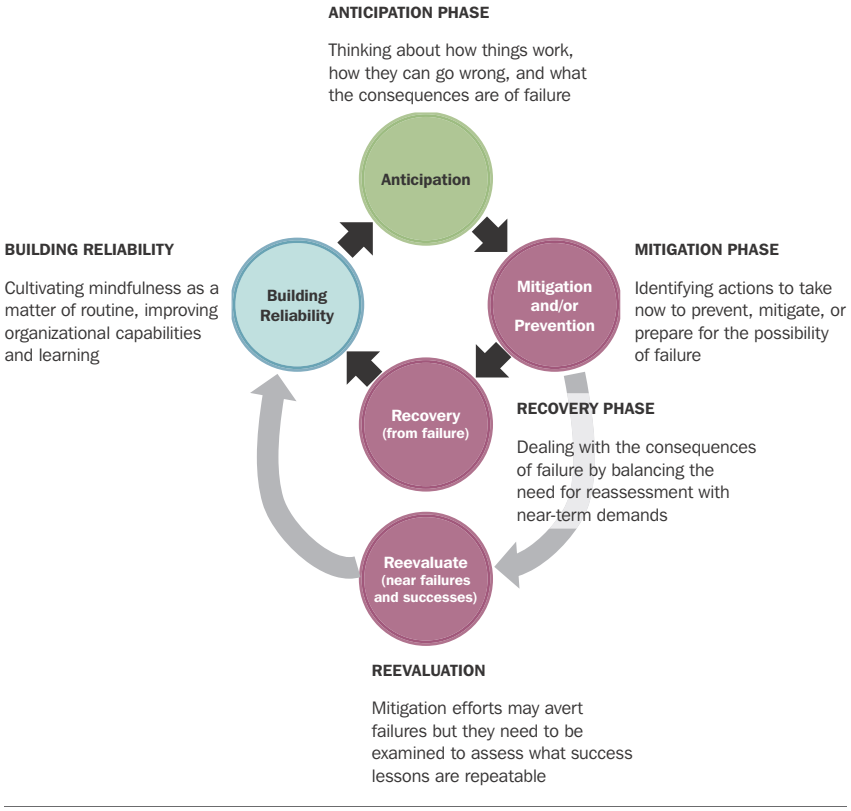
The following is my view of the roles and responsibilities of analysts and managers in this cycle.

Phase 1: Anticipation

The "preoccupation [of HROs] with failure," as Weick and Sutcliffe put it, might seem paralyzing, but that focus leads to constant self awareness. HROs consistently ask how things are supposed to work, how they are working, what could go wrong, what the consequences would be if things did go wrong, and what indicators, if any, suggest things are going wrong.

In intelligence work, this means analysts and managers need to diagnose the situations they are in, identify potential vulnerabilities, and monitor signals for evidence of weakness. Their goal is not to anticipate every possible failure—that would be impossible—but to address the most evident and biggest potential problems. At the same time, they gain familiarity with their systems so they will be able to anticipate and react to unexpected developments more quickly or establish means for prevention, mitigation, and recovery. The less done at this stage, the more that will need to be done if failure does occur.

(U) THE RELIABILITY CYCLE



UNCLASSIFIED

DI Design Center/MPG 464612ID 8-12

Unlike cognitive or policy-environmental failures, organizational failures seldom offer single causes to be remedied.

Anticipation requires understanding the factors that contribute to failure in intelligence analysis, a topic that has been explored in the writings of Richard Betts, Richards Heuer, Robert Jervis, and others. Analysts typically offer as reasons for failure incompetence, insufficient data, or the fact that the problems they tackle are intrinsically hard.

But it is not enough, in my view, to list specific issues in specific cases after the fact. Just as Heuer has given names to mindsets, biases, and logical fallacies, so too a structured taxonomy of reasons for failure would allow us more readily to diagnose situations more precisely and act more quickly to prevent or mitigate the effects of failure.

For the business world, Max Bazerman, professor of business administration at the Harvard Business School, and Michael Watkins, a consultant in leadership strategy, have done work along these lines that offers a model for a taxonomy. They have named three categories of failure: cognitive, organizational (process or systems), and political, which, with the exception of the third, easily parallel failures in intelligence analysis. The last category refers to failures of businesses to address the political system within which they must operate (e.g, lobbying for legislation or regulatory changes). A more appropriate category for the intelligence world would be failures caused by factors in the "[security] policy environment" or the failure of analysis to engage with those in that environment.[2]

Introducing COPE

My shorthand for a taxonomy of failure that adopts these three categories is COPE, which I illustrate using three examples below. The elements of each category are detailed in the table on the facing page.

Cognitive Failure: Iraq WMD

The Iraq WMD case was first and foremost a cognitive failure: the IC judged that Iraq had ongoing WMD programs and stockpiles of WMD, even though Saddam Hussein's regime had destroyed what it had and was only trying to preserve a capability to reconstitute aspects of the program when sanctions ended. While organizational and policy-environmental factors contributed to the failure, it was nevertheless a cognitive failure driven by mind-set issues. Had the cognitive factors been recognized early on—probably years earlier—the IC, using structured analytic techniques or other methods, might have reexamined its assumptions and considered alternative judgments about Saddam and his programs.

Organizational Failure: 9/11

Organizational (or systems) failure may be the most difficult kind of problem we can face. Counterterrorism analysts knew before the 9/11 attacks that al-Qa'ida was planning a major attack in the United States, but they did not know where, when, how, or what kind of targets.

The *9/11 Commission Report* and the declassified CIA Inspector General's *Report on Accountability With Respect to the 9/11 Attacks* detailed organizational issues that contributed to the US government's failure to act before the attacks.[3] These included problems with watchlisting, poor communication within and between agencies, unclear lines of authority, murky legal authorities, and so forth.

Unlike cognitive or policy-environmental failures, organizational failures seldom offer single causes to be remedied: rather, they usually involve multiple breakdowns that, in the aggregate, cause the failure. In intelligence work, tackling this kind of failure requires examination of analytical and work processes and their individual vulnerabilities. Often this requires analysis of processes across bureaucratic boundaries.

Policy-Environmental Failure: CIA and Vietnam Analysis

CIA's pessimistic assessments of the situation in Vietnam for much of the 1960s were largely accurate, and cognitive challenges (though they existed) had little or no bearing on analysis. The challenges lay in the problems senior CIA officers faced

---

[2] Max H. Bazerman and Michael D. Watkins, *Predictable Surprises*: *The Disasters You Should Have Seen Coming, and How to Prevent Them* (Harvard Business Review Press, 2008).

[3] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (US Government Printing Office, 2004) and CIA Inspector General, *Report on Accountability With Respect to the 9/11 Attacks* (Central Intelligence Agency: 2007), declassified/redacted available at www.cia.gov.

(U) TABLE 1: A TAXONOMY OF FAILURE

Cognitive Challenges in Analysis	Organizational Challenges	Policy Environmental Challenges
MIND-SET ISSUES » Paradox of expertise *(incl. overconfidence)*, especially on estimates; » Mind-sets and biases *(e.g. confirmation bias, mirror-imaging, rational actor, etc.)*; » Denial and deception.	**GROUP MIND-SET ISSUES** » Groupthink or denial *(unwillingness to see a problem is real or serious)*; » Intangibility *(reluctance to invest in a future that is distant or vague)*; » Abstractness *(hard to focus on a problem not experienced or imagined vividly)*.	**CONSUMER MIND-SETS** » Overconfidence in their own ideological beliefs or capabilities; » Overreliance on their own judgments or experience, perception of having better information or insights; » Experience breeds the need for certainty, not hedging or ambiguity; » Tendency to focus on persons rather than systemic issues; » Perception that analysts lack experience, judgment, perspective or loyalty.
NATURE OF CHANGE » Complexity of change; » Recognizing paradigm shifts; » Identifying the salient underlying drivers.	**RESOURCING ISSUES** » Inadequate personnel and/or resources to cover the issue; » Individuals acting in their own narrow self-interest deplete common resources; » Competing or gapped coverage.	**CONSUMER LIMITATIONS AND GAUGING IMPACT** » Distractions, as they are beset by immediate and pressing problems; » Have to respond to constituencies, limiting options, flexibility, or ability to develop a long-term horizon; » Beholden to or advocates of a specific approach, program, or option; » Inadequate capabilities to resolve or exert leverage on the problem. » Factoring in US actions.
DIFFICULTY THINKING IN TIME » Status quo bias; » Limited ability to imagine discontinuities; » Rapid or incremental change; » Limited or lack of alternative scenarios.	**PROCESS ISSUES** » Overly rigid or, conversely, ambiguous lines of authority; » Subordinates tend to stress good news or what their boss wants to hear; » Data collection based on consumer demands but unaligned with actual needs; » Information compartmentation between components or units; » Legal, customary, or internal policy constraints or prohibitions.	**EFFECTIVELY MANAGING RELATIONS WITH CONSUMERS** » Meeting consumer needs; » Providing solid argumentation; » Soliciting feedback.
LITTLE CLEAR REPORTING » Collection not tasked because gaps not clearly identified or understood; » Collection tasked, but reporting insufficient to answer specific problems.	**RISK MANAGEMENT CALCULATIONS** » Easier to ignore the harm from inaction or pay more attention to harm from action than to take steps with small, known costs; » Willingness to incur a large but low-probability risk rather than accept a smaller, sure loss now.	**PROVIDING EFFECTIVE WARNING** » Warning not given at all or not given clearly enough for the decisionmaker; » Cry-wolf syndrome *(repeated warnings become ignored over time)*.
POOR QUALITY REPORTING » Overreliance on single or limited sources; » Reporting very fragmentary or indirect.		
SIGNIFICANT NOISE OVER CLEAR SIGNALS » Heavy volume of reporting; » Significant processing needed to be useful.		

UNCLASSIFIED

DI Design Center/MPG 464610ID 8-12

in engaging presidential administrations that declined to accept CIA analysis. let alone act on it, which represents failure to have an impact. Indeed, intelligence histories tout as successful CIA's analytic performance during the period, but that analysis cost CIA one director, John McCone, who resigned in frustration, and kept CIA out of Oval Office deliberations on the issue for nearly two years after he left. In this case, the real challenge (and ultimate failure) was on the policy-environmental side of the equation.

COPE's Utility

The COPE framework can clarify causes of failure in three ways. First, the mere act of determining which of the three types of failure a situation falls into will help triage it to make further diagnosis easier.

The second way in which the framework can help is in providing approaches to diagnosing a very complex process. Intelligence analysis has been evaluated from a number of angles, each more advanced than the simple five-part loop that is known as the traditional intelligence cycle. Rob Johnston's taxonomy of intelligence analysis variables in his *Analytic Culture in the U.S. Intelligence Community,* for example, illustrates the complexity in the four types of variables he lists in a taxonomy of factors that influence analysis: *systemic* (those factors that affect the intelligence organization and the analytical environment); *systematic* (factors, especially external influences, that affect the analytical environment); *idiosyncratic* (matters that affect individuals and their analytic performance); and *communicative* (those that affect communication between groups involved in the analytic process).[4]

For the purposes of this discussion I prefer to think in terms of five critical areas of vulnerability, each of which has elements that can be monitored during an analytic process or examined in the event of a failure. These points are:

- Assessment—the cognitive elements of the analytical problem.
- Collection—the continuous effort to expand knowledge about a situation.
- Support—provision to consumers of products, warning memos, efforts to brief them, etc.
- Response from consumers—feedback, further tasking, etc.

[4] Dr. Rob Johnston, *Analytic Culture in the U.S. Intelligence Community* (Central Intelligence Agency, Center for the Study of Intelligence, 2005), 33–44.

Identification of responsibilities and degrees of influence over given situations will set components up to address prevention and mitigation.

- Organizational—resourcing and process issues, group mind-sets, or poor risk management calculations.

The third way in which the COPE framework can help is in identifying what individual or component would be best able to remedy problems that caused a failure (after the fact) or appear to be contributing to an increasing risk of failure (before one occurs). Identification of responsibilities and degrees of influence over given situations will set components up to address prevention and mitigation.

In the case of *cognitive* issues or cognitive failures, analysts are likely to bear the most responsibility. They will also have the greatest ability to address problems. In the *policy-environmental* arena, analysts should be aware of dynamics, but managers will most likely have to take the lead in addressing issues. Neither analyst nor manager is likely to have much influence over the consumer environment, as each is most likely to be in a reactive mode as they see it unfold, especially in a relatively new situation.

Analysts and managers most likely will have to share responsibility for resolving *organizational* issues. Managers will have decisionmaking responsibility and depend on analysts to contribute substantive and working-levels insights on processes to inform decisionmaking. This is likely to be more difficult than it might seem on the surface. Even first line managers don't always have complete knowledge of the interactions of their people within the system. When multiple systems are involved and are involved at higher levels, the challenge grows substantially.

Phase 2: Prevention, Risk Reduction, and Mitigation

Accepting that we cannot always prevent failure, we should always think about the things that could be done to reduce the risk of failure. At the same time, we should position ourselves to deal with failures and mitigate their consequences.

As with anticipation, mitigation involves shared responsibilities. While managers will make the decisions on resources and processes, the analysts closest to the substance of a problem can speak most authoritatively on the consequences in a region or subject area, should the unforeseen or unlikely actually take place. Their understanding of how things could unfold, including dynamics previously unforeseen that could affect the actors in the region and US interests will provide the basis for decisions about resources and processes to follow.

Analysts may be weaker in their understanding of the consequences of a failure for their component and the larger organization than managers. Experience, training, and management engagement can help sensitize them to these dimensions and help them contribute more effectively to the decisions management will have to make.

By using the COPE framework, analysts can also improve their ability to identify areas in which they can (and should) take the lead in addressing shortcomings. It can also help them recognize areas in which higher management is needed or cases in which a component—or organization as a whole—must react. The more analysts can anticipate management concerns, the more they and management can be proactive in risk-reduction and post-failure activities.

Phase 3: Recovery and/or Reevaluation

This is the phase of the process usually given the least thought in organizations that work from the assumption that "failure is not an option." When failure does happen, two simultaneous, interrelated tasks must follow:

- A retrospective of what went wrong must be completed.
- The organization must rebuild credibility with both higher management and consumers.

These tasks will have to be completed in an environment of increased workloads as consumers will demand intelligence support to manage the new situation.

In this stressful time, the natural temptation is to postpone a reassessment until things quiet down—which often leads to never doing one at all. But a rapid assessment is vital. The more quickly mental models are adjusted, the sooner a component can begin to reestablish its credibility. Being proactive and taking responsibility for failure will buy goodwill, improve the confidence of

higher ups, and possibly earn more latitude to tackle the situation.

Management must play a bigger role than analysts in the recovery phase. First-line managers in particular need to lead the reassessment, but they must do so without alienating individuals—analysts, other managers, or policymakers. The first-line managers also need to preserve team cohesion and deal with resource challenges created by new circumstances. In such an environment, the potential goes up for missteps and counterproductive reactions. It is vital, therefore, to understand what kind of reactions are the most and least helpful. On this score, some useful insights can be gleaned from normal accident theory.

Normal Accident Theory

Normal accident theory was introduced by Charles Perrow in his 1984 book in which he observed that complex technological systems are more likely to fail when "tight coupling" and "interactive complexity" occur.[5] "Tight coupling" describes a situation in which incidents in one part of a system will have prompt and major effects on other parts of the same system. In a sense, "tight coupling" defines rigidities in systems. "Interactive complexity" describes a situation in which two or more individual events or failures in a system interact and create unexpected effects on the system as a whole. In short, the more complex the system, the more likely "normal accidents" are to occur.

For Perrow, an ineffective response to failure would be one in which an organization either "tightens the coupling"—for example, by adding redundant backup systems—or adds complexity to its processes, such as by adding new procedures. While Perrow is focused on technological systems, these insights can be applied to organizational behavior more generally.

In short, components should look at both success and failure to sharpen lessons learned.

These insights also dovetail with conclusions Richard Betts and others have made about the inevitability of intelligence failure.[6] In particular, reflexive organizational responses to intelligence failure have increased redundancy, multiplied organizational components, and added more procedures while making work processes more complex, burdening analysts and managers alike with more tasks. These changes, it could be argued, have made the IC system more vulnerable to failure by increasing the incentives people have to ignore even good practices to "get the job done."

A better response, per Perrow, would have been to find ways to "loosen the coupling" and/or "reduce complexity." In the environment of intelligence analysis, this could involve substituting greater ownership, accountability, and learning in place of adding redundancy. It could also mean streamlining procedures and components rather than multiplying them.

While recovery assumes that failure has happened, what about those situations in which anticipation and mitigation efforts have led to an intelligence success or averted an outright failure? It is important to assess these situations as well, even when a failure has not occurred.

In this case, one would want to engage in a reevaluation of the success or avoided failure. The natural organizational tendency is simply to accept a success and to allow it to become a new "template," without an examination of what might have made the seemingly successful procedures work and what actual limitations remain. Determining why success was achieved and what characteristics were unique or repeatable helps to make a clear headed determination of what should be emulated in the future. In short, components should look at both success and failure to sharpen lessons learned.

Phase 4: Building Reliability

Unlike the other three phases of the Reliability Cycle, this phase is less tied to a specific situation, although it can flow out of one. In this phase, the focus is on how organizations can improve their ability to learn and more consistently cultivate the practices necessary for high reliability.

Harvard business professor David Garvin and others have described at least four characteristics of learning organizations: (1) a supportive learning environment; (2) concrete learning processes; (3) a leadership that reinforces learning; and (4) the transfer of knowledge throughout

[5] Charles Perrow, *Normal Accidents; Living with High-Risk Technologies* (Princeton University Press, 1984 updated 1999).
[6] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable." *World Politics* 31, no. 1 (Oct. 1978): 61–69.

Inculcating practices of mindfulness and reliability will be done mostly at work, and that is mainly the responsibility of managers—especially first-line managers.

the organization.[7] It should be added that building reliability requires looking at the organizational processes that may be inhibiting effectiveness and thinking through how to realign them to be more conducive to intelligence success. The key here is not simply compiling lessons learned but finding ways of integrating and habituating them into daily work processes.

Climate and Culture. To be effective, efforts to build reliability need to operate on two organizational levels, climate and culture.[8] Climate is the perception within an organization that senior leaders are committed to achieving greater reliability and are actively facilitating the effort. Culture alludes to how the values have been adopted in the rank-and-file and have become part of daily processes.

A true HRO will operate on both levels simultaneously. If senior management is trying to promote a reliability climate but is not thinking about how these values and practices are inculcated at the working level, then efforts to become more reliable are likely to falter. Conversely, a good culture of reliability and tradecraft can be eroded and undermined if working-level personnel perceive that senior managers are only mouthing slogans. Harmonizing these two levels is a significant challenge.

Training. Training is necessary, but it is only part of the process. Training can facilitate skills development and spread values within organizations, but inculcating practices of mindfulness and reliability will be done mostly at work, and that is mainly the responsibility of managers—especially first-line managers.

Management Focus. Managers set the tone in their units and should foster environments in which analysts are free to present minority viewpoints and alternative views and to question key assumptions. Managers have levers for doing this:

- They have the power of example. Experience shows that the tone set by first-line managers and senior analysts, whether positive or negative, will be embraced by more junior analysts.
- Managers have the power to reward behavior that contributes to constructive questioning environments or curb behavior that undercuts them.
- They can mandate papers that question existing points of view or institute regular "stand downs" to review analytic lines or explore vulnerabilities that could lead to failure.
- They can establish performance benchmarks for individuals and their components.
- They can encourage and provide the means their analysts can use to pursue outreach to bring new or different ideas to their teams.

Accomplishing all this, however, places a premium on deliberate planning on the part of the manager.

Knowledge Capture. Also needed are improvements in the capture and transfer of knowledge within components. This is not about better information sharing, which usually is about getting access to more data from outside of components. Knowledge capture and transfer is about preserving insights gained within a component, enabling their recovery and regular reexamination, and passing them along to new and future members of the component. Despite improvements in our IT systems over the years, we are arguably doing worse in knowledge capture than we have in the past. In my experience components shared common sets of "read" files for all team members. Today analysts tend to maintain their own personal files which few others can see or use.

Willingness to Countenance Failure. On a day-to-day basis, managers must demonstrate willingness to discuss near failures and see them as such. Organizationally, there can be a strong disincentive to do this, as higher management and outsiders could perceive such discussion as an indication of poor perfor-

---

[7] David A. Garvin, Amy C. Edmondson, and Francesca Gino, "Is Yours a Learning Organization?" *Harvard Business Review*, March 2008. See also, David A. Garvin, "Building a Learning Organization" *Harvard Business Review*, July–August 1993.

[8] Anthony Ciavarelli and Jeffrey Crowson, "Organizational Factors in Accident Risk Assessment," unpublished paper presented to the Safety Across High-Consequences Industries Conference, 9–10 March 2004, 1. Ciavarelli and Crowson are from the Naval Postgraduate School and are focused on aviation safety. I have taken their distinction between climate and culture and adapted it to the issue of intelligence reliability.

mance. In reality, however, discussion of smaller or near failures actually can help components get better reads on situations they face and better position themselves to help prevent or mitigate big failures.

Consumer Relationships. Focus must be kept on developing relationships with consumers. This can improve reliability by helping to better focus support for them, but it can also help mitigate one effect of failure. While consumers are never happy about failure, a component with a strong track record as a reliable partner that does due diligence will be more likely to be given leeway after a failure, especially if the component demonstrates positively that it is taking responsibility for its mistakes and is learning from and correcting them.

By seeing the analytical process in a more integrated and holistic way, we can develop a better sense of where discrete actions fit into the process and how they may affect other parts of the process and its outcomes.

Conclusion: The Value of This Paradigm

The value of the conceptual framework sketched out here is in its comprehensiveness and forward-leaning orientation. At a minimum, it can give us a more consistent vocabulary as we continue to explore intelligence success and failure. No doubt elements of this framework touch on existing practices, although they are probably carried out in ad hoc and inconsistent ways. No doubt as well that much more could be said about specific parts of the COPE framework and practices that would flesh it out in even more practical terms.

Nevertheless, by seeing the analytical process in a more integrated and holistic way we can develop a better sense of where discrete actions fit into the process and how they may affect other aspects of the process and its outcomes. Such recognition would enable us to go beyond either reorganizations or ad hoc solutions and short-term fixes and allow us to develop better organizational and systemic approaches for improving our reliability.

All of this, however, hinges on attitudes toward failure. Component leaders who deny that failure is a possibility almost certainly have set themselves up for failure. If they acknowledge they are almost always one step away from failure and apply the reliability cycle to manage the risks they face, they will have taken their organizations to the place they should aim—and need—to be.

v v v